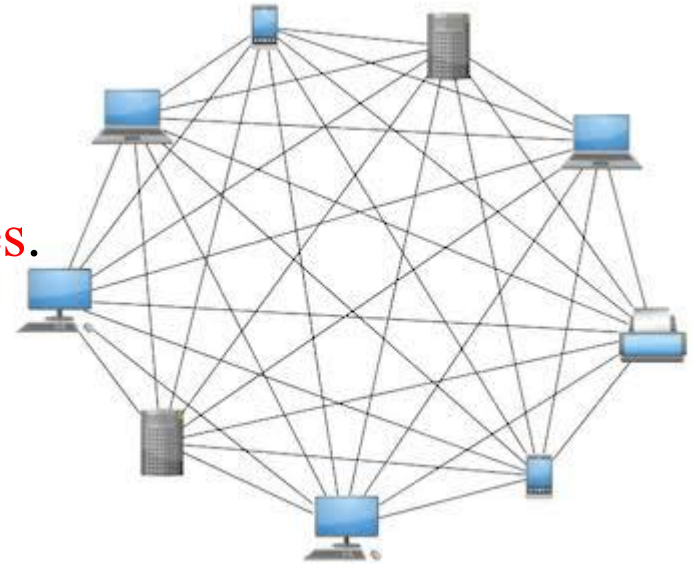
CCNA Revision

A **computer network** is a system that connects two or more computing devices (such as computers, servers, phones, and peripherals) using physical cables, optical fibers, or wireless radio signals to enable communication and the sharing of data, hardware resources, and services.



Network components

Nodes (Devices): Any endpoint or hardware device capable of sending, receiving, or processing data (e.g., computers, printers, routers, and switches).

- **Transmission Media:** The physical or wireless pathways used to transfer data, including **Ethernet cables**, **fiber optics**, or **Wi-Fi** radio waves.
- **Protocols:** The standardized sets of rules (such as TCP/IP or HTTP) that govern how data is formatted, transmitted, and received across the network.

WAN, LAN, PAN, MAN Explained

PAN
Personal Area Network

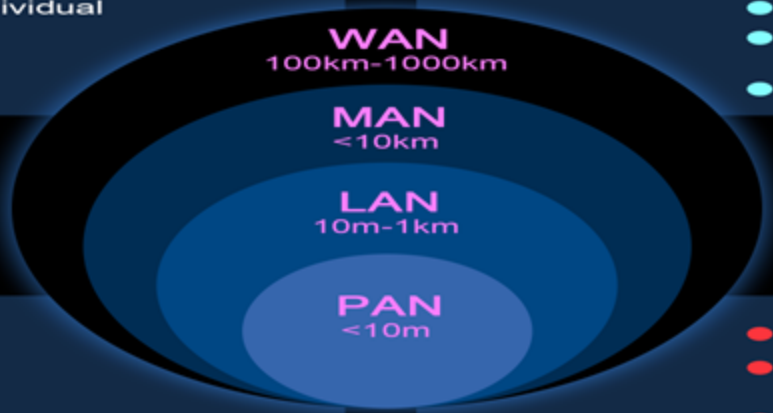


- a small network based on an individual
- connect multiple devices
- only used in one building

LAN
Local Area Network



- a bigger network than PAN
- can cover larger buildings
- office local network connecting PCs, file servers,printers etc
- cannot be used outside the building



- much larger than PAN or LAN
- cover entire towns or cities
- connect several LANs



MAN
Metropolitan Area Network

- largest network in the world
- connect different MANs or LANs or create huge networks
- The World Wide Web(WWW)is an example of WAN



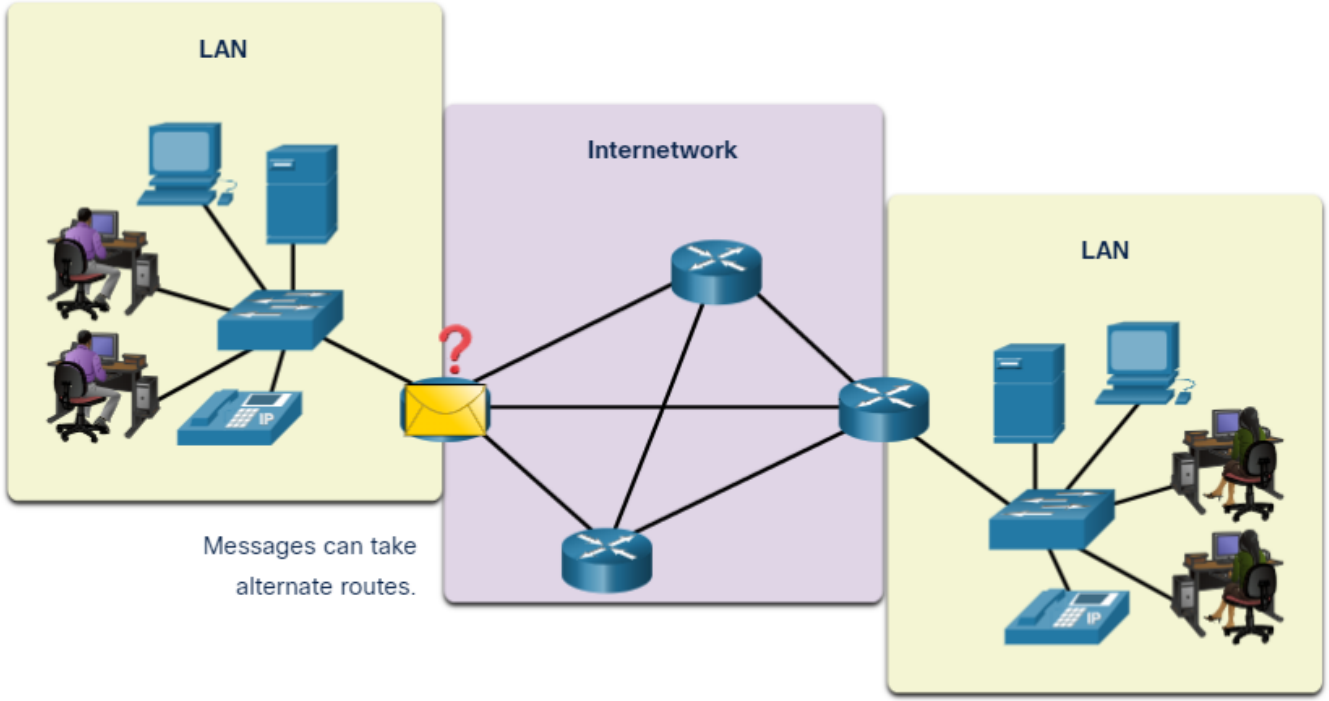
WAN
Wide Area Network

Network components

End devices

Network media

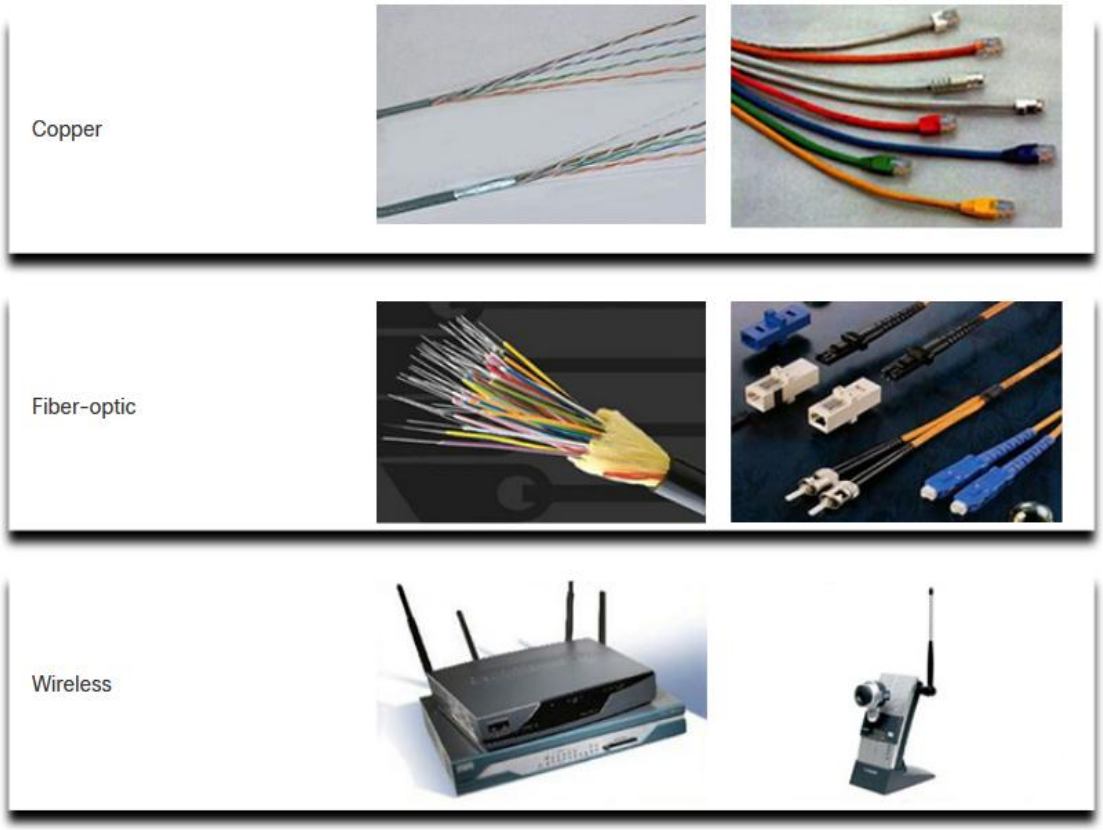
Network interface



Network Media

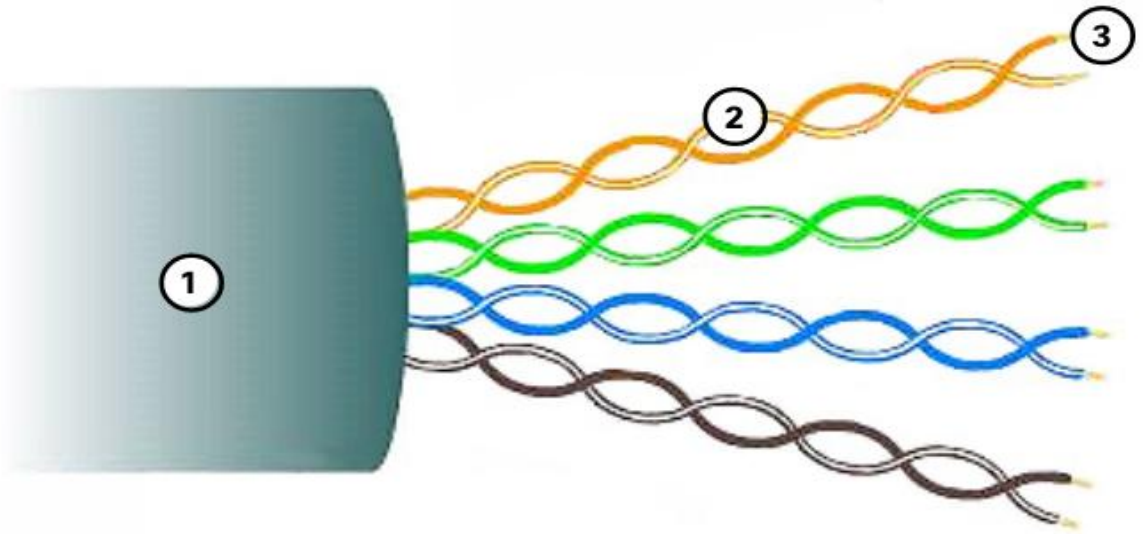
Communication across a network is carried through a medium which allows a message to travel from source to destination.

Media Types	Description
Metal wires within cables	Uses electrical impulses
Glass or plastic fibers within cables (fiber-optic cable)	Uses pulses of light.
Wireless transmission	Uses modulation of specific frequencies of electromagnetic waves.



Copper Cabling

Unshielded Twisted Pair (UTP)



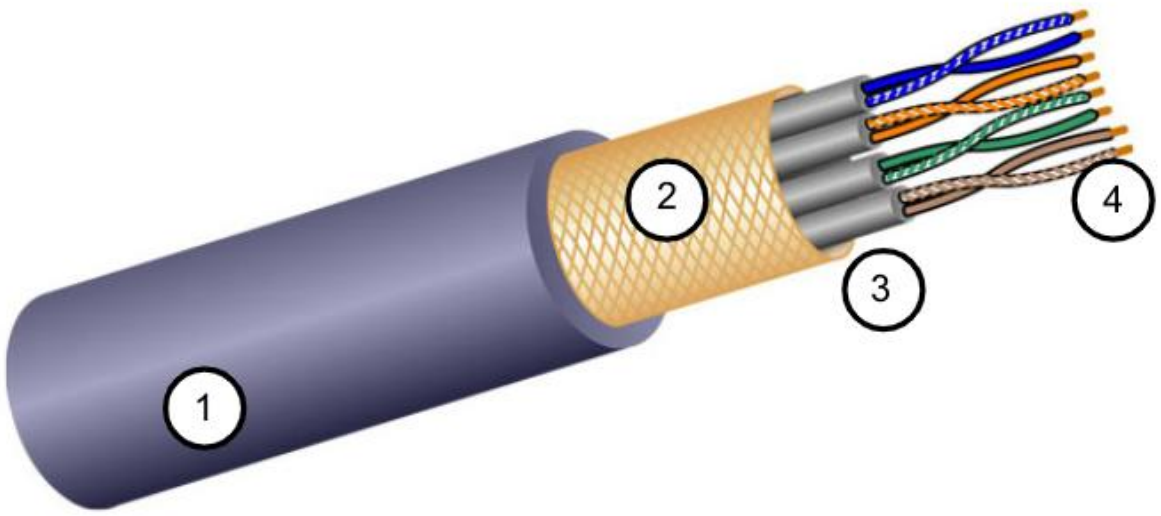
- **UTP** is the **most common** networking media.
- Terminated with **RJ-45 connectors**
- Interconnects hosts with intermediary network devices.

Key Characteristics of UTP

1. The outer jacket protects the copper wires from physical damage.
2. Twisted pairs protect the signal from interference.
3. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair.

Copper Cabling

Shielded Twisted Pair (STP)



- Better noise protection than UTP
- More expensive than UTP
- Harder to install than UTP
- Terminated with RJ-45 connectors

Key Characteristics of STP

1. The outer jacket protects the copper wires from physical damage
2. Braided or foil shield provides EMI/RFI protection
3. Foil shield for each pair of wires provides EMI/RFI protection
4. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair

Cat 5 vs Cat 6 vs Cat 7: How to Choose the Right Ethernet Cable



Unshielded Twisted Pairs (UTP) | Unshielded Twisted Pairs with Spline (UTP) | Shielded Twisted Pairs (S/FTP)

	Cat5e	Cat6	Cat7
Speed / Bandwidth	Up to 1 Gbps / 100 MHz	Up to 10 Gbps / 250 MHz	Up to 10 Gbps / 600 MHz
Shielding	UTP (Unshielded)	UTP (Unshielded)	S/FTP (Overall Shield + Foil Shielded Pairs)
Best Installation Environment	Home, Small Office, Basic Networking	Office, Commercial Buildings, High-Speed LAN	Data Centers, Industrial, High EMI Environments
RFQ / Selection Considerations	Cost-effective for standard 1 Gbps applications	Balanced performance and cost for 1G/10G networks	Maximum performance and EMI protection for demanding installations

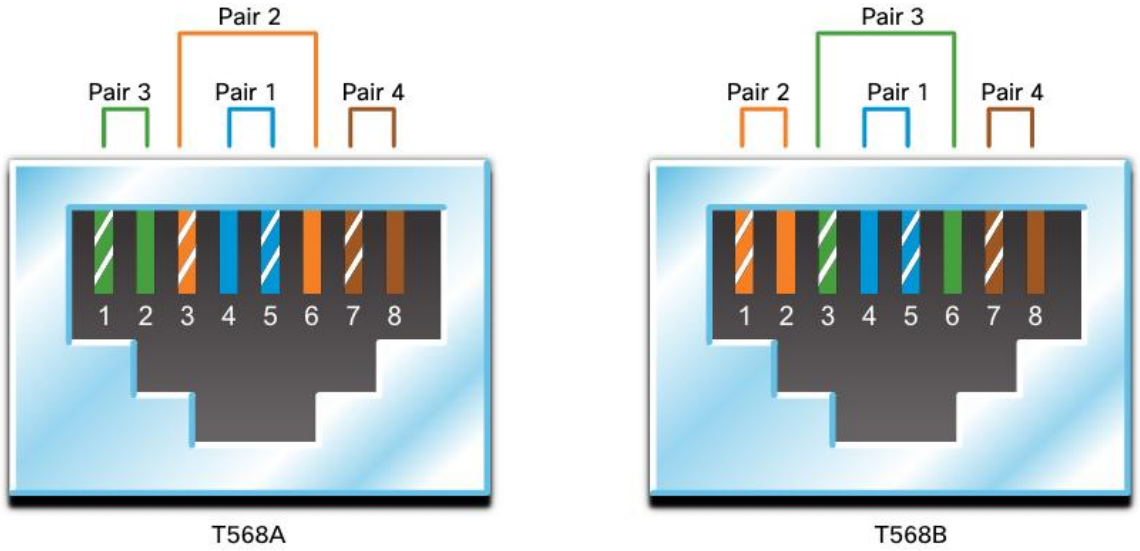
Higher MHz = More Capacity
Wider bandwidth supports faster data speeds.

Shielding Matters
More shielding reduces interference and improves signal integrity.

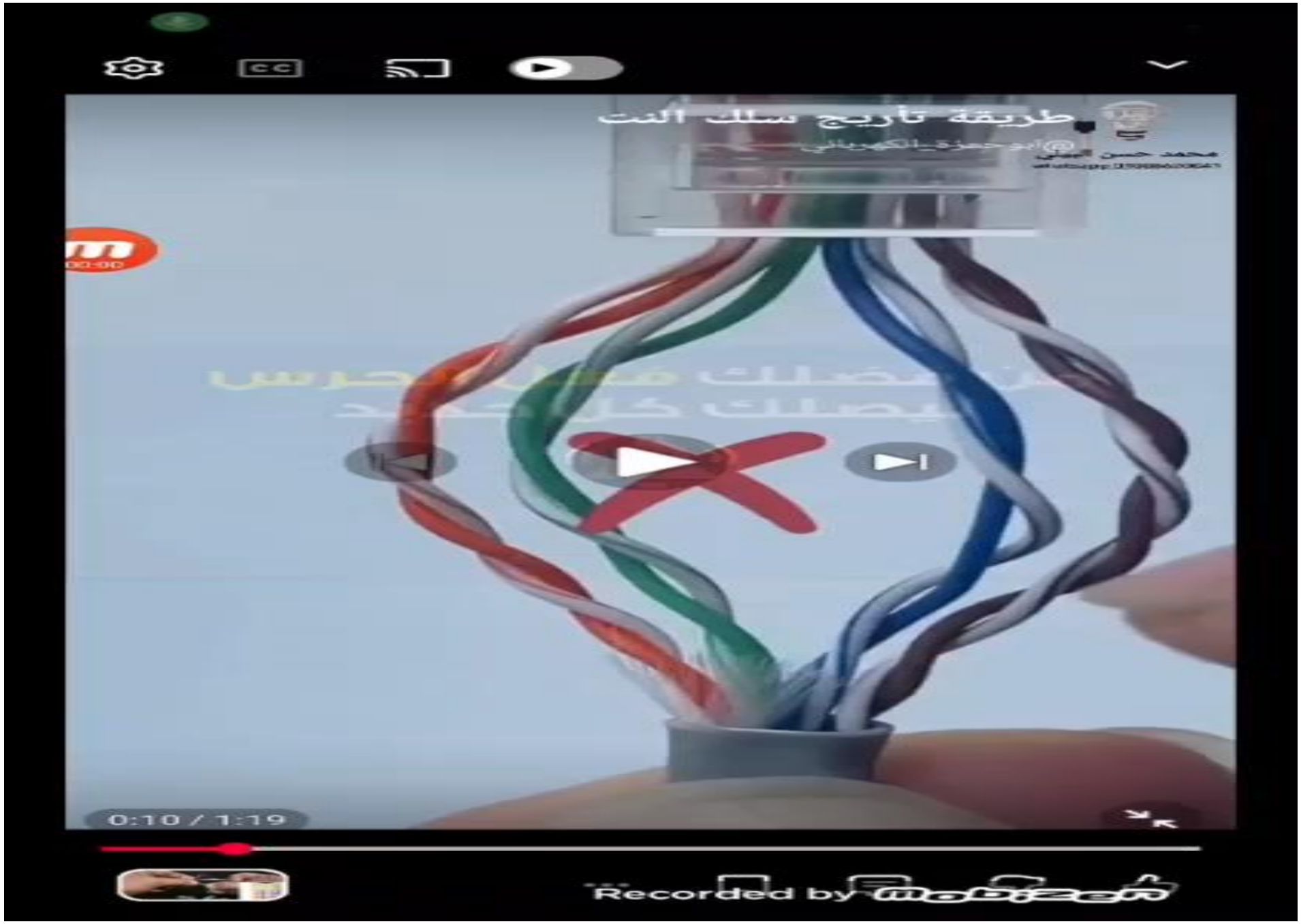
Choose for Your Environment
Match the cable type to your speed needs, budget, and installation conditions.

UTP Cabling

Straight-through and Crossover UTP Cables

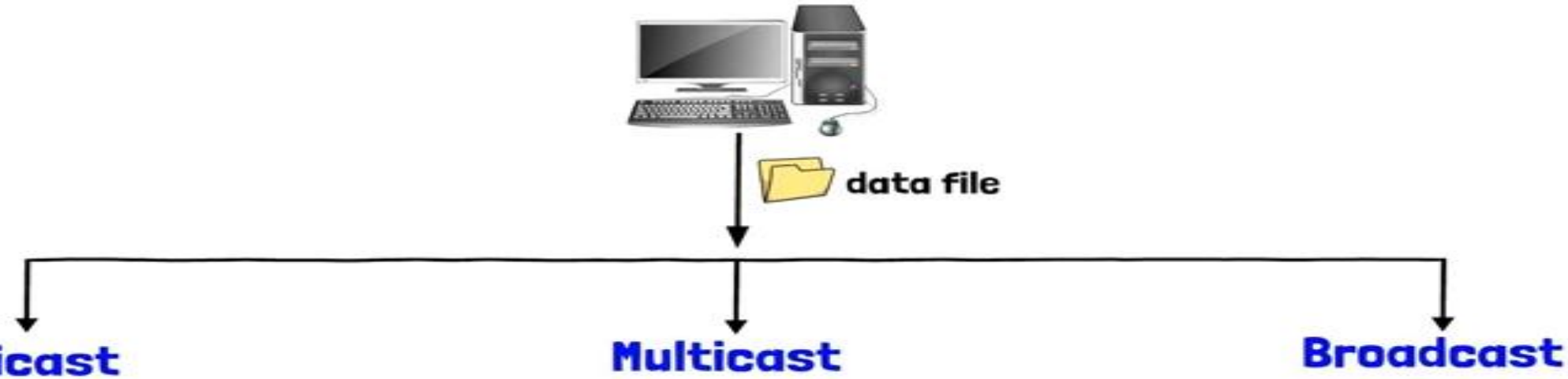


Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or T568B	Host to Network Device
Ethernet Crossover *	One end T568A, other end T568B	Host-to-Host, Switch-to-Switch, Router-to-Router

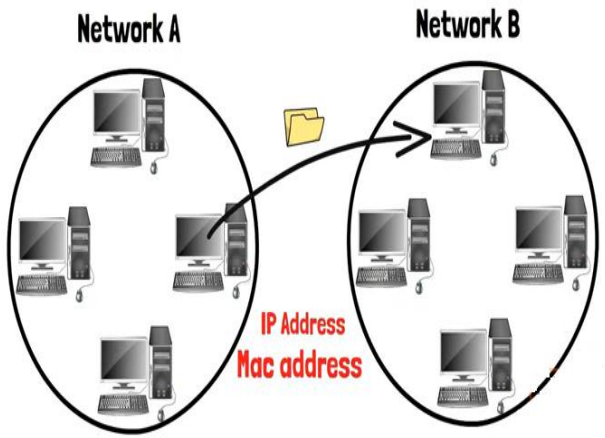

طريقة تاريخ سلك ألنت
0:10 / 1:19
Recorded by

Types of casting

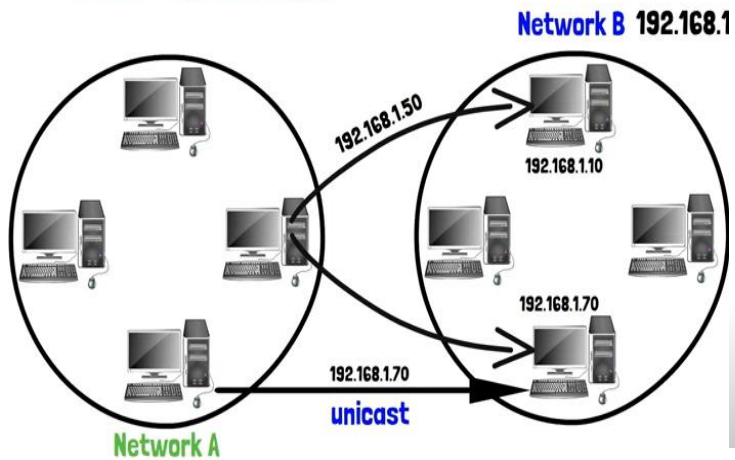
Casting : Transmitting data over the network

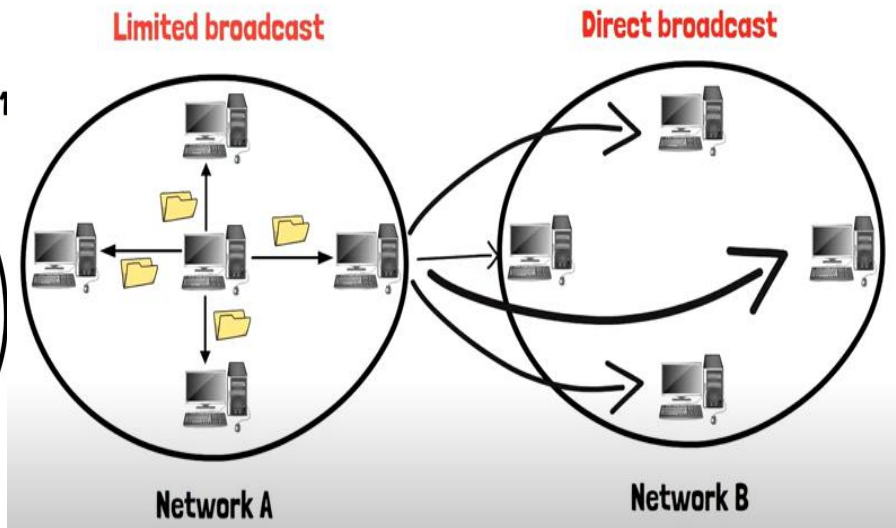


Unicast: (one-to-one)



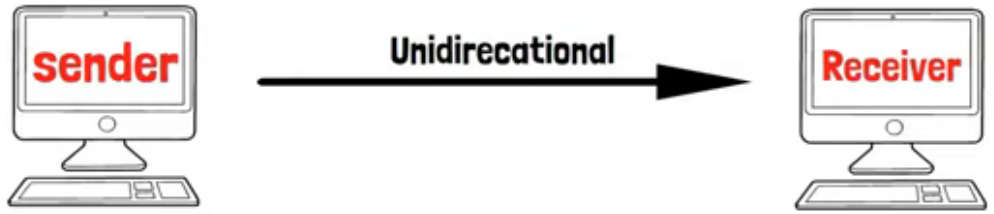
Multicast : (one-to-many)



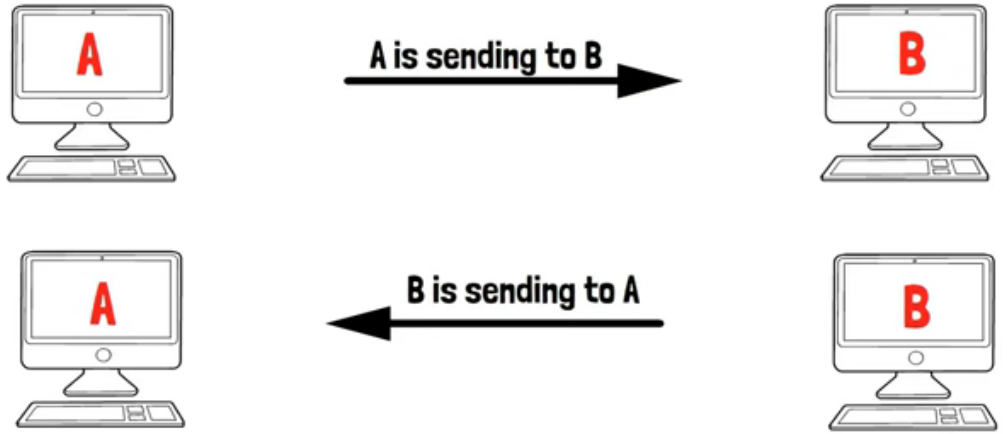


Transmission modes

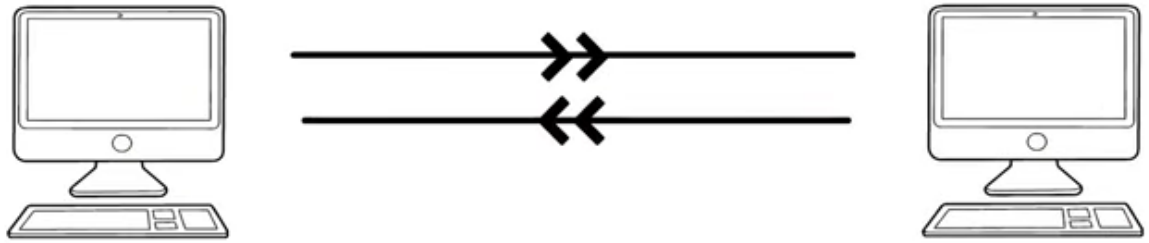
Simplex mode



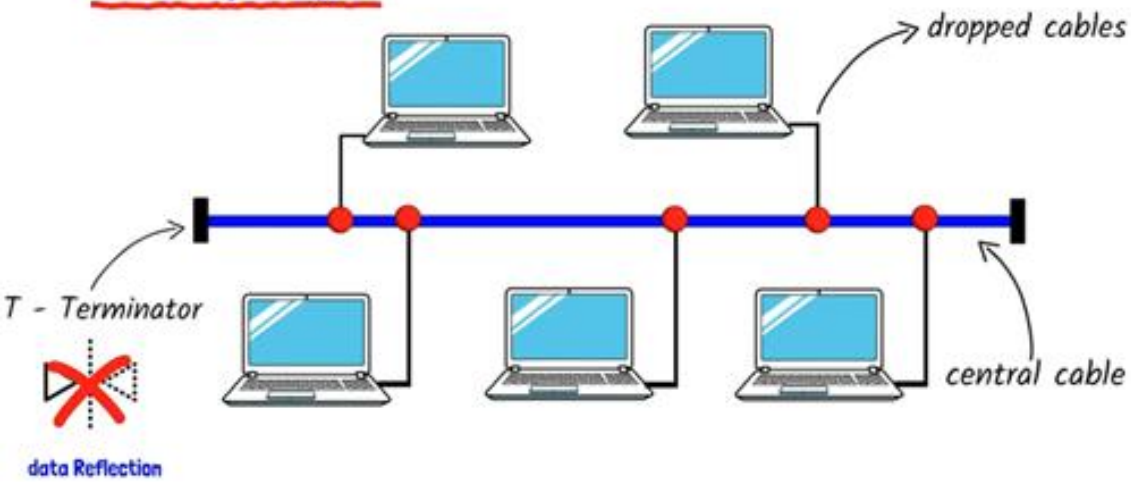
Half-Duplex mode



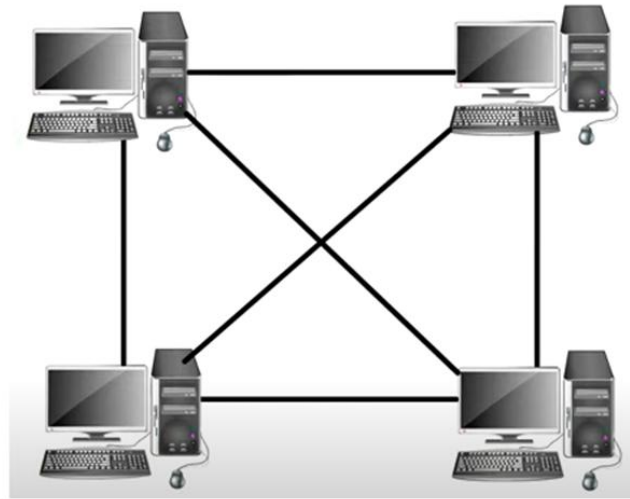
Full-duplex mode



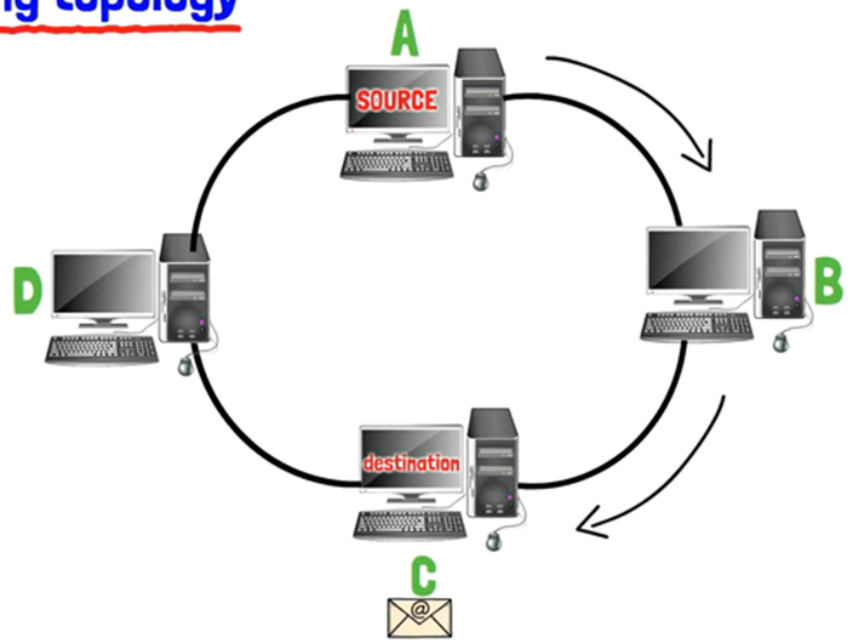
BUS Topology :



Mesh topology

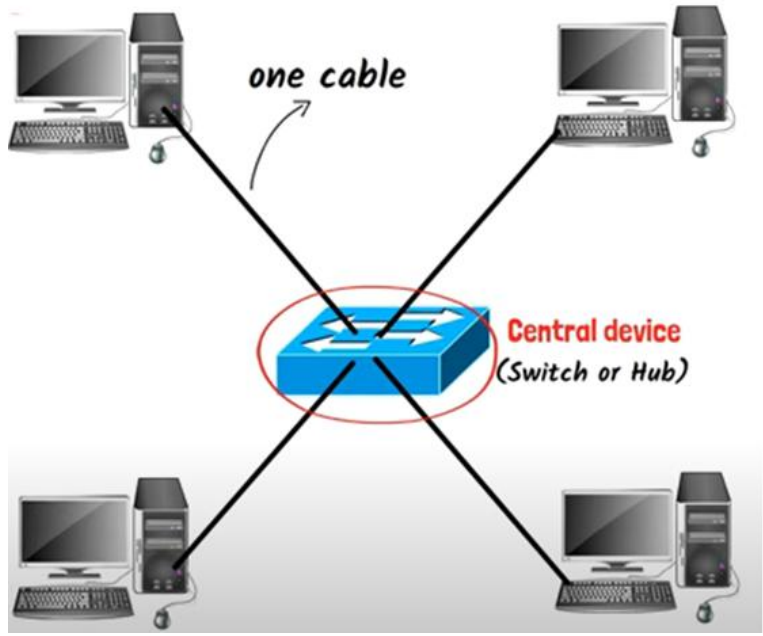


Ring topology



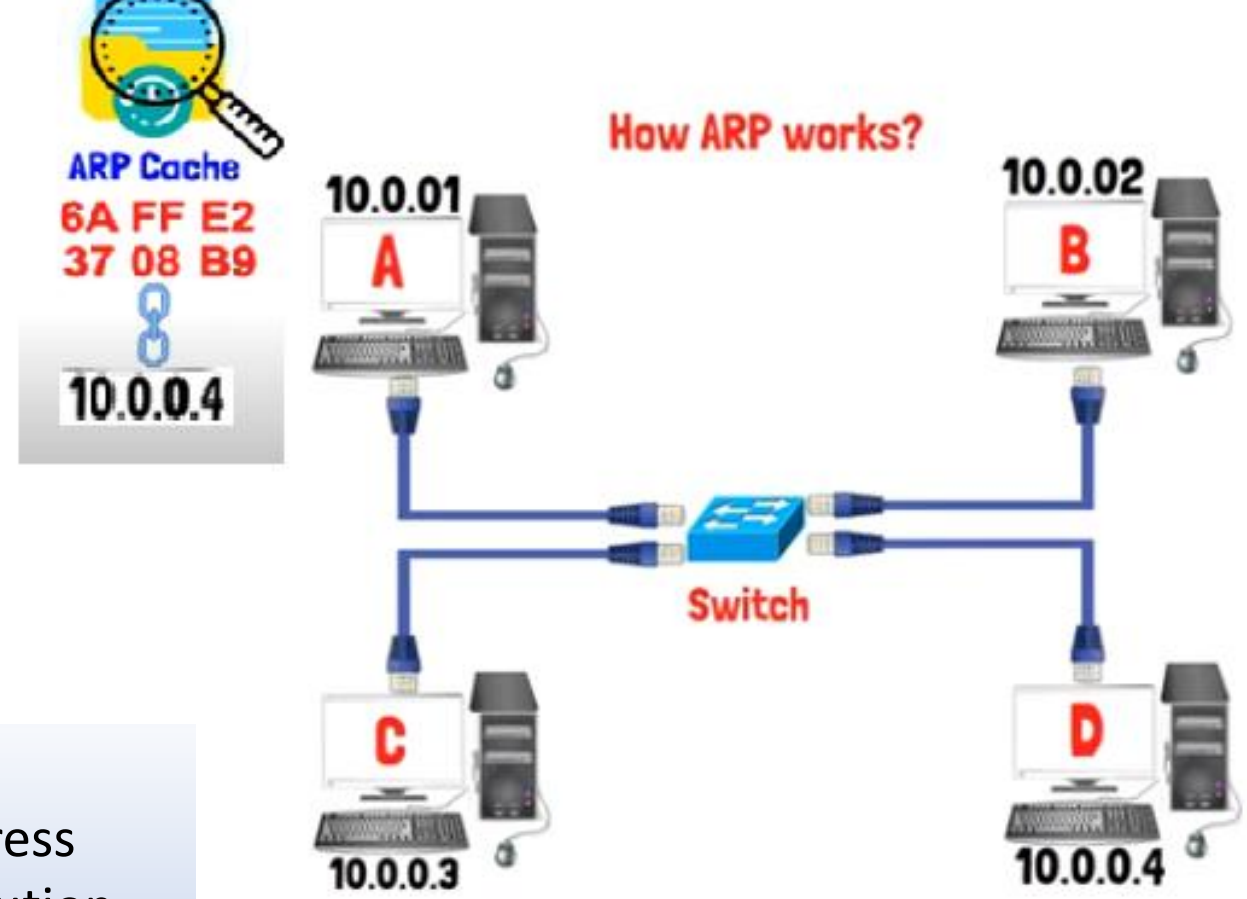
Star topology

(common use)



S.No	HUB	SWITCH	ROUTER
1.	Works in Half Duplex mode	Full Duplex	Full Duplex
2.	Sends data in form of bits	Sends data in form of frames	Sends data in form of packets
3.	Broadcast Device	Multicast device	Routing Device
4.	Works in physical layer of OSI model	Works in Data link / Network layer of OSI model	Works in Network layer of OSI model
5.	Used to connect devices to the same network.	Used to connect devices to the network.	Used to connect two networks.
6.	Does not store any MAC address of a node in the network.	Stores MAC address and IP address of nodes in the network.	Stores MAC address and IP address of nodes in the network.
7.	Types are :- Active hub, Passive hub and Intelligent hub.	Types are Layer 2 and layer 3 switch.	Types are Broadband router, Wireless router, Edge router, core router.
8.			

Interface	Mac Address
1	AA-AA-AA-AA-AA-AA
6	BB-BB-BL



If A want to send message to D. Switch uses MAC so A need to associate MAC for D in its message. A uses ARP cache to know the MAC for IP.

IF ARP don't has the MAC then Computer A send message for all computers to ask about the MAC for certain IP.

ARP (address resolution protocol)

Save the *IP and MAC for connected devices*

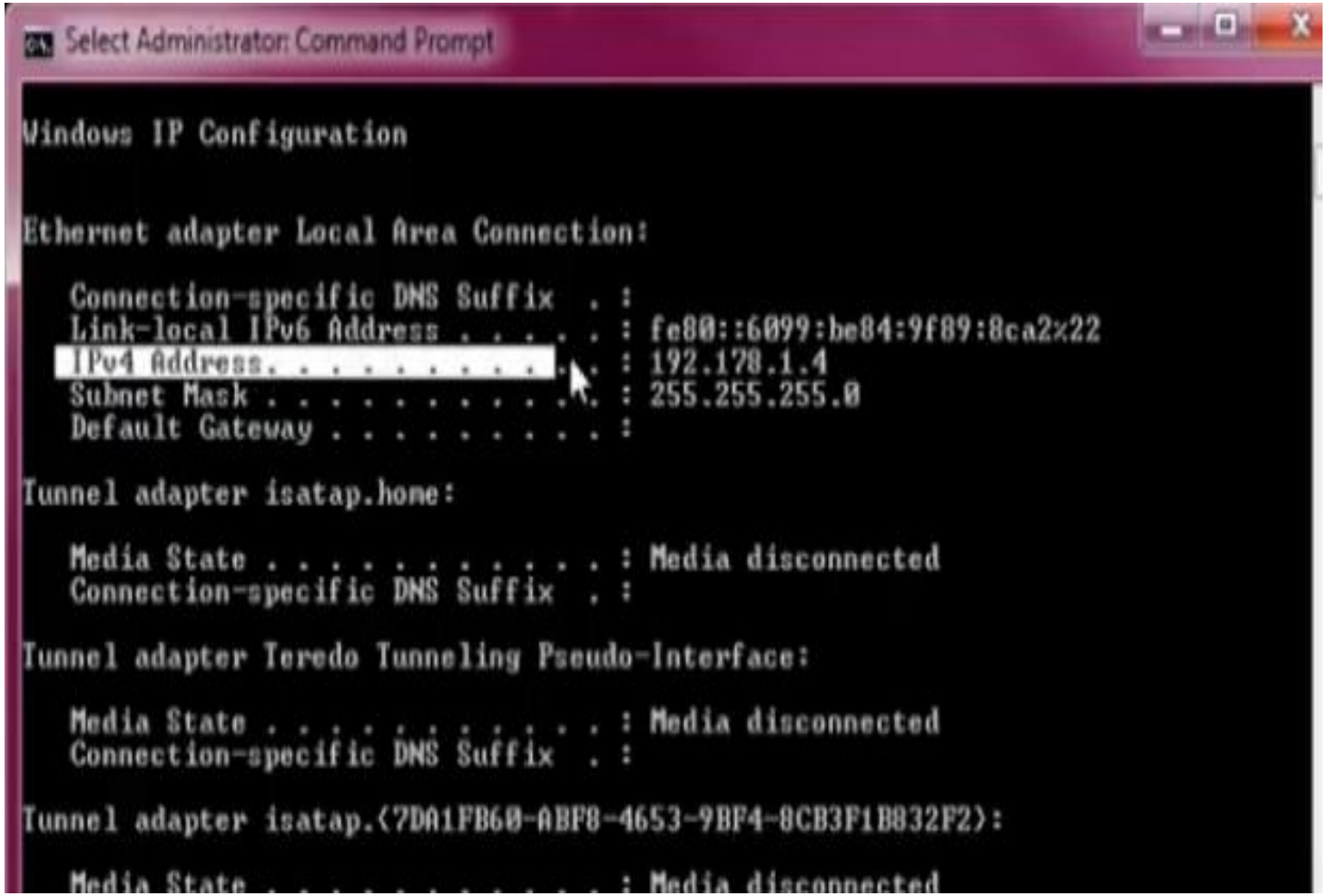
Uses DNS (domain name system) - to **get** **IP** address (1.2.3.4) **from** a **DNS** domain(www.google.com).

ARP (address resolution protocol) is used to **get** **MAC** address (11:22:33:44:55:66) **from IP** (1.2.3.4).

IP address

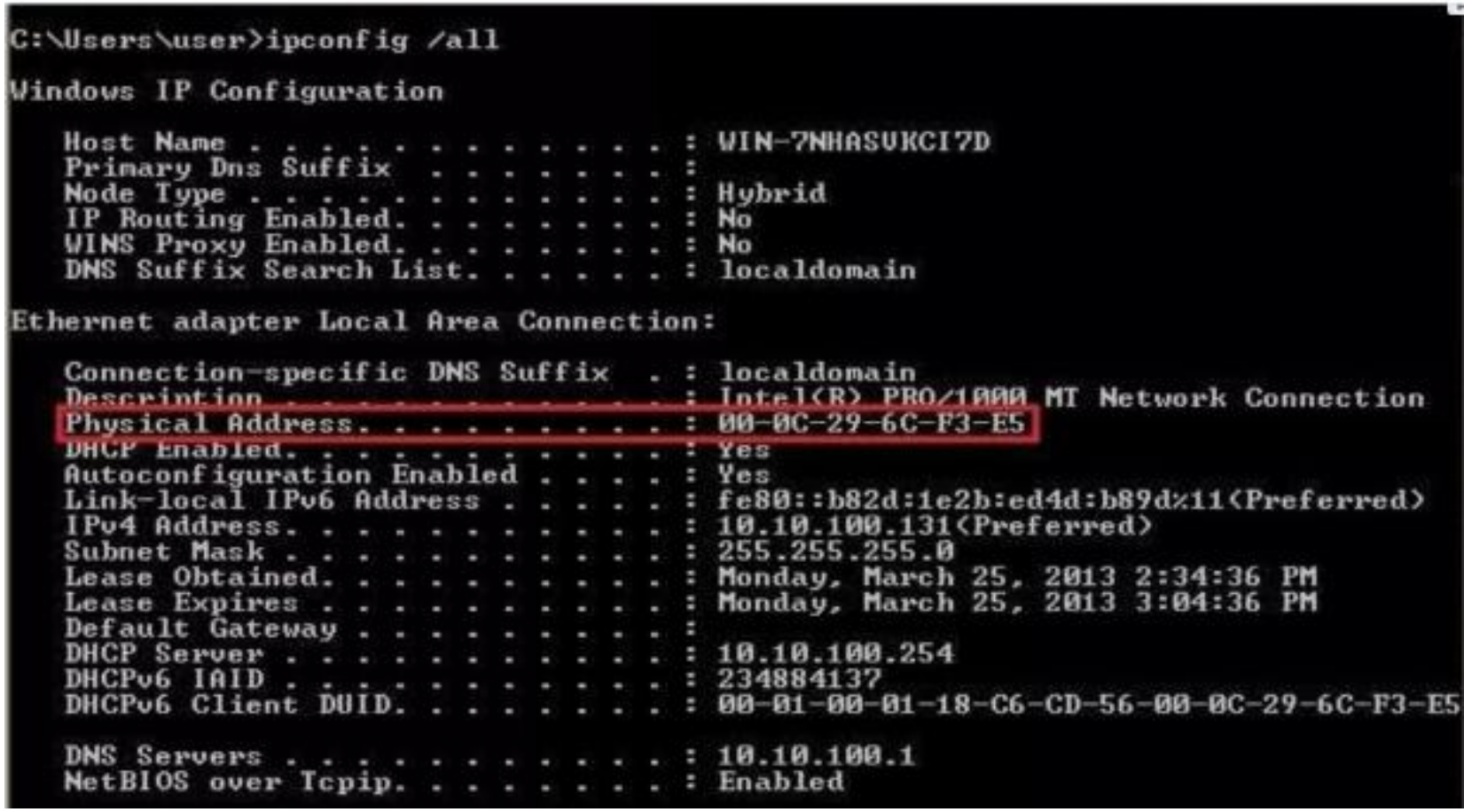
- ✓It is address used to identify the host on the network.
- ✓It is a logical address
- ✓32 bits (12 hexadecimal digits)
- ✓Used to connect between two devices in the ethernet environment
- ✓IP address usually used for IPv4 which is the fourth version of IP protocol.
- ✓A newer version IPv6 which is 128 bit addressing.

cmd → ipconfig



MAC address

- ✓Media access control.
- ✓It is a hardware address
- ✓48 bits (12 hexadecimal digits)
- ✓Used to connect between two hosts in the ethernet environment
- ✓Stored in firmware of the network card.
- ✓Globally unique.



Subnet Mask: 32bit IP Address



Network Address

Host Address



IP Address : 192 . 168 . 1 . 1

11000000 . 10101000 . 00000001 . 00000001

Subnet Mask: 255 . 255 . 255 . 0

11111111 . 11111111 . 11111111 . 00000000

IP Address

(First octet : Determine class of Ip Address)

Class A

1st octet range: (1 ⟹ 126)

Subnet Mask:

Network	Host	Host	Host
255	0	0	0

-NO. of Network ↓ < 255

-Many Hosts

Class B

1st octet range: (128 ⟹ 191)

Subnet Mask

Network	Network	Host	Host
255	255	0	0

Class C

1st octet range: (192 ⟹ 223)

Subnet Mask

Network	Network	Network	Host
255	255	255	0

-Many Networks
-Low No Of Hosts

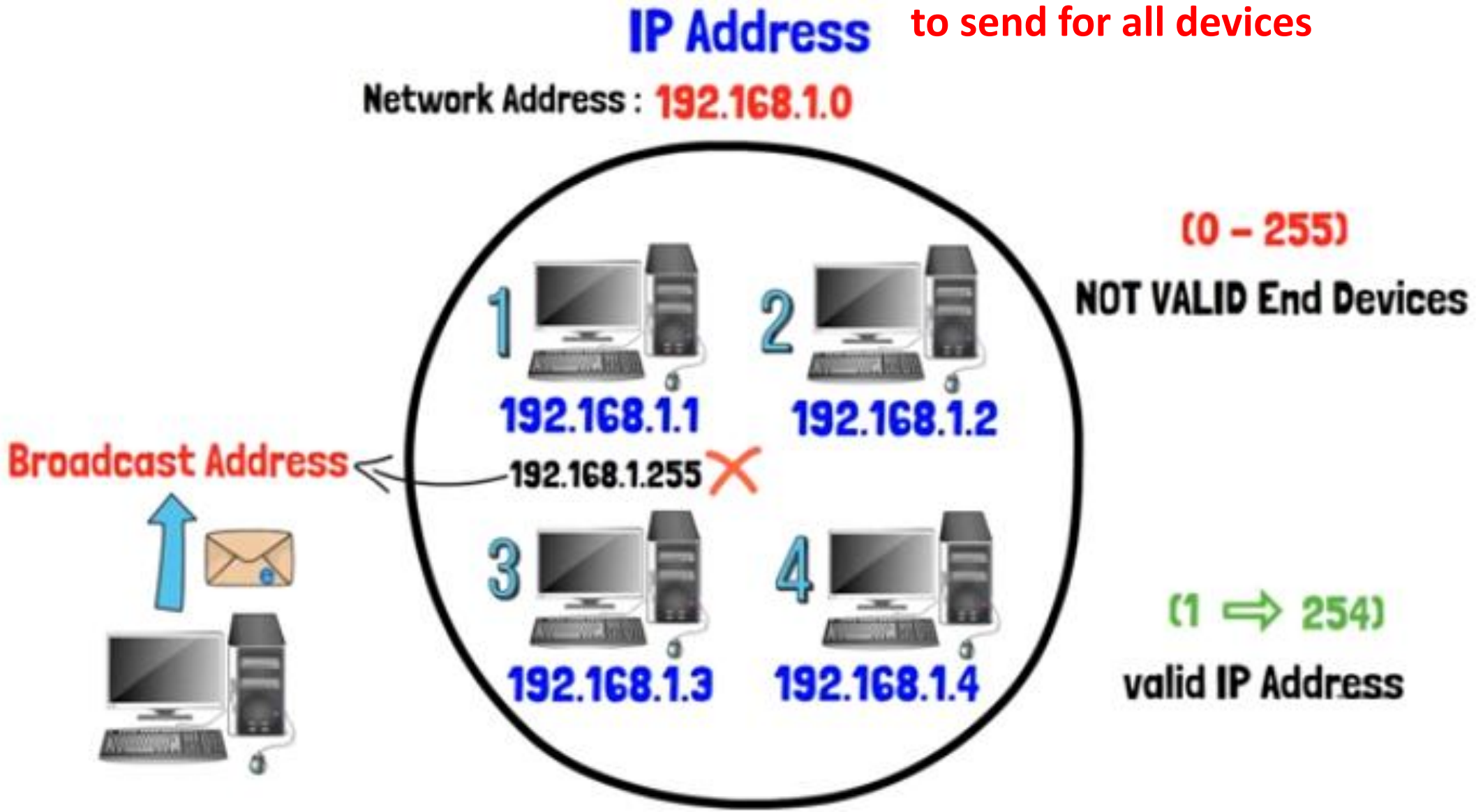


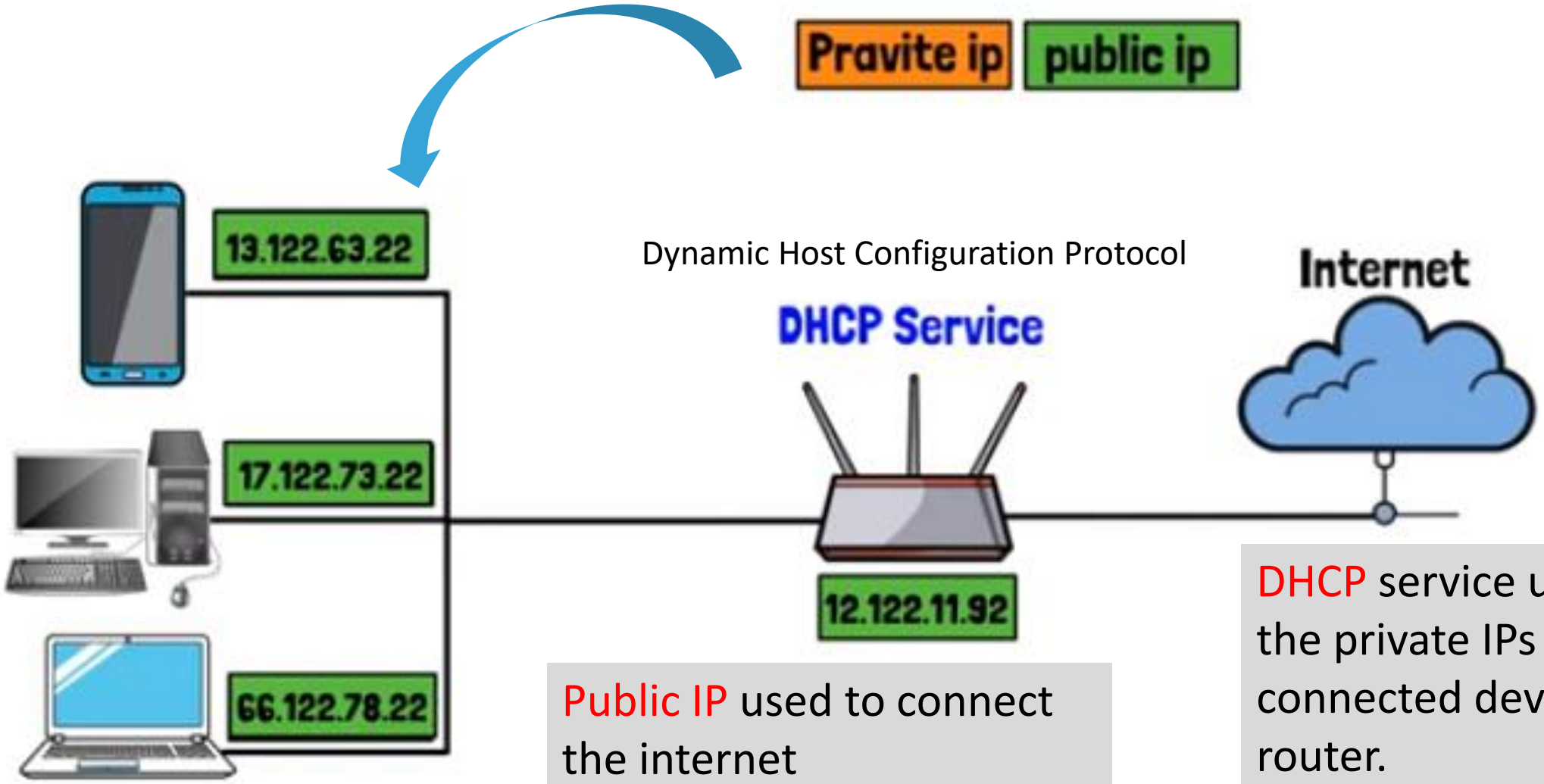
Ping 127.0.0.1

Can check NIC by ping

To distribute the IPs for the devices

192.168.1.0 → network address
192.168.1.255 → broadcast address
to send for all devices





Public IP used to connect the internet
The router gives the devices private IP to contact via public IP to internet

DHCP service used to give the private IPs to the connected device with router.

NAT: network address translation used to convert from private IP to public IP and vice versa.

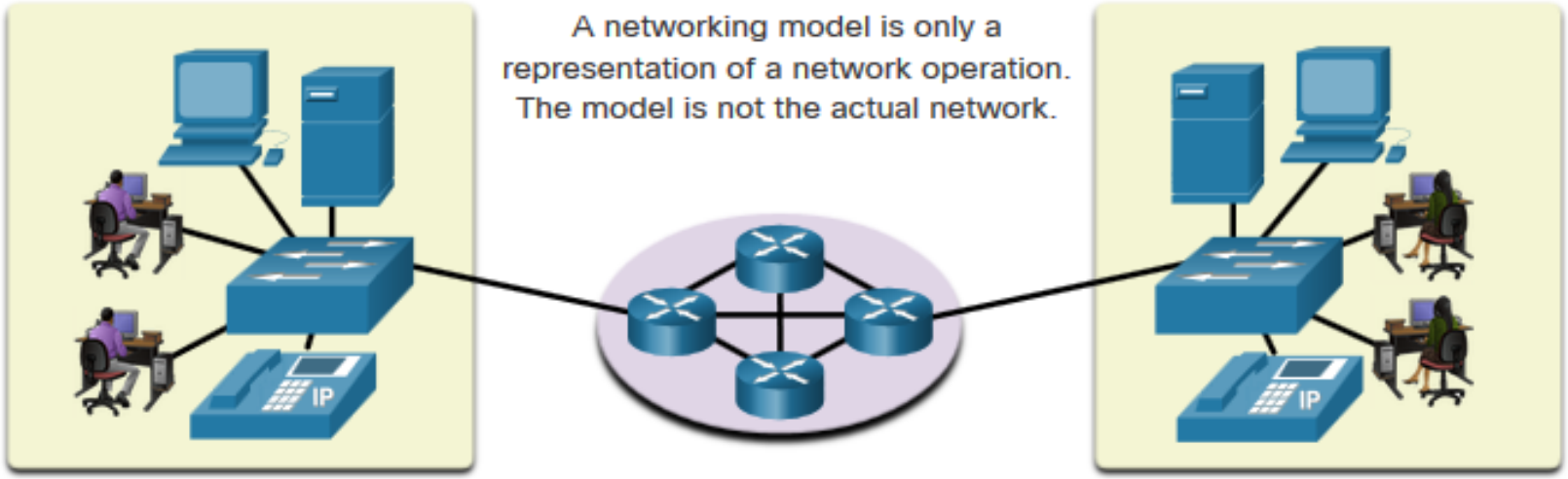
DHCP (Dynamic Host Configuration Protocol) Vs. APIPA (Automatic Private IP Addressing)

DHCP is a network protocol that uses a central server to automatically assign IP addresses and network settings to devices, while APIPA is a backup feature that lets a device give itself a temporary IP address when it cannot reach a DHCP serve.

Pravite IP Address Classes

Class	IP Address Range	Dafult Subnet Mask	For
Class A	10.0.0.0 - 10.255.255.255	N H H H 255.0.0.0	Large Organisation
Class B	172.16.0.0 - 172.31.255.255	N N H H 255.255.0.0	Mid size Organisation
Class C	192.168.0.0 - 192.168.255.255	N N N H 255.255.255.0	home, office and small company

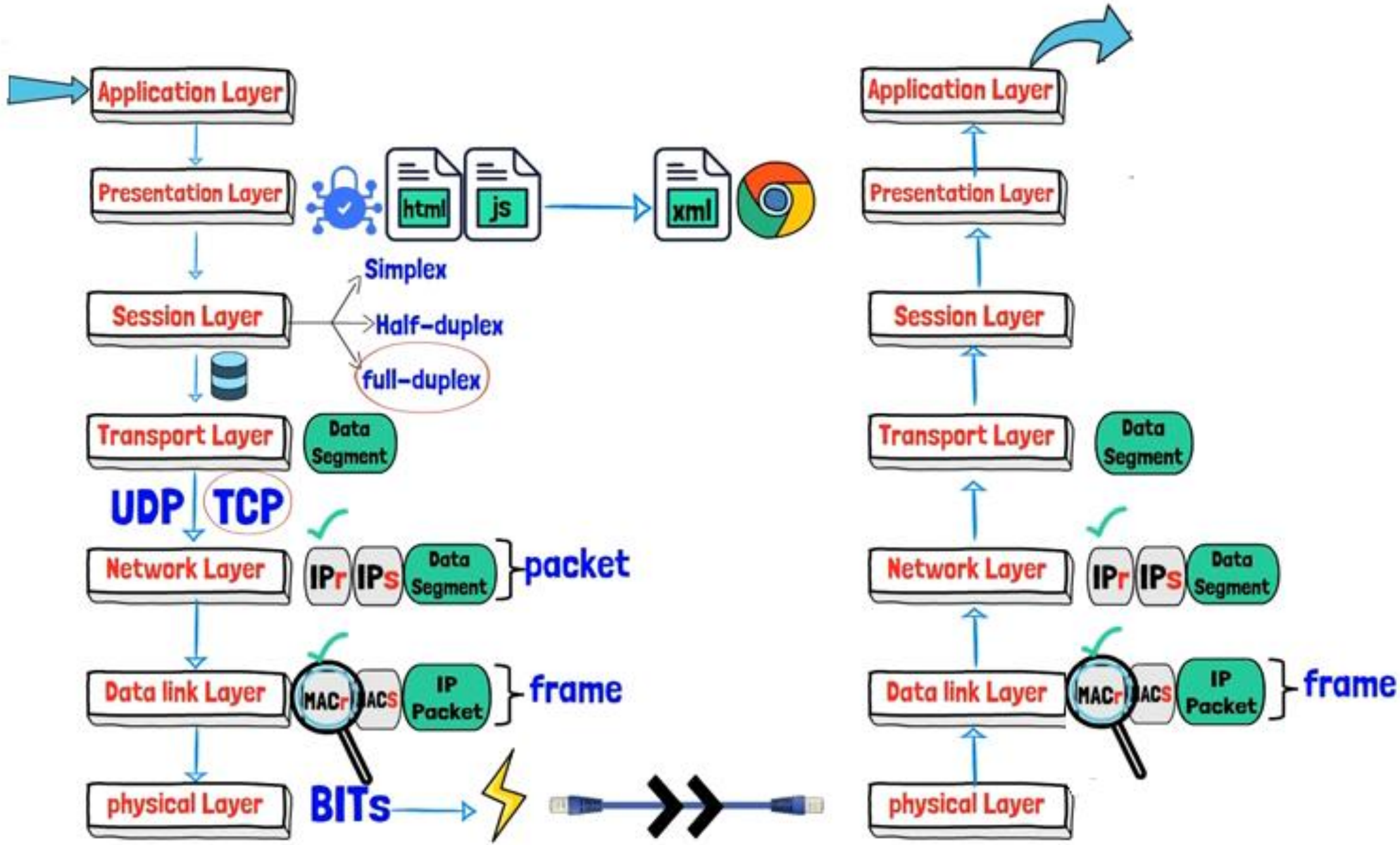
A networking model is only a representation of a network operation. The model is not the actual network.



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	Ethernet, WLAN, SONET, SDH	Network Access
Physical		

TCP/IP Model Layer (Transmission Control Protocol/Internet Protocol)	Description
Application	Represents data to the user, plus encoding and dialog control.
Transport	Supports communication between various devices across diverse networks.
Internet	Determines the best path through the network.
Network Access	Controls the hardware devices and media that make up the network.

OSI Model Layer (open system interconnection)	Description
7 - Application	Contains protocols used for process-to-process communications.
6 - Presentation	Provides for common representation of the data transferred between application layer services.
5 - Session	Provides services to the presentation layer and to manage data exchange.
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications.
3 - Network	Provides services to exchange the individual pieces of data over the network.
2 - Data Link	Describes methods for exchanging data frames over a common media.
1 - Physical	Describes the means to activate, maintain, and de-activate physical connections.


Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data link Layer
physical Layer
html
js
xml
Simplex
Half-duplex
full-duplex
Data Segment
UDP
TCP
IPr
IPs
Data Segment
packet
MACr
MACs
IP Packet
frame
BITs
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data link Layer
physical Layer
Data Segment
IPr
IPs
Data Segment
MACr
MACs
IP Packet
frame

- **The 7 Layers of the OSI Model**

Physical Layer (layer 1)

- **The input of physical layer is stream of bits and the layer converts the input bits to suitable signal related to the type of transmission media.**
- (exchange the data between the hosts through communication media)

Data Link Layer(layer 2)

- At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into **frames**. The data link layer also detect and **correct errors** that may have occurred at the physical layer.
- In another words when the host receives a frame and discards it after determining its corrupt, data link layer can check frame for errors.
- The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols. ***Use CSMA protocol to control the traffic to avoid data collision.***

Network Layer(layer 3)

• The network layer finds (IP) the destination by using logical addresses, such as **IP** (internet protocol) as packet. At this layer, ***routing used to select the best path for signal*** (use ICMP protocol-internet control message protocol).

- It delivery the packet from source to destination.

Transport Layer(layer 4)

• Use Sequence package exchange protocol.

• The transport layer manages the delivery of data. It regulates the size, sequencing, and flow control ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol and UDP(User Datagram Protocol).

• TCP is best used for direct communication in which a reliable connection is needed, such as web browsing, email, text messaging, and file transfers. UDP is best used for live and real-time data transmission when speed is more important than reliability

Session Layer(layer 5)

- The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and termined at layer 5. Session layer services also include determine transmission modes, authentication and authorization session management which Store the last data in the site as videos and can be shown in disconnection case .

Presentation Layer(layer 6)

- The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts (convert to bits). Because of this, it at times also called the syntax layer, compress data by compression process. This layer can also handle the **encryption** and **decryption** required by the application layer.

Application Layer(layer 7) --- user interaction

- At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.
- Determine the suitable protocol for the action
- Example: http for web site(**Hypertext Transfer Protocol**)
- FTP for download (file transfer protocol)
- SMTP- pop3 for mails.

Protocol Suites

TCP/IP Protocol Suite

