

What is a network?

- A network is two devices connected to each other with a physical medium, such as wires or radio signals
- The connection allows those two devices to exchange data



INTRODUCING NETWORK DEVICES

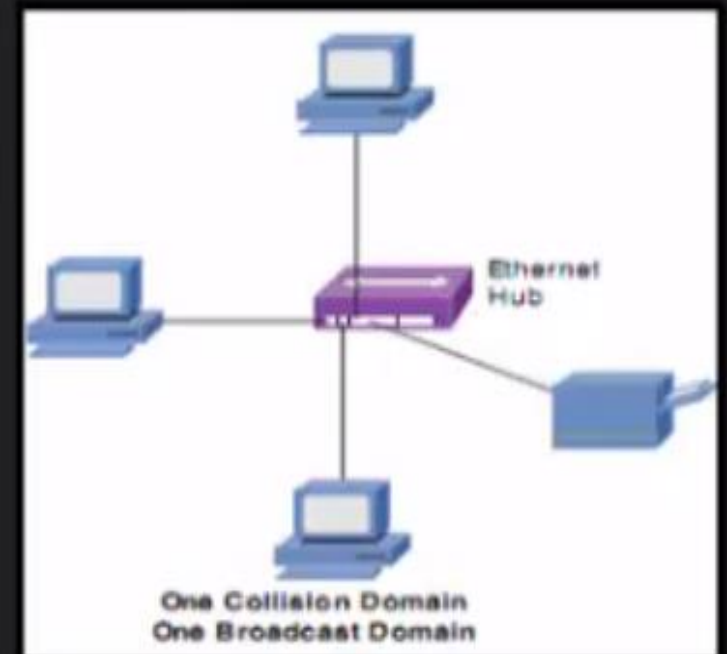
Al-Nahrain University/ECC
Eng.vian adnan farman

- Physical Layer: Repeaters
- repeaters regenerate incoming electrical, wireless or optical signals. With physical media like Ethernet or Wi-Fi
- Distance limitation in local-area networks
 - Electrical signal becomes weaker as it travels
- Repeaters join LANs together



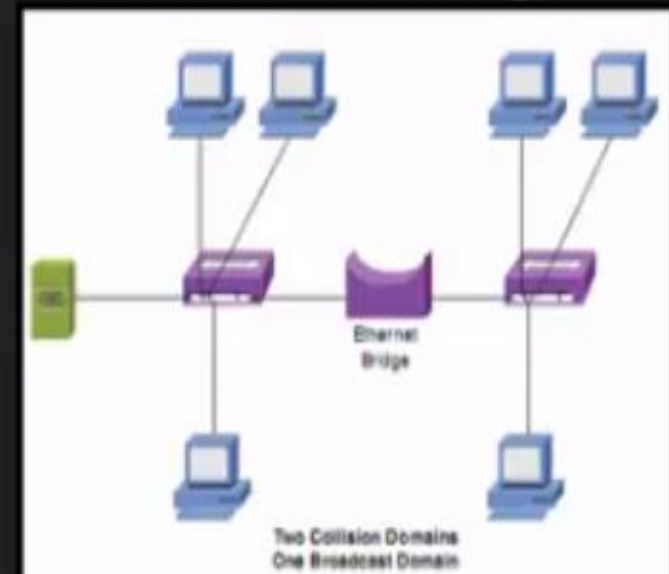
Introducing Network Devices

- Physical Layer: Hubs
- A hub is a common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.



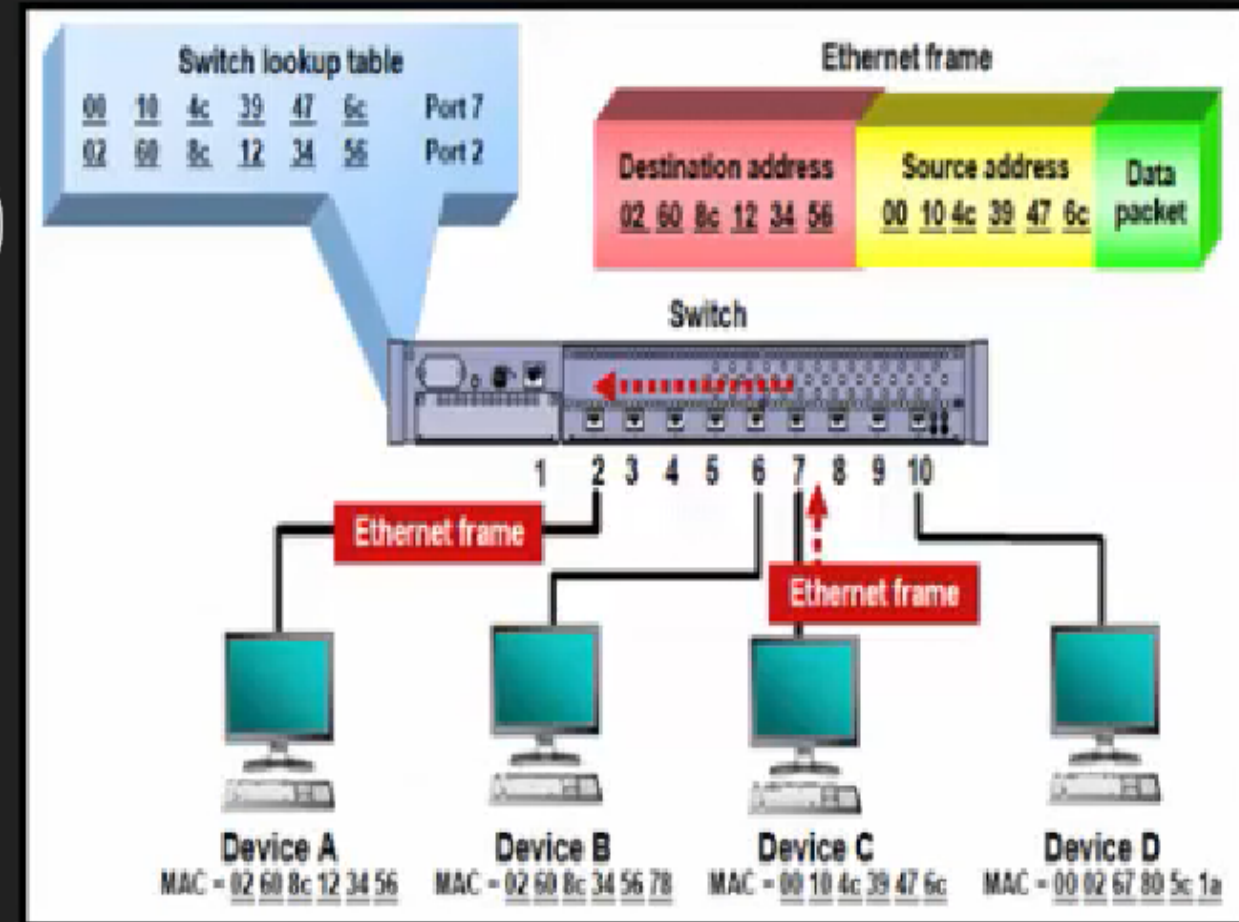
Introducing Network Devices

- Link Layer: Bridges
- In telecommunication networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).



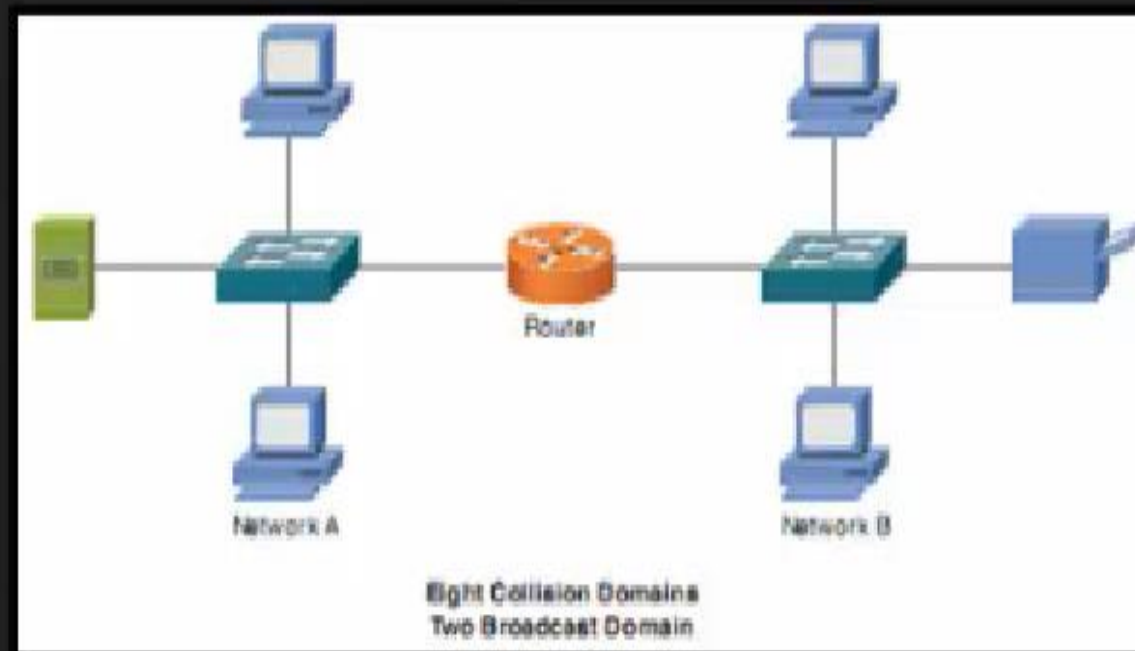
Introducing Network Devices

- Link Layer: Switches
- In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.



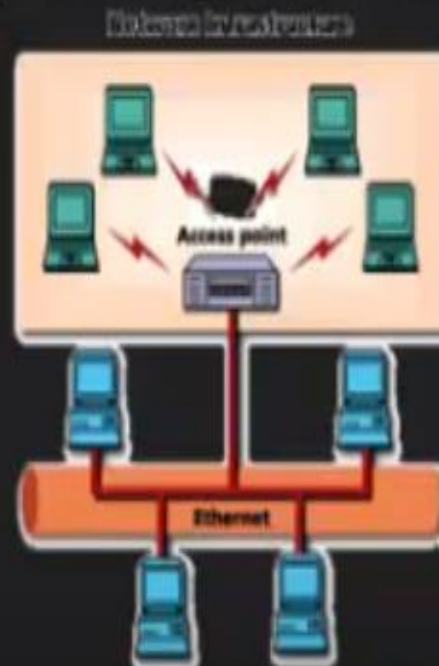
Introducing Network Devices

- Network Layer: Routers
- A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.



Introducing Network Devices

- Link Layer: Access Points
- a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.

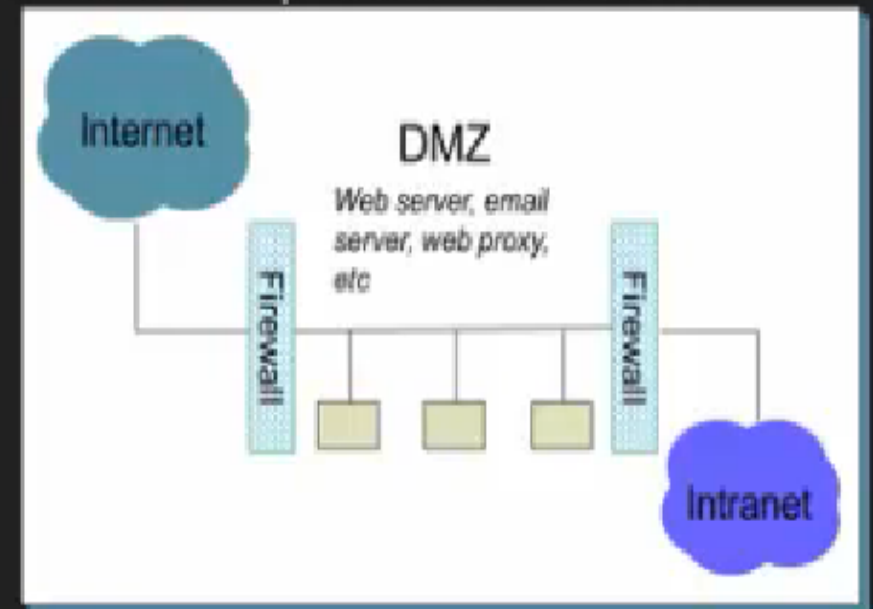


Introducing Network Devices

- Firewalls

- A firewall is a system designed to prevent

unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.



Introducing Network Devices

Al-Nahrain University/ECC
Eng.vian adnan farman

- IDS/IPS
- IDS — A Passive Security Solution
- An intrusion detection system (IDS) is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
- An IDS specifically looks for suspicious activity and events that might be the result of a virus, worm or hacker. This is done by looking for known intrusion signatures or attack signatures
- Network-based , Host-based IDS



Introducing Network Devices

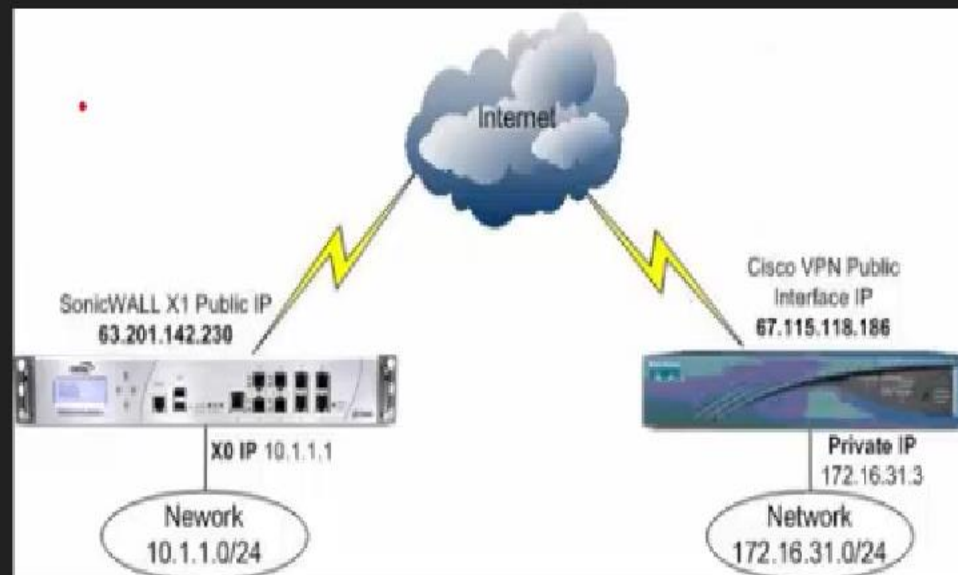
Al-Nahrain University/ECC
Eng.vian adnan farman

- IDS/IPS
- IPS or intrusion prevention system, is definitely the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets. It provides policies and rules for network traffic along with an IDS for alerting system or network administrators to suspicious traffic, but allows the administrator to provide the action upon being alerted. Where IDS informs of a potential attack, an IPS makes attempts to stop it. Another huge leap over IDS
- Network-based , Host-based IDS



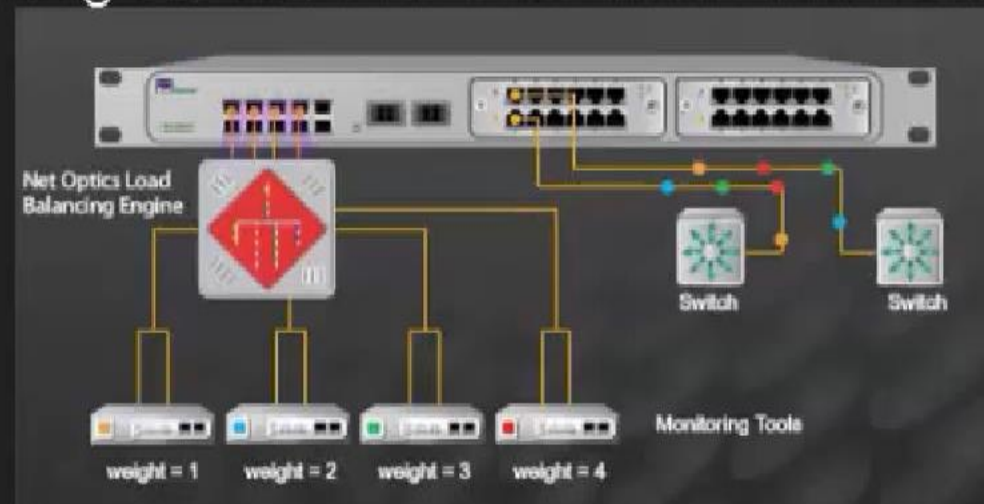
Introducing Network Devices

- VPN Concentrator
- A VPN concentrator is a type of networking device that provides secure creation of VPN connections and delivery of messages between VPN nodes.
- It is a type of router device, built specifically for creating and managing VPN communication infrastructures.



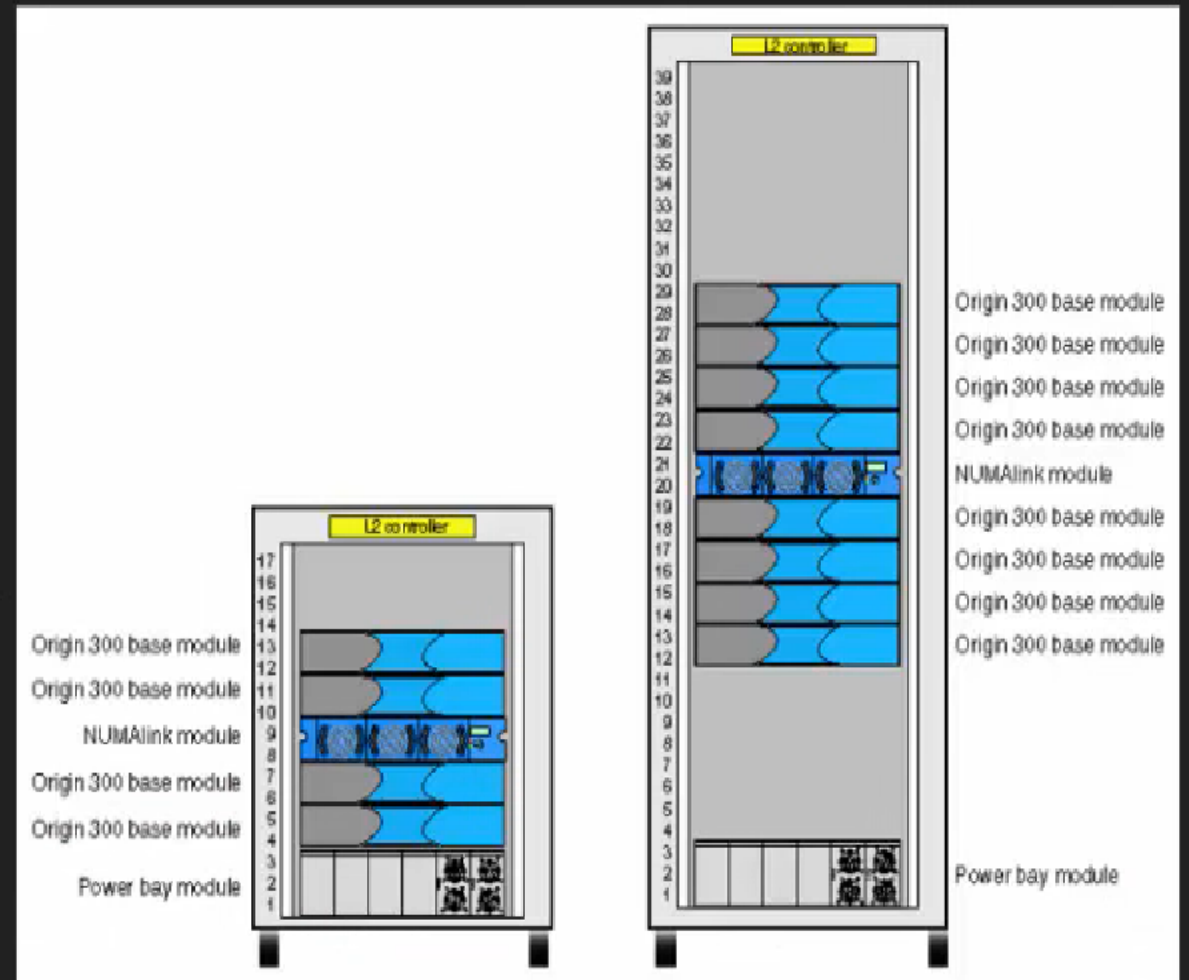
Introducing Network Devices

- Load Balancer
- Distributing processing and communications activity evenly across a computer network so that no single device is overwhelmed. Load balancing is especially important for networks where it's difficult to predict the number of requests that will be issued to a server. Busy Web sites typically employ two or more Web servers in a load balancing scheme. If one server starts to get swamped, requests are forwarded to another server with more capacity. Load balancing can also refer to the communications channels themselves.



Introducing Network Devices

- The Rack Unit
- A rack unit is a unit of measure used to describe the height of a server, network switch or other similar device mounted in a 19-inch rack or a 23-inch rack.

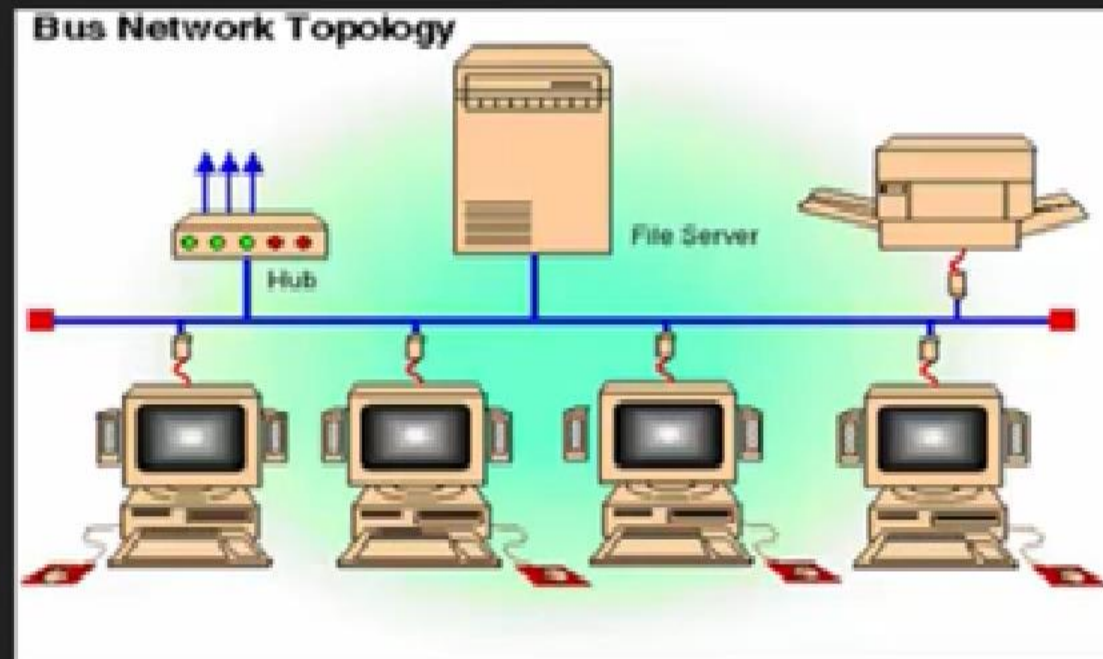


What is a network topology?

- A **network topology** defines the physical connections of hosts in a network
- There are multiple types of topologies, including:
 - Bus
 - Star
 - Ring
 - Mesh

Network Topologies

- Bus Topology
- What is Bus Topology?
- a bus topology is a network setup where each computer and network device are connected to a single cable or backbone. Bus networks are useful in small networks (like those setup in a small offices)



Network Topologies

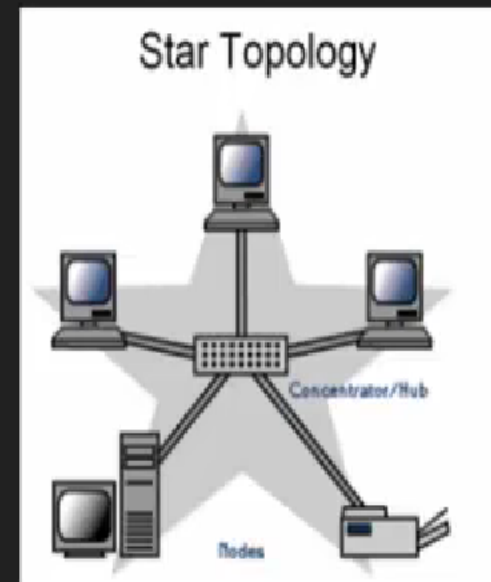
- **Advantages (benefits)**

- 1) It is easy to set-up and extend bus network.
- 2) Cable length required for this topology is the least compared to other networks.
- 3) Bus topology costs very less.
- 4) Linear Bus network is mostly used in small networks. Good for LAN.

- **Disadvantages (Drawbacks)**

- 1) There is a limit on central cable length and number of nodes that can be connected.
- 2) Dependency on central cable in this topology has its disadvantages.If the main cable (i.e. bus) encounters some problem, whole network breaks down.
- 3) Proper termination is required to dump signals. Use of terminators is must.
- 4) It is difficult to detect and troubleshoot fault at individual station.
- 5) Maintenance costs can get higher with time.
- 6) Efficiency of Bus network reduces, as the number of devices connected to it increases.
- 7) It is not suitable for networks with heavy traffic.
- 8) Security is very low because all the computers receive the sent signal from the source.

- Star topology
- In Star topology, all the components of network are connected to the central device called “hub” which may be a hub, a router or a switch. Unlike Bus topology (discussed earlier), where nodes were connected to central cable, here all the workstations are connected to central device with a point-to-point connection. So it can be said that every computer is indirectly connected to every other node by the help of “hub”.



Advantages of Star Topology

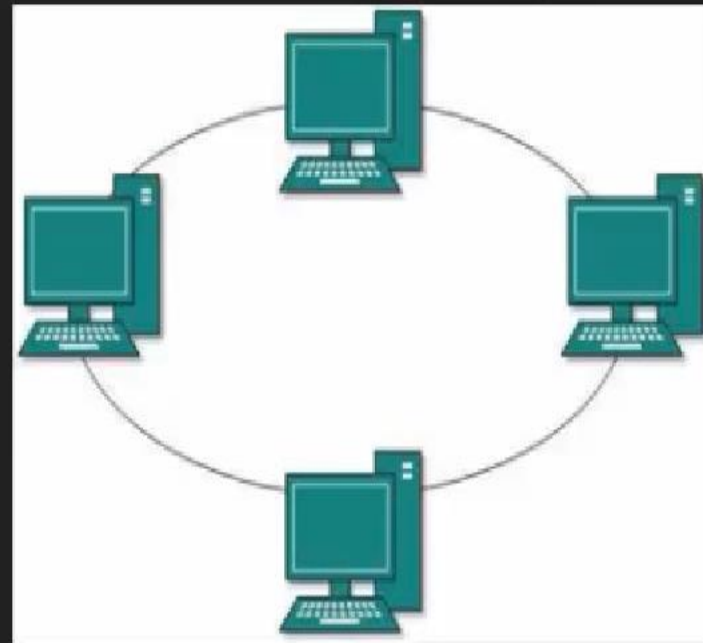
- 1) As compared to Bus topology it gives far much better performance, signals don't necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central hub.
- 2) Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.
- 3) Centralized management. It helps in monitoring the network.
- 4) Failure of one node or link doesn't affect the rest of network. At the same time its easy to detect the failure and troubleshoot it.

Disadvantages of Star Topology

- 1) Too much dependency on central device has its own drawbacks. If it fails whole network goes down.
- 2) The use of hub, a router or a switch as central device increases the overall cost of the network.
- 3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.

Network Topologies

- Ring Topology
- In Ring Topology, all the nodes are connected to each-other in such a way that they make a closed loop. Each workstation is connected to two other components on either side, and it communicates with these two adjacent neighbors. Data travels around the network, in one direction. Sending and receiving of data takes place by the help of TOKEN.



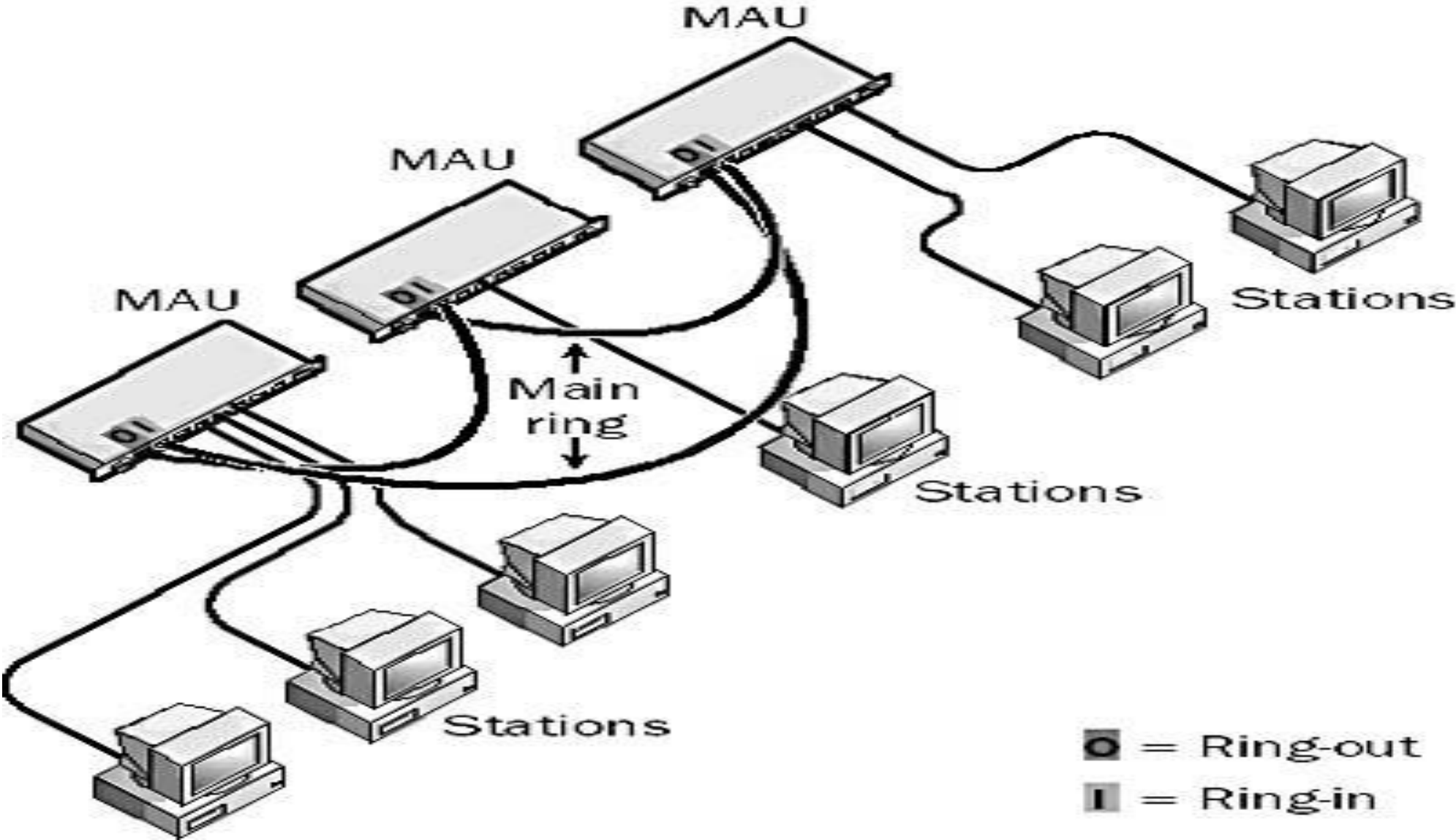
○ Advantages of Ring Topology

- 1) This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduce chances of collision. Also in ring topology all the traffic flows in only one direction at very high speed.
- 2) Even when the load on the network increases, its performance is better than that of Bus topology.
- 3) There is no need for network server to control the connectivity between workstations.
- 4) Additional components do not affect the performance of network.
- 5) Each computer has equal access to resources.

○ Disadvantages of Ring Topology

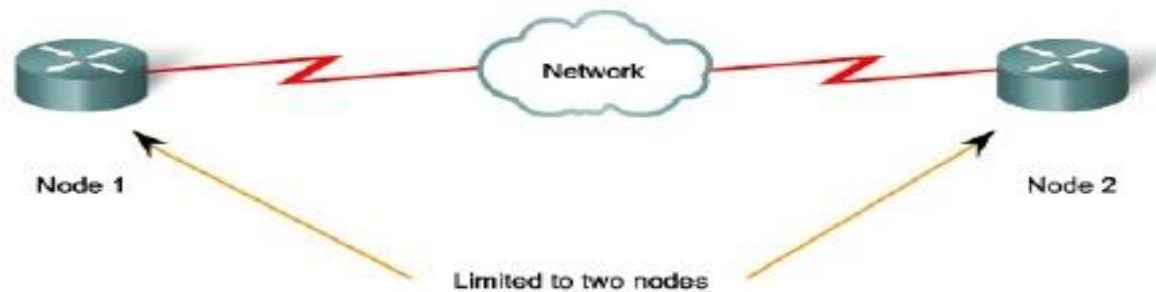
- 1) Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
- 2) If one workstation or port goes down, the entire network gets affected.
- 3) MAU's and network cards are expensive as compared to Ethernet cards and hubs.

MAU: multi-station access units



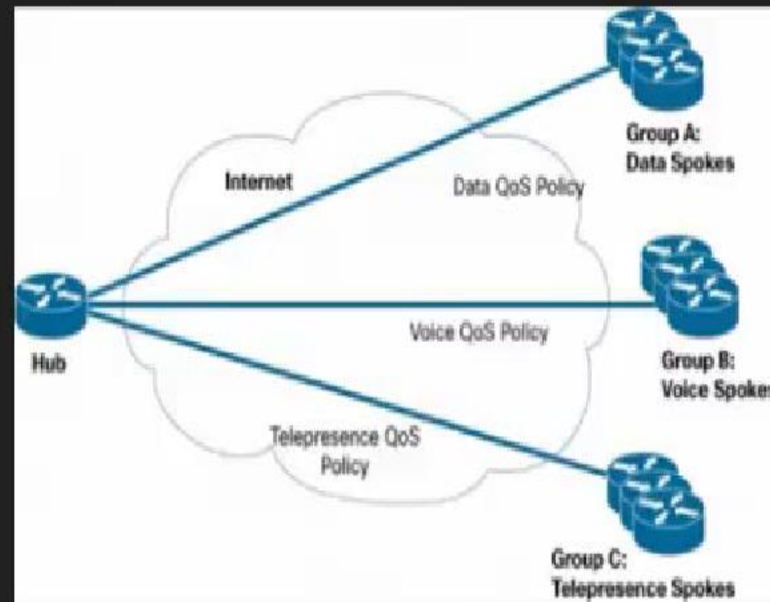
Point-to-Point Topology

- A point-to-point topology connects two nodes directly together
- The media access control protocol can be very simple
- The frames are placed on the media by the node at one end and taken off the media by the node at the other end
- Point-to-point networks can also operate either in half-duplex or full-duplex mode



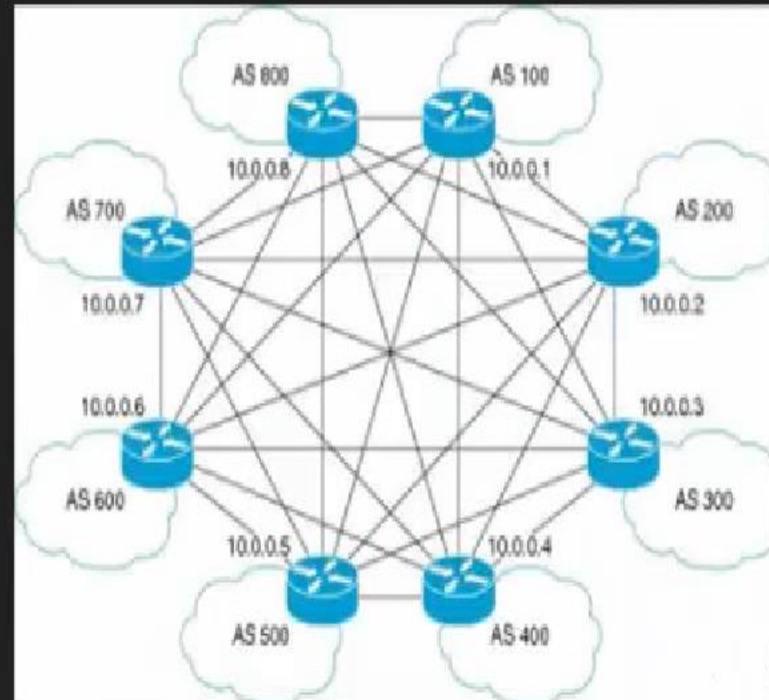
Network Topologies

- Hub-and-Spoke Topology
- In a Hub-and-spoke Site-to-Site Wide Area Network (WAN) network topology, one physical site act as Hub (Example, Main Office), while other physical sites act as spokes. Spoke sites are connected to each other via Hub site. In Hub-and-spoke Wide Area Network (WAN) topology, the network communication between two spokes always travel through the hub.



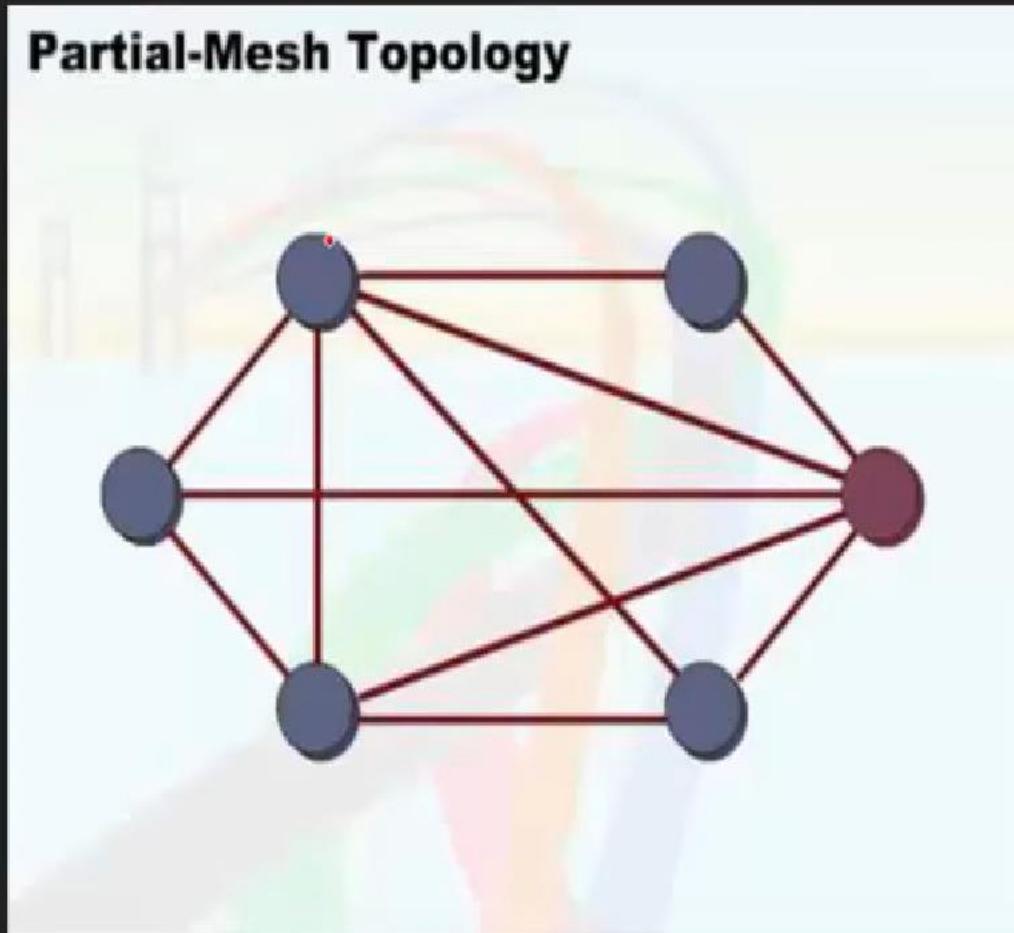
Network Topologies

- Full-Mesh Topology
- A mesh network topology is a decentralized design in which each node on the network connects to at least two other nodes. Mesh networks are expected to play an important part in the Internet of Things



Network Topologies

- Partial-Mesh Topology



Types of topology

There are two types of network topologies:

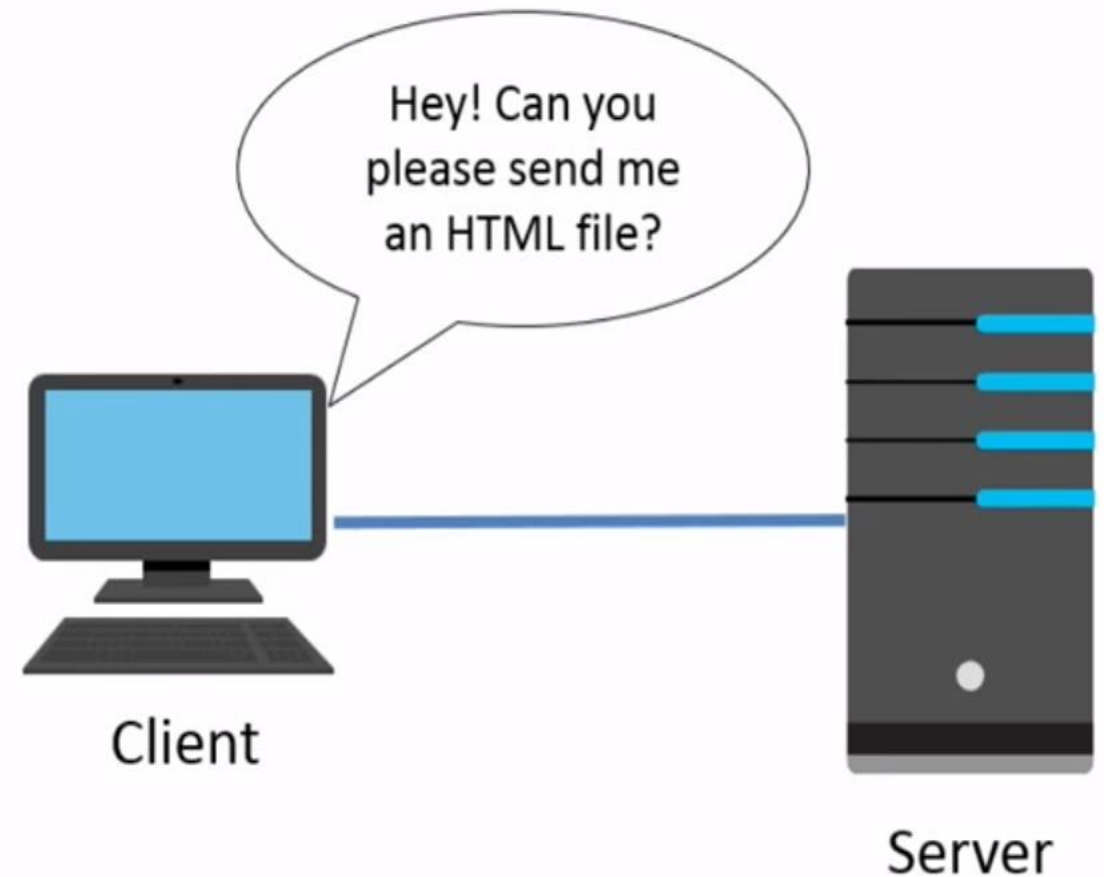
- *Physical Topology*
- *Logical Topology*

Physical Topology emphasizes the physical layout of the connected devices and nodes.

Logical Topology focuses the pattern of data transfer between network nodes.

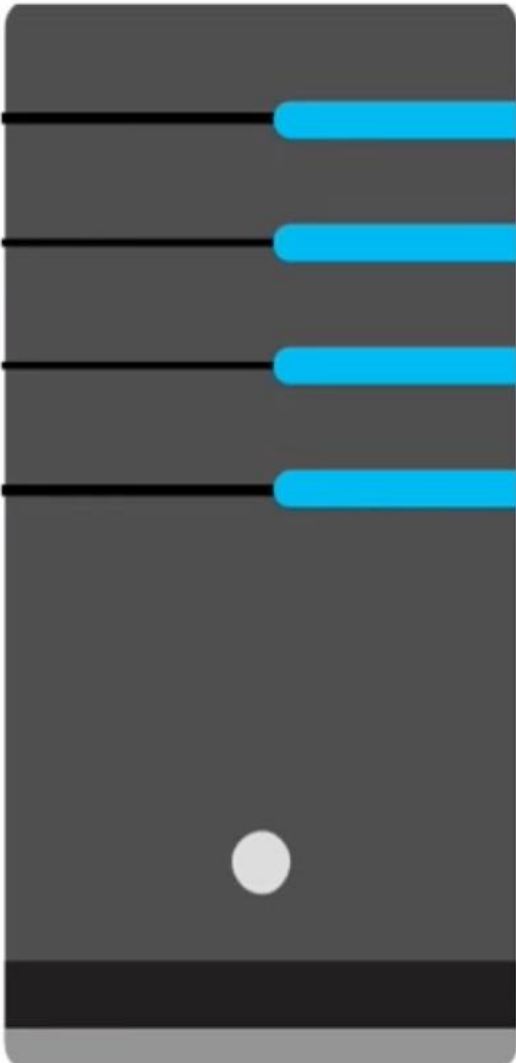
The Client/Server Model

- Servers are computers dedicated to providing specific types of services or data
- A client (a computer) uses software to ask a server for data or services
- The server provides the data or service to the client



Types of Servers

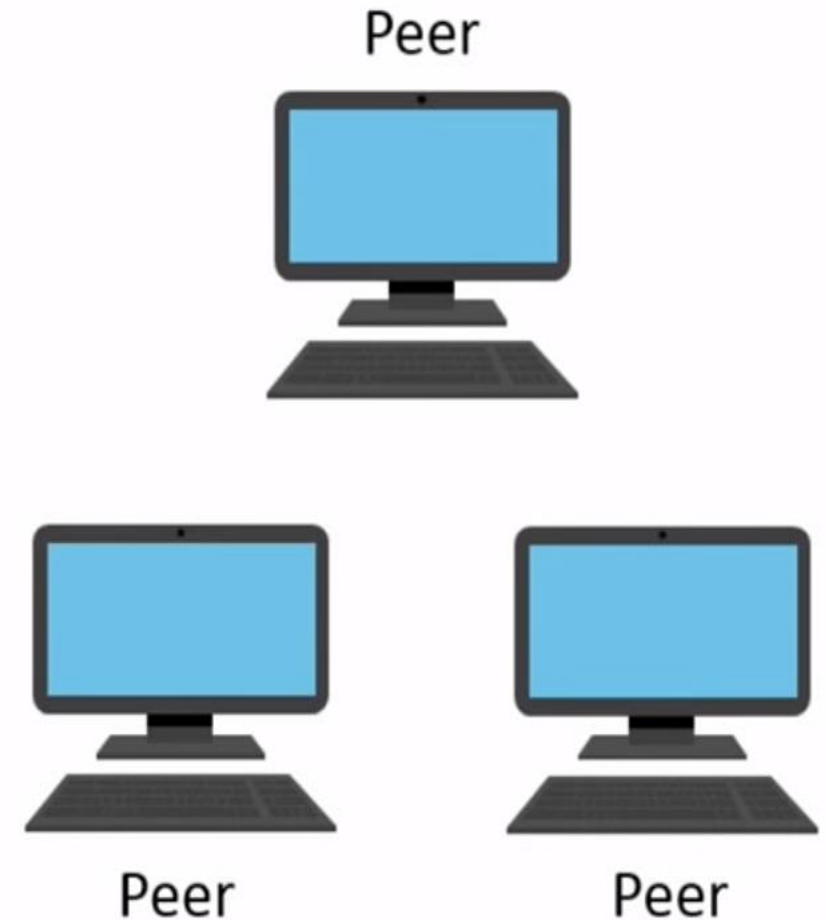
Al-Nahrain University/ECC
Eng.vian adnan farman



Server type	Function(s)
File server	Store files, software, or data for access by computers on a network.
Print server	Allows computers that are connected to a network to control printers on the network.
Database server	Houses a relational database made up of multiple files.
Network controller	Controls accounts that are domain, as well as the devices that belong to a network.
Messaging server	Provide services related to email, fax, instant messaging and collaboration.
Web server	Provides access to HTML documents for computers on a network.
CTI-based server	Responsible for Computer Telephony Integration, which integrates a network's telephone and computer systems.

The Peer -to- Peer Model

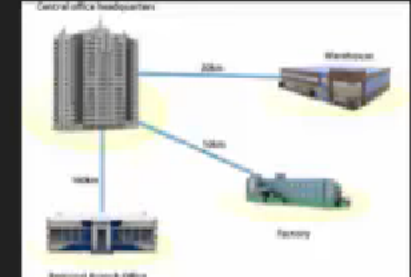
- Peers are clients that have equal capabilities and responsibilities in this model
 - Ability to serve and request data
 - No server in this model
- Examples of file sharing networks
 - Napster
 - Gnutella
 - G2
- Other technologies also take advantage of P2P file sharing:
 - Skype
 - VoIP
 - Cloud computing



Network Infrastructures

○ Based on the geographical dispersion of network components, networks can be classified into various categories, including the following:

- ■ Local-area network (LAN)
- ■ Wide-area network (WAN)
- ■ Campus-area network (CAN)
- ■ Metropolitan-area network (MAN)
- ■ Personal-area network (PAN)



- Local-area network (LAN)
- A local-area network (LAN) is a computer network that spans a relatively small area. Most often, a LAN is confined to a single room, building or group of buildings, however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).



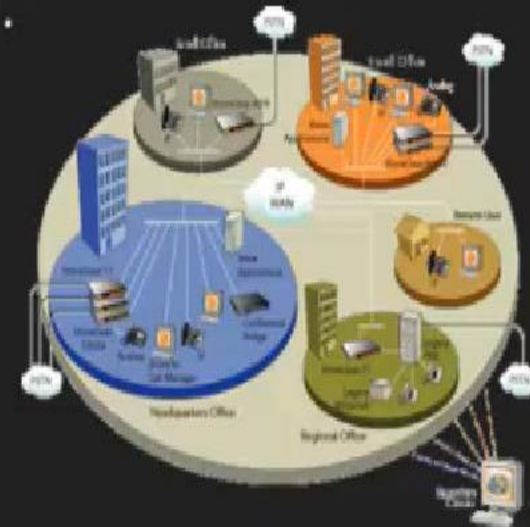
WLAN

Al-Nahrain University/ECC
Eng.vian adnan farman

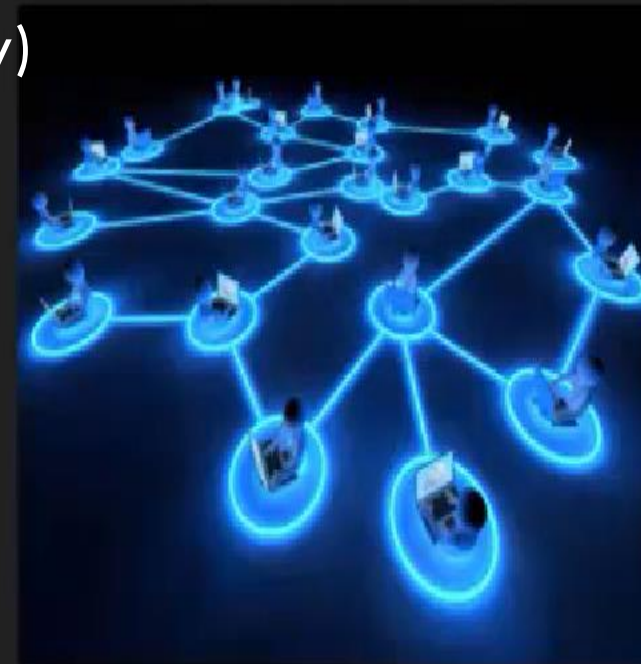


Network Infrastructures

- WAN - wide area network
- A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).
- Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

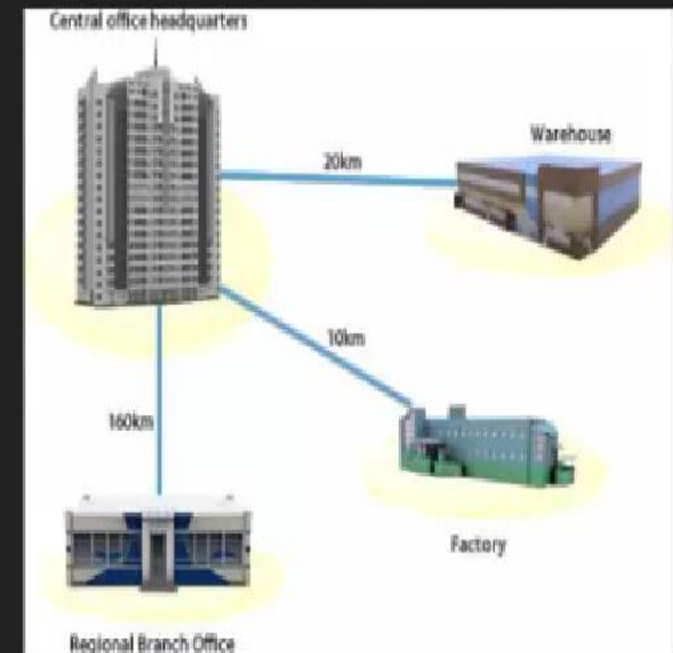


- Campus-area network (CAN)
- A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area. A CAN is smaller than a wide area network (WAN) or metropolitan area network (MAN).
(network in university)



Network Infrastructures

- Metropolitan-area network (MAN)
- Short for Metropolitan Area Network, a data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media.



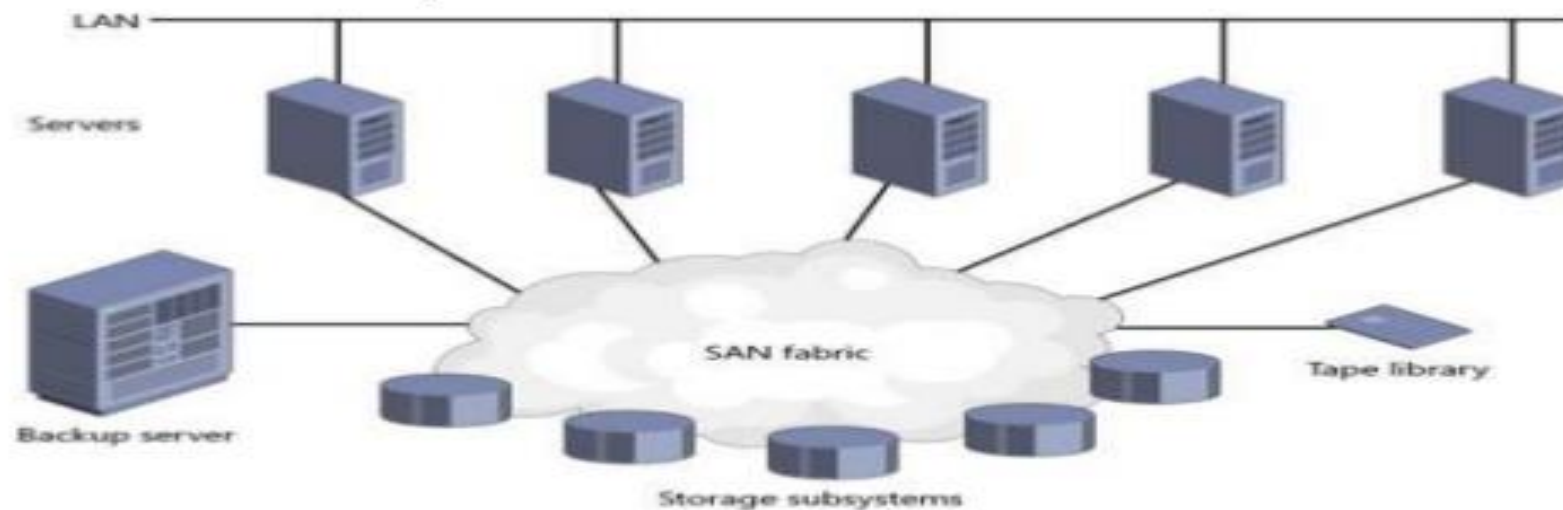
Network Infrastructures

- Personal-area network (PAN) Such as Bluetooth or camera connect to computer
- is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication),



Storage Area Network (SAN) Also cloud

- **SAN is a Network Whose Primary aim is to transfer data between storage devices like disk array and servers.**



Cables And Connectors

Coaxial
Cable

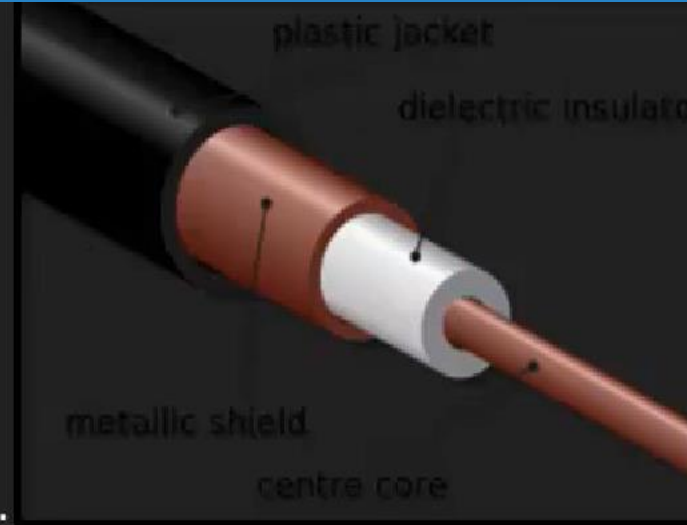
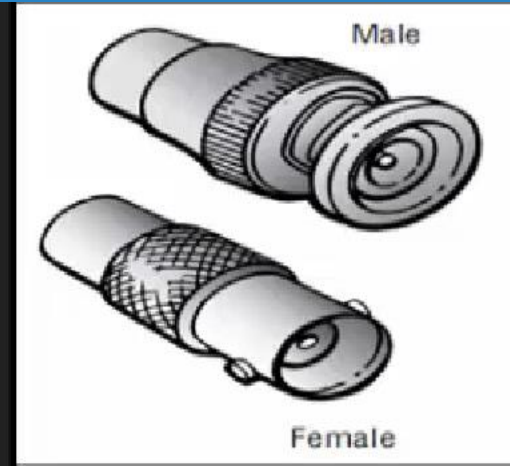
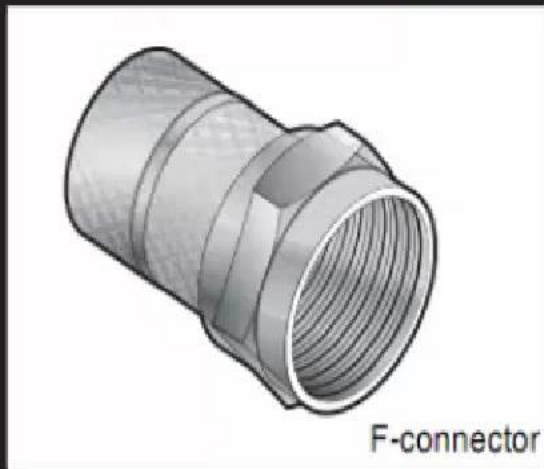
Twisted-Pair
Cable

Fiber-Optic
Cable

Media

By definition, a network is an interconnection of devices. Those interconnections occur over some type of media. The media might be physical, such as a copper or fiber-optic cable. Alternately, the media might be the air, through which radio waves propagate (as is the case with wireless networking technologies).

Cables And Connectors



Three of the most common types of coaxial cables include the following:

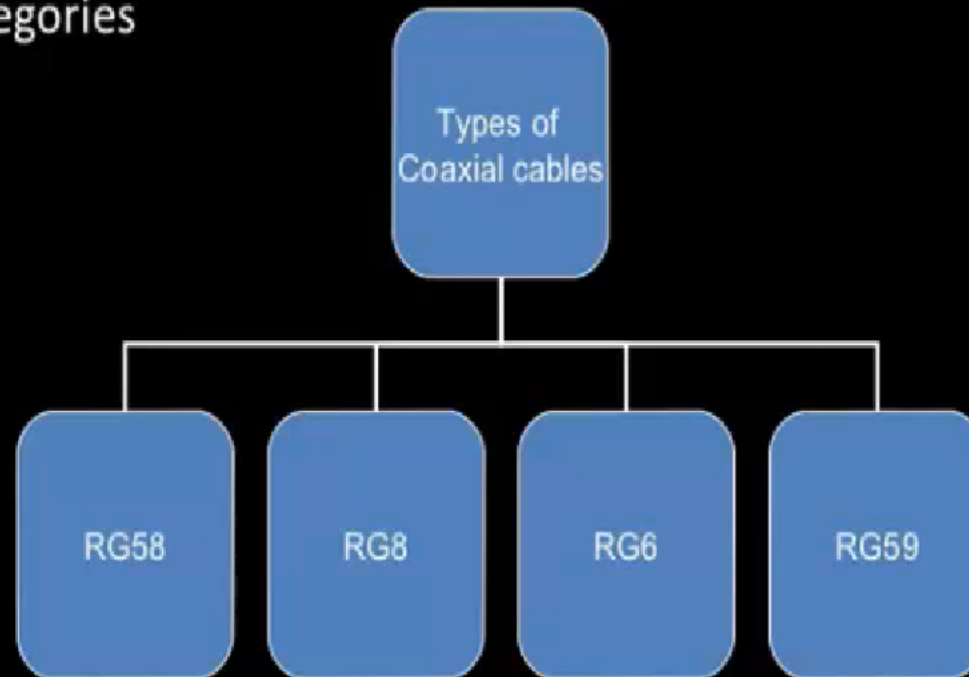
- **RG-59:** Typically used for short-distance applications, such as carrying composite video between two nearby devices. This cable type has loss characteristics such that it is not appropriate for long-distance applications. RG-59 cable has a characteristic impedance of 75 Ohms.
- **RG-6:** Commonly used by local cable companies to connect individual homes to the cable company's distribution network. Like RG-59 cable, RG-6 cable has a characteristic impedance of 75 Ohms.
- **RG-58:** Has loss characteristics and distance limitations similar to those of RG-59. However, the characteristic impedance of RG-58 is 50 Ohms, and this type of coax was popular with early 10BASE2 Ethernet networks .

Common connectors used on coaxial cables are as follows:

- **BNC:** A Bayonet Neill-Concelman (BNC) (also referred to as British Naval Connector in some literature) connector can be used for a variety of applications, including being used as a connector in a 10BASE2 Ethernet network.
- **F-connector:** An F-connector is frequently used for cable TV (including cable modem) connections.

Types of Coaxial cable

- Coaxial cables are mainly divided into four categories

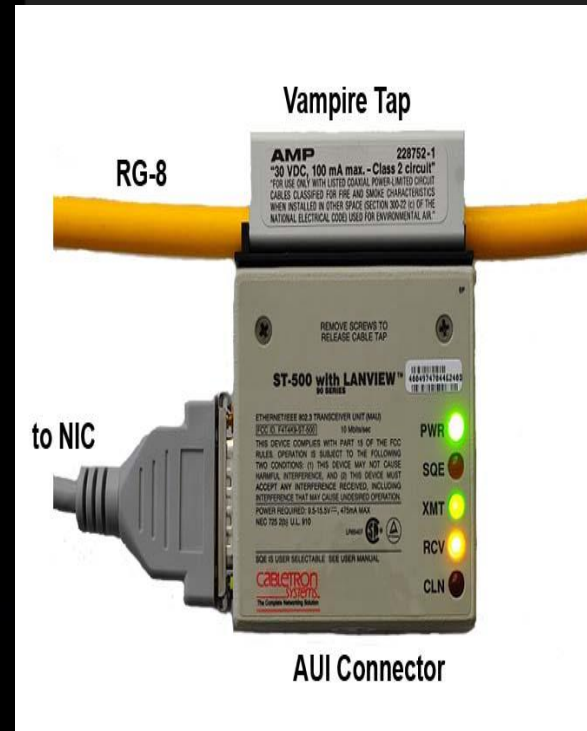


RG58

- Maximum segment length is 200 meters
- Interference protection is better than twisted pair cables
- Offers resistance of **50 ohms**
- BNC-T connector is used to connect this cable
- Used in thinnet (**10BASE2**) network
- Mostly used in changing environments
- Easy to add/remove devices form the network using RG58 cable
- Cheapest form of coaxial cable

RG8

- Maximum segment length is 500 meters
- Interference protection is good compared to any copper cable
- Offers resistance of 50 ohms
- AUI and Vampire Tap connector is used to connect this cable
- Used in **10BASE5** network
- Expensive than RG58
- Disadvantage is rigidity due to which it is only used as a backbone

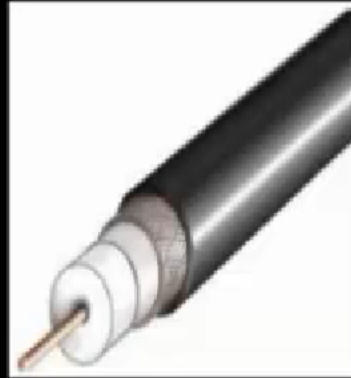


RG6

- Broadband quad-shielded cable that offers an impedance of **75 ohms**
- Provides **lower attenuation** characteristics
- Useful in cable TV, CCTV and satellite dish antenna
- Covers distance up to 1500 feet (450m approx)



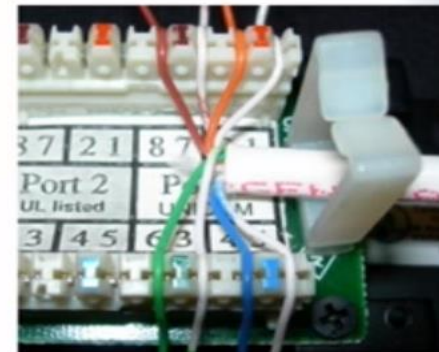
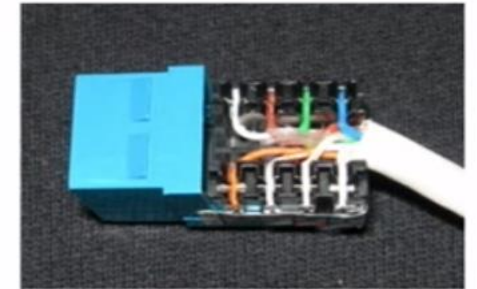
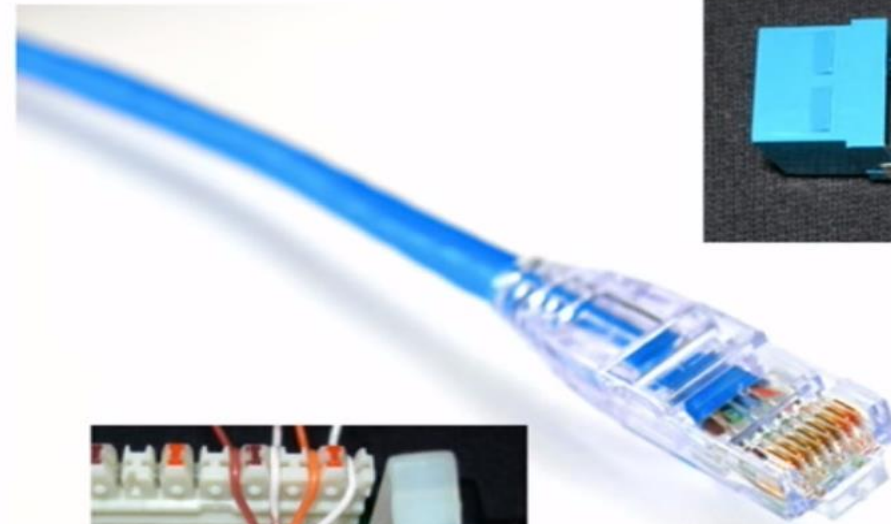
RG59

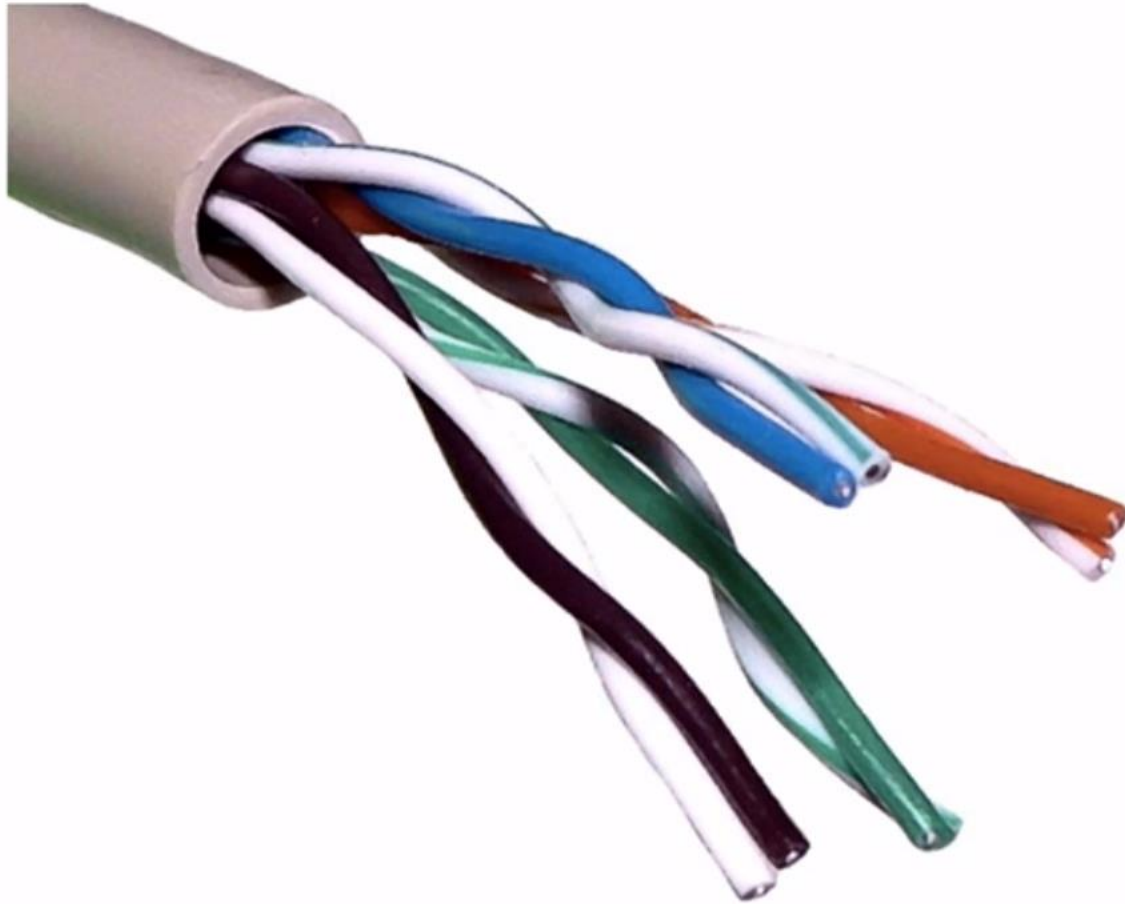


- Solid conductor is surrounded by a foam polyethylene dielectric
- Offers impedance of 75 ohm and used with **BNC connector**
- Useful in security camera, cable TV and home theatre
- Covers a distance up to 1000 feet (300m approx)
- Has a **higher attenuation** as compared to other coaxial cables

Twisted-pair cables:

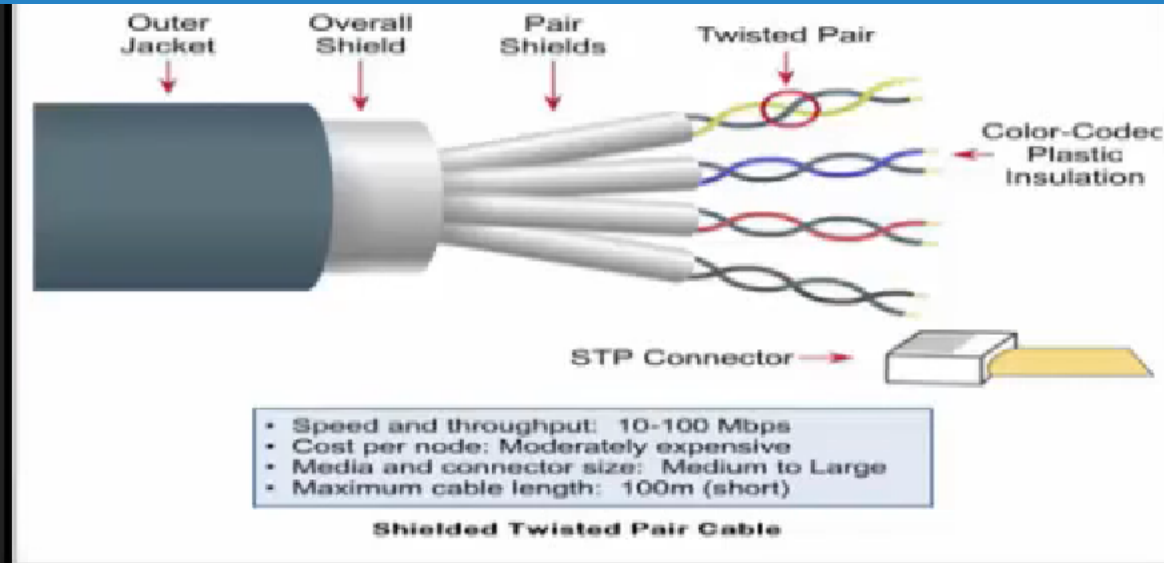
- Twisted-pair cables are the most common cables found in LANs
 - fast
 - efficient
 - cheap when compared to other connection types
- There are multiple types of twisted-pair cables, and they can be installed temporarily or permanently



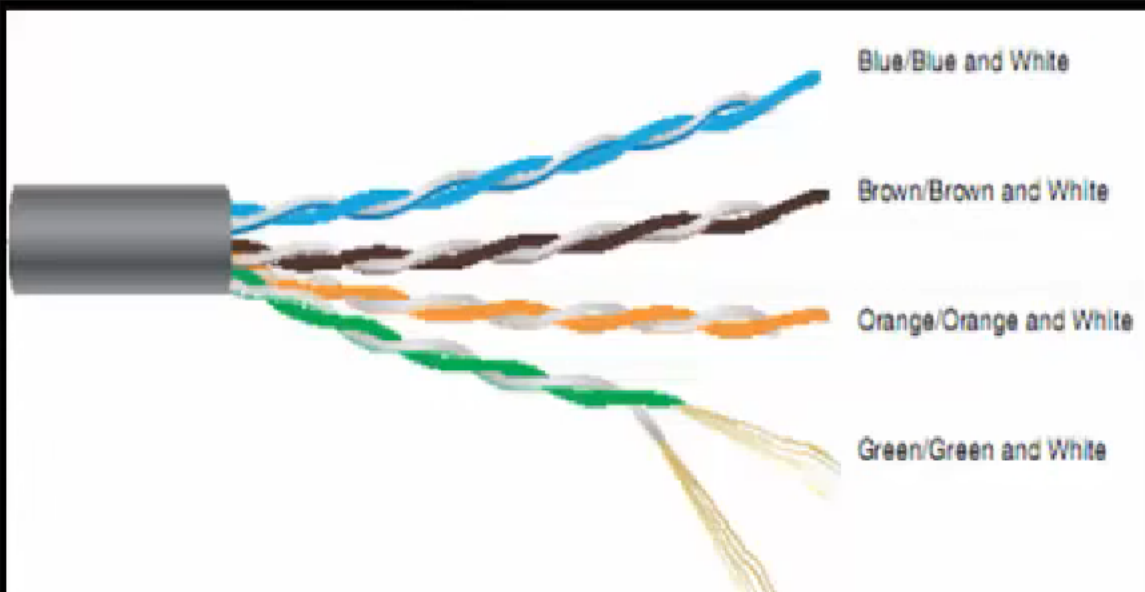


- Each twisted-pair cable has eight wires
- The eight wires are grouped into four pairs: blue, orange, green, and brown
- Each pair is twisted along the entire length of the cable, then all pairs are twisted together and surrounded by a plastic jacket
 - Twisting reduces crosstalk and interference

Cables And Connectors



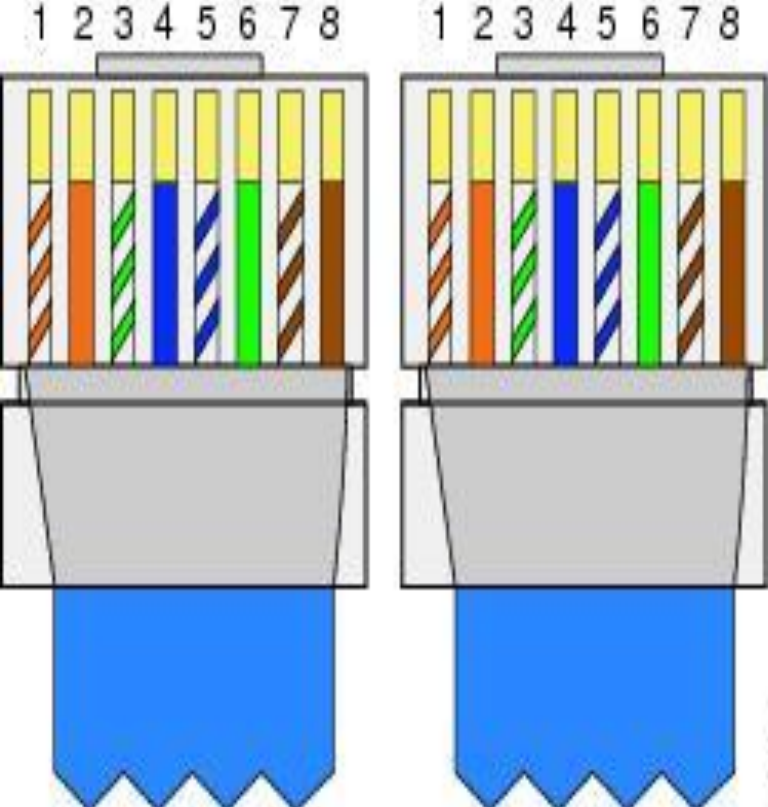
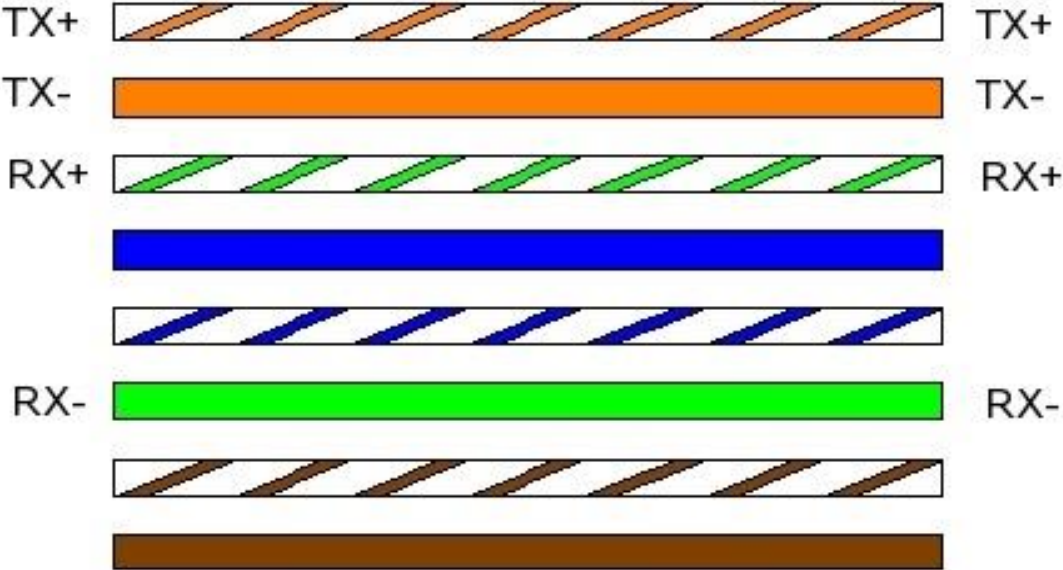
Shielded Twisted Pair



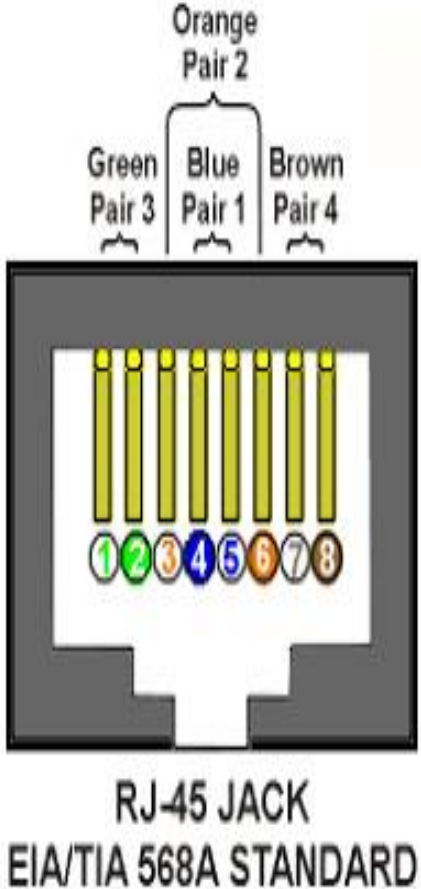
Unshielded Twisted Pair

straight through

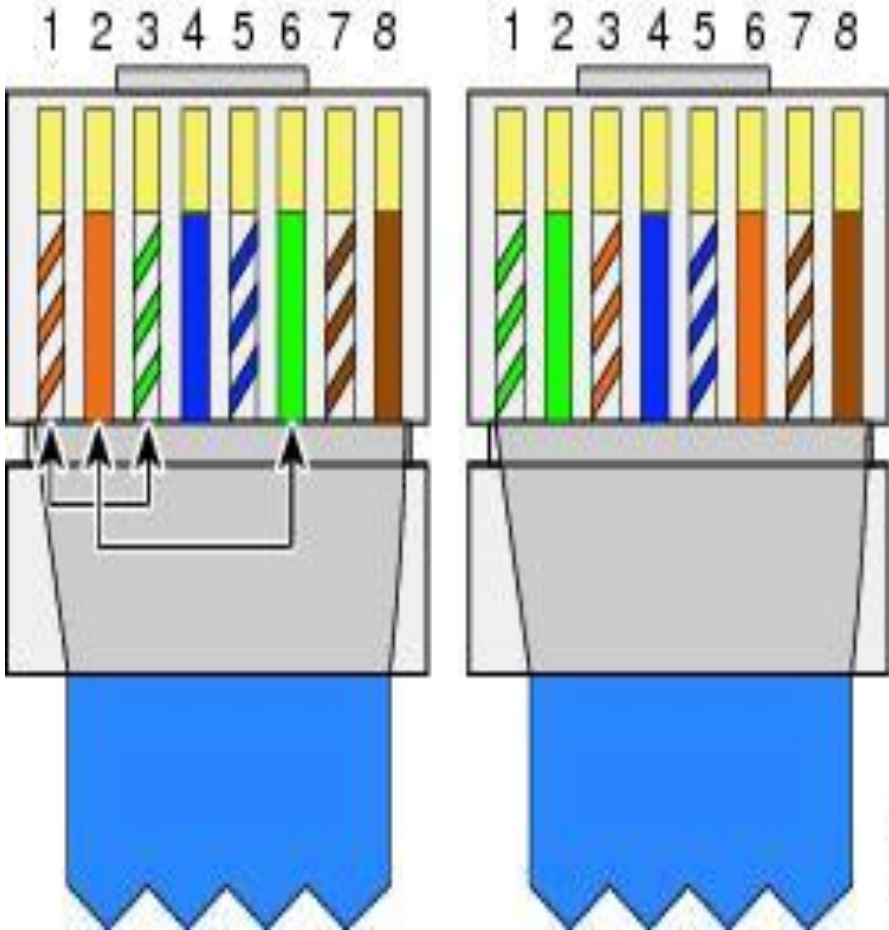
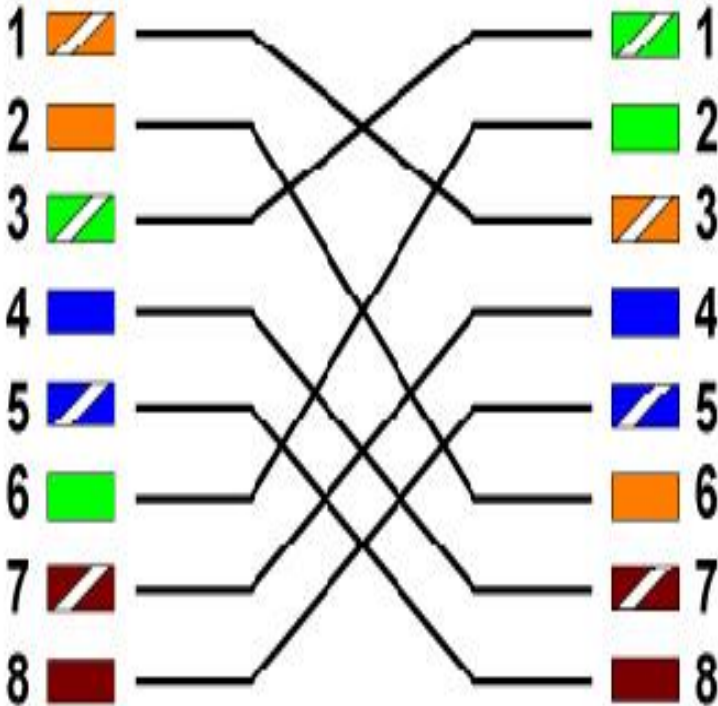
TIA/EIA 568B
Ethernet Cable Wiring



Crossover

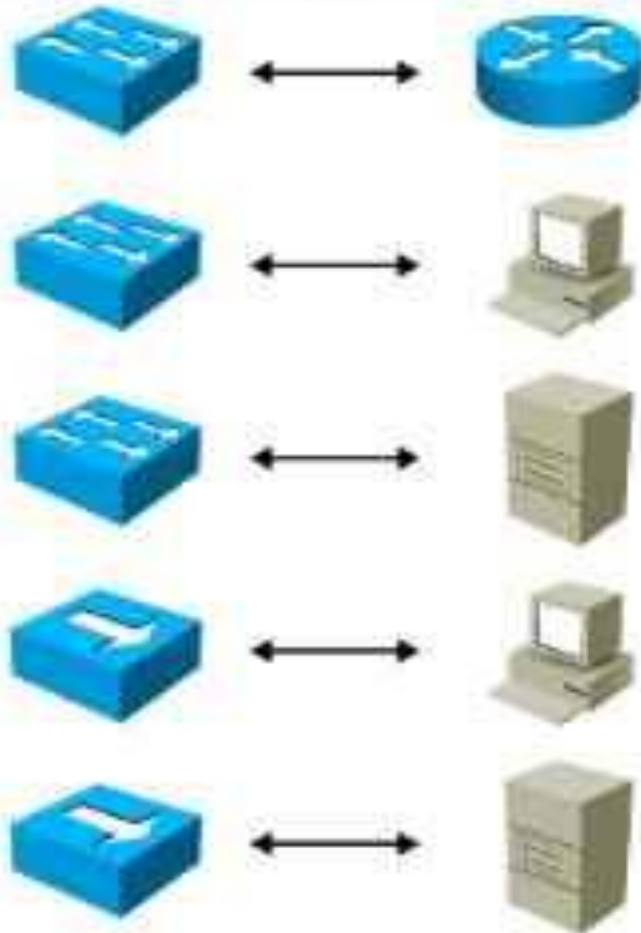


EIA/TIA T568B Crossover Diagram

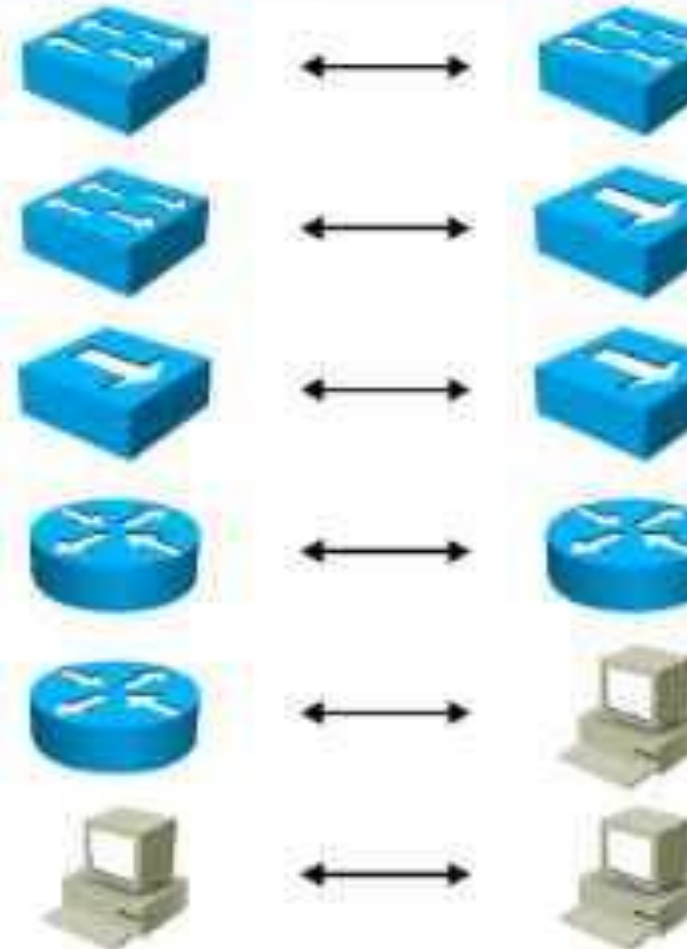


Cables And Connectors

Straight-Through Cable



Crossover Cable



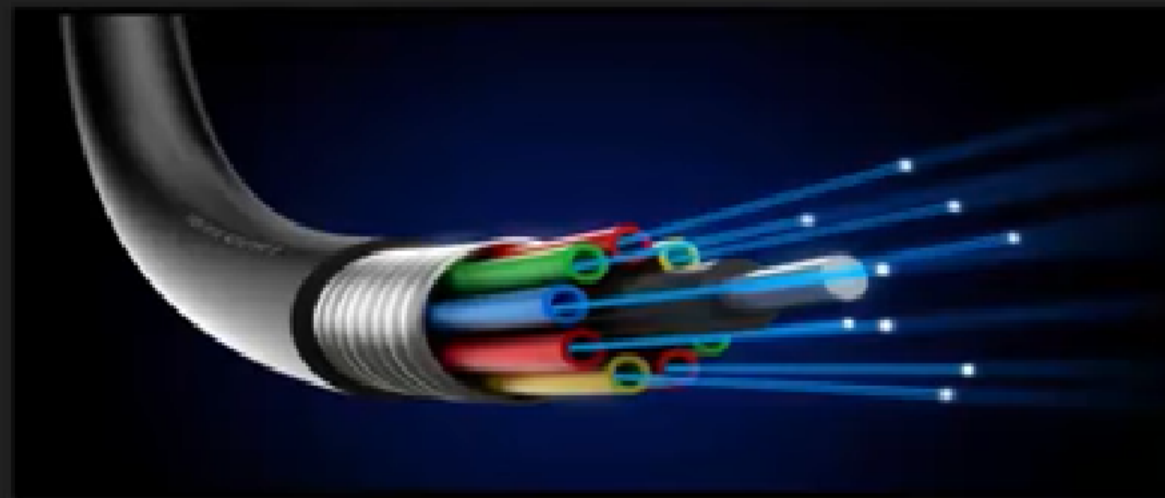
medium dependent interface:- enables connection between like devices

MDIX Auto Feature

- Certain cable types (straight-through or crossover) were required when connecting devices
- The automatic medium-dependent interface crossover (auto-MDIX) feature eliminates this problem
- When auto-MDIX is enabled, the interface automatically detects and configures the connection appropriately
- When using auto-MDIX on an interface, the interface speed and duplex must be set to **auto**

Fiber-Optic Cable

- An alternative to copper cabling is fiber-optic cabling, which sends light (instead of electricity) through an optical fiber (typically made of glass). Using light instead of electricity makes fiber optics immune to EMI



Advantages and Disadvantages of fibre-Optic Cables

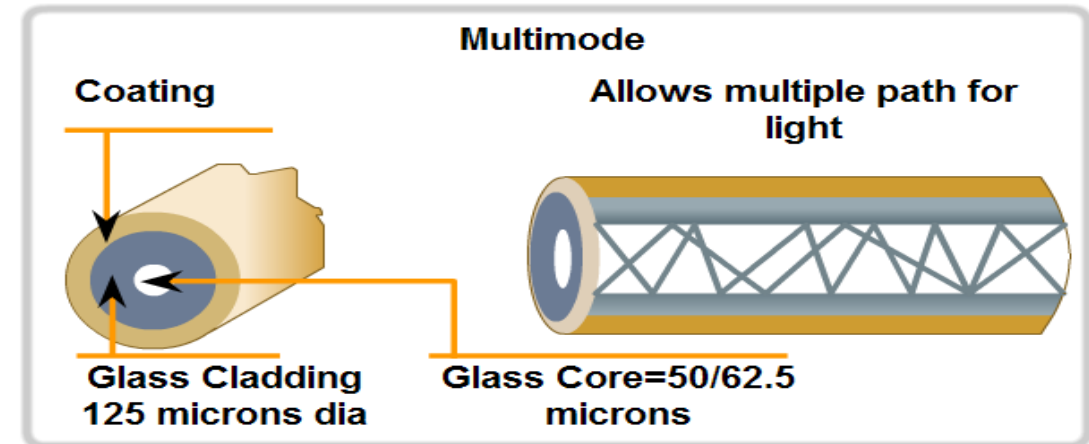
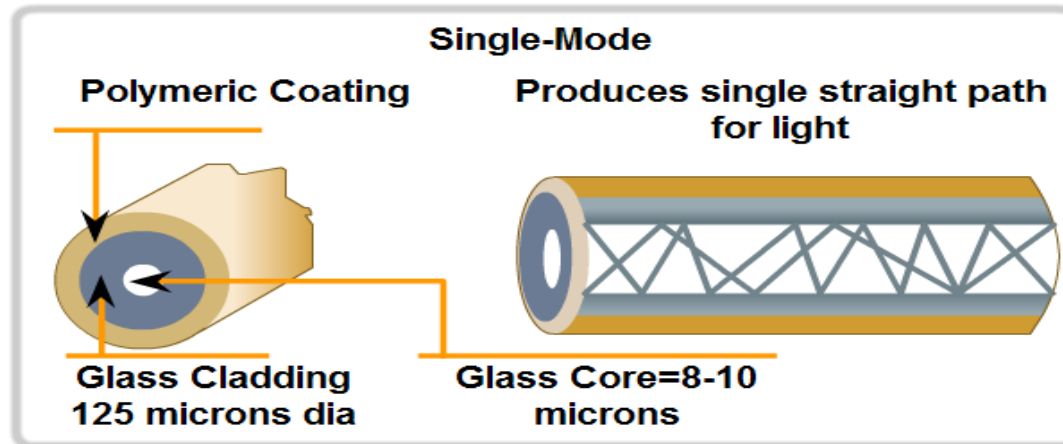
Advantages

- Able to carry significantly more signals than wire
- Faster data transmission
- Less susceptible to noise from other devices
- Better security for signals during transmission
- Smaller physical size

Disadvantages

- Costs more than twisted pair and coaxial cable
- Can be difficult to install and modify
- More expensive over shorter distances

Fiber Media Modes



- Small Core
- Less Dispersion
- Suited for long distance applications (up to 100 km, 62,14 mi.)
- Uses lasers as the light source often within campus backbones for distance of several thousand meters

- Larger core than single-mode cable (50 microns or greater)
- Allows greater dispersion and therefore, loss of signal
- Used for long distance application, but shorter than single-mode (up to ~2km, 6560 ft)
- Uses LEDs as the light source often within LANs or distances of couple hundred meters within a campus network

Fiber optic connectors



SC/APC Duplex



SC SM Duplex



SC MM Duplex



SC Duplex



SC SM Simplex



LC/APC Duplex



LC MM Duplex



SC MM Simplex



ST-FC Duplex



SC/APC Simplex



LC SM Duplex



LC MM Simplex



ST-FC Simplex



ST-SC Simplex



ST-SC Duplex



ST-FC Duplex



FC-SC Simplex



FC Duplex



FC Simplex

- **What is Ethernet?**
- A local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards

802.3 Version	Data Transfer Rate	Cable Standard	Cabling Used
802.3	10 Mbps	10BASE5	Thick coaxial
802.3a	10 Mbps	10BASE2	Thin coaxial
802.3i	10 Mbps	10BASE-T	Twisted pair (TP)
802.3j	10 Mbps	10BASE-F	Fiber optic
802.3u	100 Mbps	10BASE-TX 100BASE-T4 100BASE-FX	TP using 2 pairs TP using 4 pairs Fiber optic
802.3ab	1000 Mbps or 1 Gbps	1000BASE-T	Twisted pair
802.3z	1000 Mbps or 1 Gbps	1000BASE-X	Fiber optic
802.3ae	10 Gbps	10GBASE-SR, 10GBASE-LR, 10GBASE-ER, and so on	Fiber optic

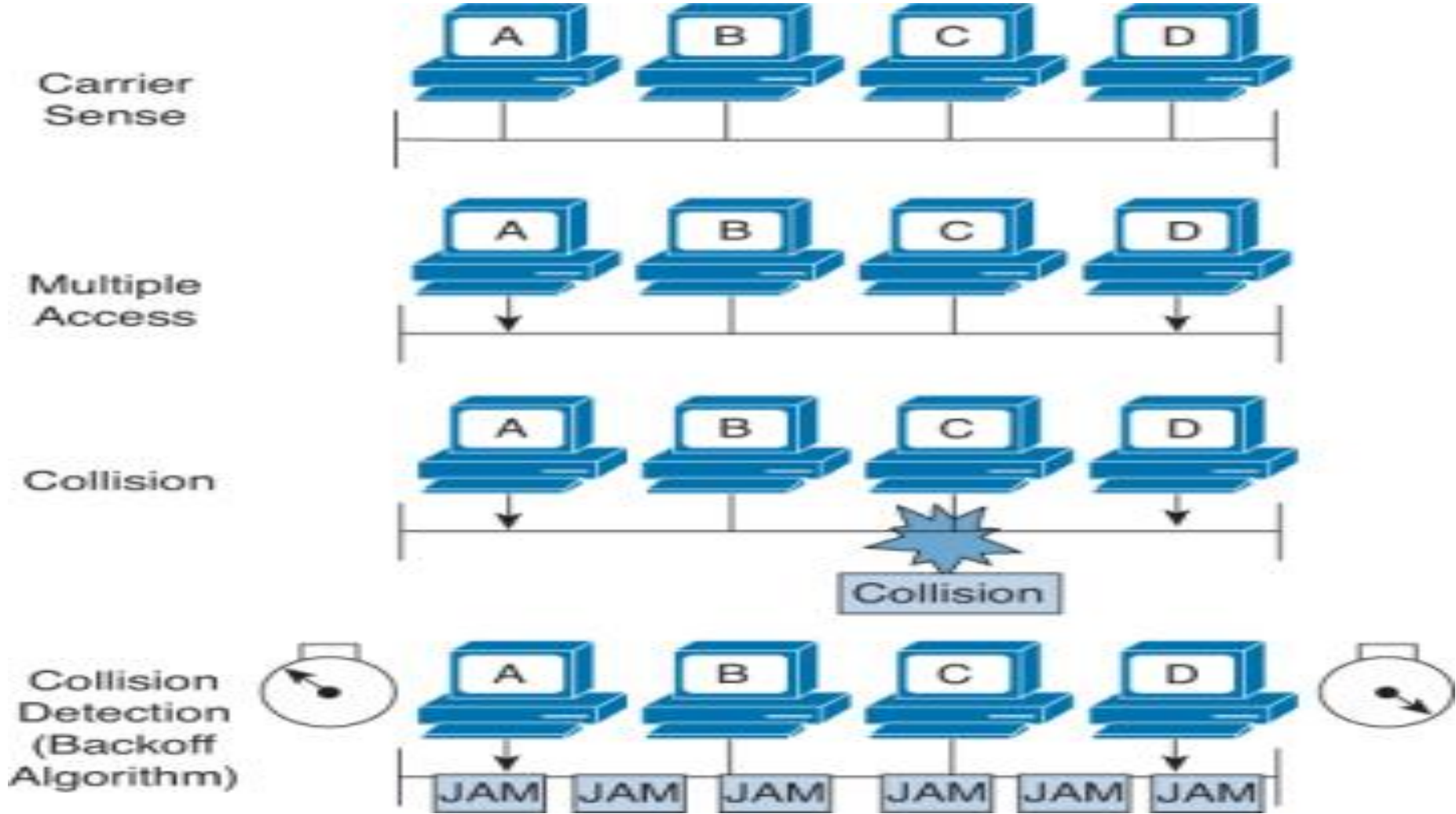
- Defines **carrier sense multiple access with collision detection (CSMA/CD)**
 - Devices share a connection
 - If they send data at the same time, collisions occur
 - So, only one computer can transmit at a time
- CSMA/CD allows devices to send/receive data by limiting collisions

1. Assemble a frame
2. Check if the medium is free
 - a. If free, transmit a bit of the frame
 - b. If not, don't transmit and repeat step 2
3. Check if a collision was detected
 - a. If so, implement the **collision detected procedure**
 - b. If not, transmit the remaining bits in the frame

What is the “collision detected procedure”?

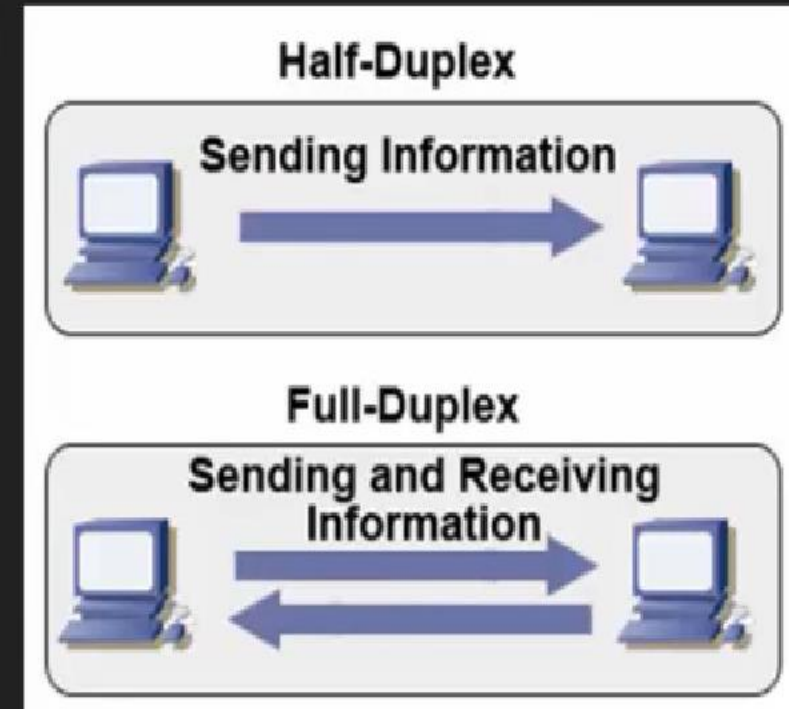
If a collision is detected, then a network adapter will perform the following steps:

1. Send out a jam signal to stop all communication on the medium
2. Wait based on the number of collisions detected
3. Starts sending the remaining bits of the frame



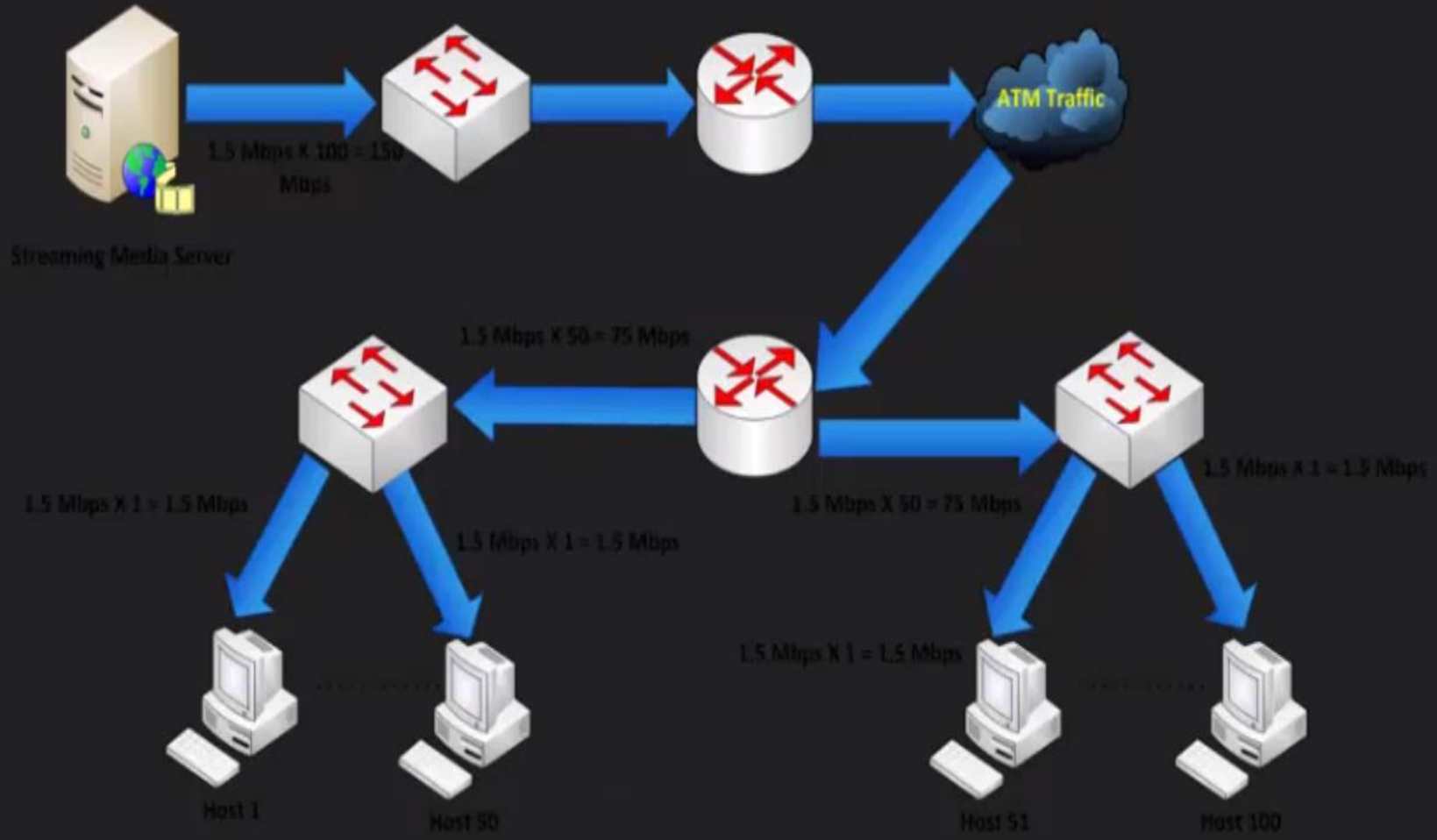
Network's Terminologies

- Duplex definition
- In telecommunication, duplex communication means that both ends of the communication can send and receive signals at the same time. **Full-duplex** communication is the same thing. **Half-duplex** is also bidirectional communication but signals can only flow in one direction at a time. Simplex communication means that communication can only flow in one direction and never flow back the other way



Network's Terminologies

○ Unicast

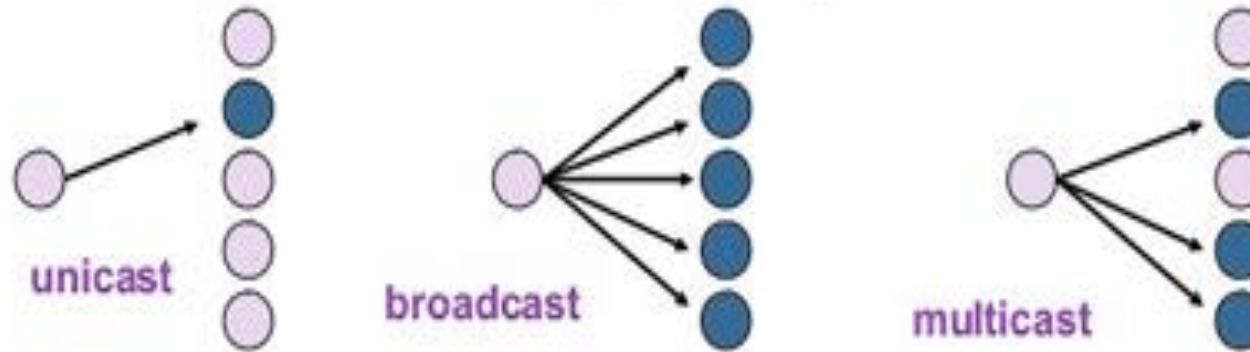


Unicast Does not Scale to Large Numbers of Receivers



IP Service

- IP supports the following services:
 - one-to-one (unicast)
 - one-to-all (broadcast)
 - one-to-several (multicast)



- IP multicast also supports a many-to-many service.
- IP multicast requires support of other protocols (IGMP, multicast routing)

Network's Terminologies

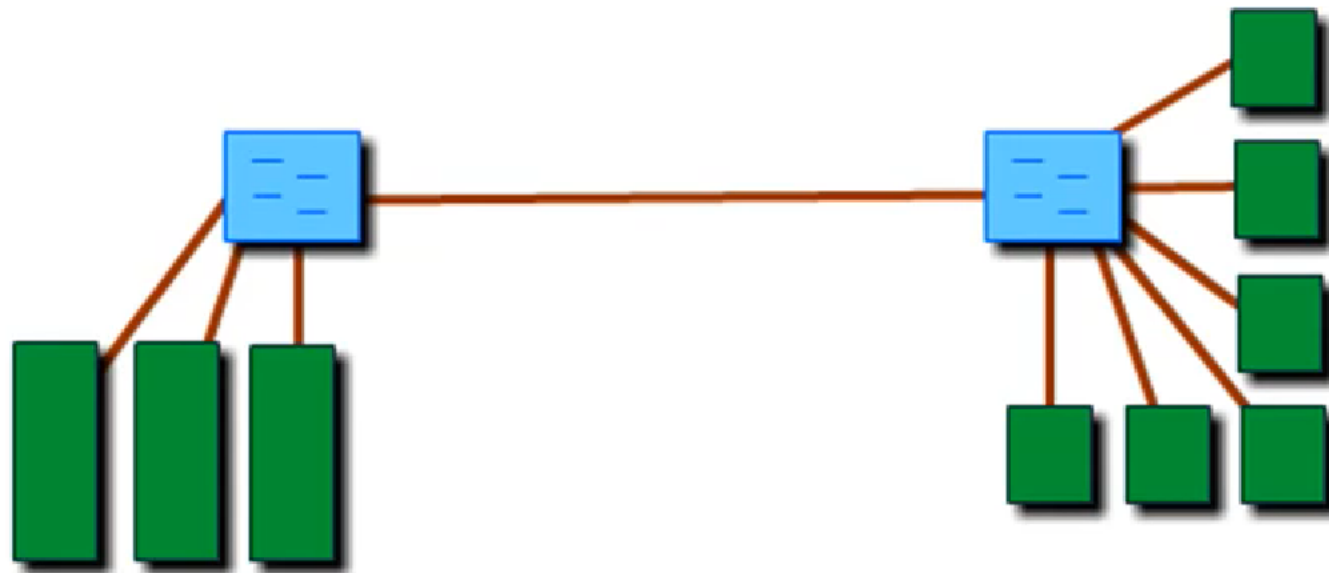
○ Calculate broadcast and collision domain

Device	Number of Collision Domains Possible	Number of Broadcast Domains Possible	OSI Layer of Operation
Hub	1	1	1
Bridge	1 per port	1	2
Switch	1 per port	1	2
Multilayer switch	1 per port	1 per port	3+
Router	1 per port	1 per port	3+

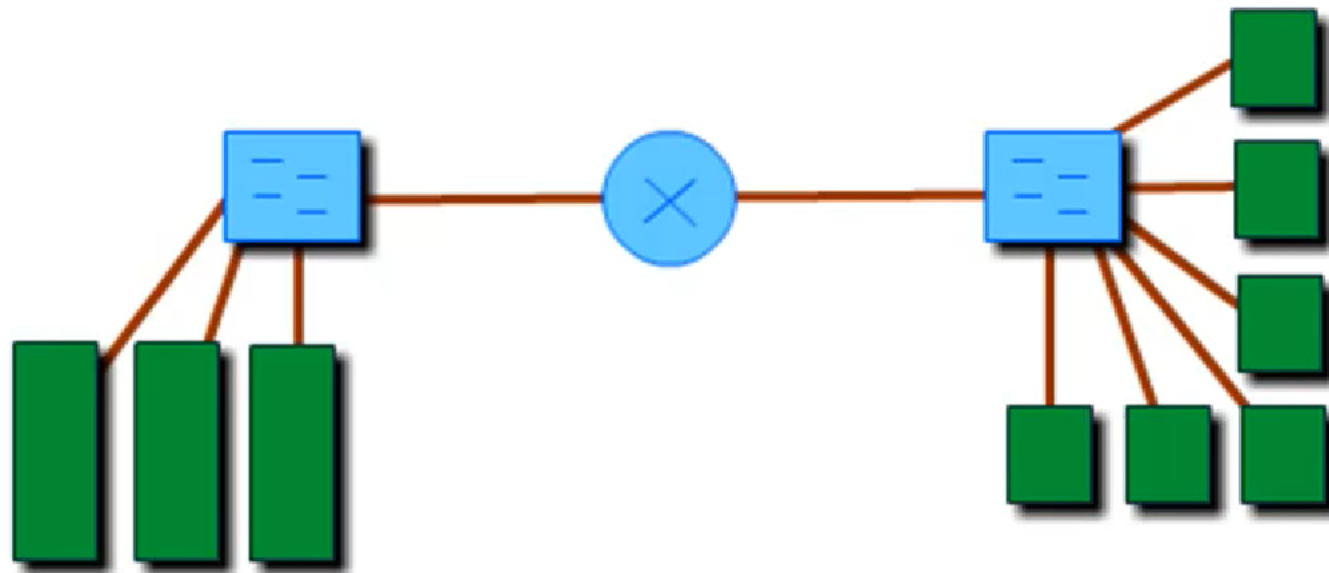
How many Collision Domains?



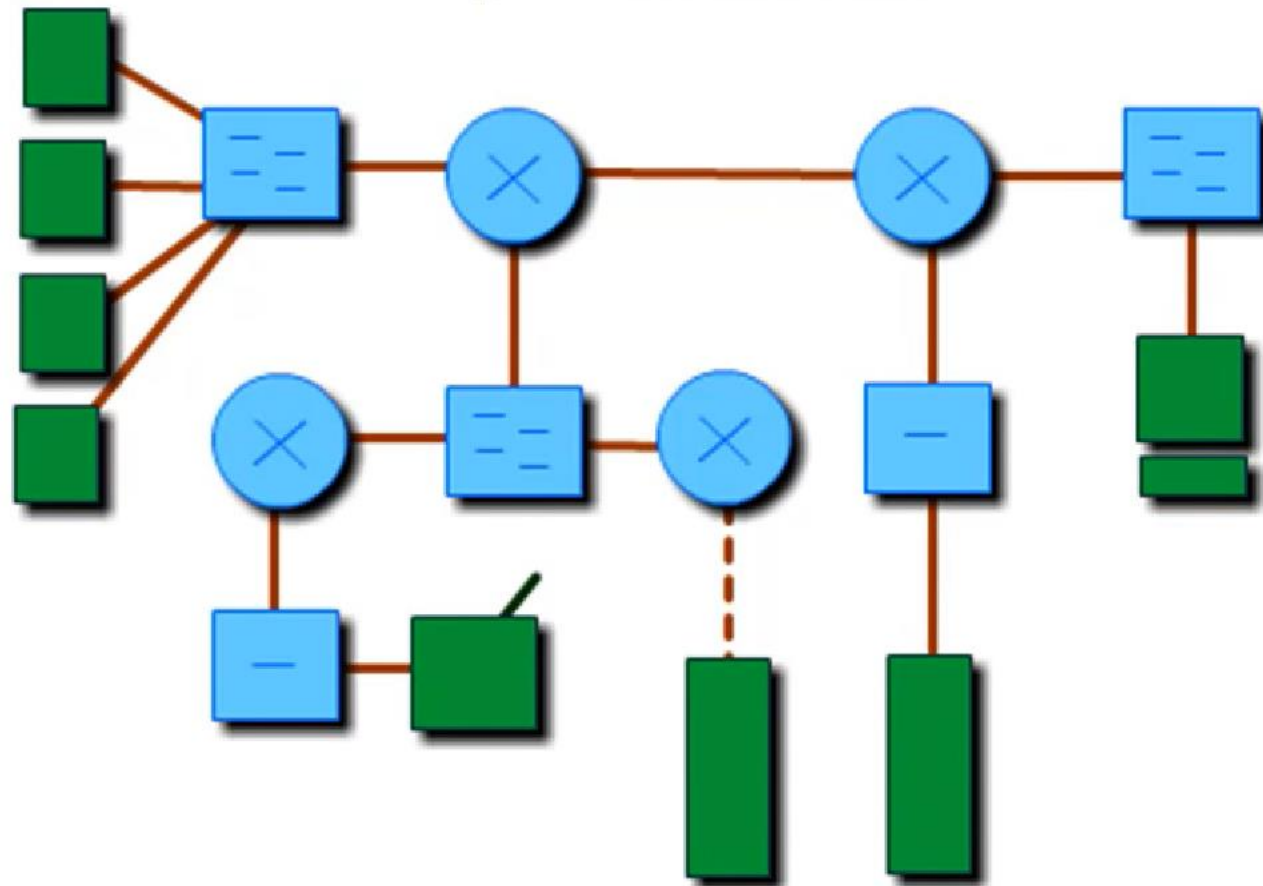
How many Collision Domains?



How many Collision Domains?



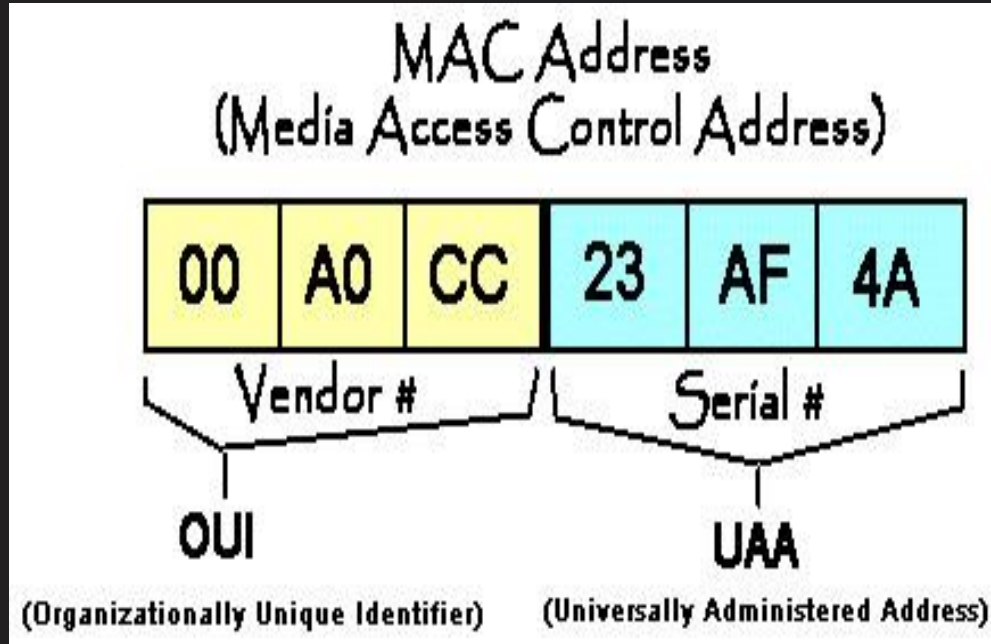
How many Collision Domains?



What is MAC Address?

MAC Address - Media Access Control Address

CMD :- Ipconfig /all



What is IP Address?

○ IP address - Internet Protocol (IP) address

○ CMD :- ipconfig /all

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1



10101100 . 00010000 . 11111110 . 00000001



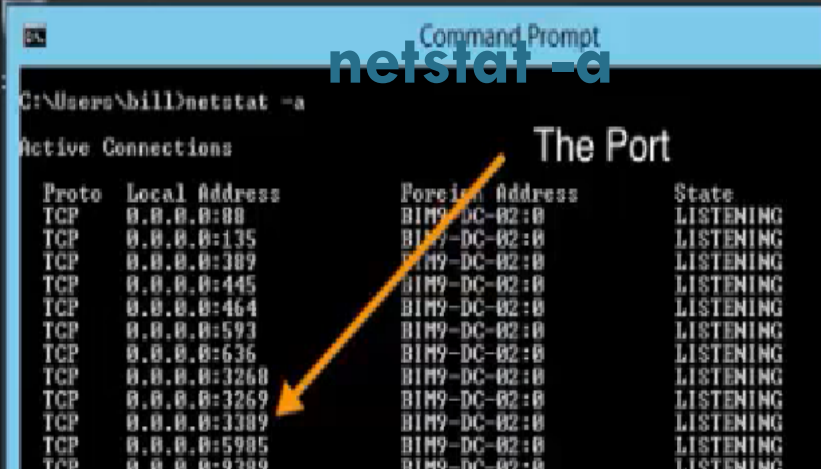
One byte = Eight bits



Thirty-two bits (4 x 8), or 4 bytes

What is Port Address?

- Virtual ports are part of TCP/IP networking. These ports allow software applications to share hardware resources without interfering with each other.
- port numbers start at 0 and go up to 65535.



```
Command Prompt
C:\Users\bill>netstat -a
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:80 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:135 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:389 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:445 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:464 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:593 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:636 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:3268 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:3269 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:3389 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:5985 B1M9-DC-02:0 LISTENING
TCP 0.0.0.0:9389 B1M9-DC-02:0 LISTENING
```

The Port

- Standards are sets of rules that ensure hardware and software released from different companies work together
- Examples of organizations that coordinate standards:



International Organization for Standardization (ISO) – Federation of standards organizations from multiple nations



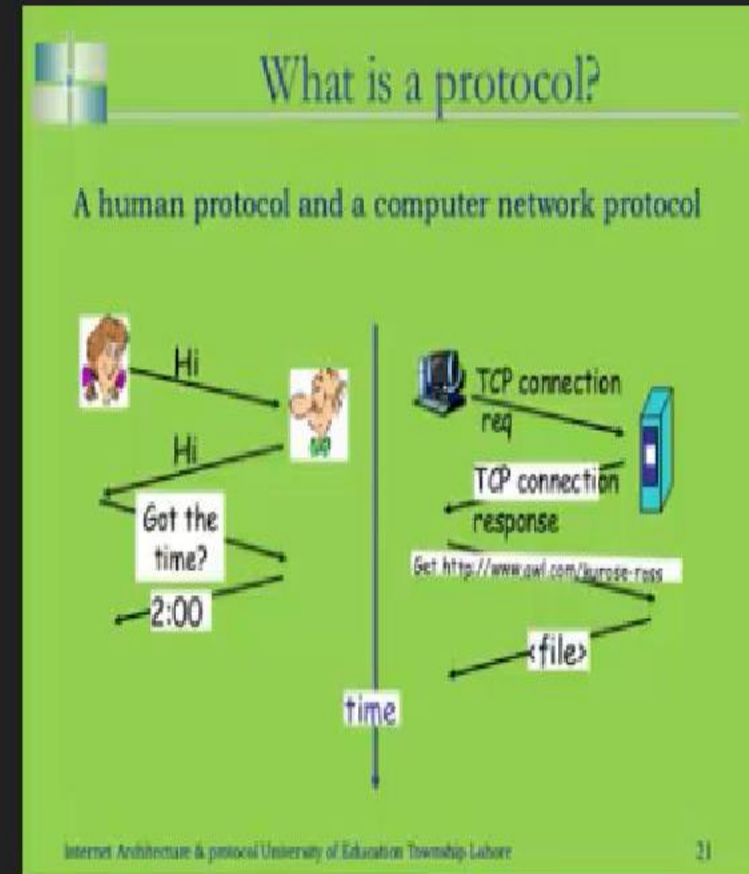
American National Standards Institute (ANSI) – Responsible for coordinating and publishing computer and information technology standards in the United States



International Electrical and Electronics Engineers (IEEE) – Professional organization for the electrical and electronics field

What is protocol?

- In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.

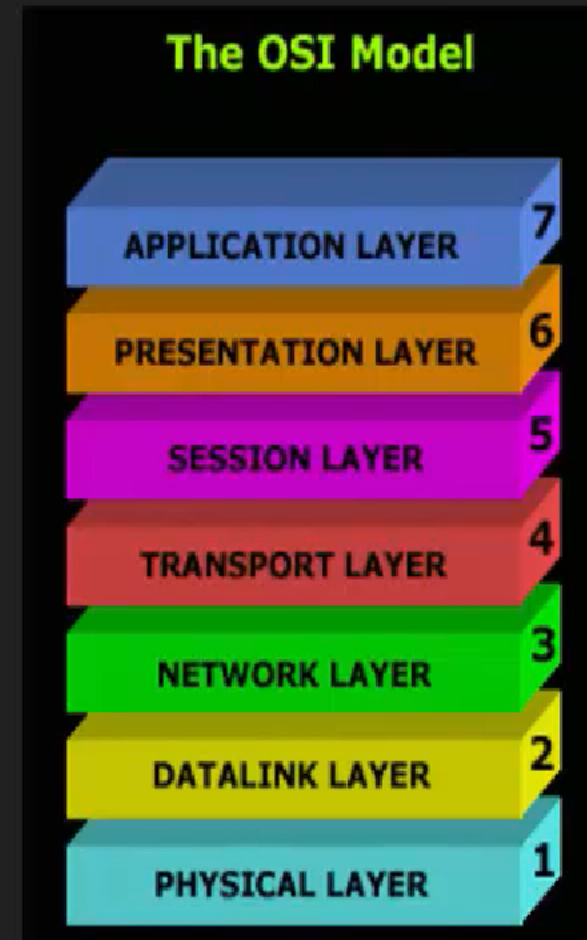


- Way back in 1977, the International Organization for Standardization (ISO) developed a subcommittee to focus on the interoperability of multivendor communications systems. What sprang from this subcommittee was the Open Systems Interconnection (OSI) reference model (commonly referred to as the OSI model or the OSI stack). With this model, you can take just about any networking technology and categorize that technology as residing at one or more of the seven layers of the model.



○ The OSI Model As previously stated, the OSI model is comprised of seven layers:

- ■ Layer 1: The physical layer
- ■ Layer 2: The data link layer
- ■ Layer 3: The network layer
- ■ Layer 4: The transport layer
- ■ Layer 5: The session layer
- ■ Layer 6: The presentation layer
- ■ Layer 7: The application layer



TCP/IP Model

Application Layer

Transport Layer

Internet Layer

Network Access Layer

OSI Model

Application Layer

Presentation Layer

Session Layer

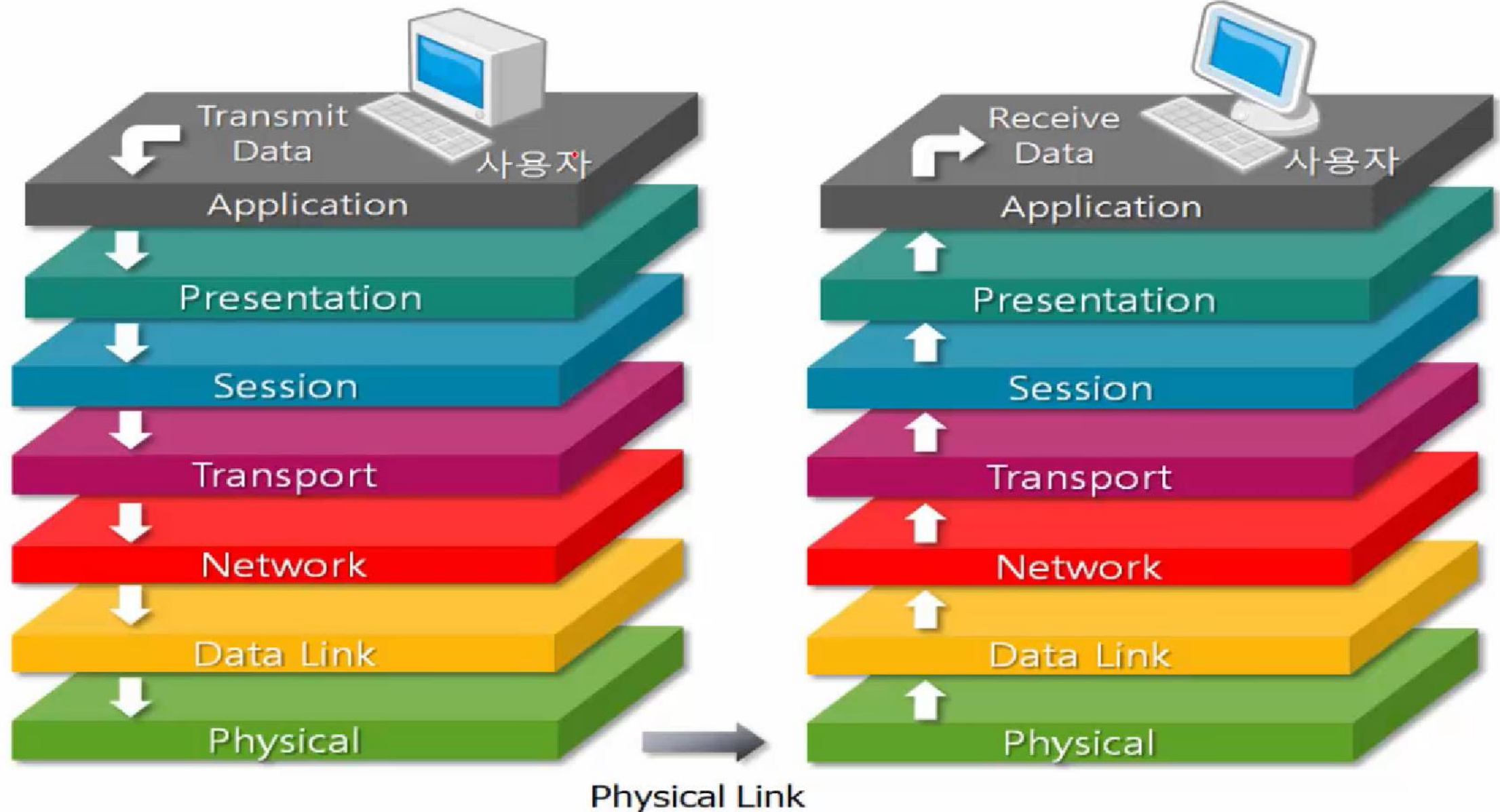
Transport Layer

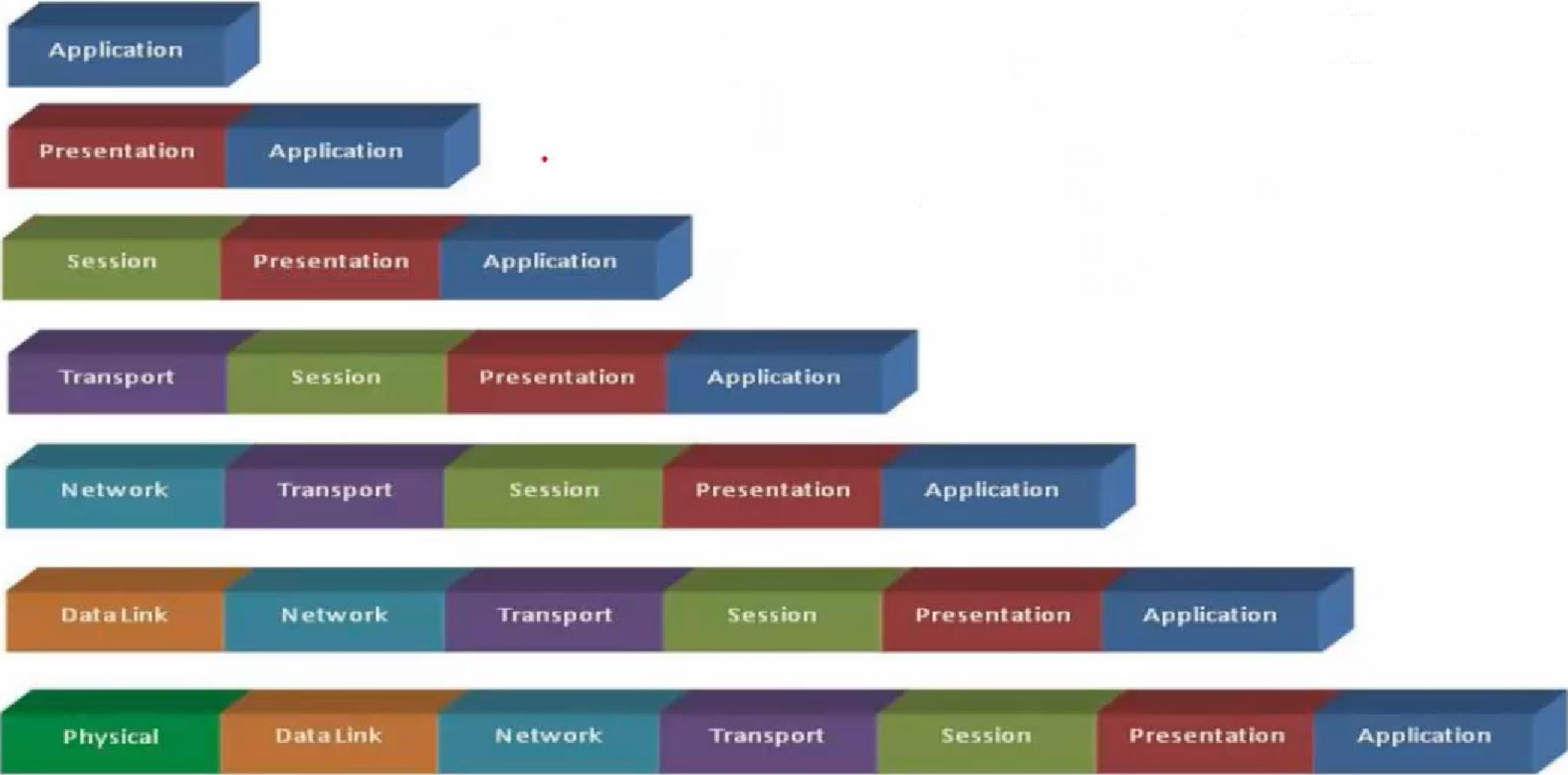
Network Layer

Data Link Layer

Physical Layer

OSI 7 Layer

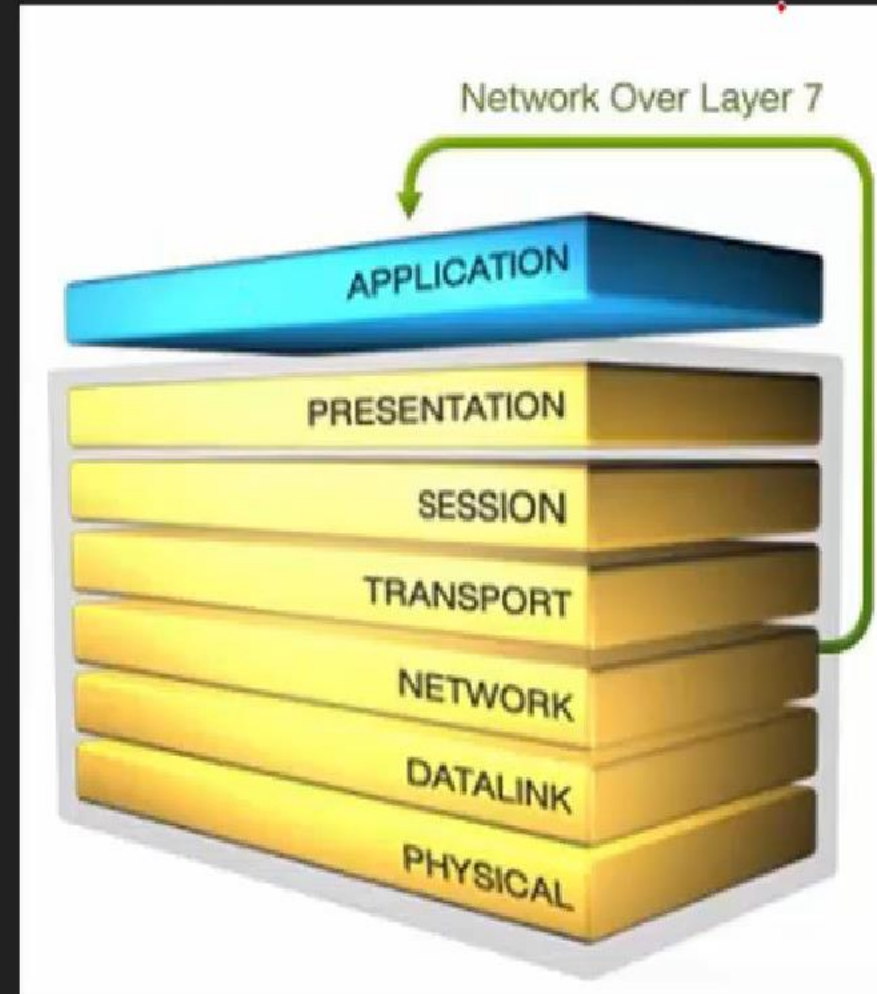




OSI Model Packet Encapsulation

Layer 7- Application Layer

- Recall that even though the application layer is numbered as Layer 7, it is considered to be at the top of the OSI stack, because its functions are closest to the end user.



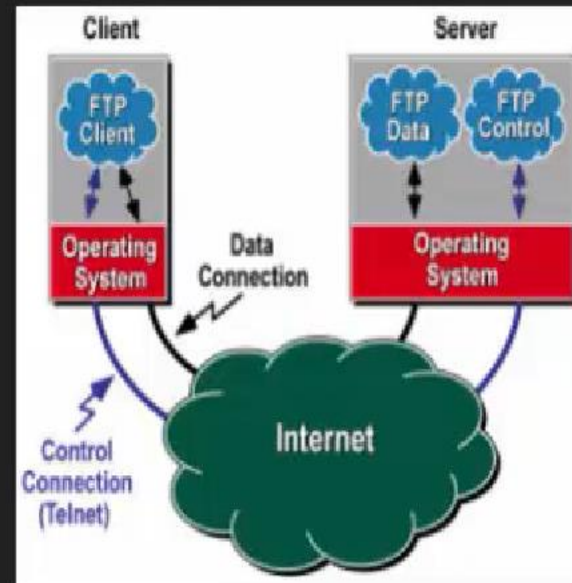
OSI Layer 7 Application Layer

- The following describes the functions of the application layer in more detail:
- ■ Application services: Examples of the application services residing at the application layer include file sharing and e-mail.
-
- ■ Service advertisement: Some applications' services (for example, some networked printers) periodically send out advertisements, making the availability of their service known to other devices on the network. Other services, however, register themselves and their services with a centralized directory (for example, Microsoft Active Directory), which can be queried by other network devices seeking such services.

HTTP: HyperText Transfer Protocol



○ The Application Layer Protocols Examples



- **DNS** is a worldwide service that resolves host names to IP addresses
- DNS architecture is a hierarchical distributed database and an associated set of protocols that define:
 - A mechanism for querying and updating the database
 - A mechanism for replicating the information in the database among servers
- DNS is part of the application layer of the TCP/IP reference model
- DNS servers use inbound port 53 to accept name resolution requests

DNS: Domain Name System.

FORWARD DNS

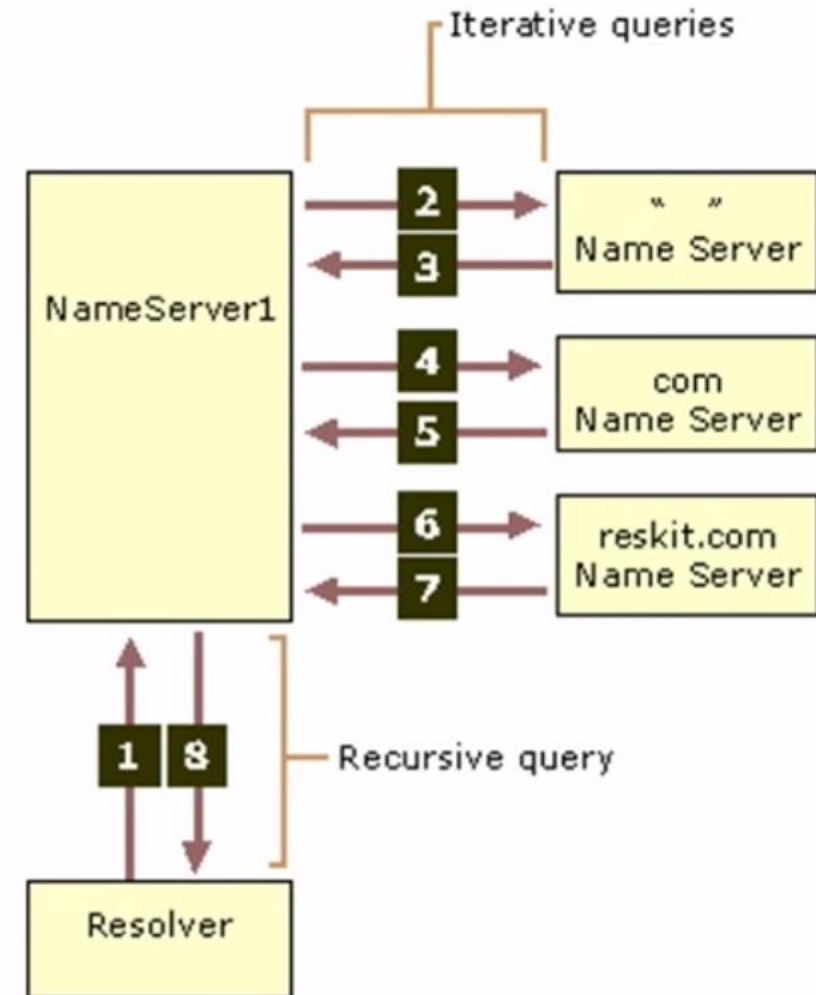


REVERSE DNS



How does DNS work?

- Clients access libraries called resolvers to perform DNS queries
- There are two types of DNS queries:
 - **Recursive:** Server responds with destination IP address or an error message
 - **Iterative:** Server points client to a different DNS server



DHCP: Dynamic Host Configuration Protocol.

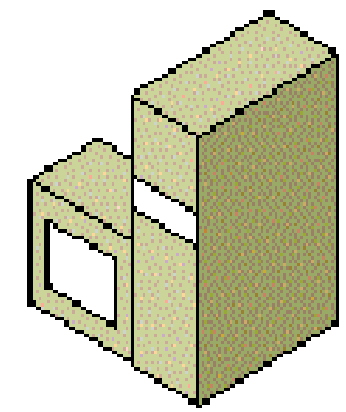
Al-Nahrain University/ECC
Eng.vian adnan farman

- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that enables configured client computers to obtain IP addresses automatically
- The IP information obtained might include the following:
 - IP addresses
 - Subnet masks
 - Gateway addresses
 - DNS server addresses
 - Other advanced options
- The DHCP Server service provides the following benefits:
 - Reliable IP address configuration
 - Reduced network administration

- DHCP sessions use a four-step process known as DORA.
 - **Discovery:** The client sends a broadcast to the network to find a DHCP server
 - **Offer:** The DHCP server sends a unicast “offering” of an IP address to the client
 - **Request:** The client broadcasts to all servers that it has accepted the offer
 - **Acknowledge:** The DHCP server sends a final unicast to the client that includes the IP information the client will use
- DHCP utilizes ports 67 and 68

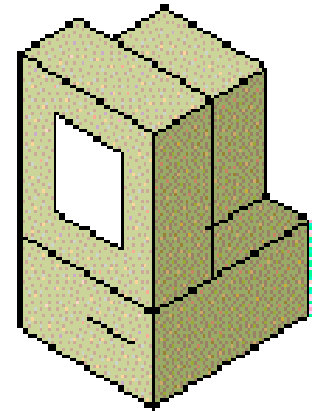


سيرفر ال DHCP

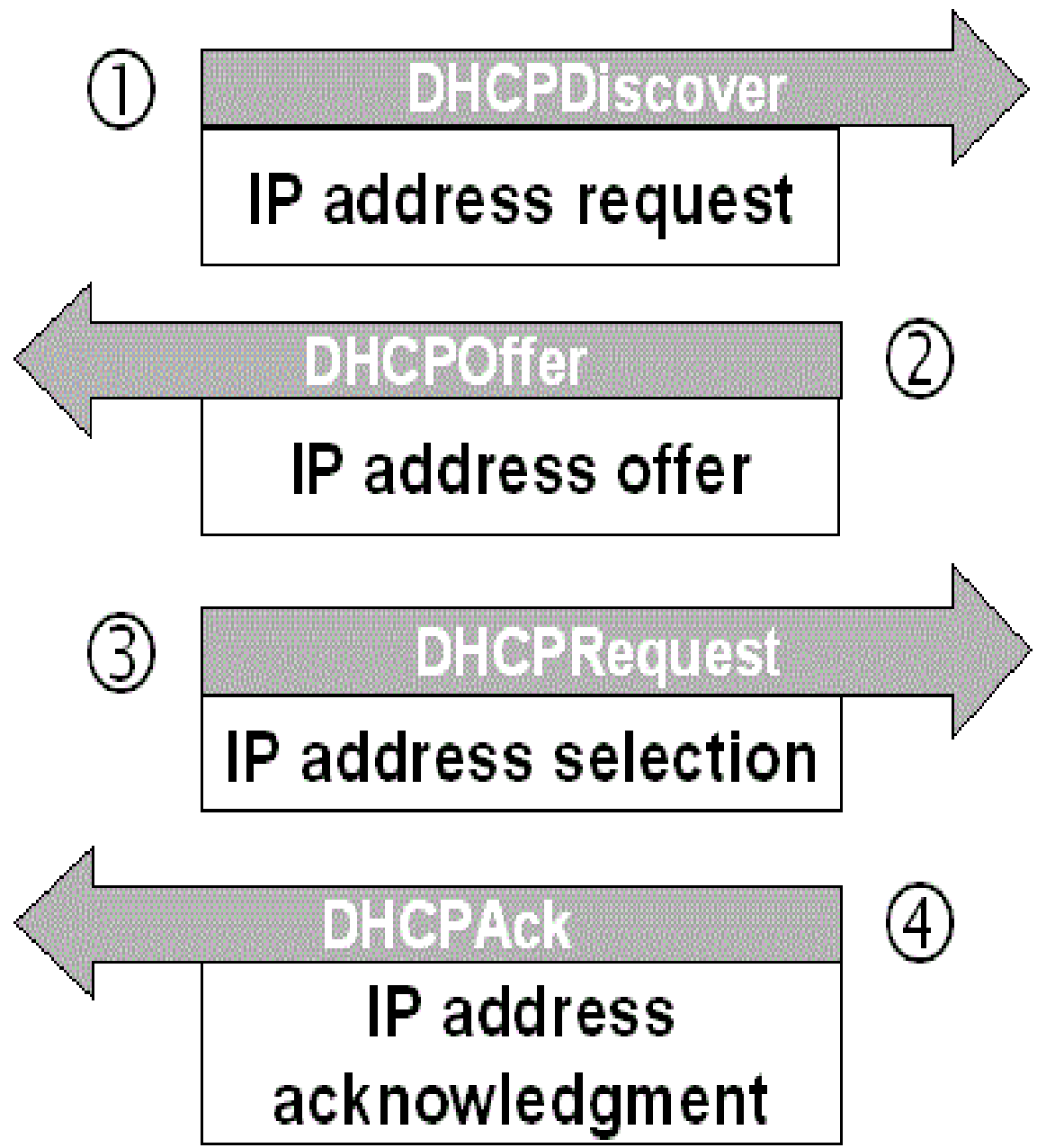


DHCP server

المستخدم

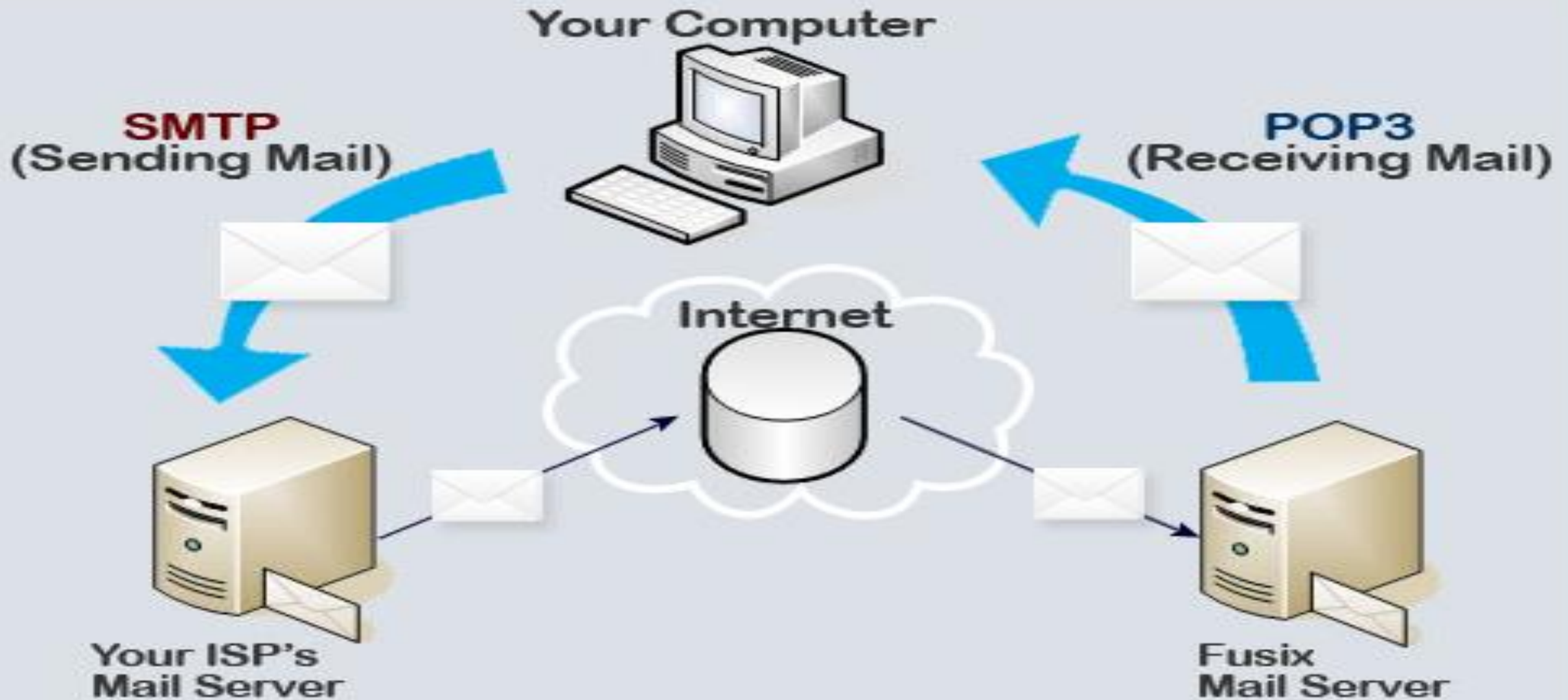


DHCP client

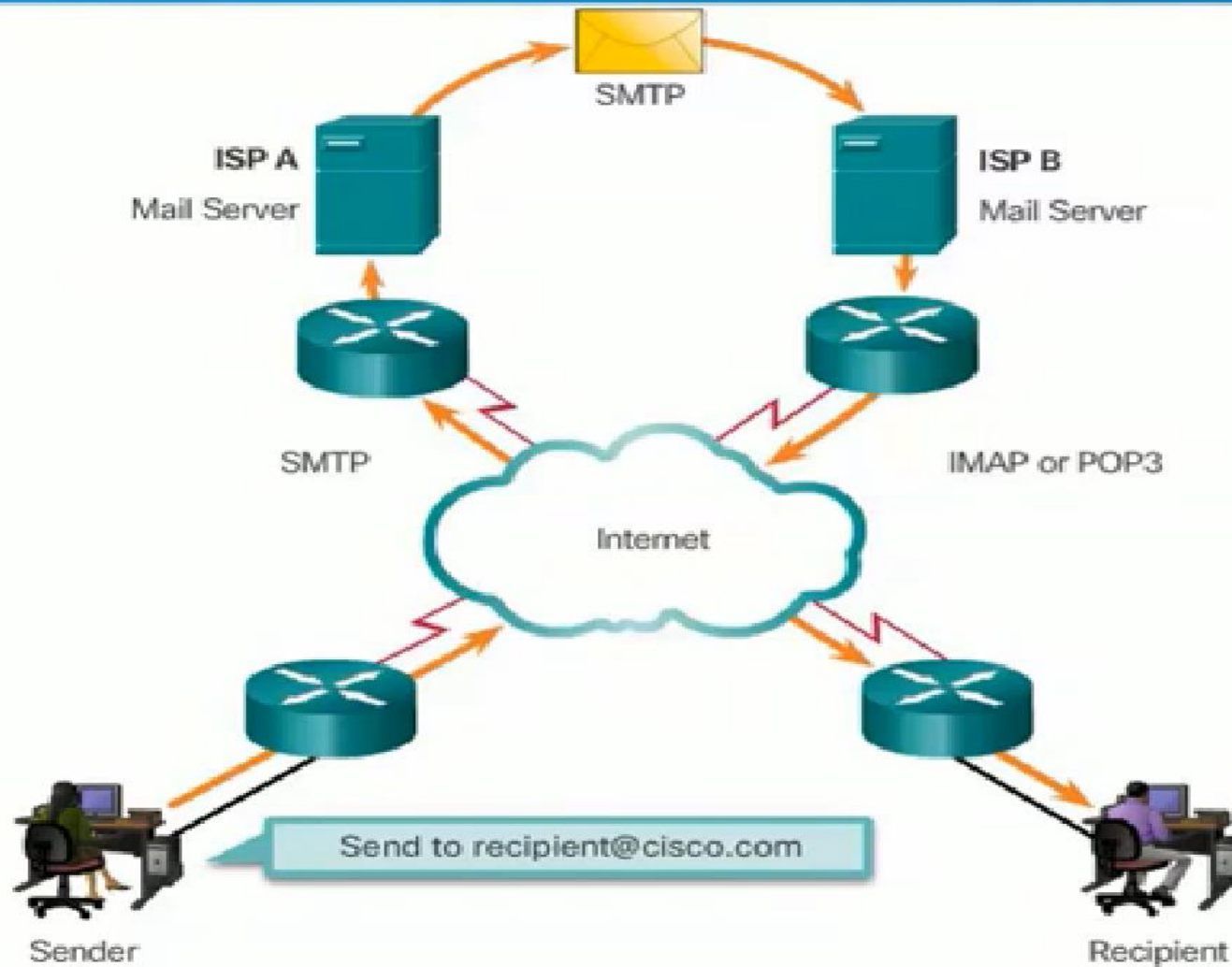


SMTP: SIMPLE MAIL TRANSFER PROTOCOL.
POP : POST OFFICE PROTOCOL .

Al-Nahrain University/ECC
Eng.vian adnan farman



IMAP : INTERNET MESSAGE ACCESS PROTOCOL.

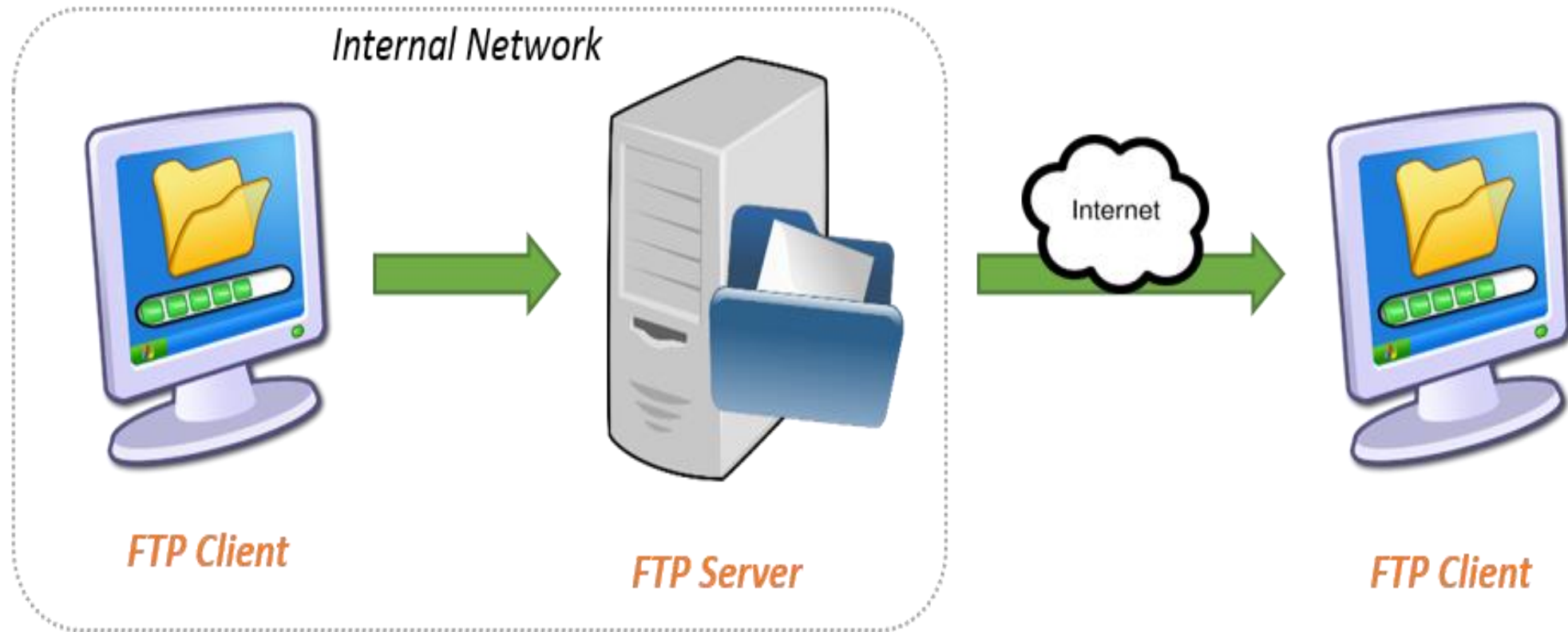


IMAP VS POP

IMAP	POP
<p>The IMAP protocol, by default, allows the user to keep all messages on the server. It constantly synchronizes the e-mail program with the server and displays what messages are currently present. All the actions performed on the messages (reading, moving, deleting...) will be done directly on the server.</p>	<p>The POP protocol, by default, is set to download all the messages from the e-mail server onto your computer. This means that all the actions performed on the messages (reading, moving, deleting...) will be performed on one's computer. Because everything is kept on the users computer, the user will not be able to reopen messages from any location other than the computer where the messages have been downloaded.</p>
<p>Because everything is kept on the server the user will be able to access the e-mail in the inbox from any computer in the world connected to the Internet and can will always find the same settings in their e-mail account.</p>	<p>Once e-mail is downloaded it can be accessed only using the same computer.</p> <p>There is an option to setup the POP protocol to save the copy of the messages on the server after downloading them on the computer.</p>
<p>Because there is a quota on the e-mail servers, it is necessary to regularly delete unnecessary e-mail messages from the server, to avoid problems.</p>	<p>The client is not limited by the amount of free space on the server. The limitation is the size of the hard drive on the personal computer.</p>

FTP: FILE TRANSFER PROTOCOL

Al-Nahrain University/ECC
Eng.vian adnan farman



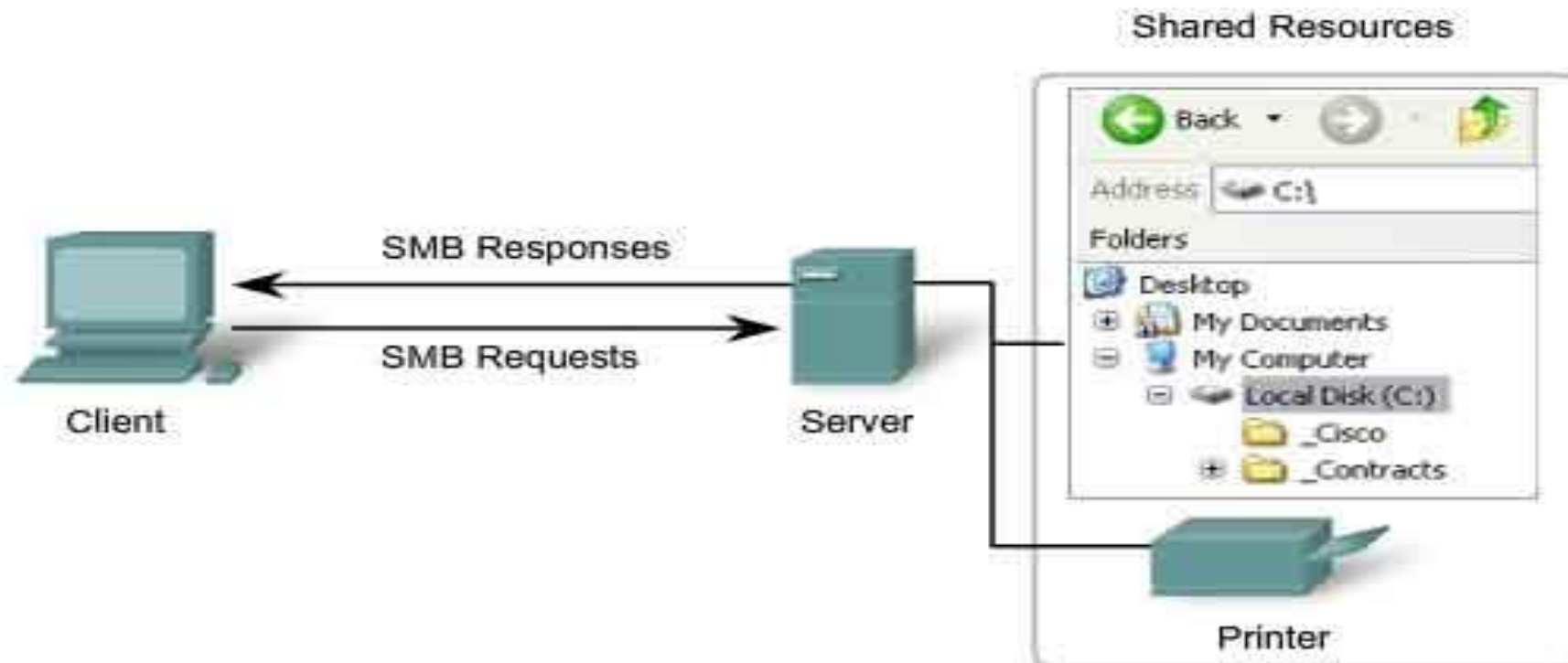
Employee uploads file to be shared with a business partner.

File is hosted on the FTP server within the corporate network.

Business partner gets access to the file by accessing the share folder on the file server.

SMB: SERVER MESSAGE BLOCK

File Sharing Using the SMB Protocol



SMB is a client-server, request-response protocol. Servers can make their resources available to clients on the network.

Layer 6- The Presentation Layer



Presentation Layer is responsible for converting data into standard format.

Examples : ASCII, EBCDIC, JPEG, MPEG, BMP, MIDI, WAV, MP3

Following tasks are perform at Presentation layer :

Encoding – Decoding

Encryption – Decryption

Compression – Decompression



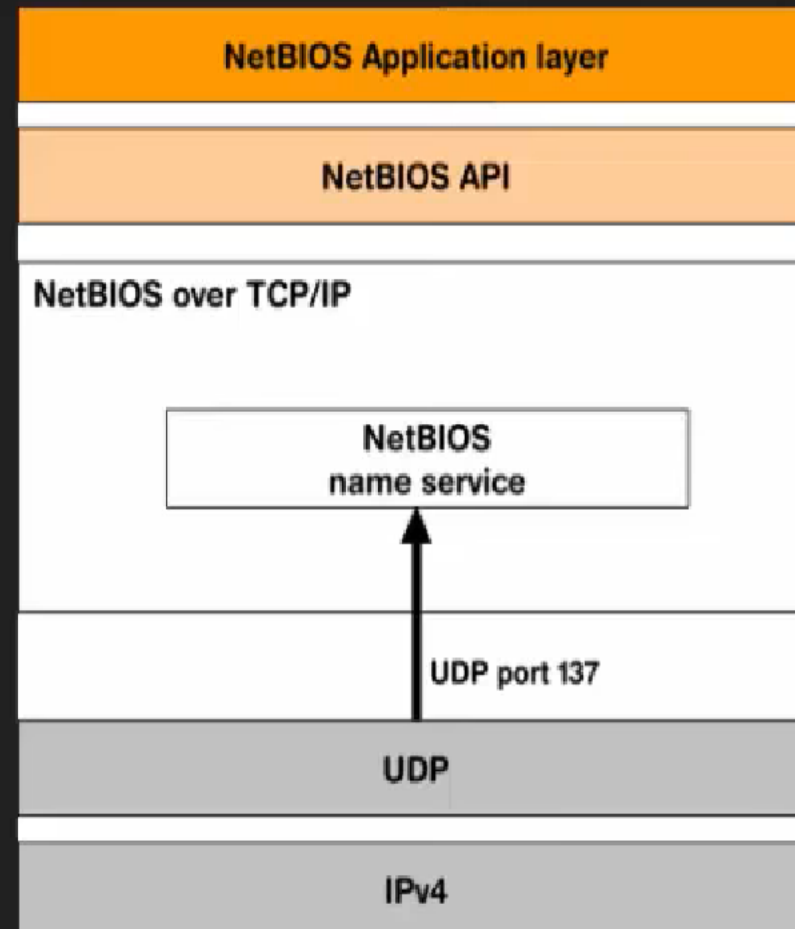
Layer 6- The Presentation Layer

- The following describes the function of data formatting and encryption in more detail:
- ■ **Data formatting:** As an example of how the presentation layer handles data formatting, consider how text is formatted. Some applications might format text using American Standard Code for Information Interchange (ASCII), while other applications might format text using Extended Binary Coded Decimal Interchange Code (EBCDIC). The presentation layer is responsible for formatting the text (or other types of data, such as multimedia or graphics files) in a format that allows compatibility between the communicating devices.
- ■ **Encryption:** Imagine that you are sending sensitive information over a network (for example, your credit-card number or bank password). If a malicious user were to intercept your transmission, he might be able to obtain this sensitive information. To add a layer of security for such transmissions, encryption can be used to scramble up (encrypt) the data in such a way that if the data were intercepted, a third party would not be able to unscramble it (decrypt). However, the intended recipient would be able to decrypt the transmission.

- Manages session establishment, maintenance and termination between network devices
 - Example: when you log on and log off
- This layer controls the name and address database for the OS
- NetBIOS (Network Basic Input Output System) is a protocol that works at this layer

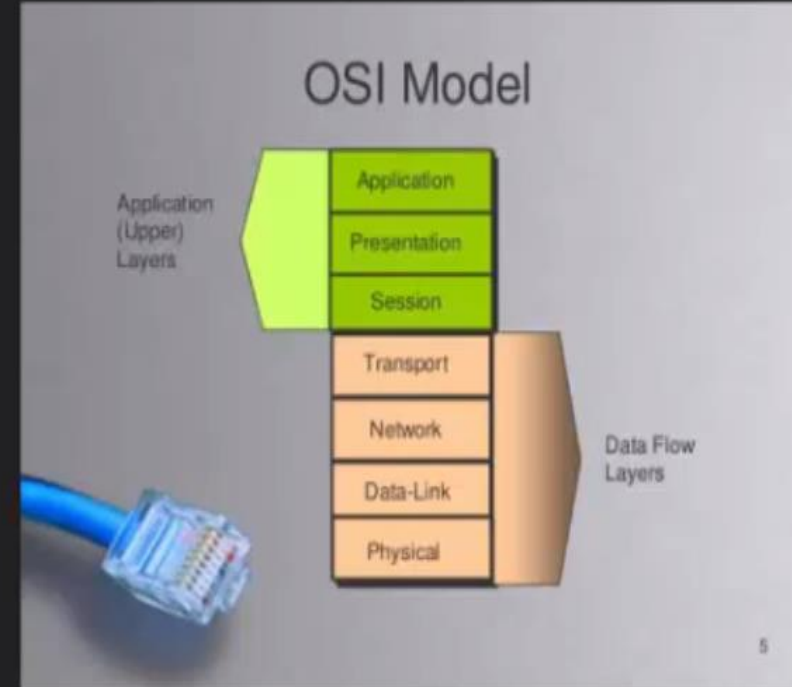
Layer 5- Session Layer

- NetBIOS Protocol `NetBIOS name =hostname in cmd`
- The Network Basic Input/Output System protocol is an API on top of the TCP/IP protocol, it provides a way of communication between separate computers within a local arena network via the session layer.



Layer 4- The Transport Layer

- acts as a dividing line between the upper layers and lower layers of the OSI model. Specifically, messages are taken from upper layers (Layers 5–7) and are encapsulated into segments for transmission to the lower layers (Layers 1–3).
- TCP/UDP
- Windowing
- Buffering



TCP : TRANSMISSION CONTROL PROTOCOL.
UDP: USER DATAGRAM PROTOCOL.

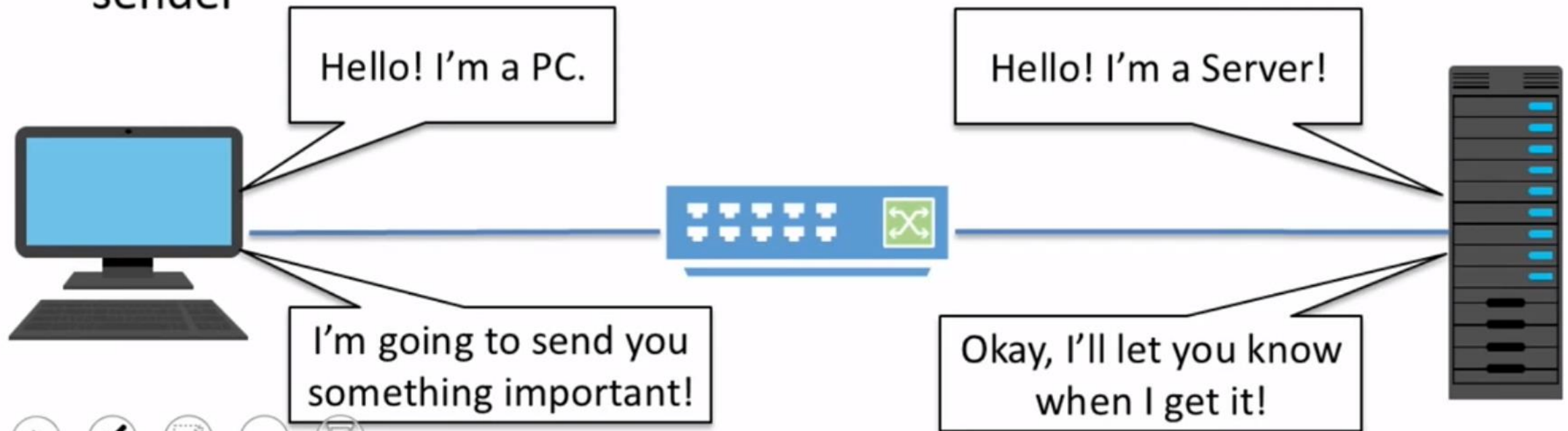
Al-Nahrain University/ECC
Eng.vian adnan farman

TCP vs UDP

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

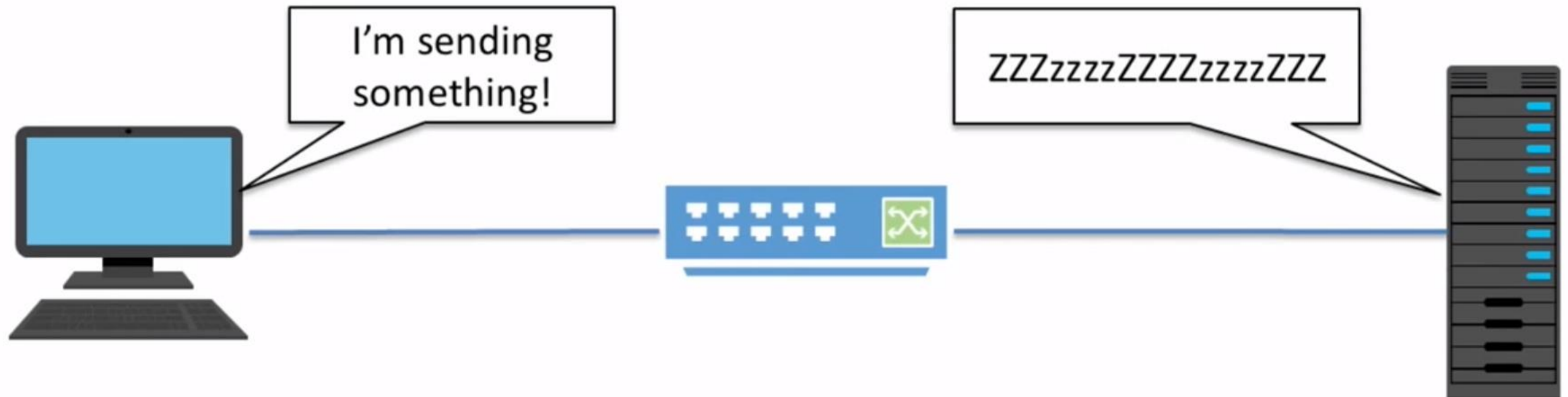
Connection-Oriented Communications

- Require both devices involved in the communication establish an end-to-end logical connection before data can be sent
- These communications are considered reliable network services
- Packets not received by the destination device can be resent by the sender



Connectionless Communications

- End-to-end connection is not necessary before data is sent
- Every packet that is sent has the destination address in the header
- Sufficient to move independent packets, such as in streaming media
- Datagram delivery is not guaranteed and lost packets cannot be resent



Port Number	Protocol	Application
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP,TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384-32,767	UDP	RTP-based Voice and Video

Port numbers are divided into three ranges:

Well Known ports: those in the range 0–1023. On Unix-like operating systems, opening a port in this range to receive incoming connections requires administrative privileges.

Registered ports: in range 1024–49151, assigned by Internet Corporation for Assigned Names and Numbers (ICANN) to a certain use.

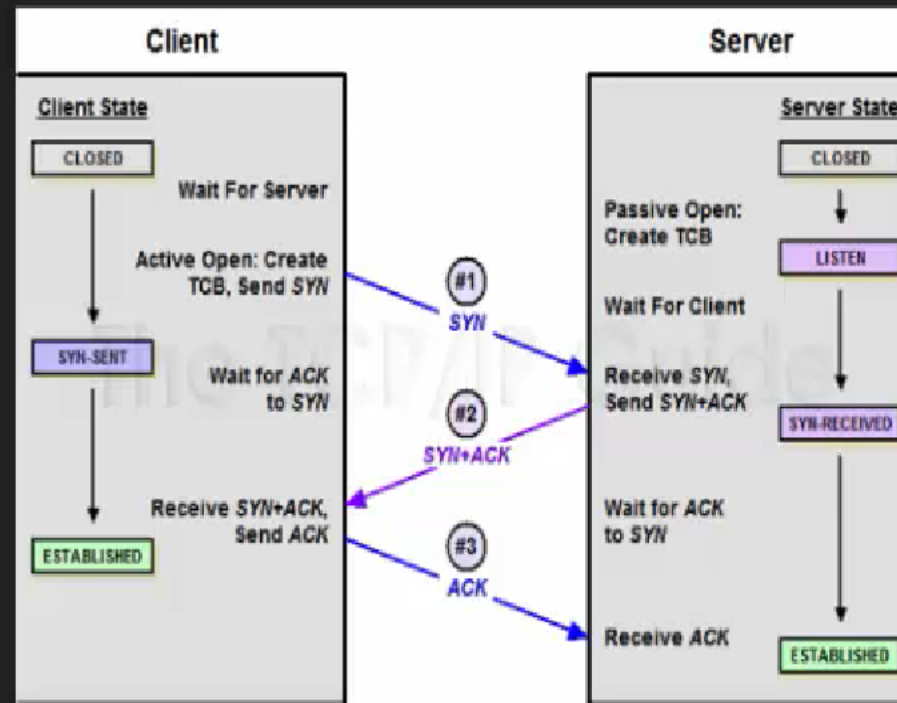
Private ports: in range 49152–65535, not permanently assigned to any application.

ICANN does not enforce this; it is simply a set of recommended uses.

Some well known ports: 20 FTP, 80 HTTP, 23 Telnet, 53 DNS, etc.

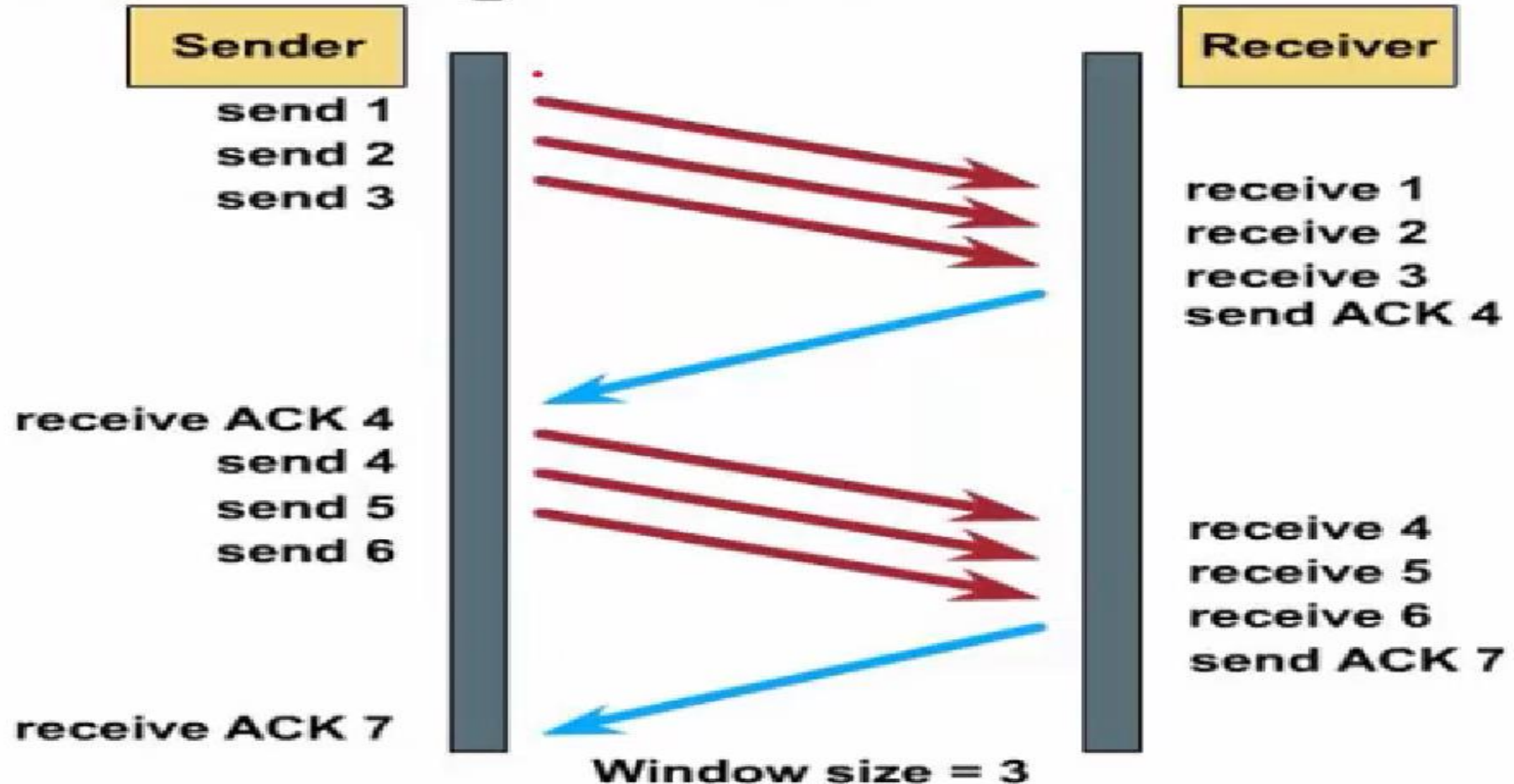
Layer 4- The Transport Layer

- **Windowing:** TCP communication uses windowing, in that one or more segments are sent at one time, and a receiver can acknowledge the receipt of all the segments in a window with a single acknowledgment. In some cases, as illustrated in Figure 2 -11 , TCP uses a sliding window, where the window size begins with one segment. If there is a successful acknowledgment of that one segment (that is, the receiver sends an acknowledgment asking for the next segment), the window size doubles to two segments. Upon successful receipt of those two segments, the next window contains four segments. This exponential increase in window size continues until the receiver does not acknowledge successful receipt of all segments within a certain time period (known as the round trip time [RTT], which is sometimes called real transfer time), or until a configured maximum window size is reached.



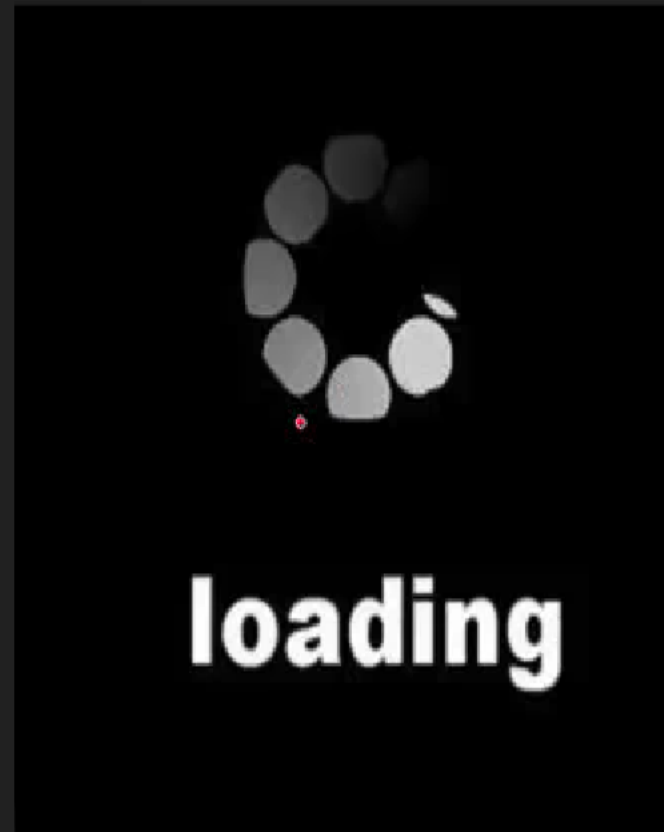
Layer 4- The Transport Layer

TCP Sliding Window



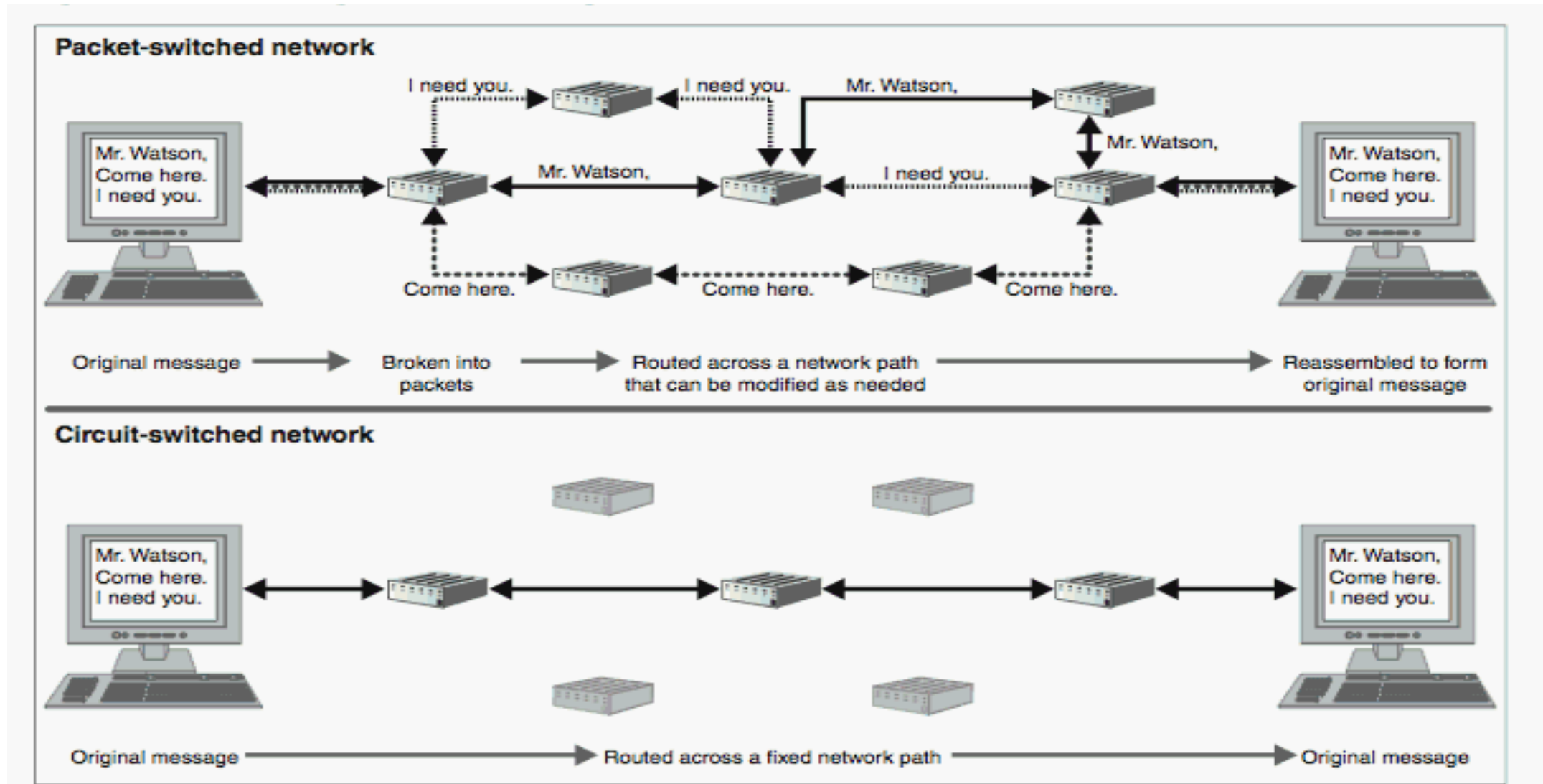
Layer 4- The Transport Layer

- **Buffering:** With buffering, a device (for example, a router) allocates a chunk of memory (sometimes called a buffer or a queue) to store segments if bandwidth is not currently available to transmit those segments. A queue has a finite capacity, however, and can overflow (that is, drop segments) in the event of sustained network congestion.

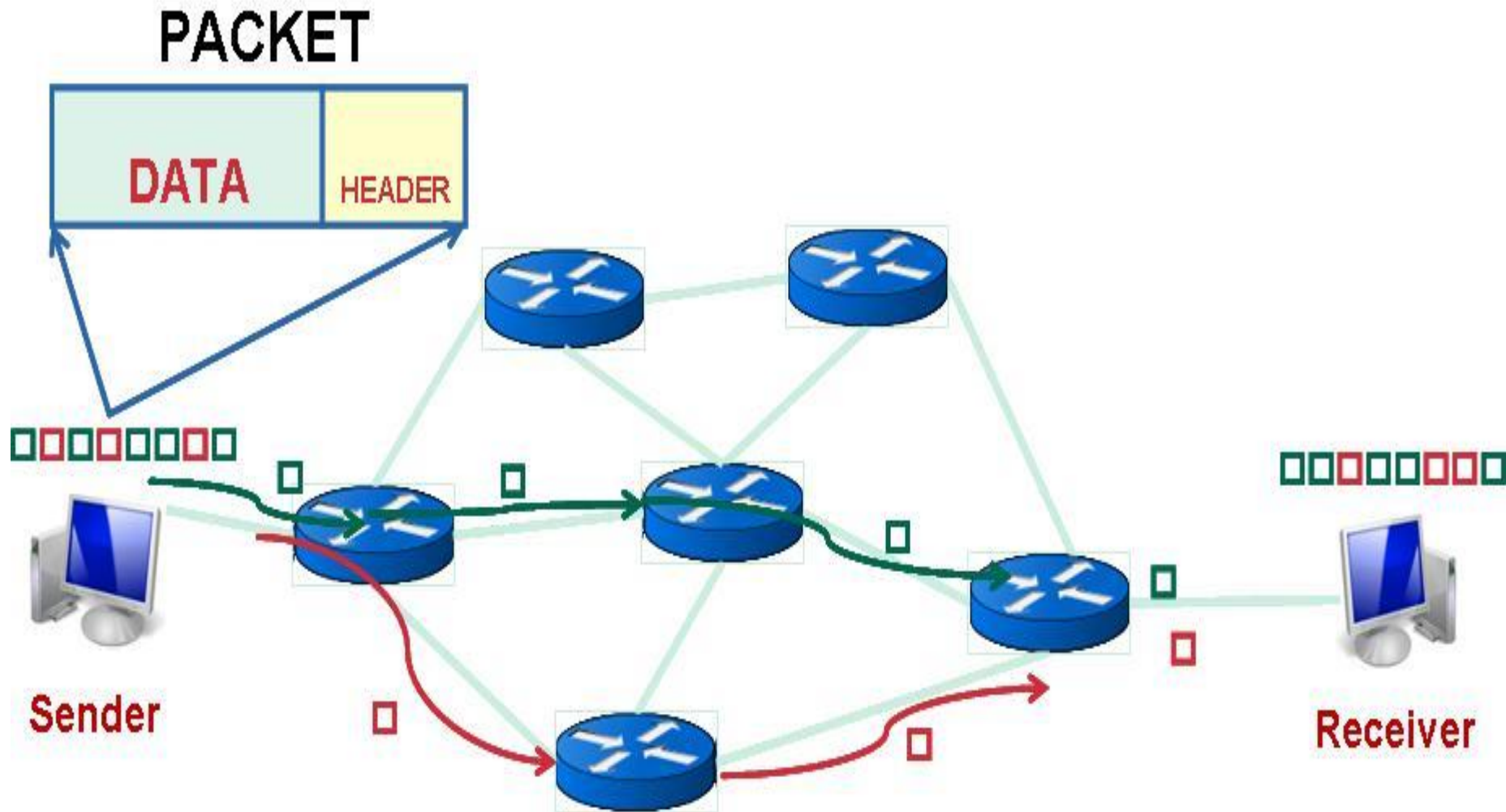


- Controls the operations of routing and switching information to different networks
- Translates logical addresses or names to physical addresses
- Internet Protocol (IP) is a Network Layer protocol
- Devices that work at the network layer are routers and IP switches
- Network Layer components: IP addresses, subnets
- Unit of measurement: packets

SWITCHING:- Either one direction (circuit-switched) or multiple direction (packet-switched) sending packets.

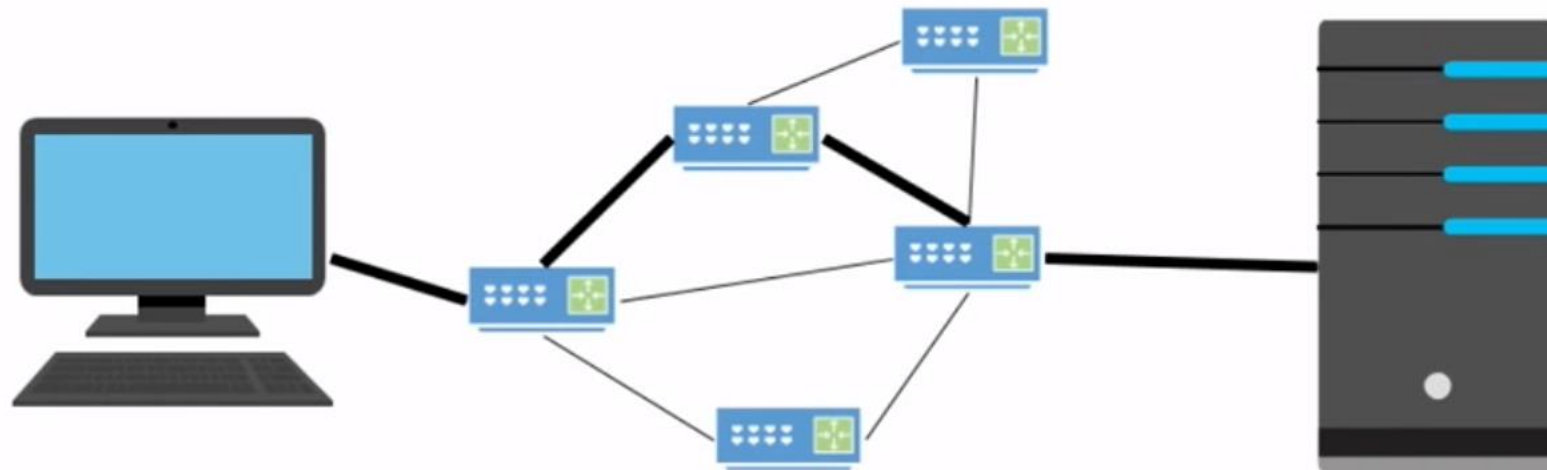


ROUTING:- Select best path for send packets according to routing protocols



What is a router?

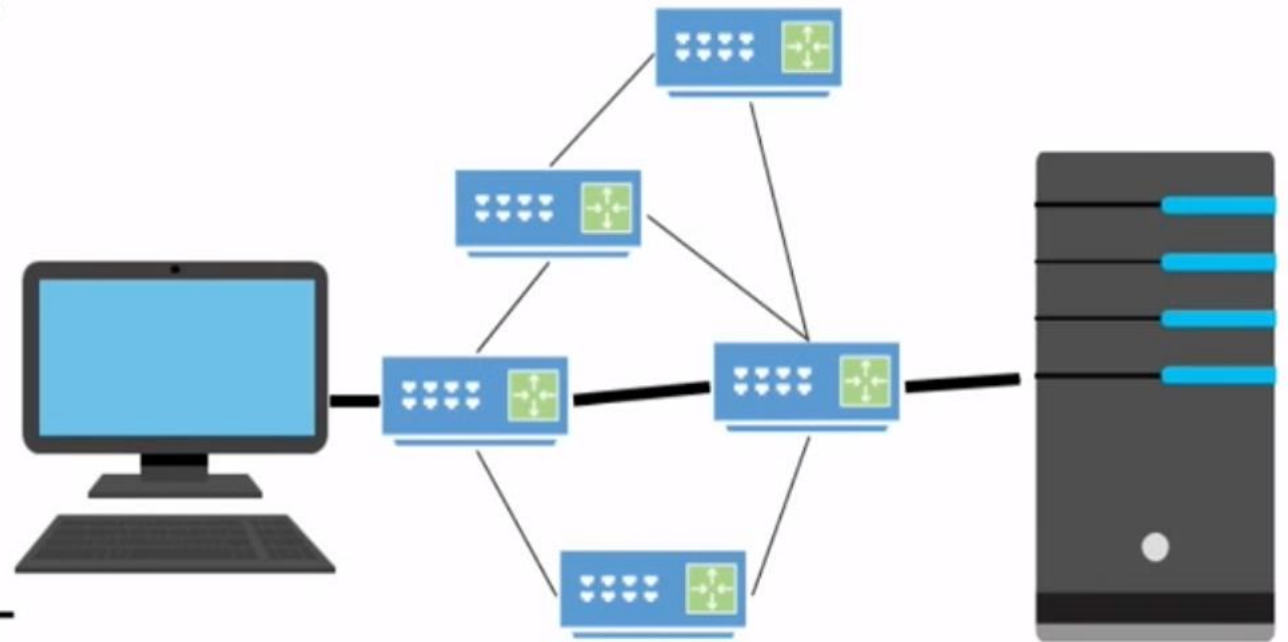
- Routers are central connecting devices that use TCP/IP routing protocols to forward packets
 - Routers use IP addresses to route data
- Routers connect LANs
- Routers allow communication between hosts on different networks



- Routers use the information in routing tables to make decisions about how to route from one host to another
 - Routing tables consist of a list of paths to various networks
- These paths can be configured manually or automatically
 - Manual configuration of pathways is known as **static routing**
 - Automatic configuration of pathways is known as **dynamic routing**

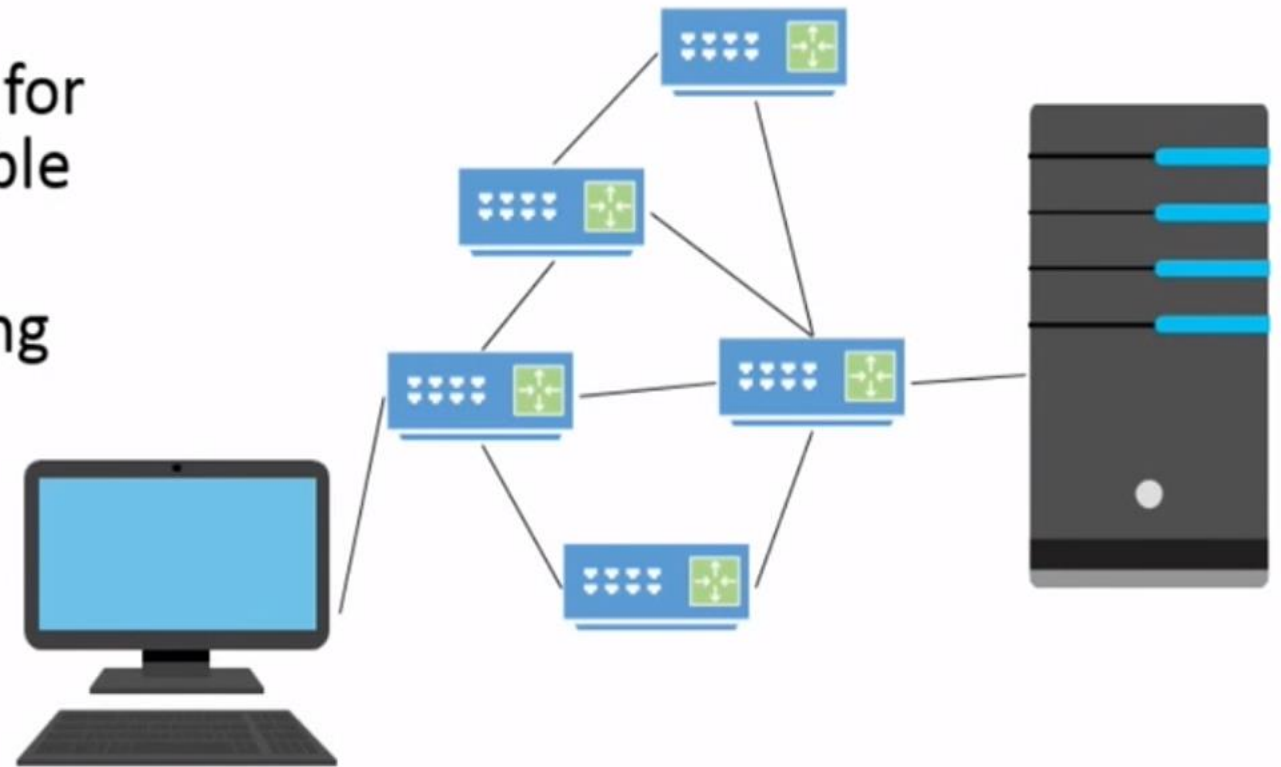
Destination	Network mask	Gateway	Interface	Metric	Protocol
10.57.76.0	255.255.255.0	10.57.76.1	Local Area C...	1	Local
10.57.76.1	255.255.255.255	127.0.0.1	Loopback	1	Local
10.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.45.0	255.255.255.0	192.168.45.1	Local Area C...	1	Local

- Static routing is used when it is desirable for data to always travel a fixed path
- A static route is a path that is manually configured and remains constant during the router's operation
- This type of routing is not fault-tolerant
 - If a connection goes down, then the route is unavailable



Static

- Dynamic routing allows a router to detect when new routers are connected to it, and new paths for sending packets become available
- The new routes are then *dynamically* added to the routing table
- This type of routing is fault-tolerant
 - When connections go down, packets can be routed via different pathways

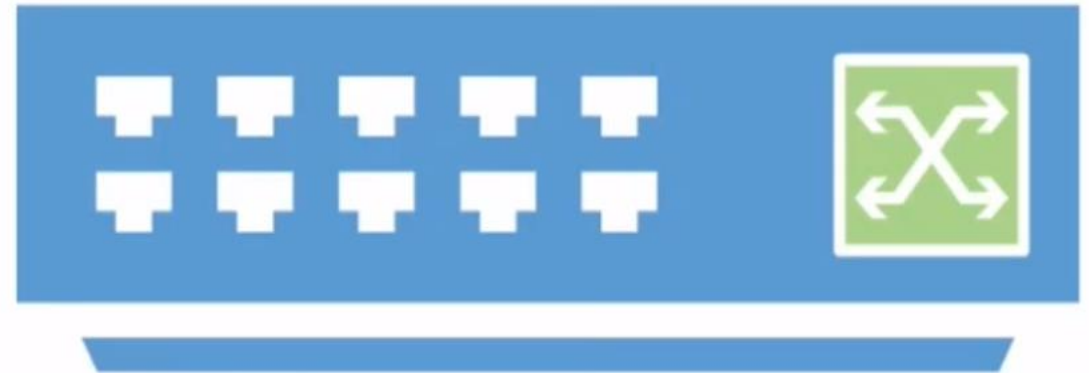


Dynamic

The dynamic configuration of a routing table wouldn't be possible without a number of dynamic routing protocols

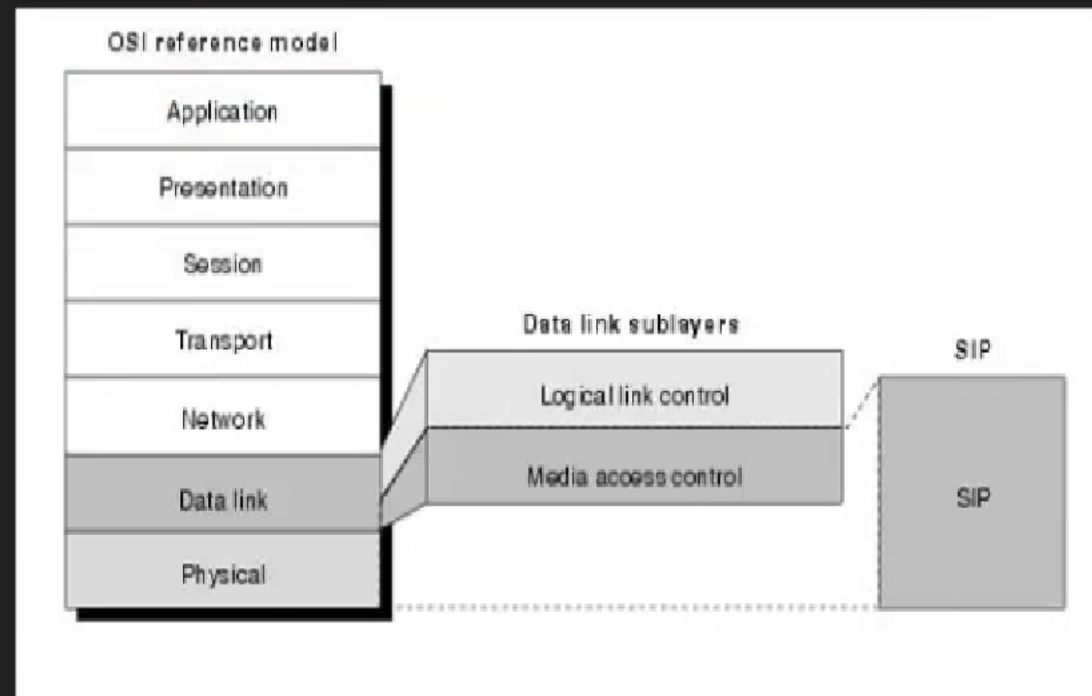
Protocol	Description
Routing Information Protocol (RIP)	Uses a distance-vector routing algorithms to determine which route should be used to send packets
Open Shortest Path First (OSPF)	A link-state protocol that monitors a network for routers that experience a change in their link-state (on to off, off to on, and so on)
Interior Gateway Routing Protocol (IGRP)	A proprietary distance-vector protocol designed by Cisco Systems, Inc.
Border Gateway Protocol (BGP)	A core routing protocol that bases routing decisions on the network path and rules

- Layer 3 switches are different from Layer 2 switches because they direct data using IP addresses instead of MAC addresses
 - This means they forward packets instead of frames
- They perform the same functions as **routers**
- The benefit of Layer 3 switches when compared to routers is that they can forward packets faster than routers



Layer 2- The Data Link Layer

- is concerned with packaging data into frames and transmitting those frames on the network, performing error detection/ correction, uniquely identifying network devices with an address, and handling flow control. These processes are collectively referred to as data link control (DLC).
- Application
- In fact, the data link layer is unique from the other layers in that it has two sublayers of its own: MAC and LLC.



Layer 2- The Data Link Layer

- Media Access Control
- Characteristics of the Media Access Control (MAC) sublayer include the following:
 - ■ Physical addressing: A common example of a Layer 2 address is a MAC address, which is a 48-bit address assigned to a device's network interface card (NIC). The address is commonly written in hexadecimal notation (for example, 58:55:ca:eb:27:83). The first 24 bits of the 48-bit address are collectively referred to as the vendor code. Vendors of networking equipment are assigned one or more unique vendor codes. You can use the list of vendor codes at <http://standards.ieee.org/develop/regauth/oui/oui.txt> to determine the manufacturer of a networking device, based on the first half of the device's MAC address. Because each vendor is responsible for using unique values in the last 24 bits of a MAC address, and because each vendor has a unique vendor code, no two MAC addresses in the world should have the same value.
 - ■ Logical topology: Layer 2 devices view a network as a logical topology. Examples of a logical topology include bus and ring topologies, as described in Chapter 1.
 - ■ Method of transmitting on the media: With several devices connected to a network, there needs to be some strategy for determining when a device is allowed to transmit on the media. Otherwise, multiple devices might transmit at the same time, and interfere with one another's transmissions.

What is a switch?

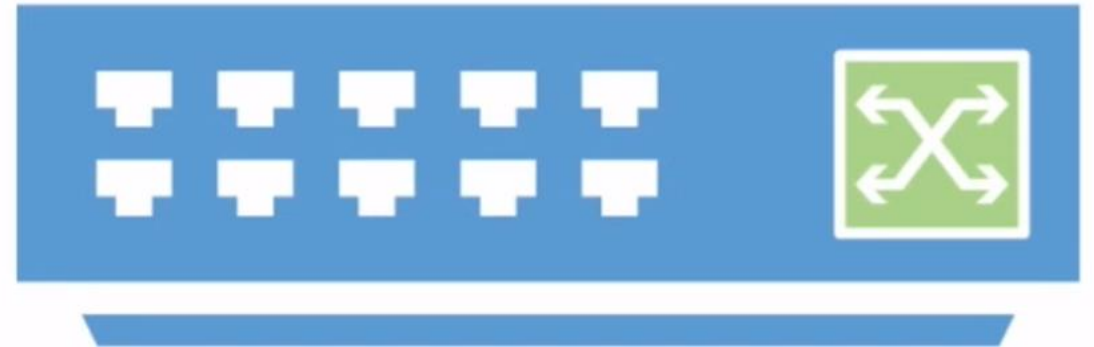
- Switches are central connecting devices
- They use **MAC addresses** to establish point-to-point connections between devices
 - In contrast, **hubs** broadcast frames to all connected devices
- Hosts connect to switches by plugging into their ports



A switch port

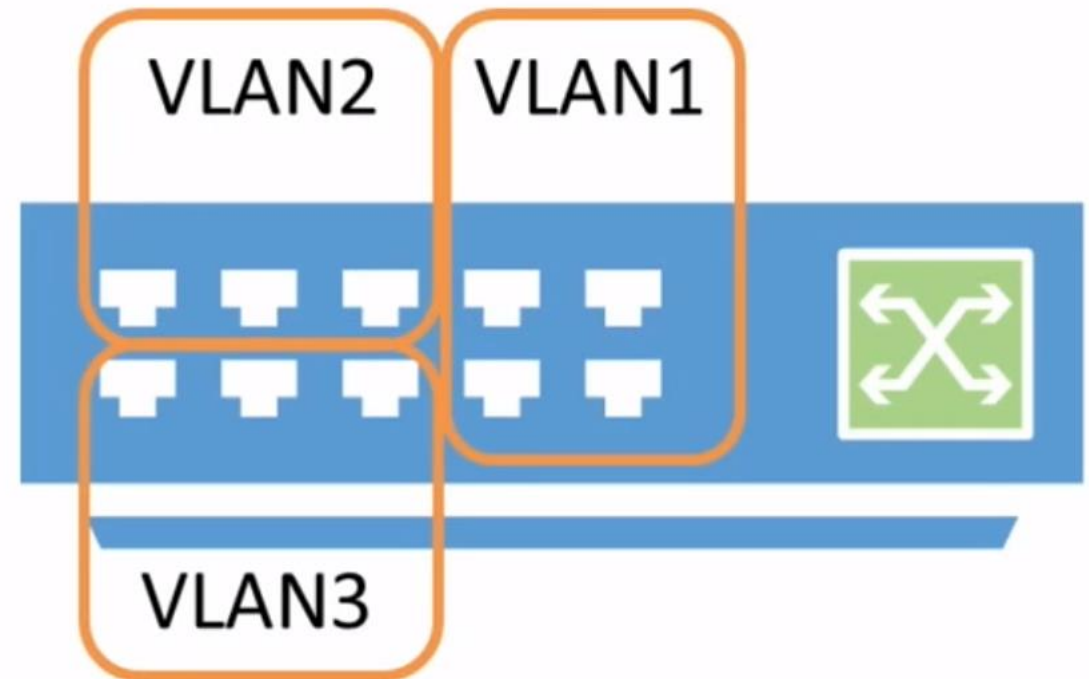
What is a Layer 2 switch?

- A **layer 2 switch** is the most common type of switch used on a LAN
- Layer 2 switches direct frames on a LAN based on the MAC address of each host's network adapter
- Each port of a switch is mapped to the MAC address of the device that is connected



Virtual LAN (VLAN)

- Layer 2 switching can also allow for a virtual LAN (VLAN) to be implemented
- **IEEE 802.1Q** is the standard that supports VLANs
- A tag is added to the data frame to identify the VLAN



How do switches remember MAC addresses?

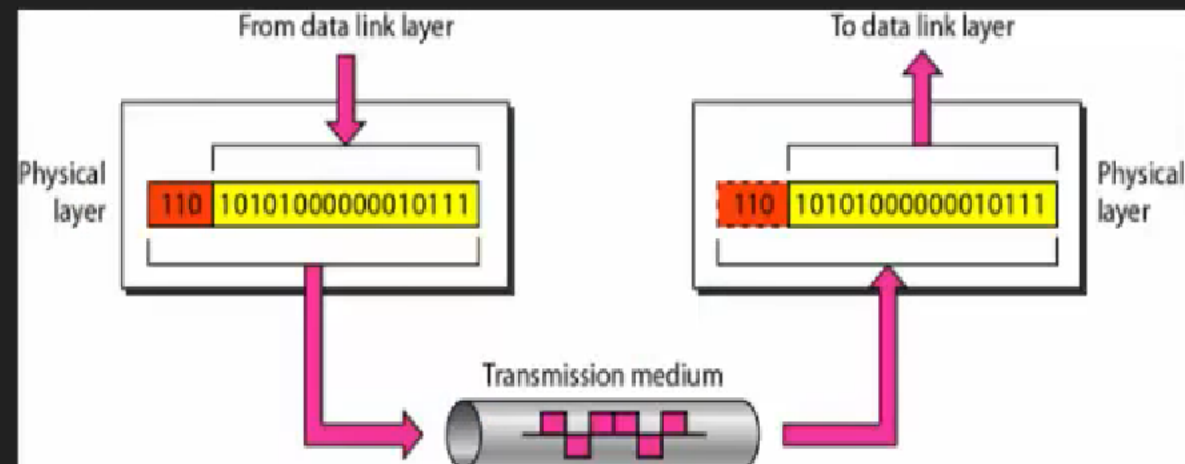
- Switches map the MAC addresses of connected computers to their ports in a **CAM table**
- CAM stands for **Content Addressable Memory**
- The CAM table is stored in the memory of a switch
 - This memory is limited

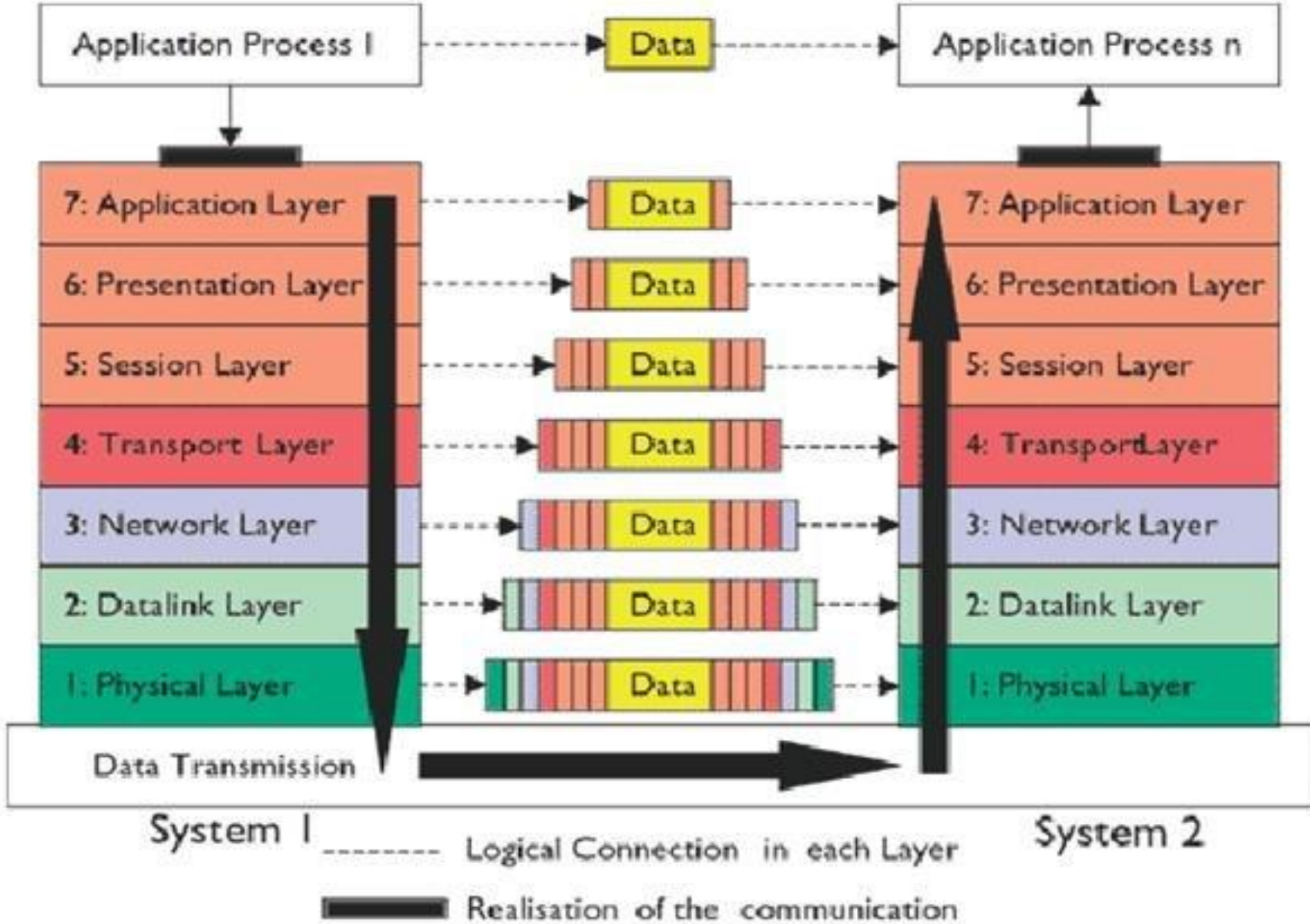
Sample CAM table

Port	MAC Address
1	38-75-2D-72-17-1E
2	
3	CB-D2-F6-98-45-9D
4	BC-85-1D-22-2E-B4
5	
6	65-46-F6-E0-FE-9D
7	
8	

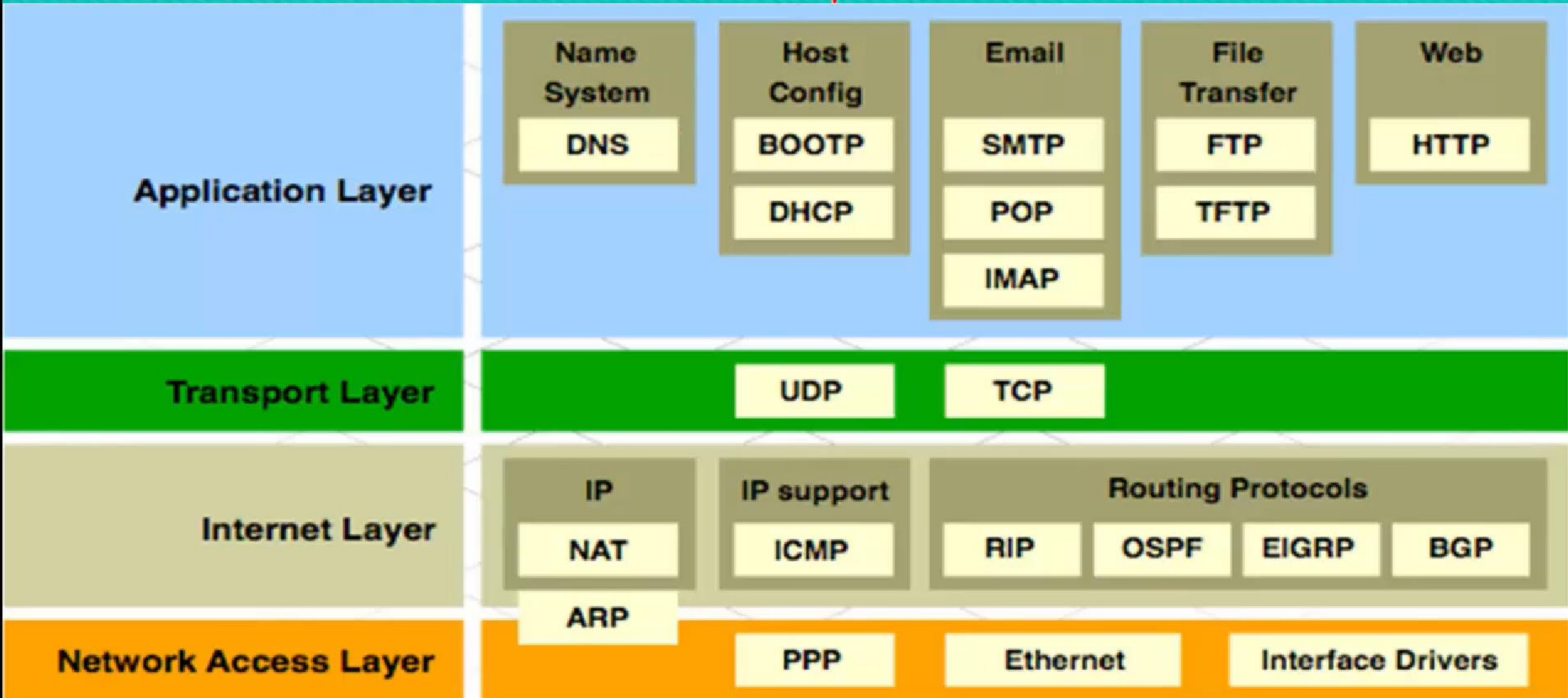
Layer 1- The Physical Layer

- is concerned with the transmission of data on the network.
- How bits are represented on the medium
- Wiring standards for connectors and jacks
- Physical topology
- Synchronizing bits
- Bandwidth usage
- Multiplexing strategy





The TCP/IP Stack



- IP resides on the network layer of the OSI model
- IP addresses are used to help devices send and receive data across networks
- IPv4 is the most commonly used communication protocol, but IPv6 is beginning to replace it

- Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol
 - it's the first version to be widely used
- IPv4 addresses consist of four octets separated by decimal points
- Each octet represents one byte, or eight bits, meaning that an IPv4 address features 32 bits

IP ADDRESS EXAMPLES

12.5.24.2

127.0.0.1

192.168.1.10

208.32.56.232

Categorizing IPv4 Addresses

- IPv4 addresses have been categorized into five IP classes
- The classification system is known as **classful network architecture**
 - In this system, the first octet of an IPv4 address defines which class the address belongs to

CLASS	IP RANGE (1 st OCTET)
A	0 - 127
B	128 - 191
C	192 - 223
D	224 - 239
E	240 - 255

Decimal to Binary Conversion

Al-Nahrain University/ECC
Eng.vian adnan farman

<i>Conversion Area</i>								<i>Decimal Equivalent</i>
128	64	32	16	8	4	2	1	
1	1	1	0	0	0	0	0	224
1	0	1	0	1	0	1	0	170
0	1	0	1	0	1	0	1	85

- Each IPv4 address has a network portion and a node portion
 - For example, the first octet of a Class A IP address is the “network” portion
- **Node** is another word for “host”

CLASS	DEFAULT SUBNET MASK	NETWORK/NODE PORTIONS
A	255.0.0.0	Net.Node.Node.Node
B	255.255.0.0	Net.Net.Node.Node
C	255.255.255.0	Net.Net.Net.Node
D	N/A	N/A
E	N/A	N/A

- The number of usable addresses is two less than what is mathematically possible
- The first and last address in a network can't be used
 - The first address is reserved for the entire network
 - The last address is a broadcast address
- A **broadcast address** is used when a device wants to communicate with ALL devices on a network

CLASS	TOTAL NUMBER OF NETWORKS	TOTAL NUMBER OF USABLE ADDRESSES
A	$2^7 = 128$	$2^{24} - 2 = 16,777,214$
B	$2^{14} = 16,384$	$2^{16} - 2 = 65,534$
C	$2^{21} = 2,097,151$	$2^9 - 2 = 254$
D	N/A	N/A
E	N/A	N/A

- IPv4 addresses are further classified as either public or private
- **Public IP addresses** are ones that are exposed to the Internet
 - Devices connected to the Internet can potentially communicate with them
- **Private IP addresses** are hidden from the Internet and any other networks
 - Usually behind an IP proxy or firewall device

Class	Start of Range	End of Range
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

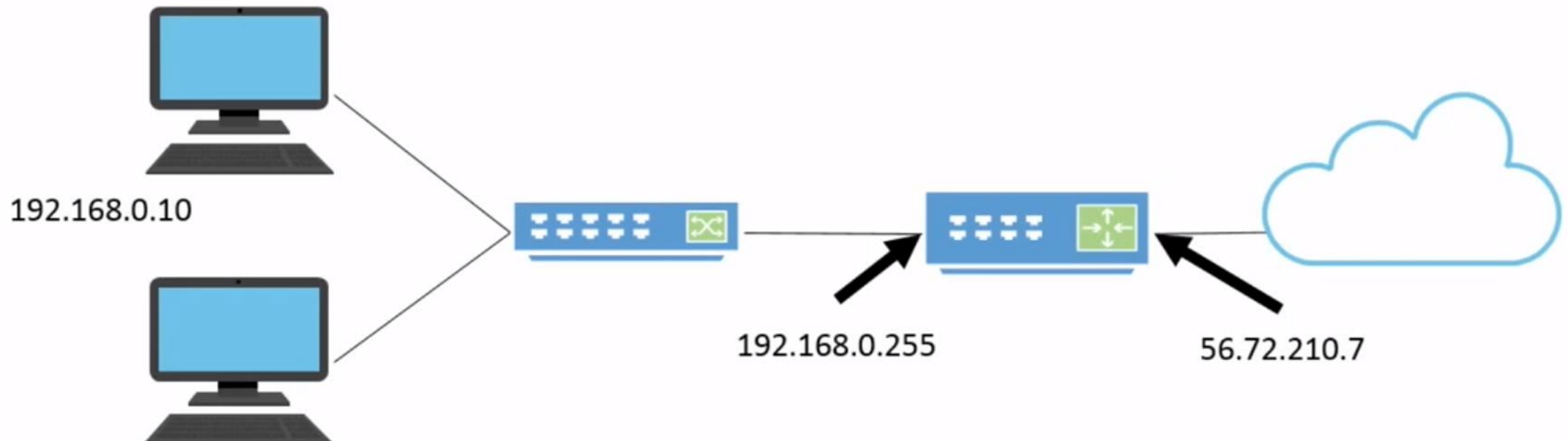
- **Static IP addresses** are addresses that are manually assigned to a host
- **Dynamic IP addresses** are more common than static IP addresses, whereas they automatically obtain an IP address (and other IP information)

- The Class A range is 0 – 127, but the 127 network is actually reserved for loopback IP addresses
- Loopback IP addresses are used for testing
- Every device is automatically assigned the 127.0.0.1 loopback IP address

- Acronym for **Automatic Private IP Addressing**
- It uses a single Class B network number:
169.254.0.0
- If a client can't get an IP address from a DHCP server and has not been configured statically, it will auto-assign a number on this network

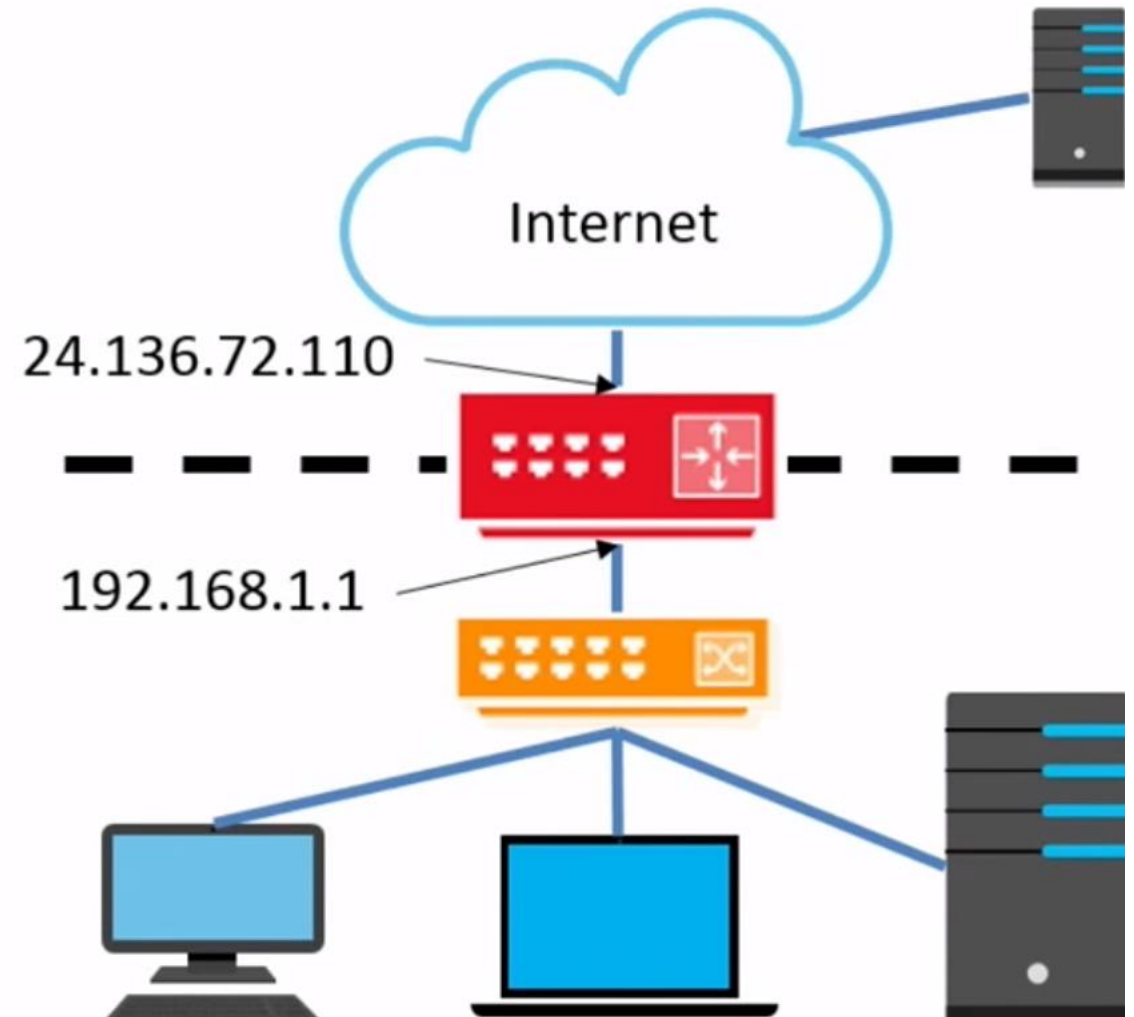
Network Address Translation (NAT)

Network Address Translation (NAT) is the process of modifying IP address information in IPv4 headers while in transit across a traffic routing device

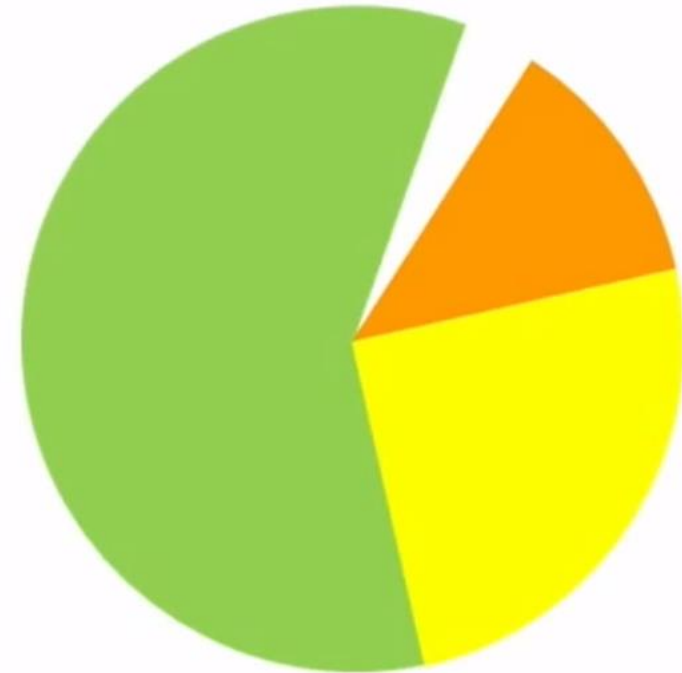


Default Gateways

- For a device to communicate on the Internet, a default gateway and DNS server must be assigned
- **Default gateway** – Provides a default route for TCP/IP hosts to use when communicating with hosts on remote networks
- The first IP address of the device that a client computer will look for when attempting to gain access outside the local network



- The act of dividing a network into smaller logical subnetworks
 - Subnetting is similar to cutting a pizza into slices
- By default, all computers are on one subnet or network with no divisions involved



- Intended to replace classful IP addressing
 - slow the exhaustion of IPv4 addresses
- Based on **Variable-length subnet masking (VLSM)**
 - allows a network to be divided into different-sized subnets to make one IP network
- To implement VLSM, networks “borrow” bits from the host portion of an address

- New generation of IP addressing for the Internet
 - Solves many of the limitations of IPv4, including address space and security
- IPv6 is a 128-bit system while IPv4 is only a 32-bit system
 - IPv4 allows approximately 4.3 billion IP addresses
 - IPv6 allows 3.4×10^{38} (340 undecillion) addresses
- IPv6 addresses are represented as 8 groups of 4 hexadecimal digits

- IPv6 addresses are broken down into three parts:
 - **Site prefix:** The first three groups of numbers that define the “network”
 - **Subnet ID:** Defines the individual subnet of the network that the address is located on
 - **Interface ID:** The individual host IP portion
 - **IPv6 Address:** 2001:4860:0000:2001:0000:0000:0000:0068

Site Prefix	Subnet ID	Interface ID
2001.4860.0000 48 bits	2001 16 bits	0000:0000:0000:0068 64 bits

- The Windows command prompt is Microsoft's version of a command-line interface or CLI
 - Running the command prompt as an Administrator is also known as running it in elevated mode
- Many tools can be run using the command prompt

- Displays the current configuration of the installed IP stack on a networked computer using TCP/IP
- The /all switch can be used to view additional details about each adapter
- Can be used to refresh Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings

```
C:\Windows\system32\cmd.exe
C:\Users\teacher>ipconfig/all

Windows IP Configuration

Host Name . . . . . : MRWHITED7D2
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 08-1C-42-E3-AB-0A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : fdh2:2c26:f4e4:8:3d3f:981:7408:4c33(Prefe
rred)
Temporary IPv6 Address. . . . . : fdh2:2c26:f4e4:8:8915:412b:5a53:b851(Pref
erred)
Link-local IPv6 Address . . . . . : fe80::3d3f:981:7408:4c33x10(Preferred)
IPv4 Address. . . . . : 10.211.55.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, June 24, 2015 12:15:48 PM
Lease Expires . . . . . : Wednesday, June 24, 2015 12:45:48 PM
Default Gateway . . . . . : 10.211.55.1
DHCP Server . . . . . : 10.211.55.1
DNS Servers . . . . . : 10.211.55.1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.localdomain:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 9:

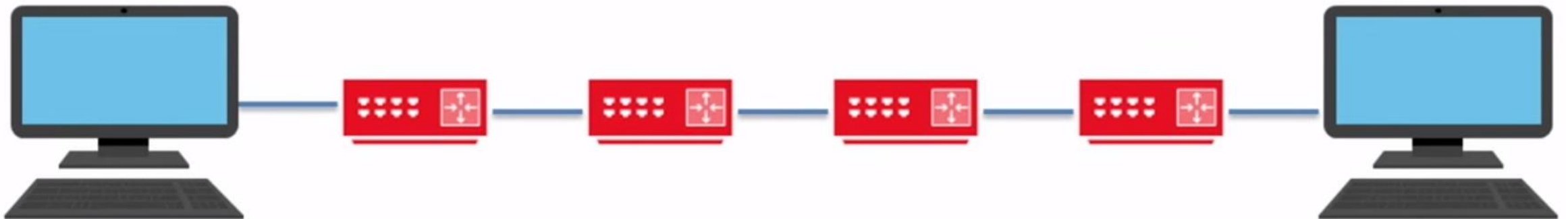
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\teacher>
```

- Verifies IP-level connectivity to another TCP/IP device by sending Internet Control Message Protocol (ICMP) Echo Request messages
- A number of switches can accommodate different testing scenarios
- Can be used to test IPv4 and IPv6 connectivity



- Determines the path taken by data to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values
- Used to “trace” the path data takes from sending to receiving device
- Helpful for identifying network issues
 - Network problems aren’t always your computer’s fault!



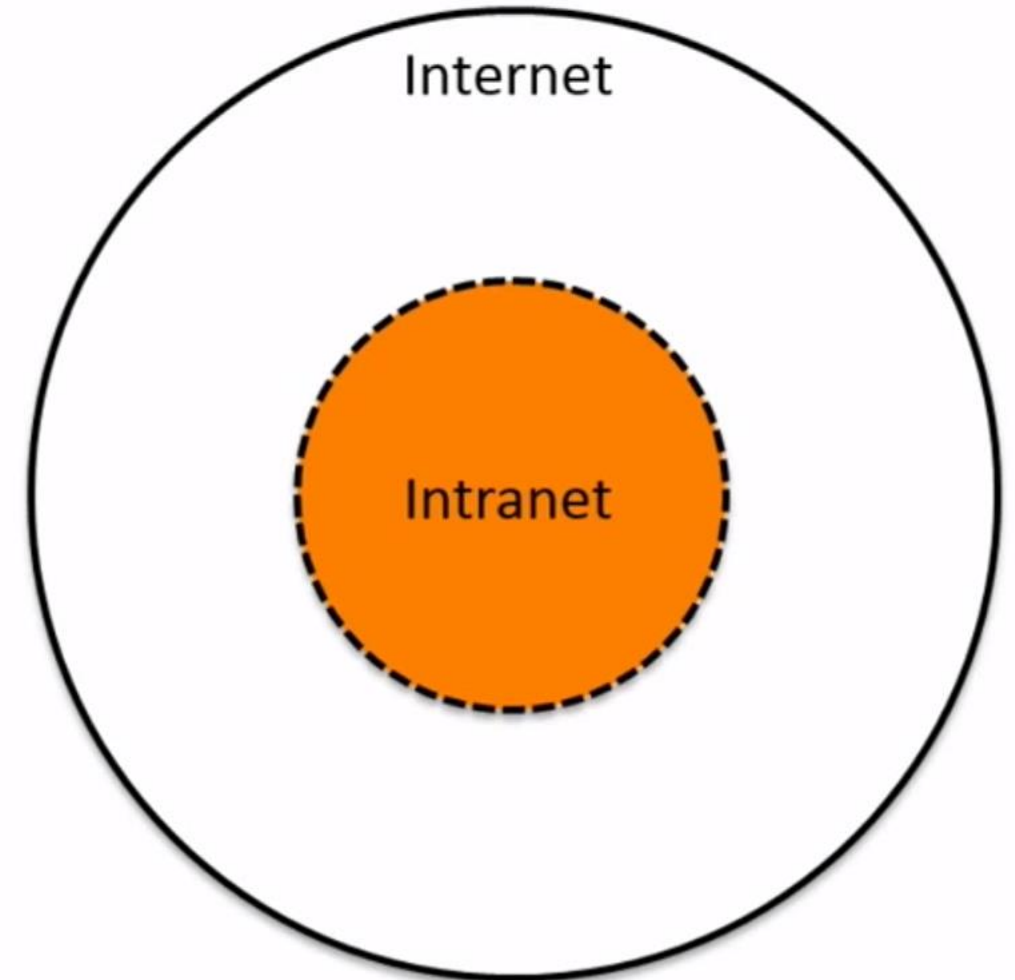
- Displays information that you can use to diagnose Domain Name System (DNS)
- The nslookup command-line tool is available only if you have installed the TCP/IP protocol
 - You should be familiar with DNS before using this tool

What is the Internet?

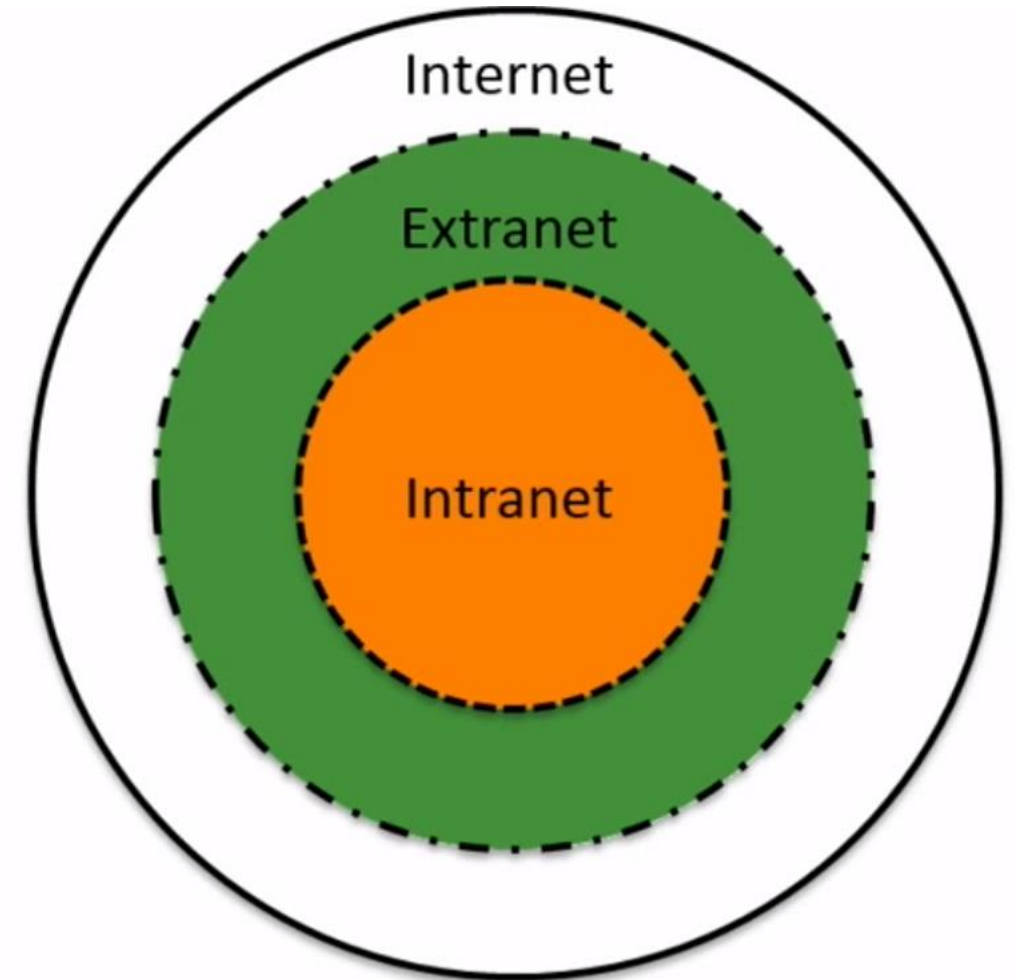
- The **Internet** is a worldwide system of connected computer networks
- Devices that connect to the Internet use the TCP/IP protocol suite
- The Internet contains a lot of information, resources and services:
 - World Wide Web (WWW) servers hosting content
 - Supporting infrastructure for email
 - Connectivity for peer-to-peer networks



- An intranet is a private computer network or single Web site that an organization implements in order to share data with employees around the world
- User **authentication** is necessary before a person can access the information in an intranet
 - This keeps the general public out as long as the intranet is properly secured

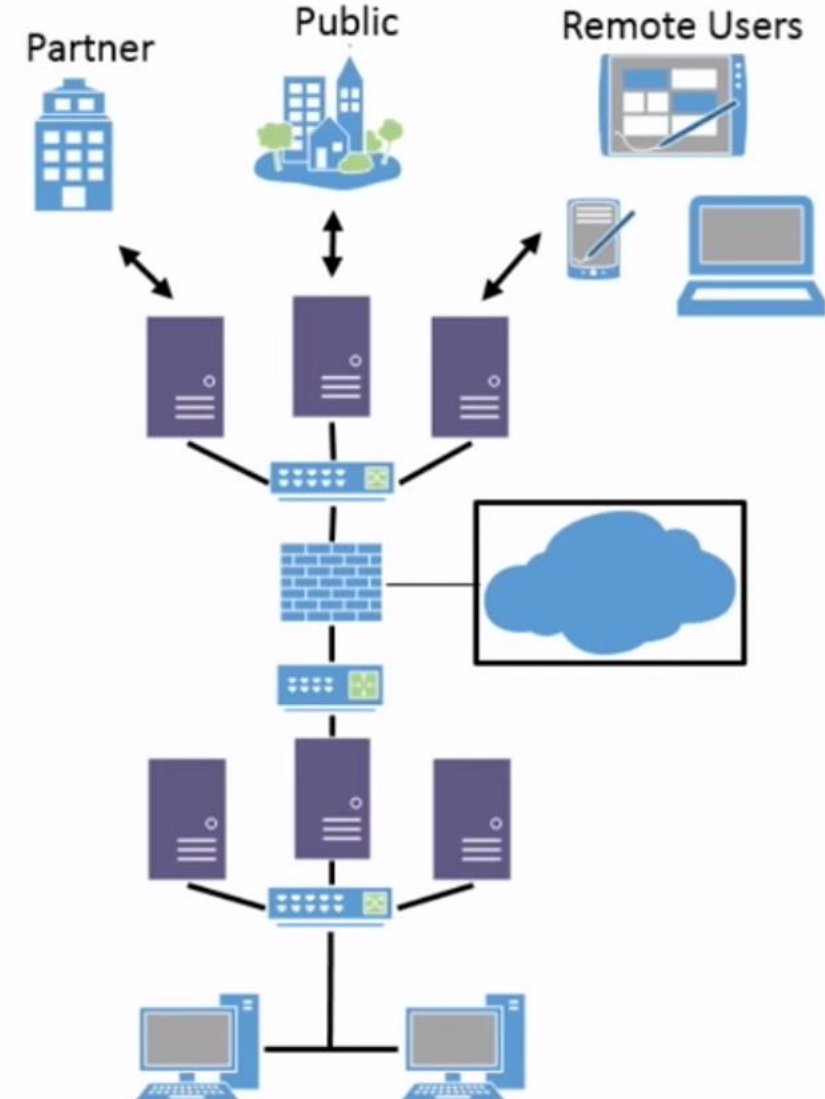


- An extranet is similar to an intranet except that it is extended to users outside a company
 - possibly to entire organizations that are separate from or lateral to the company
- User authentication is still necessary, and an extranet is not open to the general public

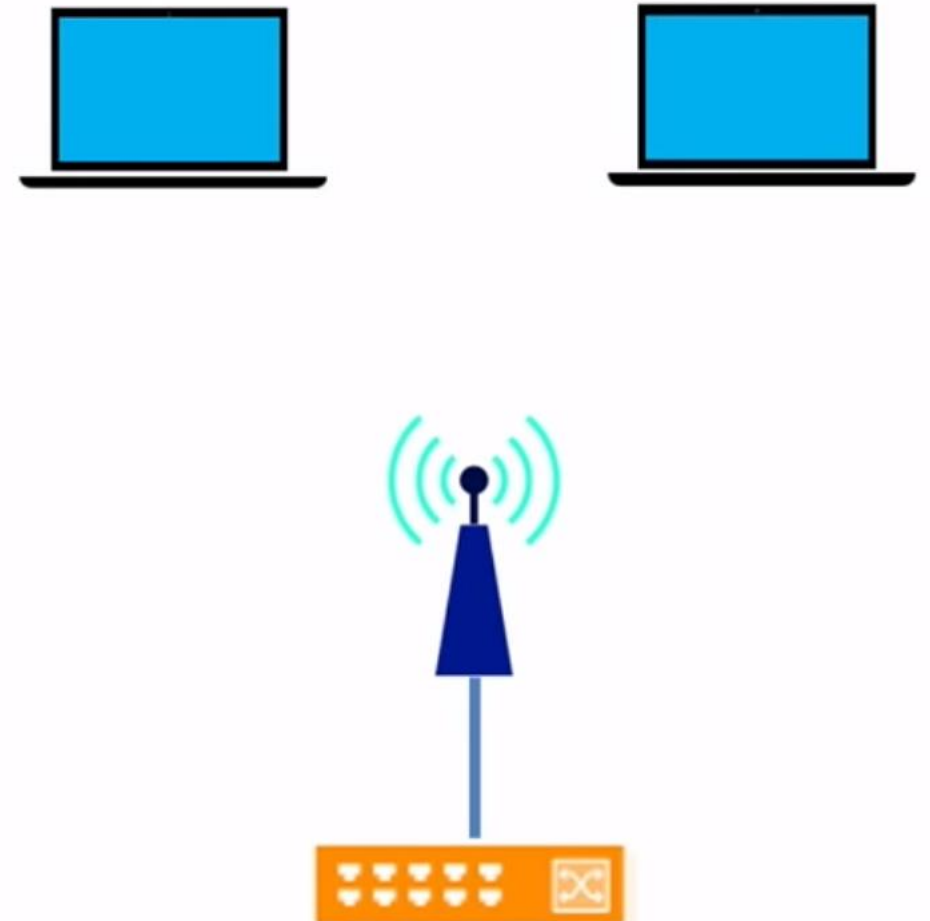


Virtual Private Network(VPN)?

- A **virtual private network (VPN)** is a virtual connection between two or more private networks
 - Allows users to access resources remotely
- VPNs use data encapsulation and encryption to ensure data is secured
- A “tunnel” is created, through the LANs and WANs that are being used

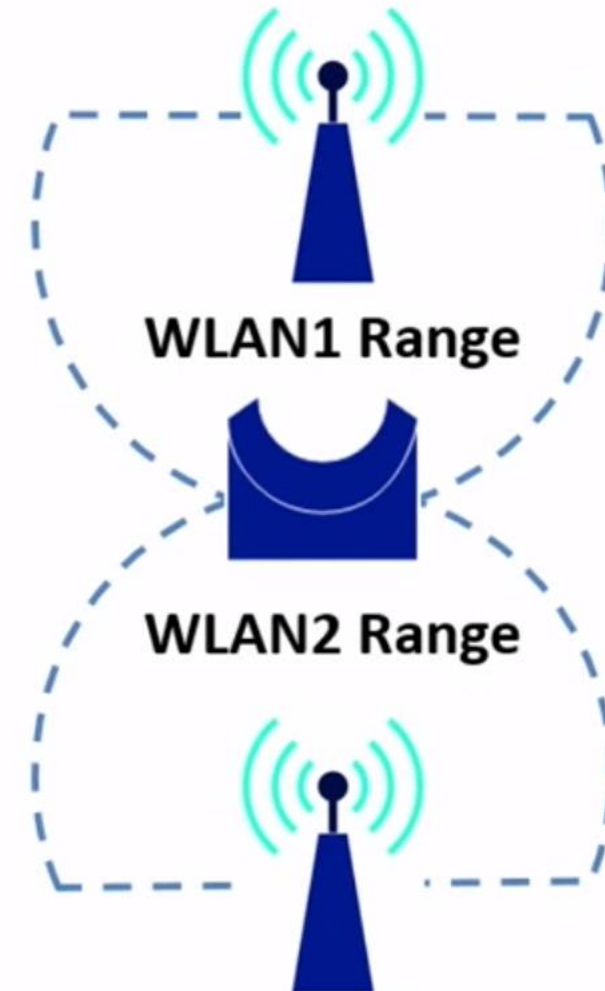


- For a wireless network to work, all devices must have a **wireless network adapter**
 - Connects to **wireless access point (WAP)** that is capable of sending and receiving data wirelessly
- Wireless access points then transmit data over a wire, such as an Ethernet cable, through a network to its final destination



- Wireless network adapters enable connectivity between devices and a WAP
- Wireless network adapters work by translating bits into radio signals, which are then sent to a WAP
- Wireless network adapters can come in many forms:
 - USB
 - internal adapter cards
 - external adapter cards
 - onboard adapters

- Function the same way that wireless repeaters do
- Wireless networks, depending on the different technologies available, can work using different standards
- Bridges are able to connect devices and networks using different technologies together
- This is known as **bridge mode**



- Wireless access points can also come in many forms:
 - SOHO routers
 - dedicated WAPs connected to switches
- Wireless access points also work by translating bits into radio signals, which are then sent to or received from devices on a network



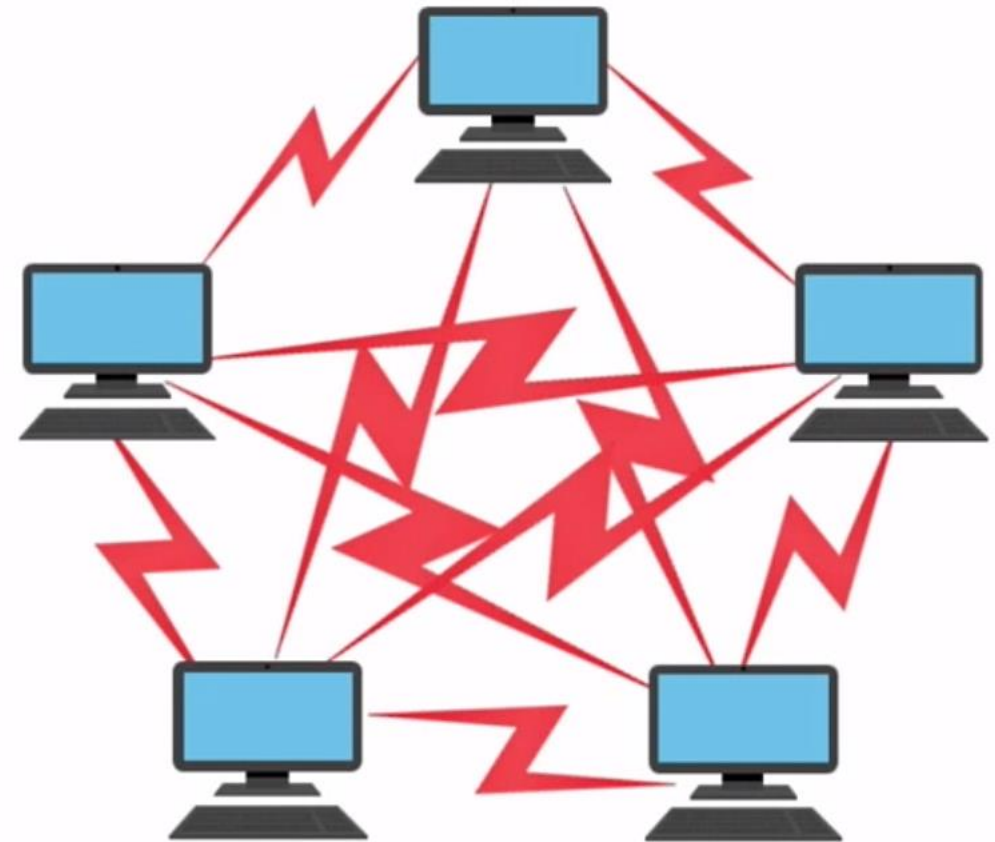
- For wireless networks to function, all devices must use the same wireless networking standard
- There are a number of standards that define wireless networking
 - These standards are also governed by the IEEE and are referred to as IEEE 802.11
- **IEEE 802.11, or Wi-Fi**, standards dictate the data transfer rate, connection frequency, and more

IEEE 802.11 Standard	Max. Data Transfer Rate	Frequency
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	600 Mbps	5 GHz and/or 2.4 GHz

- Similar to wired networks, there are different ways to connect devices in WLANs
- Recall that these arrangements are called physical topologies
- Two common ways to connect devices wirelessly are:
 - **Ad-hoc mode**
 - **Infrastructure mode**

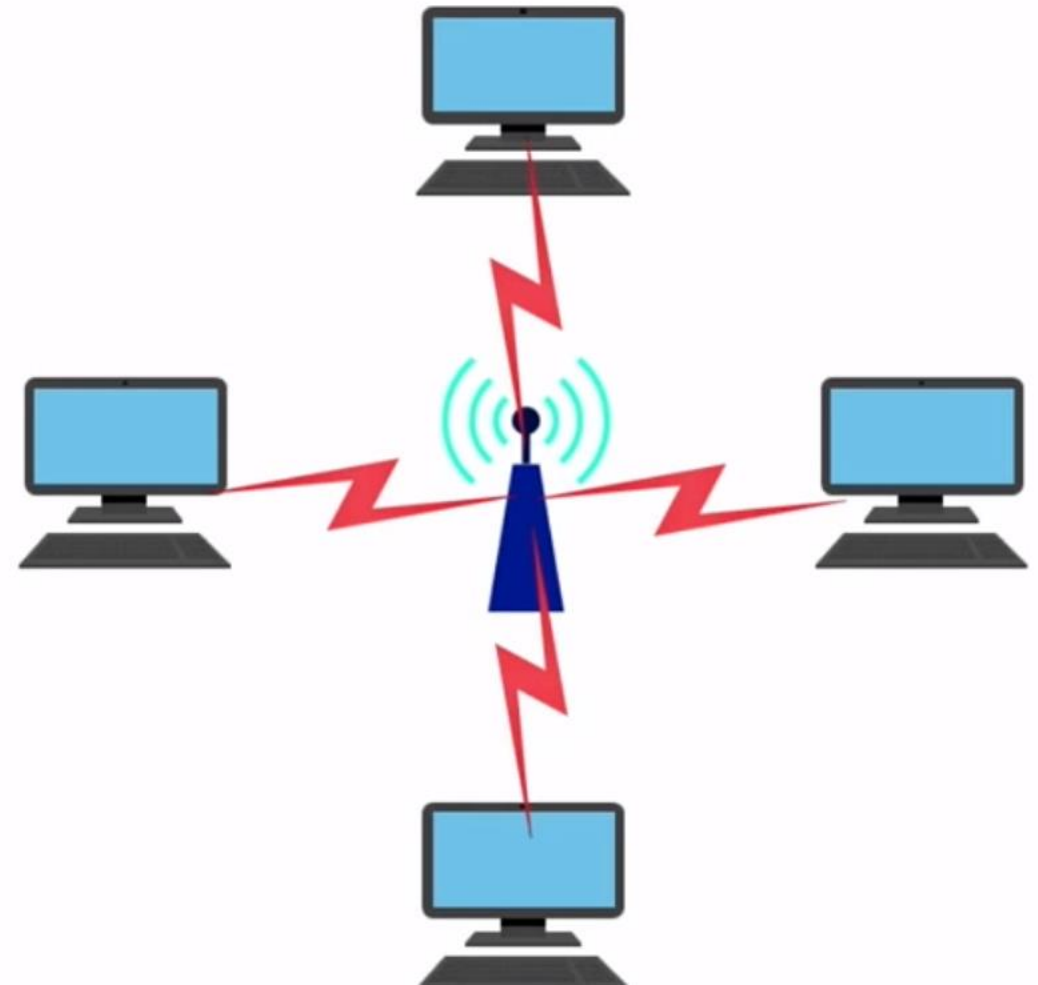
What is AD-hoc Mode?

- Wireless devices using the Ad-hoc mode are organized similar to a mesh topology in a wired network
- Clients communicate directly with one another
 - This is called a peer-to-peer network
- Ad-hoc mode is used less commonly than infrastructure mode



What is Infrastructure Mode?

- Infrastructure mode is the most common way to connect devices wirelessly
- Wireless clients connect to a WAP
- When clients want to connect, they use **the service set identifier (SSID)**
- Before a device can access the network it has to be authenticated using a password



- Name of the wireless network, and it is broadcast over the airwaves
- Can identify a WAP by its SSID
- For security, the SSID can be hidden from public discovery

Protecting Wireless Communication

- Though exceptionally convenient, wireless communication is not secure
- The reason why is that data traveling wirelessly is accessible to anyone, unless it is protected
- There are multiple **wireless encryption protocols** that can be used for wireless networks



- Encryption is the process of scrambling data to make it unreadable to hackers
- Data is scrambled and unscrambled using an encryption key
- The longer the key, the harder it is for somebody to hack your data

Wireless Encryption Protocol	Description	Encryption Level (Key Size)
WEP	Wired Equivalent Privacy	64-bit
WPA2	Wi-Fi Protected Access	256-bit
TKIP	Temporal Key Integrity Protocol	128-bit
AES	Advanced Encryption Standard	128-, 192-, and 256-bit