

CCNA (200-301) Cisco Certified Network Associate

Prepared by Eng. Taghreed Elsayed

Lecture 1

جامعة الجميع الذكية

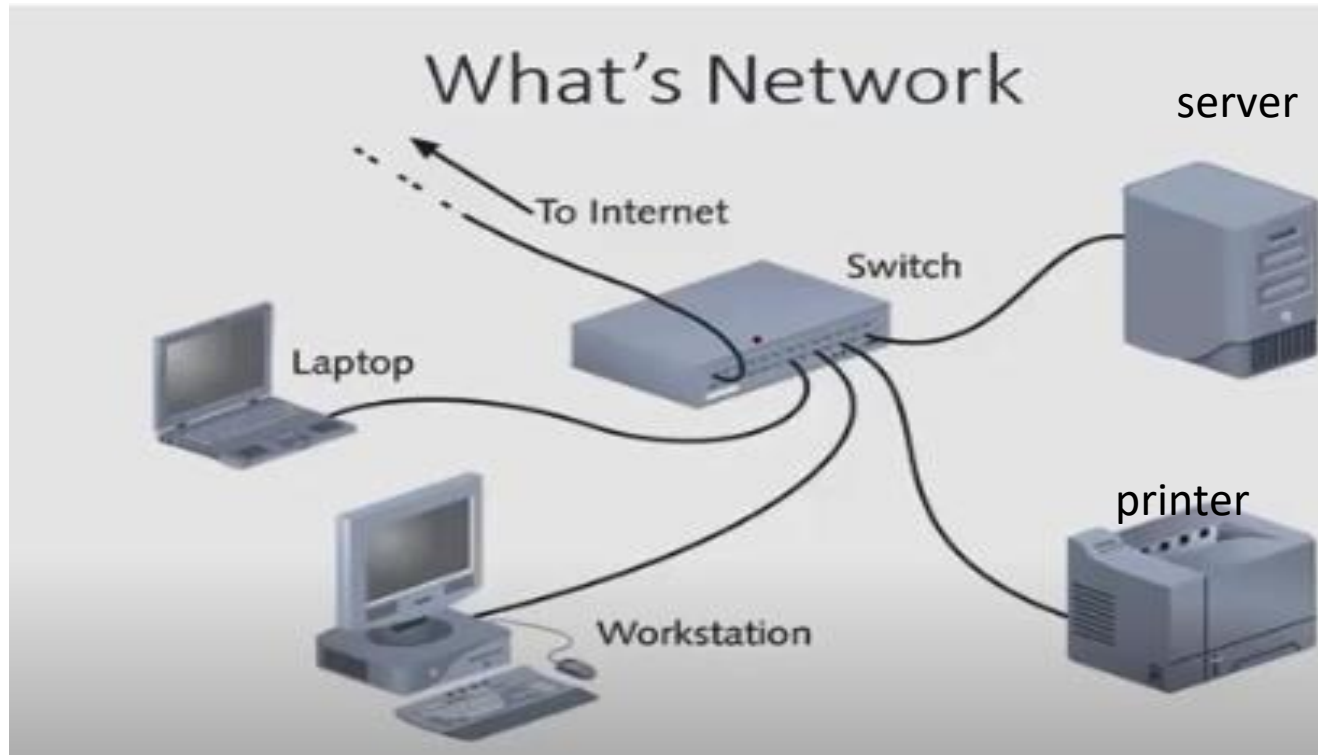
تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

مزيد من التفاصيل

Network Fundamentals



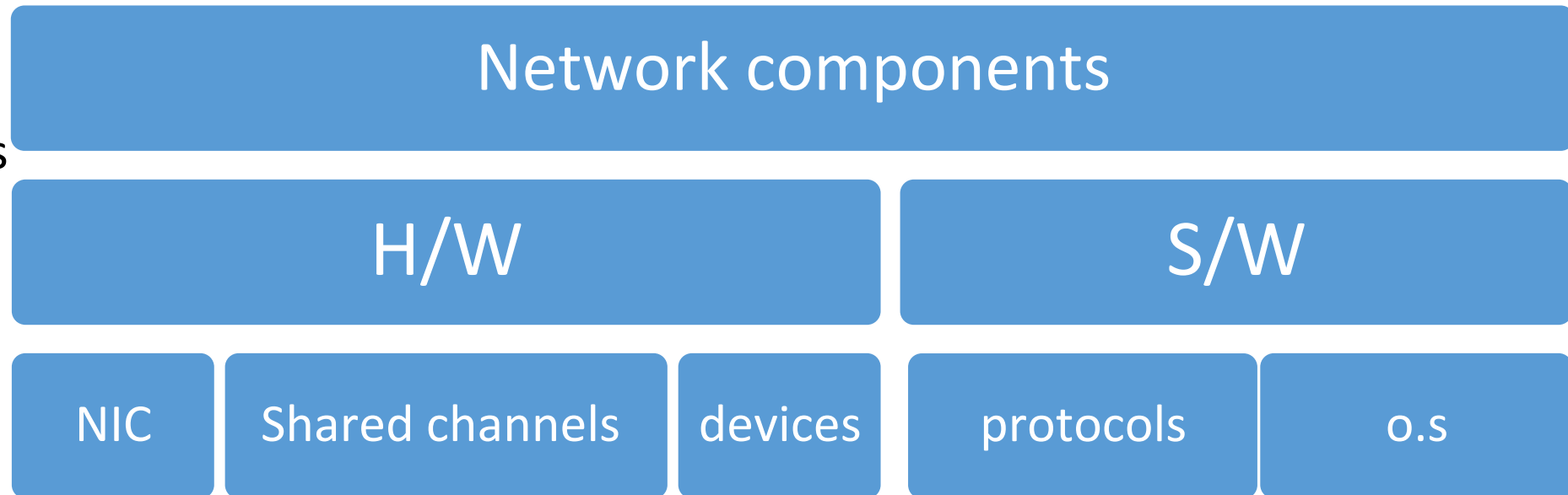
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



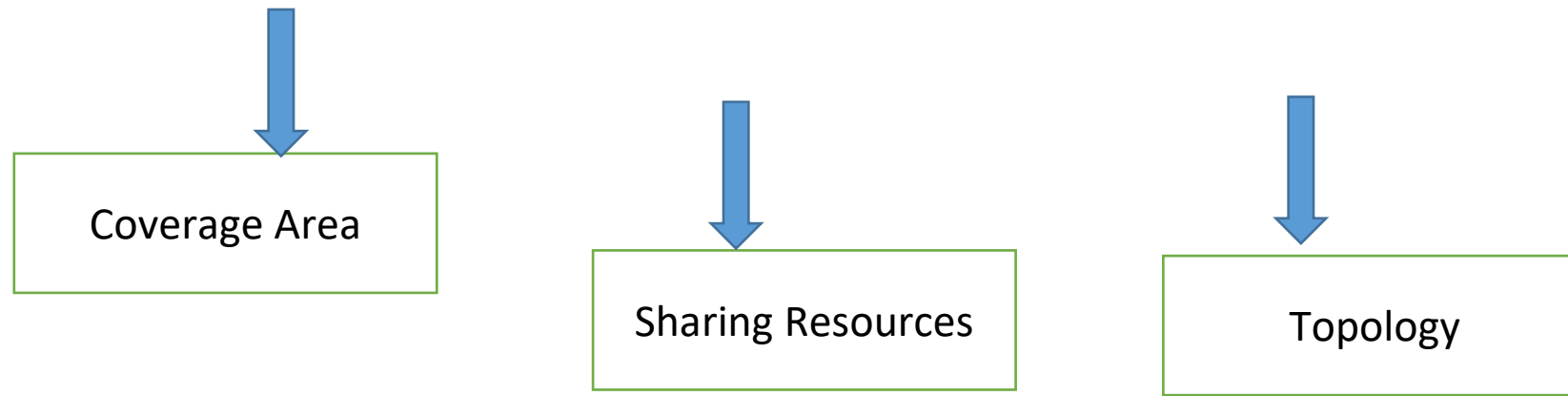
- **Network:** A set of devices connected together via shared channel plus s/w to provide service of communication

what are the benefits of network ?

- ☐ Communication
- ☐ Sharing resources
- ☐ Cost
- ☐ Modern technologies



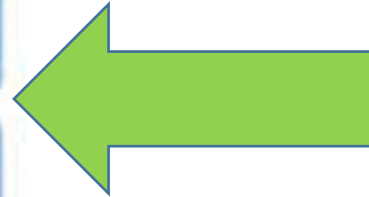
Network types



Coverage Area

Types of Computer Network

- ① LAN (Local Area Network)
- ② MAN (Metropolitan Area Network)
- ③ WAN (Wide Area Network)



Local Area Networks - (LAN)

Wide Area Networks - (WAN)

Campus Area Networks - (CAN)

Personal Area Networks - (PAN)

Metropolitan Area Networks - (MAN)

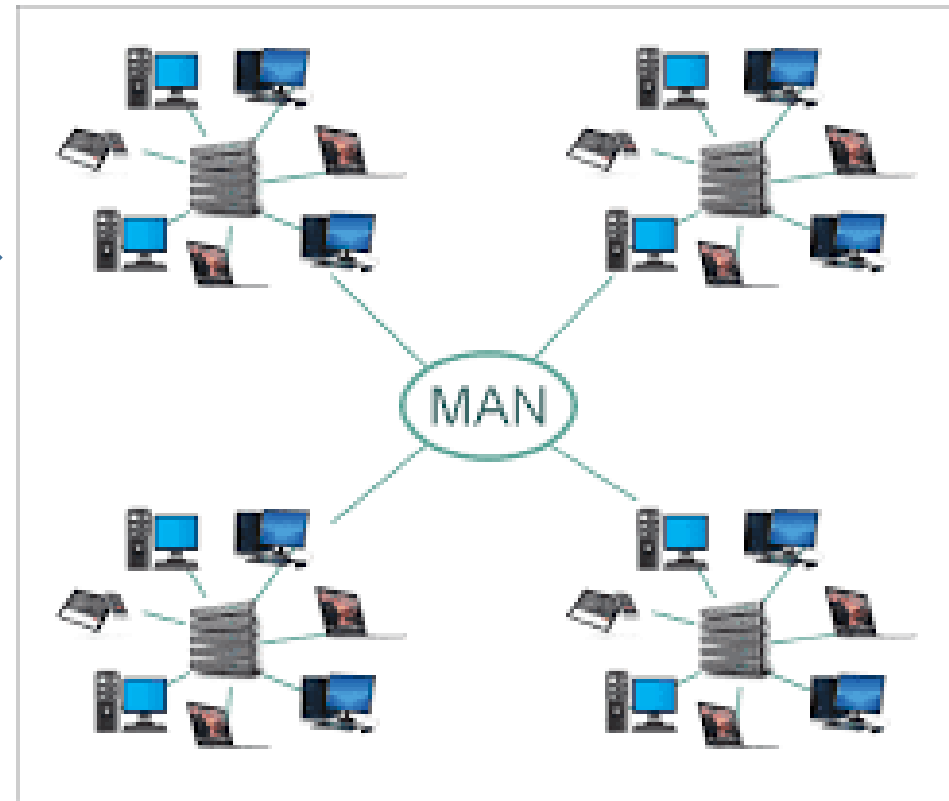
Wireless Local Area Networks - (WLAN)

Global Area Networks - (GAN)

Storage Area Networks - (SAN)

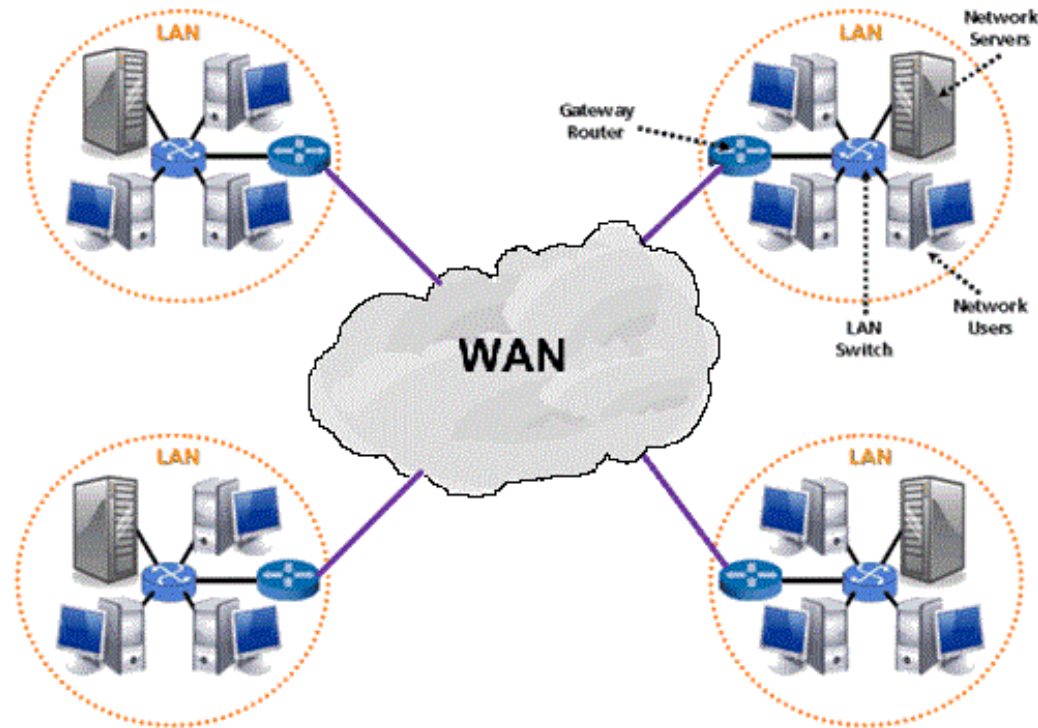
Chapter 01

Network Fundamentals



Chapter 01

Network Fundamentals



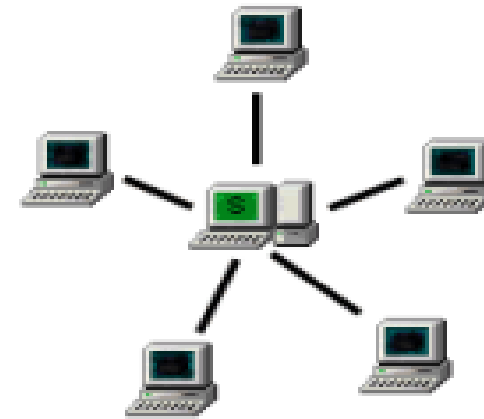
WAN - Wide Area Network



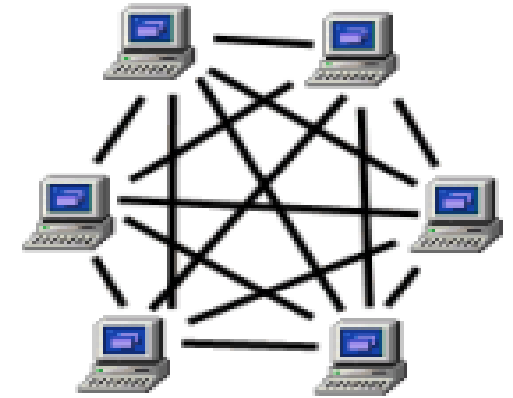
The **main difference** between peer to peer and client server network is that **in peer to peer network, each node can request for services and provide services** while in client server network, the client nodes requests for services and server node responds with services.

The devices in a network communicate with each other. Peer to peer and client server are two network types. In a client server network, multiple clients connect to a server. The clients require services, and the server provides required services. **On the other hand, in a peer to peer network, there are no specific clients or servers. Instead, all the nodes can act as clients or servers. In other words, each node can request for services and provides services.**

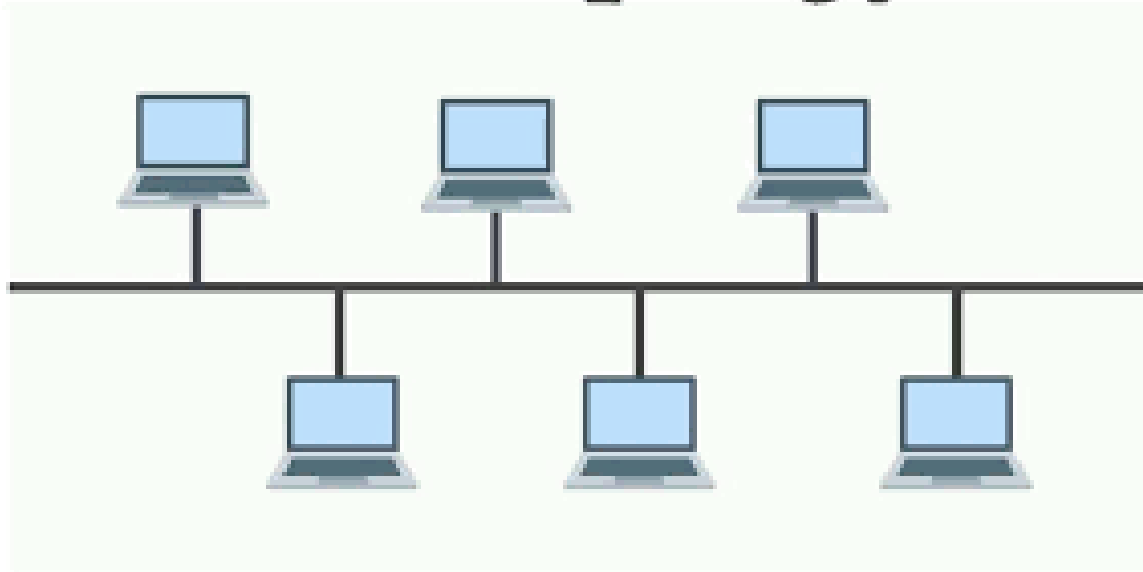
Server Based Network



Peer to Peer Network

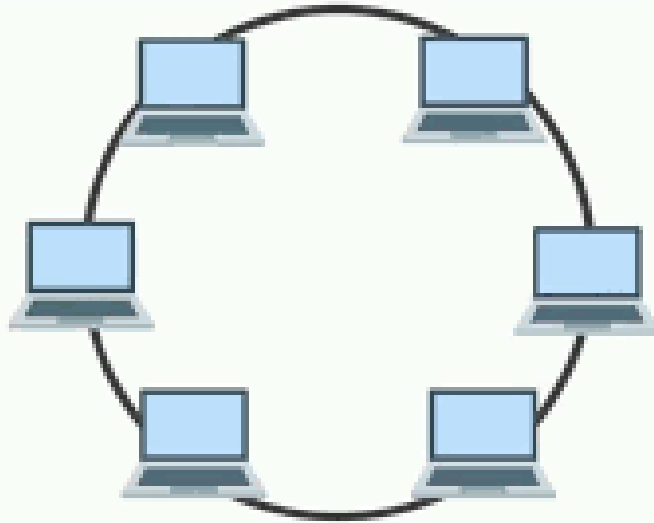


Bus Topology



A bus topology consists of a main central cable or 'backbone' as it is called, with a terminator at each end. All devices like workstations, printers, routers, servers, etc., are connected to the main cable through nodes in a linear configuration. The terminator is used at the end of the cable to absorb the signal thus preventing signal bounce.

Single-Ring Topology



A ring topology is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a ring network.

Ring topologies may be used in either [LANs](#) (local area networks) or [WANs](#) (wide area networks). Depending on the [network card](#) used in each computer of the ring topology, a [coaxial cable](#) or an [RJ-45](#) network cable is used to connect computers together.

Mesh Topology

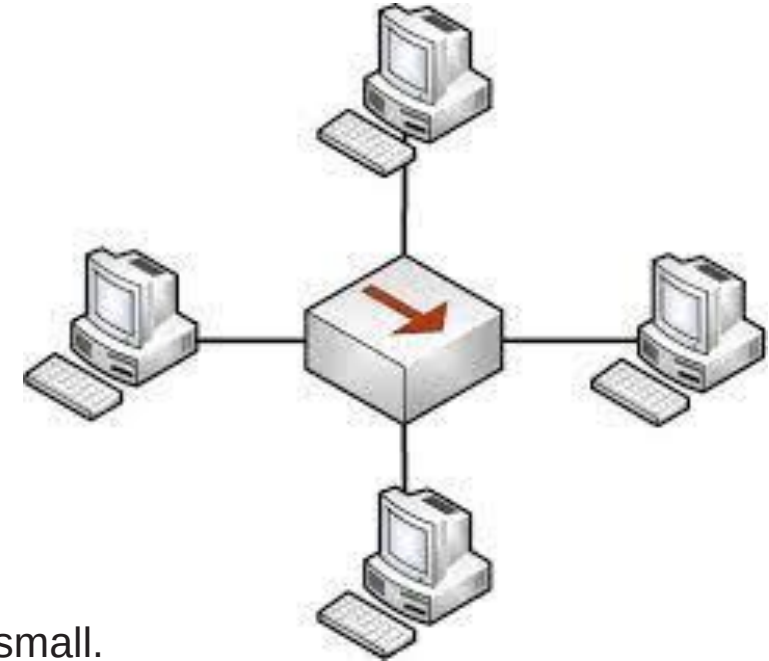


Mesh topology there is no central connection point. Instead, each **node** is connected to at least one other node and usually to more than one. Each node is capable of sending messages to and receiving messages from other nodes. The nodes act as relays, passing on a message towards its final destination. There are two types of mesh topology:

- full mesh topology
- partial mesh topology

Mesh networks are becoming increasingly popular due to their efficiency.

Star topology



Star topologies are used in many networks, large and small.

In a star topology all nodes indirectly connect to each other through one or more **switches**. The switch acts as a central point through which all communications are passed.

Large networks using a star topology are usually controlled by one or more **servers**. Hence, the **client-server** model usually uses a star topology. However, **peer-to-peer** networks can also have a star topology. Even though no single computer controls the network, all communications still pass through the central switch

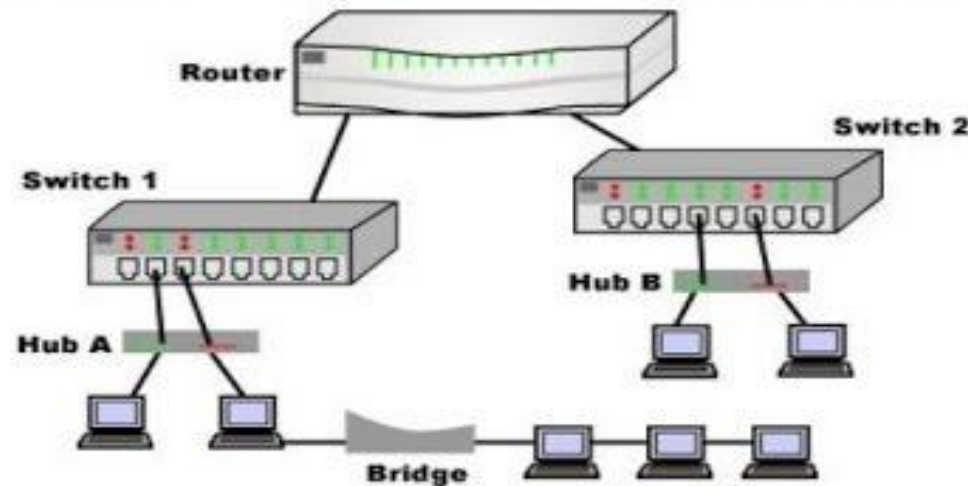
Hubs , Repeater: dump devices are sending signal to all hosts in network (broadcasting logical topology)

switches, bridges: straight forwarding devices are sending signal from source to destination in network (unicast logical topology)

source: sender

Destination: receiver

Network Devices- repeaters, hubs, switches bridges



Physical media

Cables types

1.Coaxial cables

Types of Coaxial :core of coaxial

1.**Thin** : maximum distance of signal 185 m

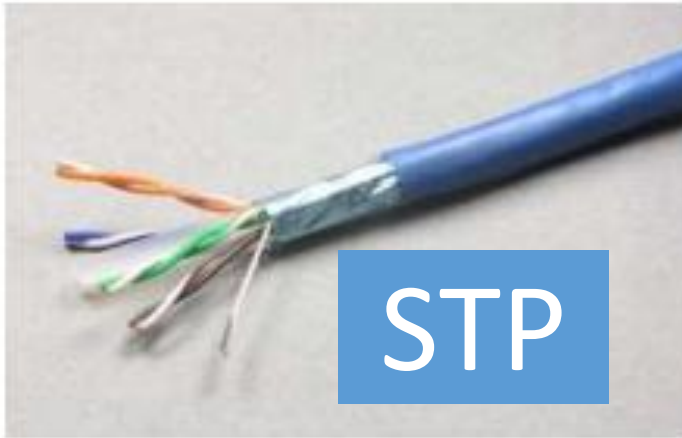
2.**Thick**:: maximum distance of signal 500 m

both of them are used in bus topology with 10MBPS

2.Twisted pair: STP /UTP

3.Fiber optics

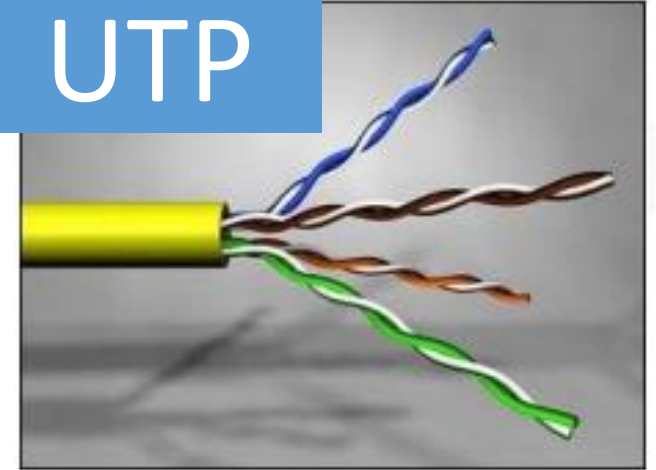




تستخدم الكابلات STP و UTP مشبك من نوع RJ-45



UTP



The basic difference between UTP and STP is UTP (Unshielded twisted pair) is a cable with wires that are twisted together to reduce noise and crosstalk. On the contrary, STP (Shielded twisted pair) is a twisted pair cable confined in foil or mesh shield that guards the cable against electromagnetic interference.

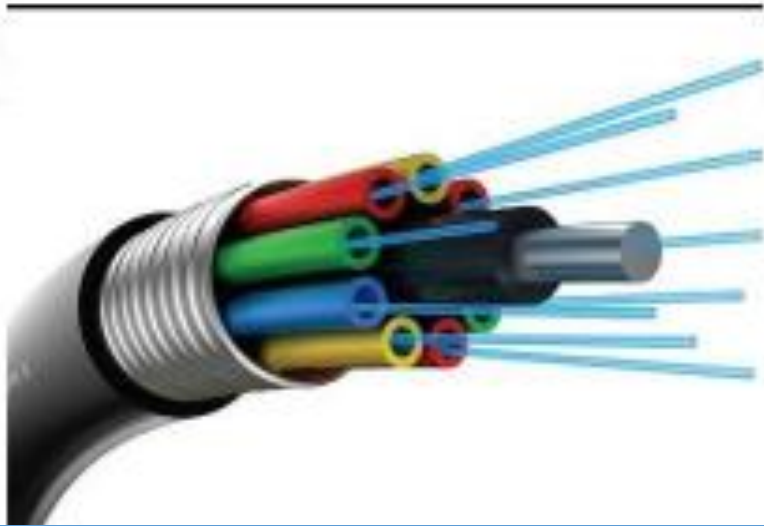
Types of UTP cables

CAT3: Rarely used today, CAT3 is usually deployed in phone lines. ...

CAT4: Typically used in token ring networks, CAT4 supports 16 Mbps for up to 100 meters.

CAT5: Used in Ethernet-based LANs, CAT5 contains two twisted pairs. ...

CAT5e: Used in Ethernet-based LANs, CAT5e contains four twisted pairs.



Fiber optics

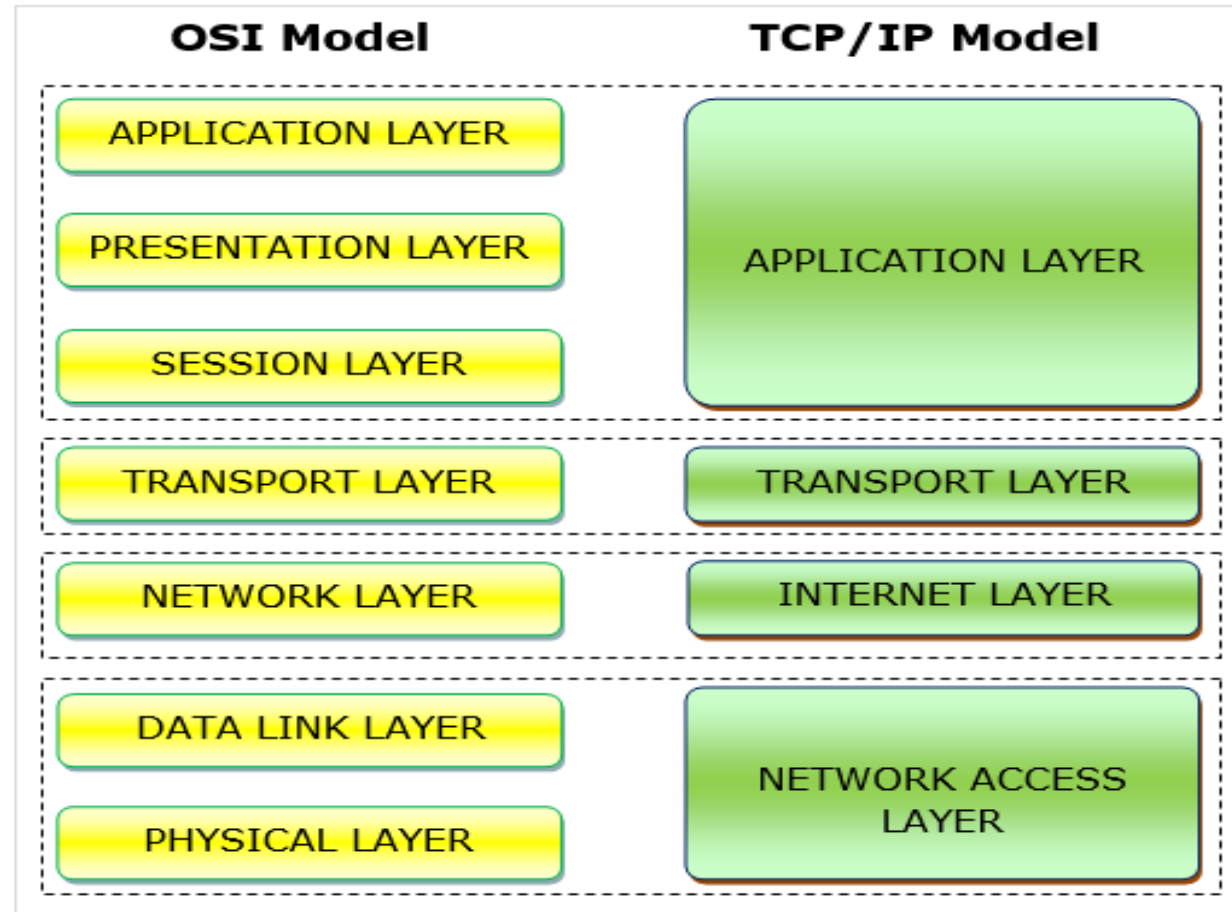
Fiber optics is the technology used to transmit information as pulses of light through strands of fiber made of glass or plastic over long distances.

There are several different types of fiber-optic networks but they all begin with optic cables running from the network hub to the curb near your home or straight to your home to provide a fiber-optic internet connection. The fastest type of fiber network is called Fiber to the Home (FTTH) or Fiber to the Premises (FTTP) because it's a 100% fiber-optic connection with optical fiber cables installed to terminals directly connected to houses, apartment buildings and businesses.

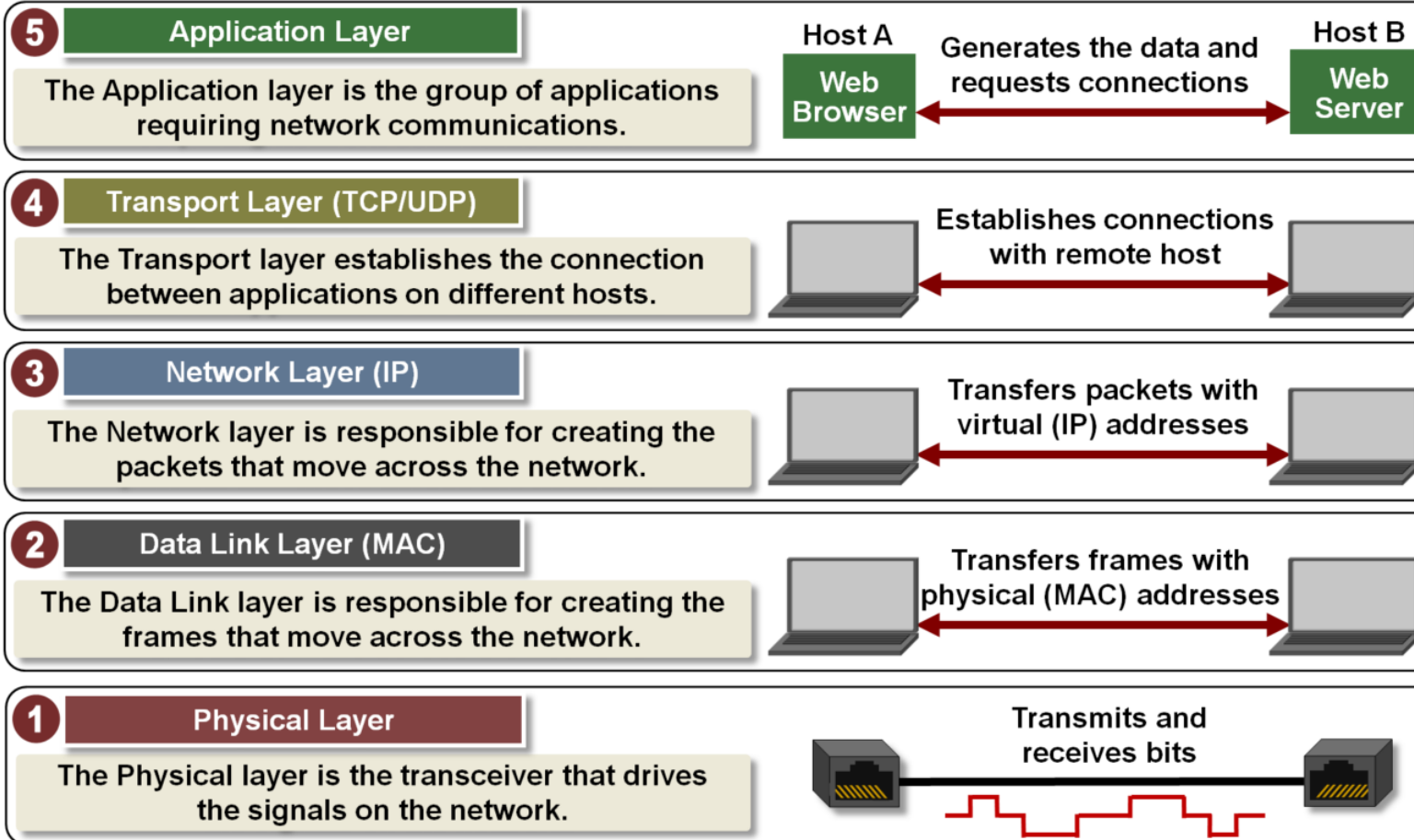
Chapter 01

Network Fundamentals (OSI Model)

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium



Network Fundamentals (OSI Model)



7. Application Layer

- ❖ The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive [information and present meaningful data to users](#). A few examples of application layer protocols are the [Hypertext Transfer Protocol](#) (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. Presentation Layer

- ❖ The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

7. Application Layer

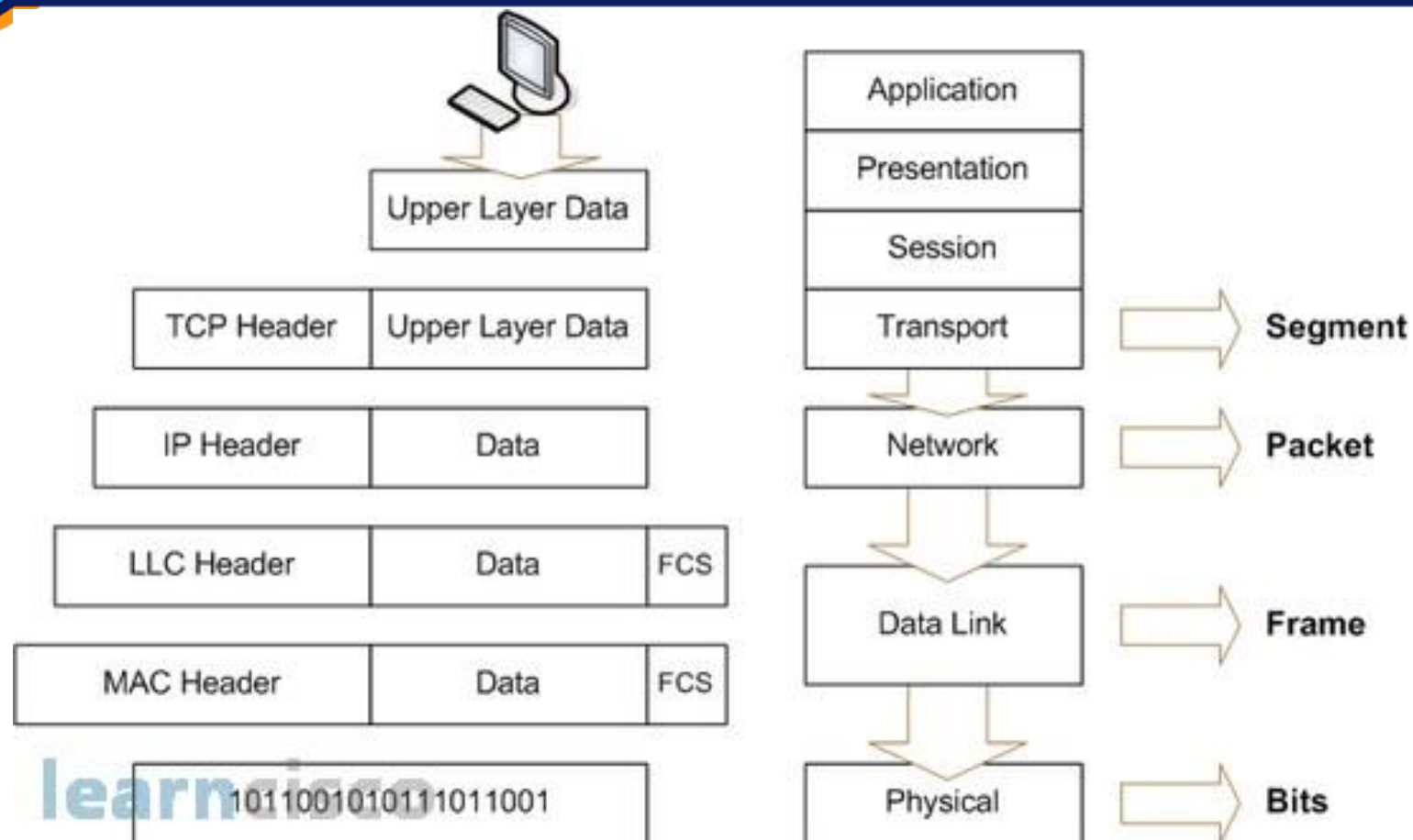
- ❖ The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive [information and present meaningful data to users](#). A few examples of application layer protocols are the [Hypertext Transfer Protocol](#) (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. Presentation Layer

- ❖ The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

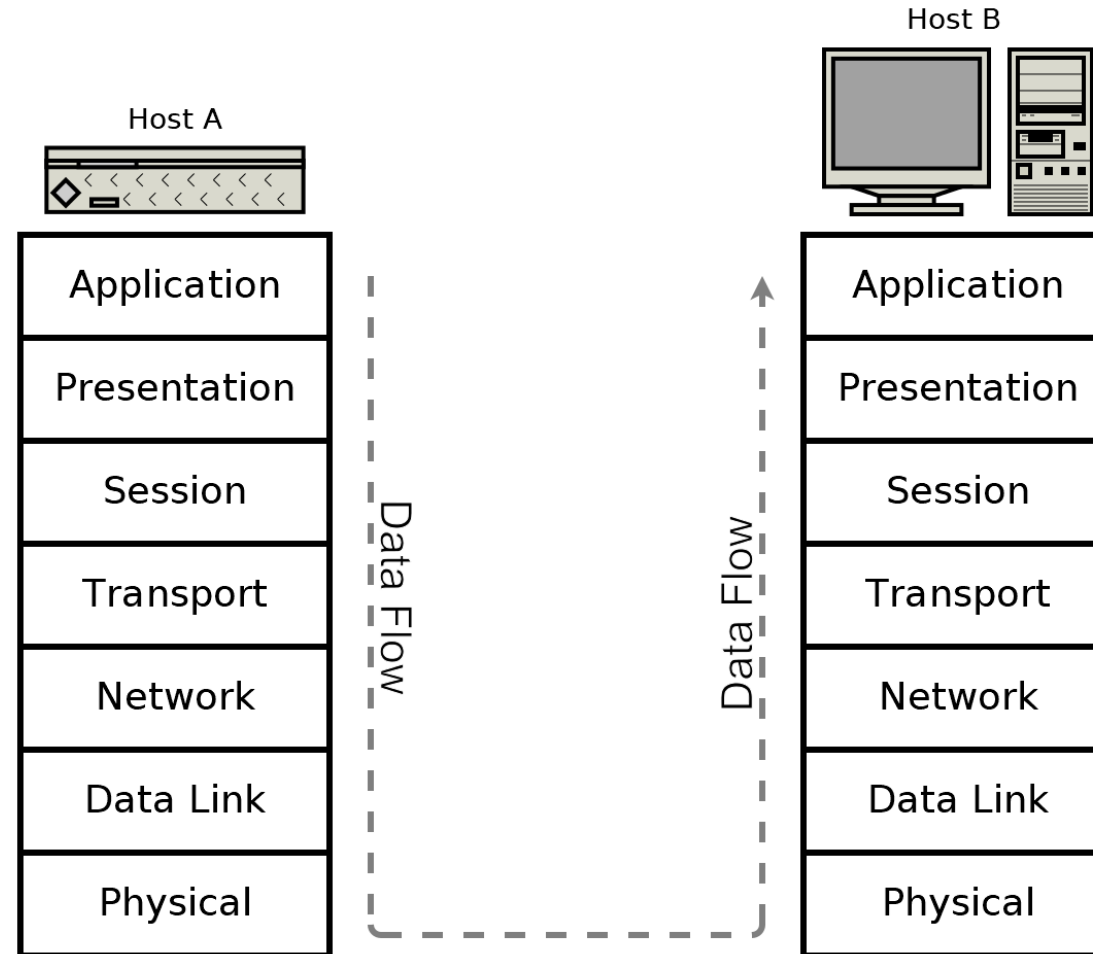
Chapter 01

Network Fundamentals / OSI Model(Encapsulation data)

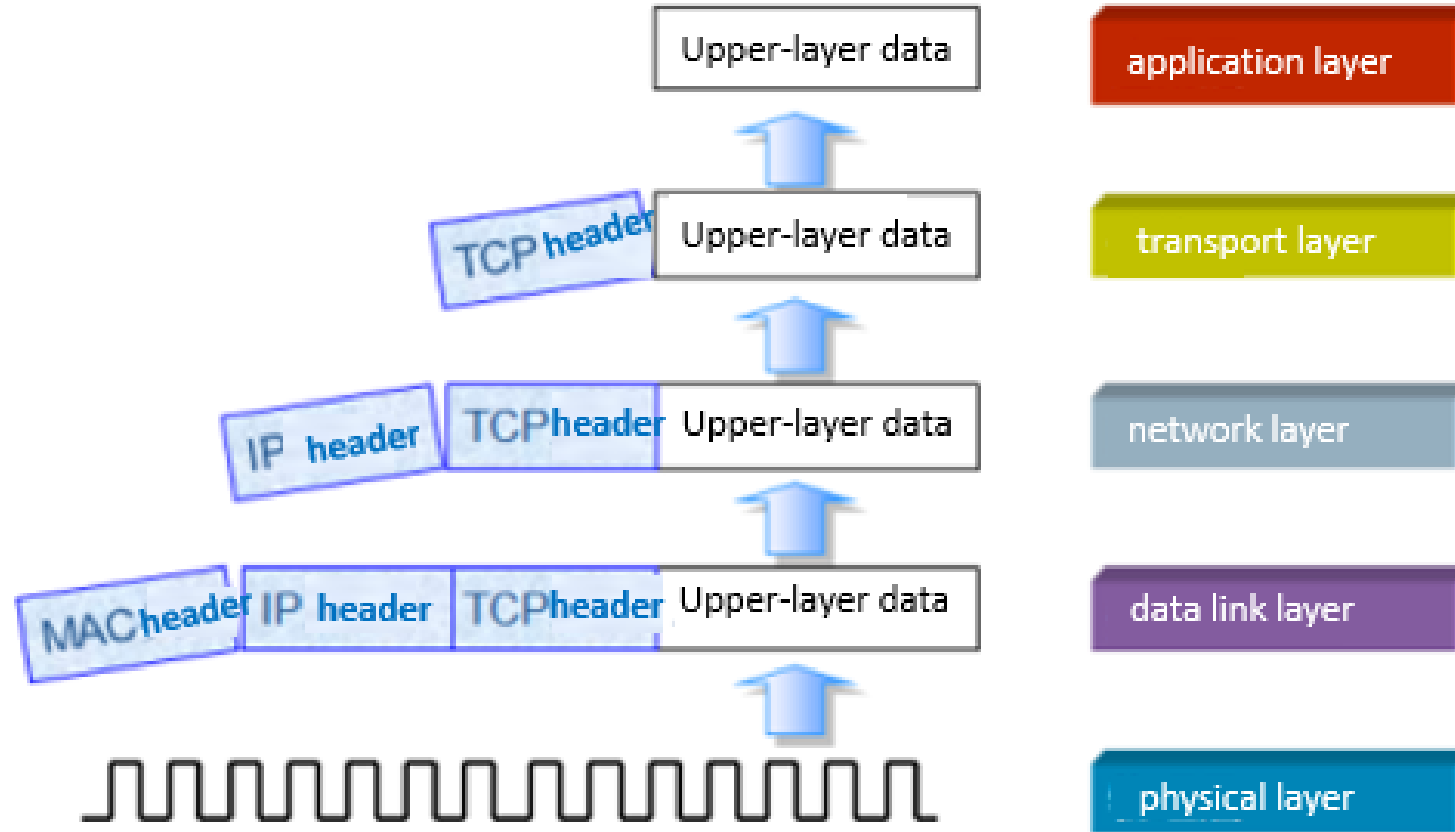


Chapter 01

Network Fundamentals (OSI Model)



De capsulation data



7. Application Layer

- ❖ The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. Presentation Layer

- ❖ The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

Domain Name System

The Domain Name System (DNS) works on Client Server model. It uses UDP protocol for transport layer communication. DNS uses hierarchical domain based naming scheme. The DNS server is configured with Fully Qualified Domain Names (FQDN) and email addresses mapped with their respective Internet Protocol addresses.

A DNS server is requested with FQDN and it responds back with the IP address mapped with it. DNS uses UDP port 53.

Simple Mail Transfer Protocol

The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.



Hyper Text Transfer Protocol (HTTP)

The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.

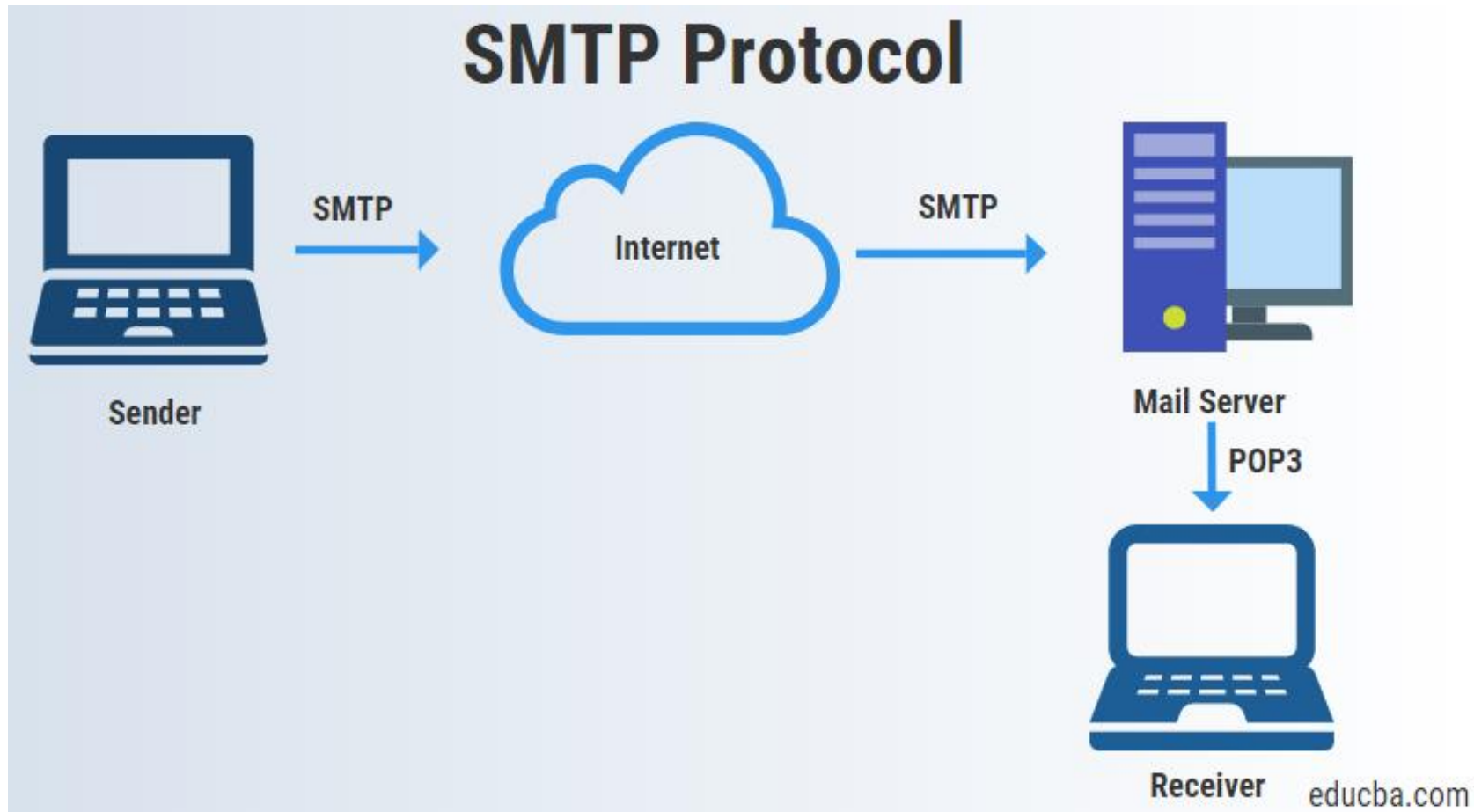
To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

HTTP versions

HTTP 1.0 uses non persistent HTTP

HTTP 1.1 uses persistent HTTP. In this version, multiple objects can be sent over a single TCP connection.



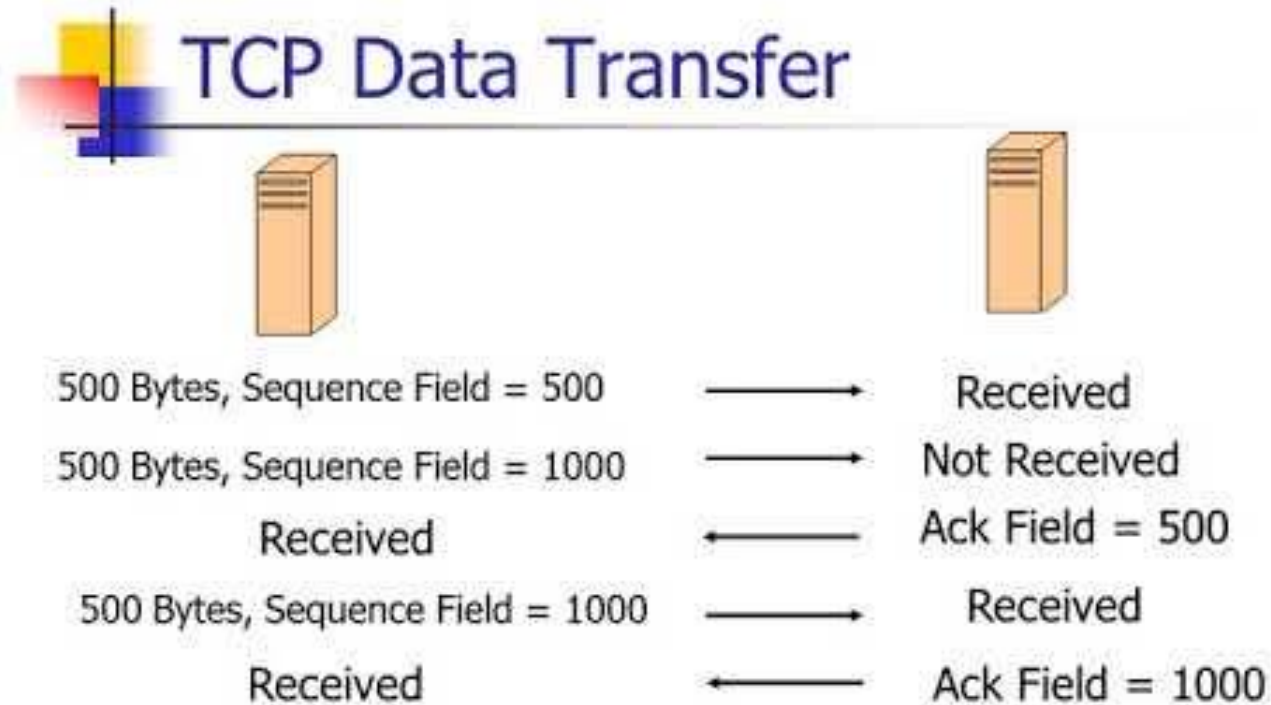


5. Session Layer

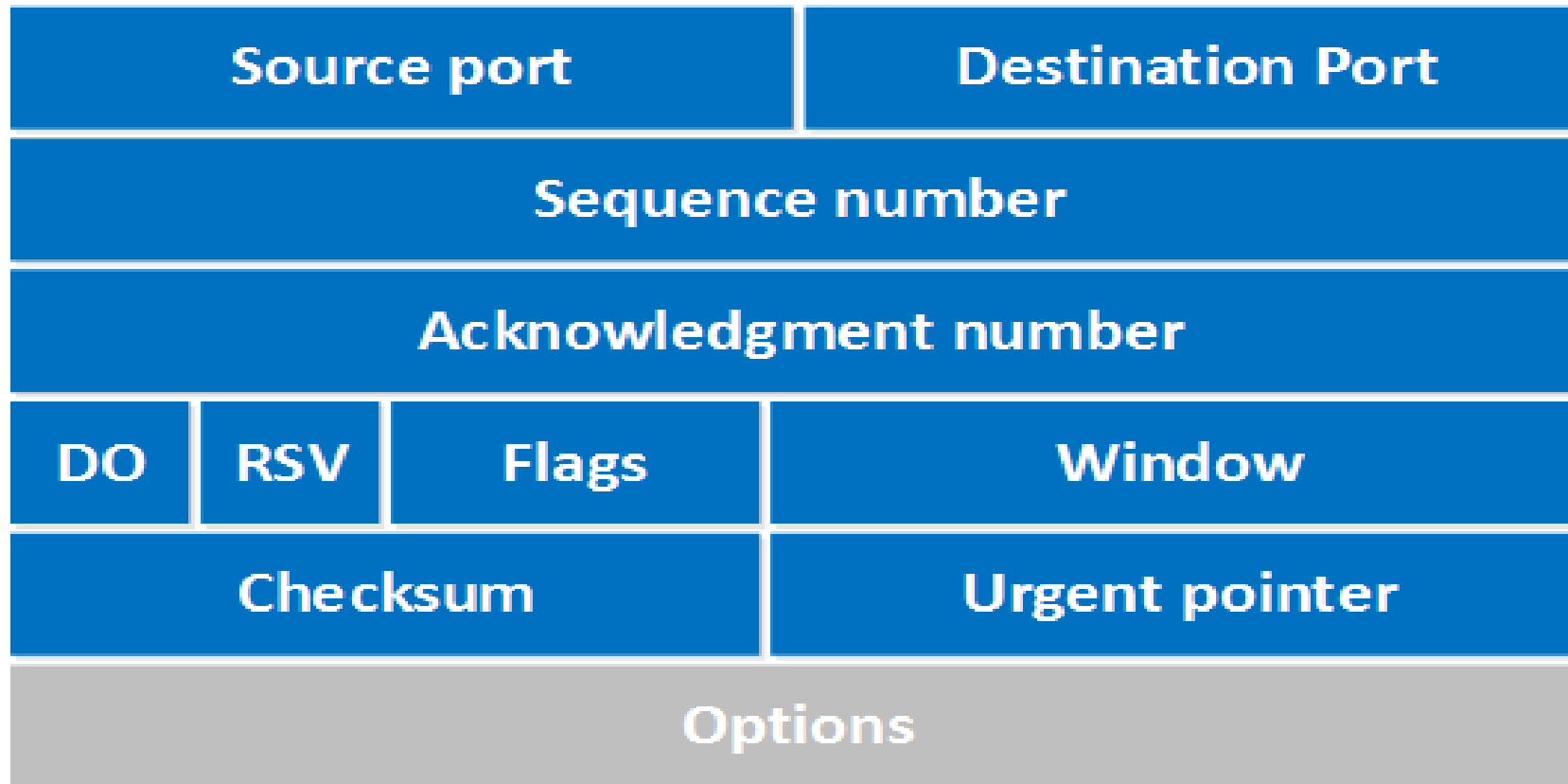
- ❖ The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

4. Transport Layer

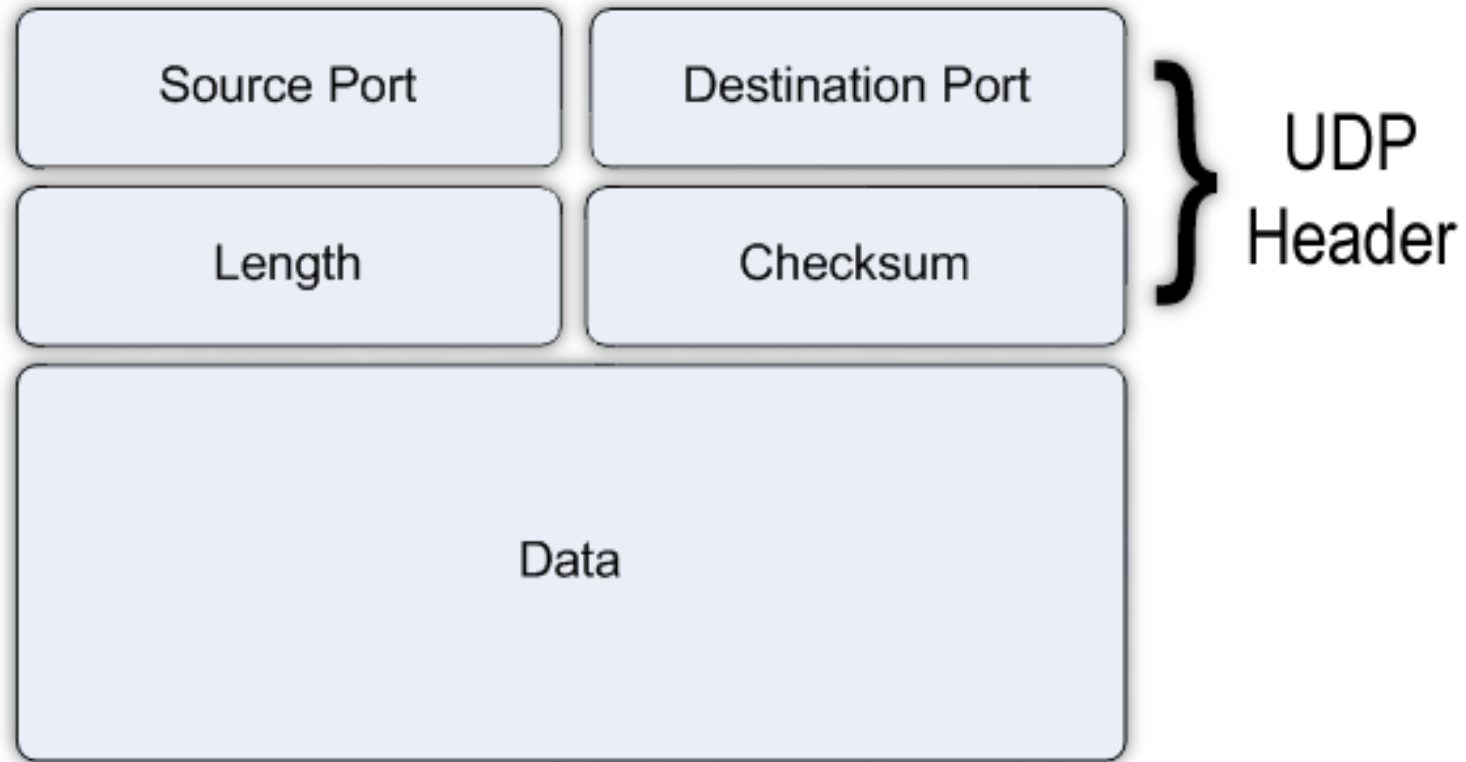
- ❖ The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.



TCP header



UDP header



UDP header

UDP has a number of benefits for different types of applications, including:

- **No retransmission delays** – UDP is suitable for time-sensitive applications that can't afford retransmission delays for dropped packets. Examples include Voice over IP (VoIP), online games, and media streaming.
- **Speed** – UDP's speed makes it useful for query-response protocols such as DNS, in which data packets are small and transactional.
- **Suitable for broadcasts** – UDP's lack of end-to-end communication makes it suitable for broadcasts, in which transmitted data packets are addressed as receivable by all devices on the internet. UDP broadcasts can be received by large numbers of clients without server-side overhead.

3. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node. Protocols (IP, ARP and ICMP).

2. Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.



Data link layer and error detection

The data link layer ensures an initial connection has been set up, divides output data into data frames and handles the acknowledgements from a receiver that the data arrived successfully. It also ensures incoming data has been received successfully by analyzing bit patterns at special places in the frames.

If an error occurs, the data link layer notifies higher-level protocols that something has happened to the physical link. Frame sequencing capabilities within the data link layer permit the receiving device to reorder frames that might have been transmitted out of sequence. The data link layer verifies the packet is unimpaired.

The data link layer also manages flows by enabling devices on a link to detect congestion.

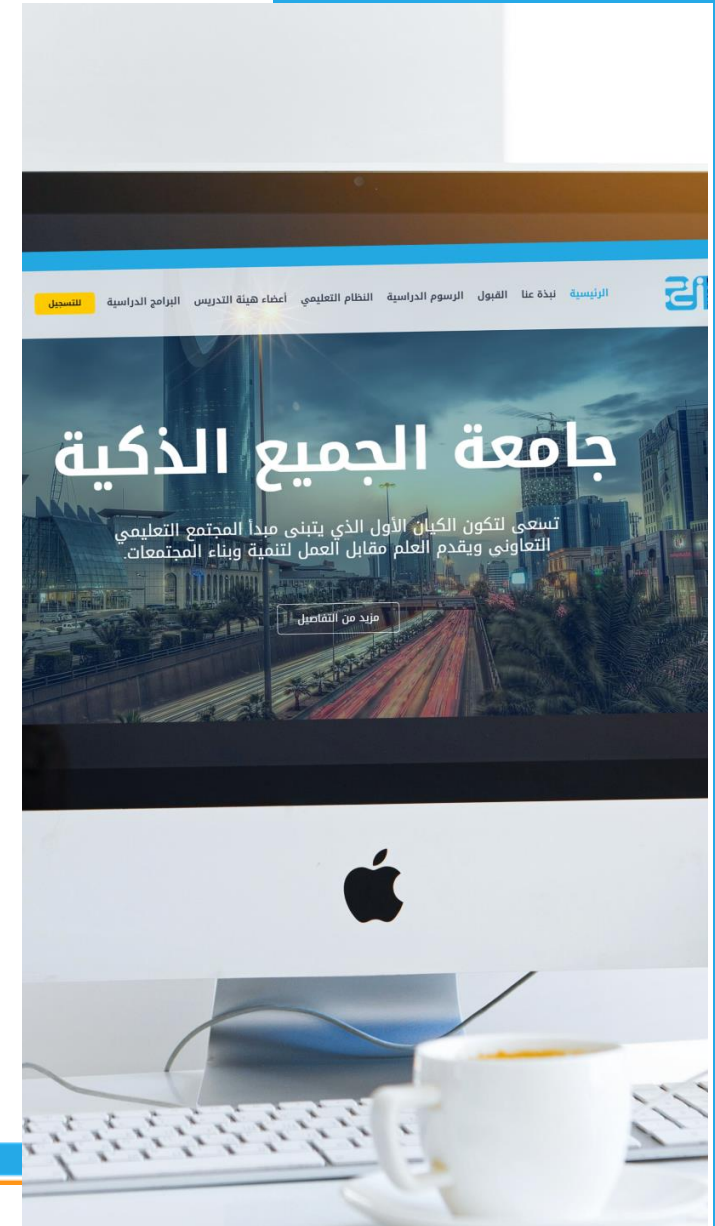
Nearby devices then transmit congestion information, so traffic can be rerouted accordingly

What is a MAC Address

Whether you work in a wired network office or a wireless one, one thing is common for both environments: It takes both network software and hardware (cables, routers, etc.) to transfer data from your computer to another—or from a computer thousands of miles away to yours. And in the end, to get the data you want right to YOU, it comes down to addresses. So not surprisingly, along with an IP address (which is networks software), there's also a hardware address. Typically it is tied to a key connection device in your computer called the network interface card, or NIC. The NIC is essentially a computer circuit card that makes it possible for your computer to connect to a network. A NIC turns data into an electrical signal that can be transmitted over the network.

1. Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.



Thanks



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY