



**ITI**

**Introduction to  
Computer Networks & Cyber Security  
Prepared By : Mohamed AboSehly**

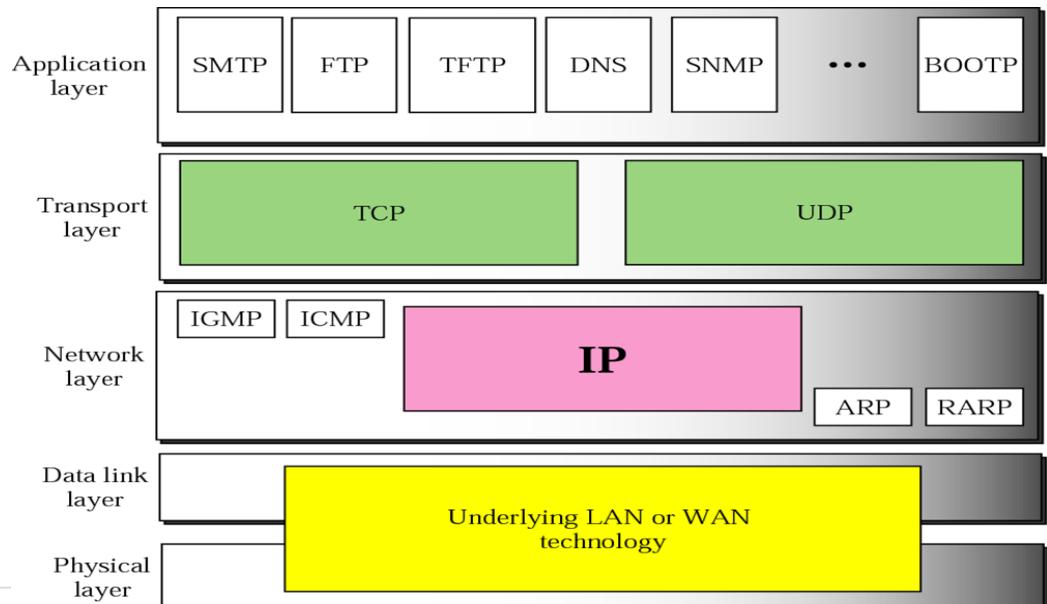
# Part 1 (TCP/IP Protocol Architecture)

## Application Layer

# Part 1 (TCP/IP Protocol Architecture)

## TCP/IP Protocol Architecture

- Application Layer
  - Communication between processes or applications



## Application Layer Protocols

- File transfer
  - FTP
  - TFTP
  - Network File System
- E-mail
  - Simple Mail Transfer Protocol
- Remote login
  - Telnet
  - rlogin
- Network management
  - Simple Network Management Protocol
- Name management
  - Domain Name System

# Part 1 (TCP/IP Protocol Architecture)



## Internet Services (Client/Web Server)

- The World Wide Web: HTTP
- Naming Service: DNS
- File Transfer: FTP
- Telnet Service
- Electronic Mail service: IMAP, POP3, SMTP

Client	Protocol	Server	Port No
Browser	HTTP	WEB	80
Browser	FTP	FTP	21
Browser Or Outlook Express Microsoft Outlook	HTTP SMTP POP3 IMAP4	Mail	110 143 25
Telnet	Telnet	Telnet	23

# Part 1 (TCP/IP Protocol Architecture)

## HTTP Protocol

- Hyper Text Transfer Protocol
- Supports the delivery of web pages to the client



# Part 1 (TCP/IP Protocol Architecture)



## Browser as a web client

- Use Internet Browser as WEB client.



# Part 1 (TCP/IP Protocol Architecture)



## URL



`https://www.microsoft.com/ar-ww/microsoft-365/`

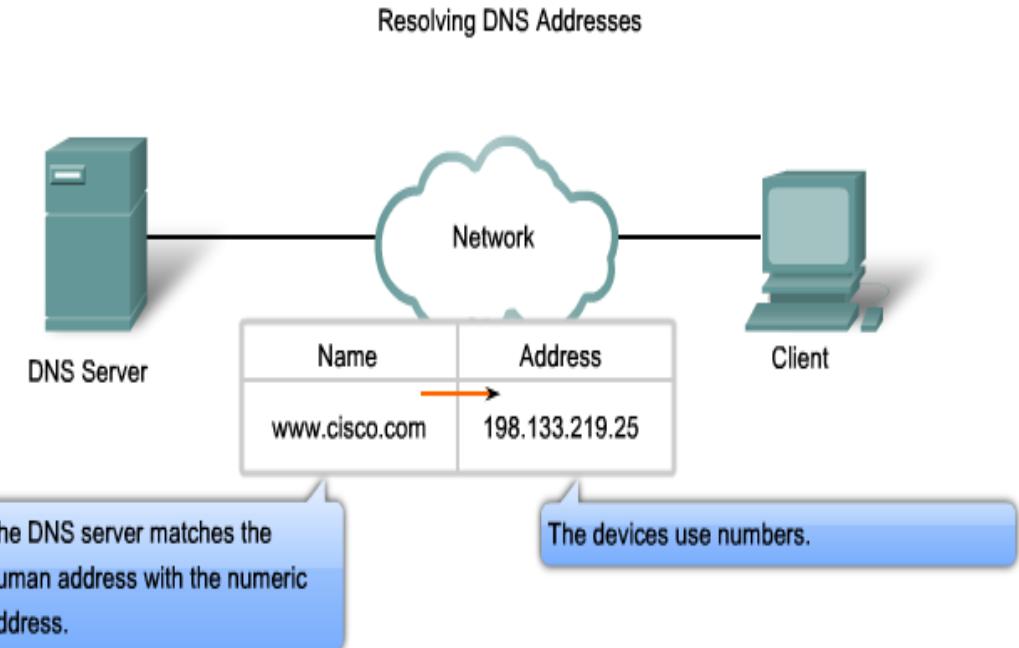
- URL is **Universal Resource Locator**
- **Protocol** : HTTP, HTTPS or FTP
- **Host** : is the domain name of the computer on which the information is located .
- **Port**: The URL can optionally contain the port number of the server
- **Path**: is the pathname of the file where the information is located

# Part 1 (TCP/IP Protocol Architecture)



## DNS

- Domain Name Servers
  - Application specified in the TCP/IP suite
  - A way to translate **human-readable** names into **IP addresses**



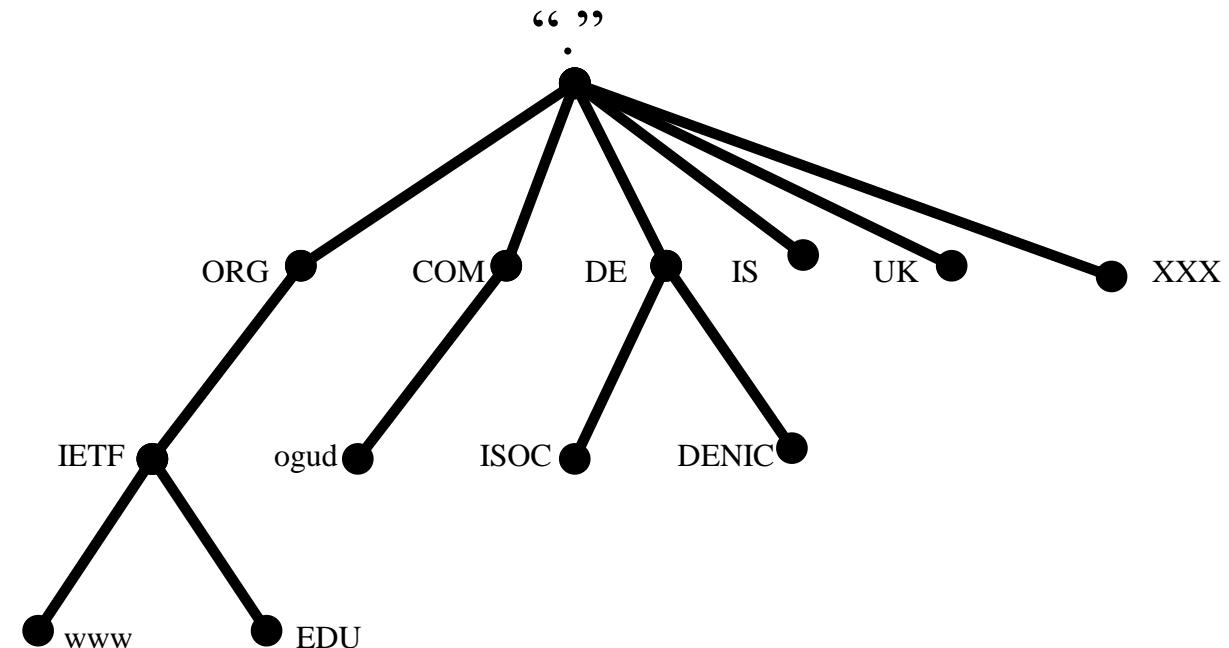
# Part 1 (TCP/IP Protocol Architecture)



## List of Top Level Domains (TLDs)

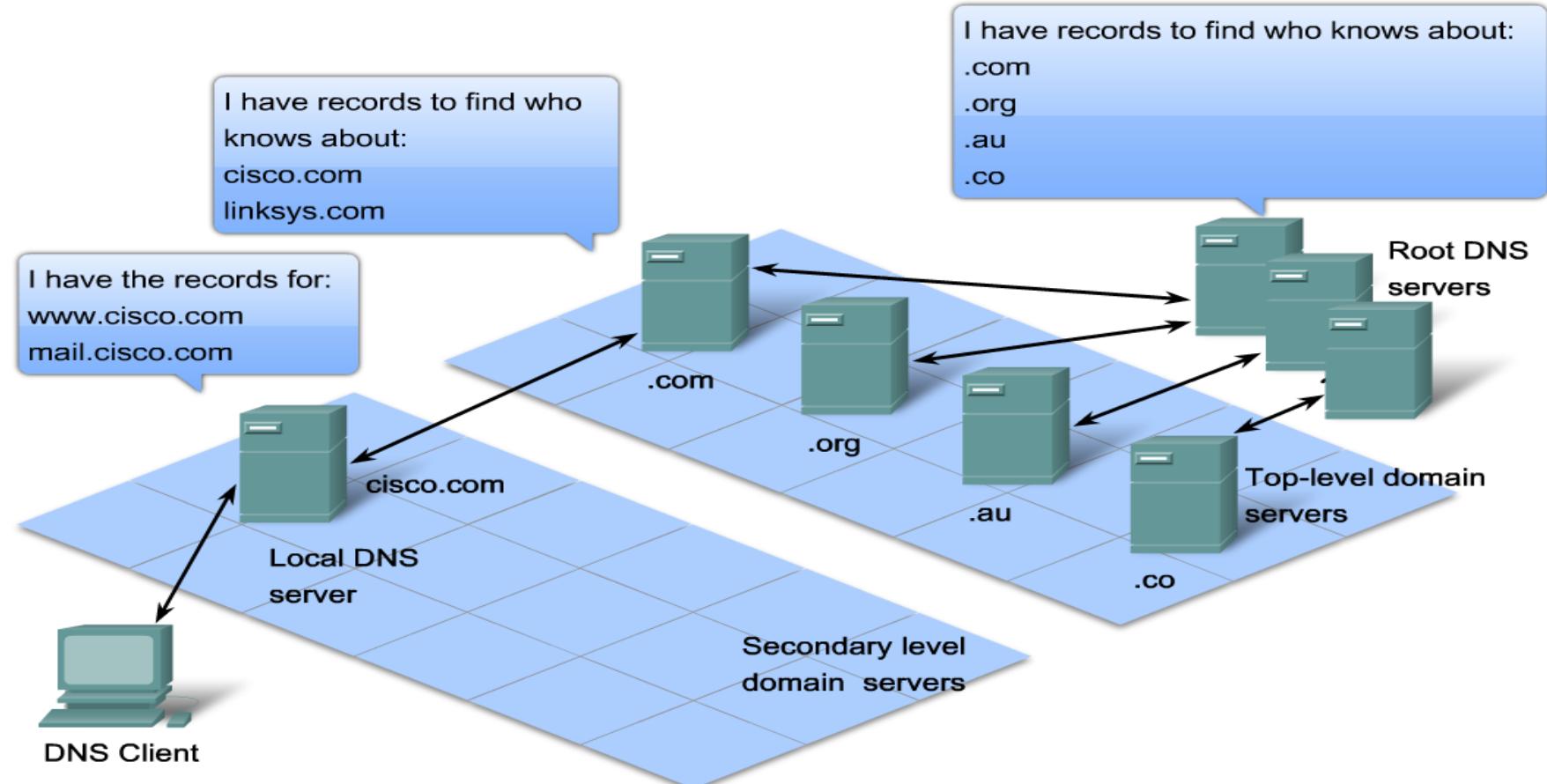
Domain Name	Assigned To
<i>com</i>	<i>Commercial organization</i>
<i>edu</i>	<i>Educational institution</i>
<i>gov</i>	<i>Government organization</i>
<i>mil</i>	<i>Military group</i>
<i>net</i>	<i>Major network support center</i>
<i>org</i>	<i>Organization other than those above</i>
<i>country code</i>	<i>A country</i>

## DNS Tree



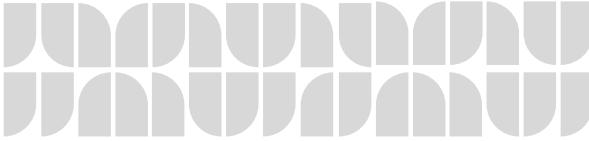
# Part 1 (TCP/IP Protocol Architecture)

## DNS Query



A hierarchy of DNS servers contains the resource records that match names with addresses.

# Part 1 (TCP/IP Protocol Architecture)



## How DNS works?

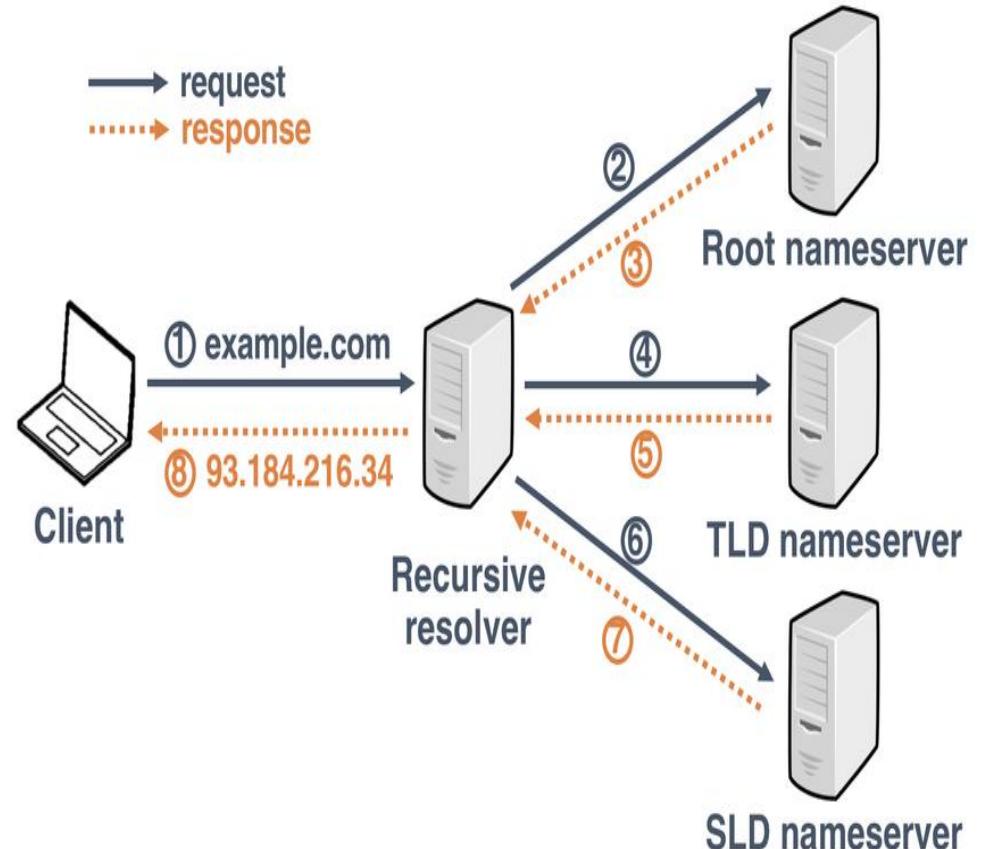
- At the beginning they use Hosts file, It maps the IP addresses to host names
- It is found at **C: Windows\System32\drivers\etc**
  - **Problems:**
    - Huge number of hosts
    - Update very dynamic
    - Searching will be too slow
- **So hosts file can be used in local networks**
- DNS Server is used for **centralize** the Domain Name Servers.
- DNS are used to convert the **addresses** into **IP addresses and vice versa**

# Part 1 (TCP/IP Protocol)

## DNS Lookup

How the client get the website:

- 1- check the cash
- 2- check the hosts file
- 3- Ask DNS server



# Basic Network Elements (Software) -



## Nslookup

- nslookup is the name of a program that lets you to **enter a host name** and **find out the corresponding IP address**

```
C:\> C:\Windows\system32\cmd.exe - nslookup
C:\Users\nour>nslookup
Default Server: vnsc-bak.sys.gtei.net
Address: 4.2.2.2:53

> www.google.com
Server: vnsc-bak.sys.gtei.net
Address: 4.2.2.2:53

Non-authoritative answer:
Name: www.l.google.com
Addresses: 64.239.161.147, 64.239.161.99, 64.239.161.103, 64.239.161.104
Aliases: www.google.com

> www.yahoo.com
Server: vnsc-bak.sys.gtei.net
Address: 4.2.2.2:53

Non-authoritative answer:
Name: www.yahoo-ht3.akadns.net
Address: 69.147.114.210
Aliases: www.yahoo.com

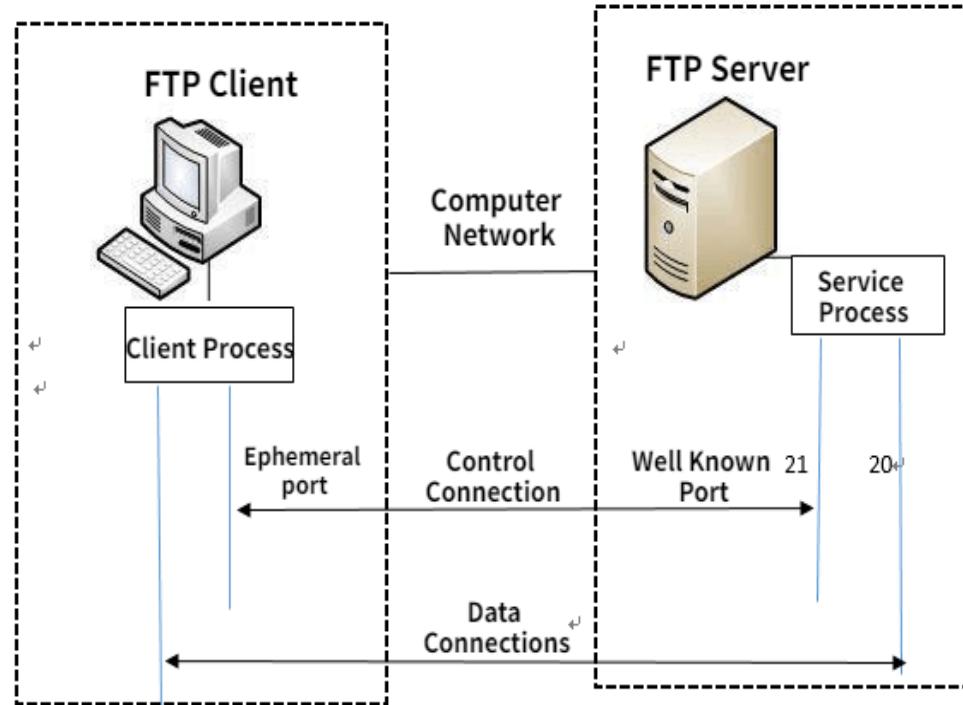
>
```

# Part 1 (TCP/IP Protocol Architecture)



## FTP

- File Transfer Protocol
- a transmission protocol that provides **reliable data transfer between hosts.**
- The default FTP port is
  - Port 21 for command and control,
  - Port 20 for data transport.



Working Principle of FTP

# Part 1 (TCP/IP Protocol)

## FTP

### FTP Client

- Browser as a FTP client
  - **Use Internet Browser as FTP client.**
  - Using **MS Windows** built-in FTP client (CLI)
  - Third party programs “FileZilla *FTP*”



```
C:\Windows\system32\cmd.exe - ftp
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\nour>ftp
ftp> open 163.121.12.40
Connected to 163.121.12.40.
220 Microsoft FTP Service
User (163.121.12.40:(none)): user
331 Password required for user.
Password:
230 User user logged in.
ftp>
```

open

ls

cd

bin

get

mget

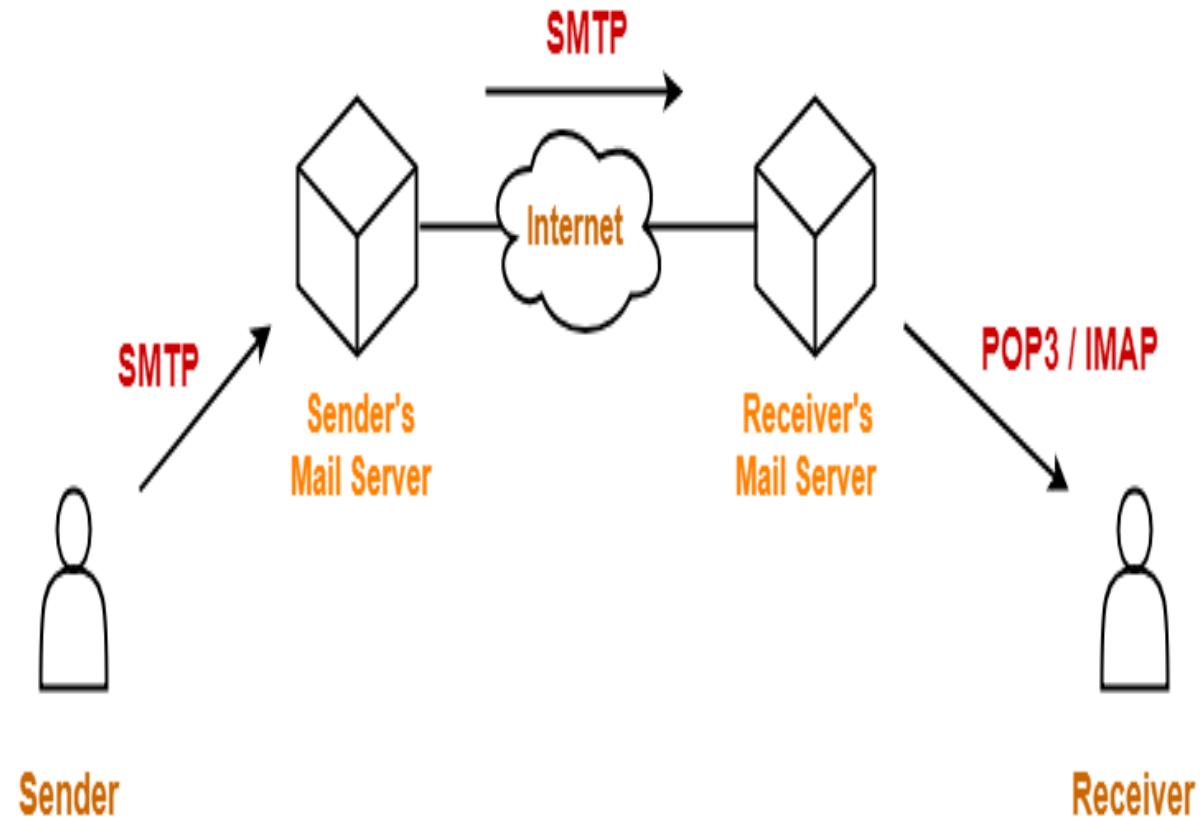
Put

bye

## Mail Server and Clients

### ❖ Mail Clients

- **Web based**
  - Hotmail
  - gmail
- **Non web based**
  - Microsoft Outlook



# Part 1 (TCP/IP Protocol)



## Mail Protocols

- **SMTP (send mail transfer Protocol)**
  - It is the common language used by the majority of Mail Servers to send messages back and forth to other Mail Servers or Email Clients
- **POP3 “Post Office Protocol version 3”**
  - In order to collect email messages from the Mail Server, the Email Client contacts the Mail Server.
  - Download messages on the hard disk
  - You can work Offline
  - Keep the user’s quota on the server
- **IMAP4 “Internet Message Access Protocol version 4”**
  - Retrieve only message header

# Part 1 (TCP/IP Protocol Architecture)



## Telnet (23)/SSH(22)

- Telnet/ssh is a user command and an underlying TCP/IP protocol for accessing remote computers.
- Through Telnet/ssh, an administrator can access someone else's computer remotely

### Telnet client (not secure)

- Built in MS-Windows Telnet client
- Third party programs

# Part 1 (TCP/IP Protocol)



- **RDP**

- **Remote Desktop Protocol (RDP)** is a Microsoft proprietary protocol that enables remote connections to other computers,



# Part 1\_Network Elements (Hardware)



## Network Hardware

Devices

Medium

# Part 1\_Network Devices ( Hardware )

## ❖ Computers / Peripherals

Any device that can connect to network with NIC

Ex: Computer

- ✓ Mobile
- ✓ Laptop-
- ✓ Printers-
- ✓ Cameras
- ✓ smart TV
- ✓ - .....etc



# Part 1\_Network Devices ( Hardware )

## NIC (Network Interface Card)

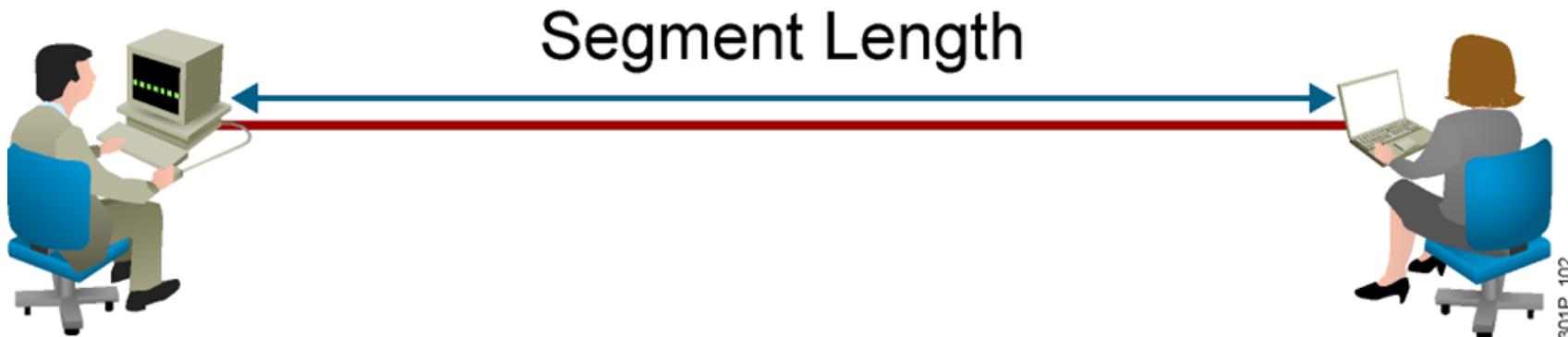
- Called **network interface controller, network adapter or LAN adapter.**
- Operate at **the physical layer of OSI/RM**
- hardware component without a computer cannot be connected over a network cable (interface between the PC and the network )
- Resides in the motherboard of the PC
  - **Internal NIC** (plugs into the motherboard directly )
  - **External NIC** (Wireless and USB based )
- Have A physical Address burned on the card called Mac.



# Part 1\_Network Devices ( Hardware )



## LAN Segment Limitations



- Signals degrade with transmission distance.
- Each Ethernet type has a maximum segment length.

# Part 1\_Network Devices ( Hardware )

## ❖ Repeater

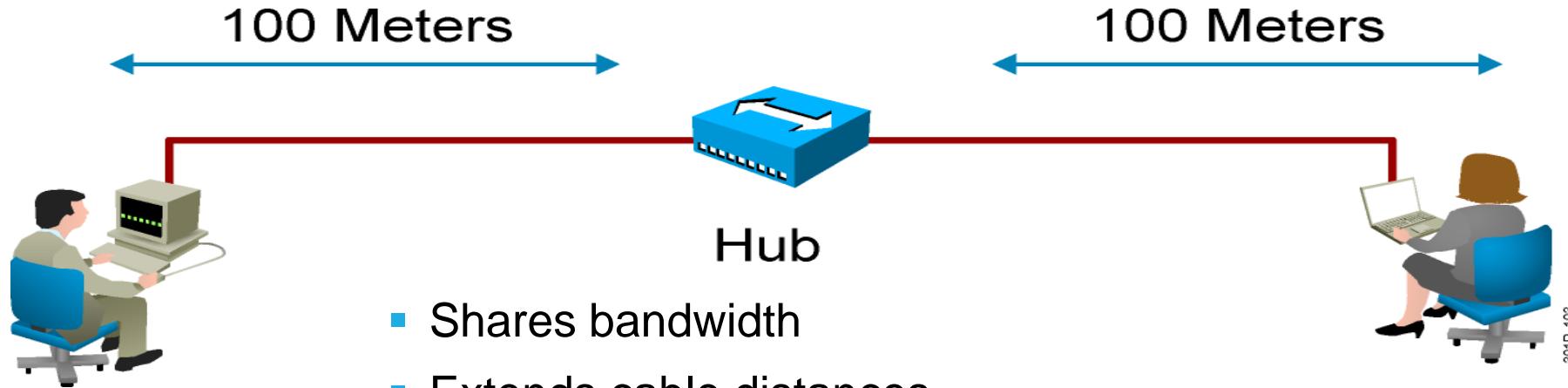
- Operates at the **physical layer**.
- **Regenerate** the **signal** over the **same network** before the signal becomes too **weak or corrupted**
- Only extend the length of the signal to its original strength
- Does not amplify the signal.
- 2 port device.



# Part 1\_Network Devices ( Hardware )



## Extending LAN Segments



Hub

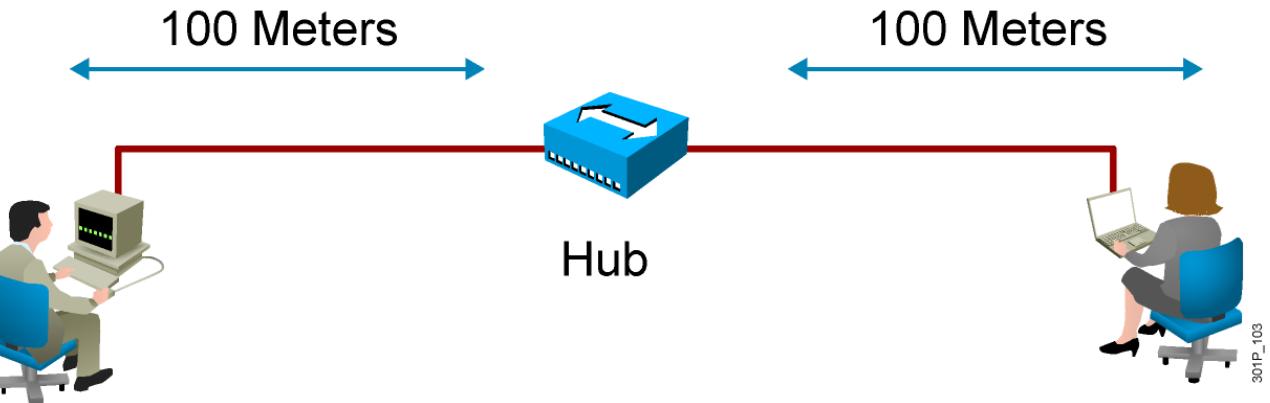
- Shares bandwidth
- Extends cable distances
- Repeats or amplifies signal
- **It is layer 1 device**
- It work only with bits
- Must work with **half duplex** communication

301P\_103

# Part 1\_Network Devices ( Hardware )

## ❖ Hub

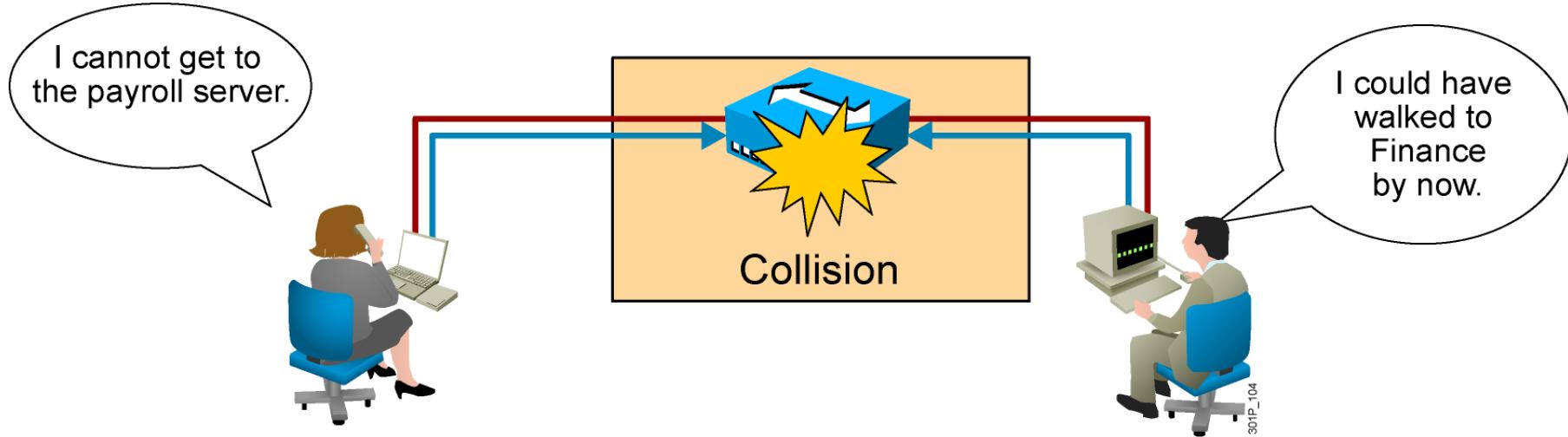
- It is **multi port repeater**
- Shares bandwidth
- Extends cable distances
- Repeats or amplifies signal
- It is **layer 1 device**
- It work **only with bits**
- Must work with **half duplex** communication
- It works by **flooding**



# Part 1\_Network Devices ( Hardware )



## Collisions



- All ports of the hub have the same collision domain and broadcast domain.
- **Collisions makes the network very slow and congested**

# Part 1\_Network Devices ( Hardware )

## CSMA/CD

### Carrier sense

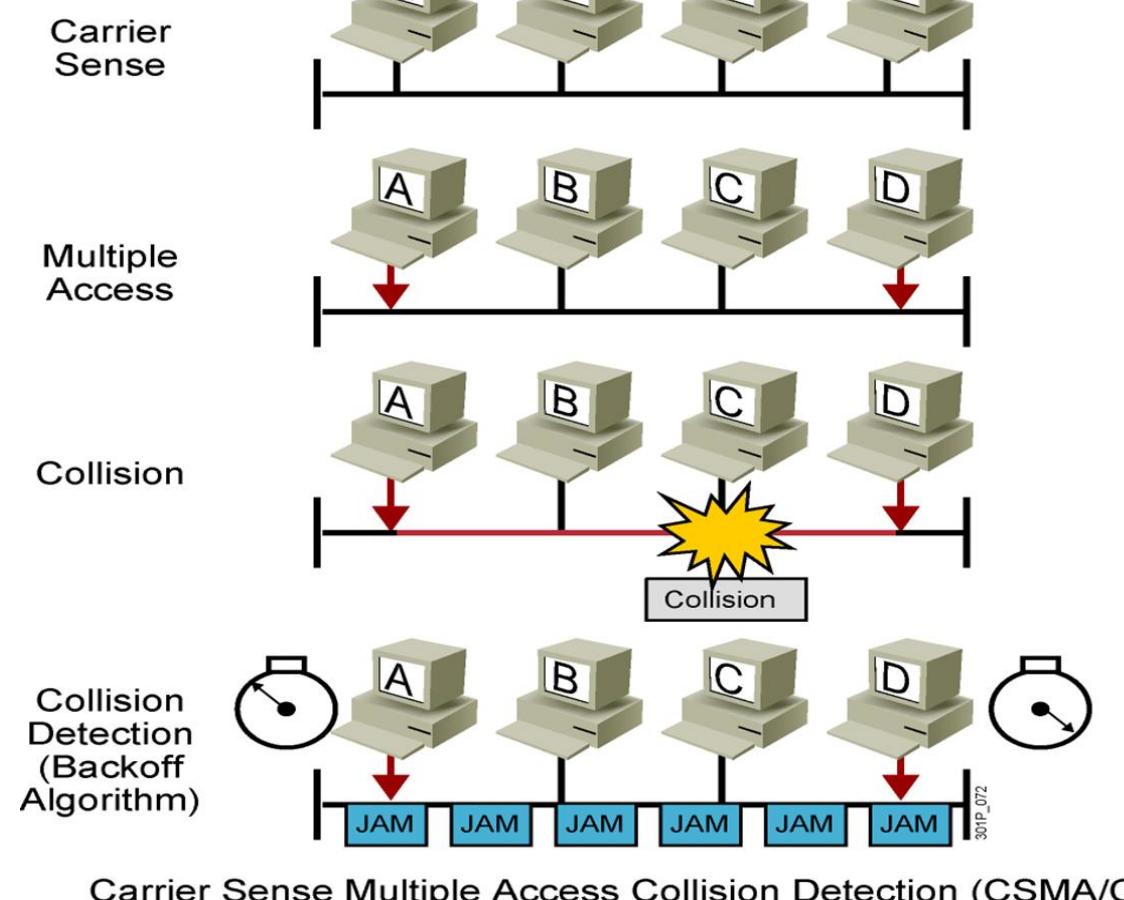
Each station continuously listens for traffic on the medium to determine when gaps between frame transmissions occur.

### Multiple access

Stations may begin transmitting any time they detect that the network is quiet (there is no traffic).

### Collision detect

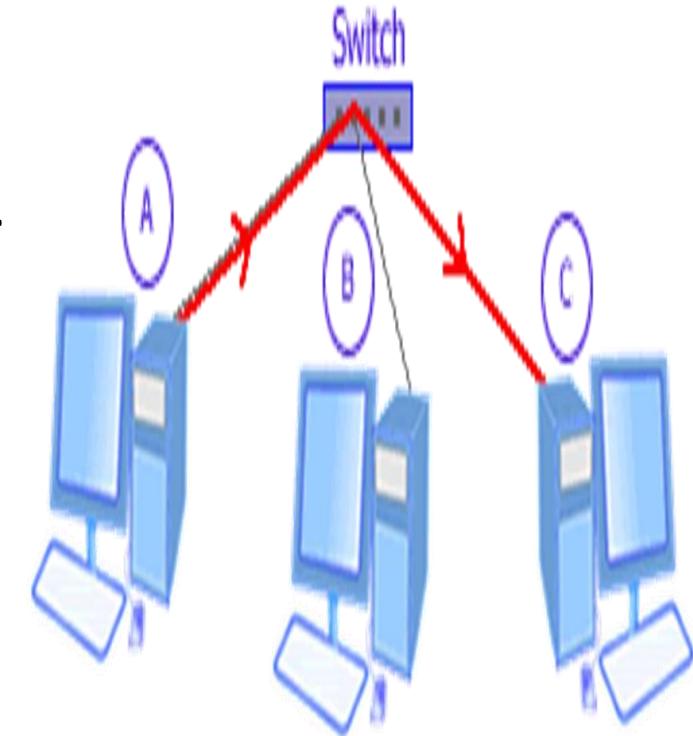
This means that if any collision occurs, it will be detected immediately



# Part 1\_Network Devices ( Hardware )

## ❖ Switch

- Allow different nodes to communicate with each other at the same time without slowing each other down.
- Imply less traffic and high performance and effective.
- Switch is data link layer device.
- The switch can perform error checking before forwarding data.
- less collision domain of hosts



# Part 1\_Network Devices ( Hardware )



## ❖ Switch

- **Layer 2 switch**
  - LAN switch
  - Forwards traffic based on the MAC address
- **Layer 3 switch**
  - Routing switch
  - Forwards traffic based on IP Address
  - Used for Inter-VLAN routing
  - Don't have WAN connectivity



# Part 1\_Network Devices ( Hardware )

## ❖ Router

- Allow different **networks** to communicate with each other (redirect packets between networks)
- Routes data packets based on their IP addresses.
- Routers are protocol dependent
- Operate at Network Layer device.
- Normally connect LANs and WANs together
- have a dynamically updating routing table based on which they make decisions on routing the data packets.



# Part 1\_Network Devices ( Hardware )



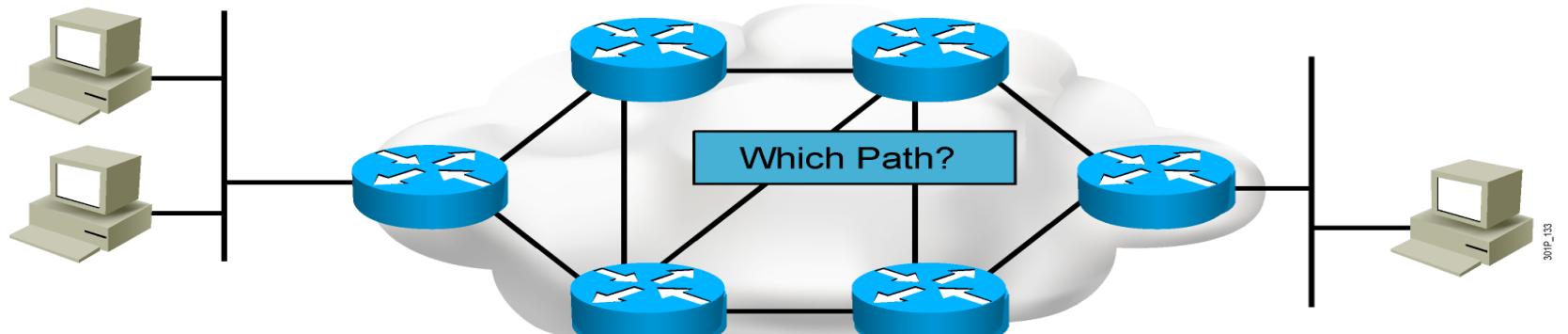
## ❖ Router

### – Path Determination :

- Getting update about the networks and send its updates to the other routers using the routing protocol configured

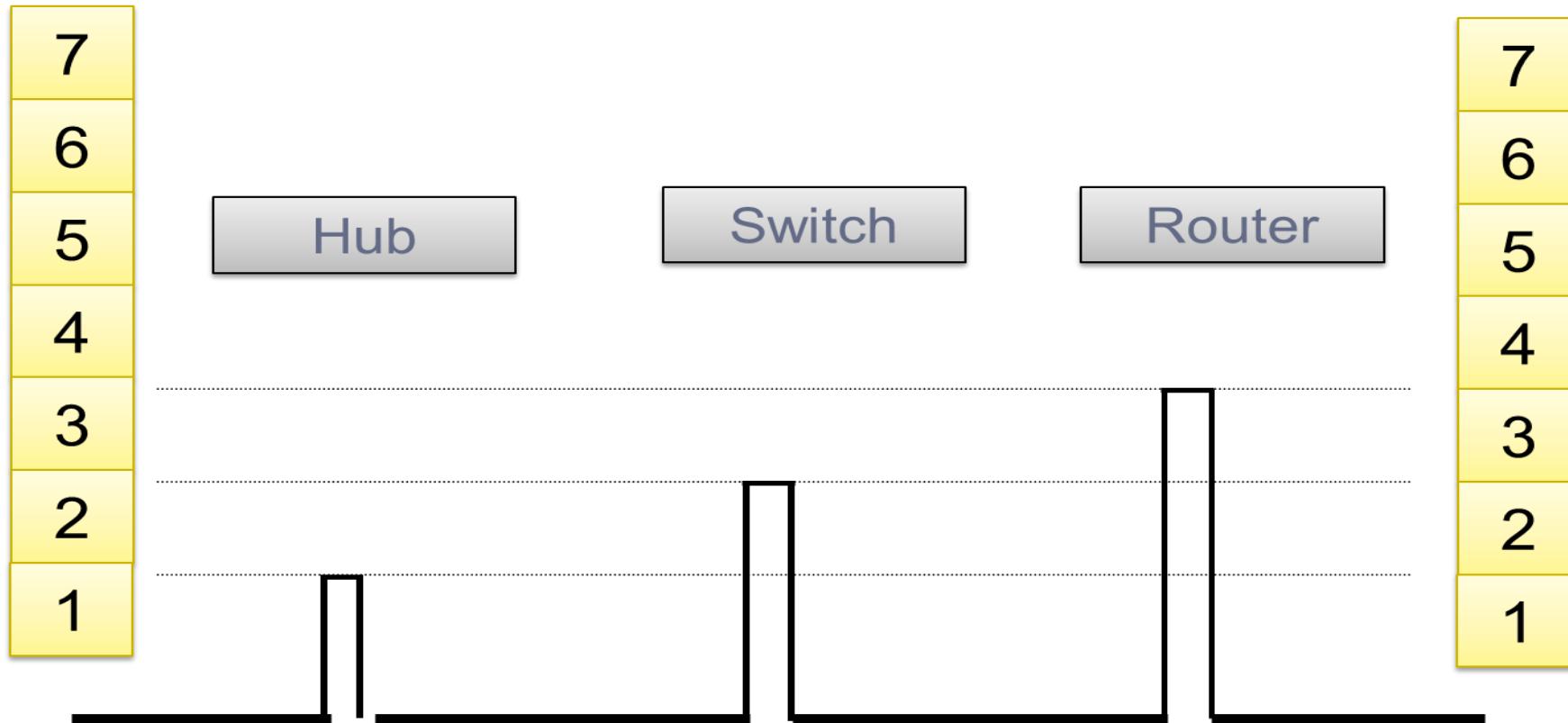
### – Packet forwarding:

- Routers use the routing table to know where to forward packets using the best path out of its serial interfaces.



# Part 1\_Network Devices ( Hardware )

## ❖ Hub, Switch, Router Layers



# Part 1\_Network Devices ( Hardware )



## ❖ Splitter

- is a device that divides a telephone signal into two or more signals,
- each carrying a selected frequency range
- can also reassemble signals from multiple signal sources into a single signal



# Part 1\_Network Devices ( Hardware )

## ❖ Your Home “Router”

- Main Function is Routing
- Act as Switch
- Act as DHCP
- Act as Firewall
- Act As Access point



# Part 1\_Network Media ( Hardware )

## Network Transmission Media

Wired Media  
Wireless Media

# Part 1\_Network Media ( Hardware )

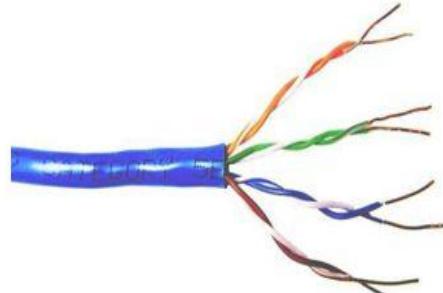


## Network Transmission Media

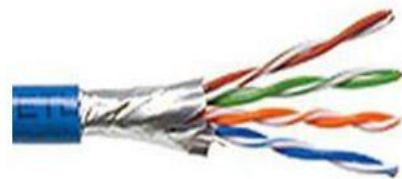
- **Cable Media**

- Twisted Pair Cables
  - UTP
  - STP
- Coaxial Cables
- Fiber Optic Cables

- Unshielded twisted pair (UTP)



- Shielded twisted pair (STP)



- **Wireless Media**

- WIFI
- Infra red
- Microwave
- Bluetooth

- Coaxial cable



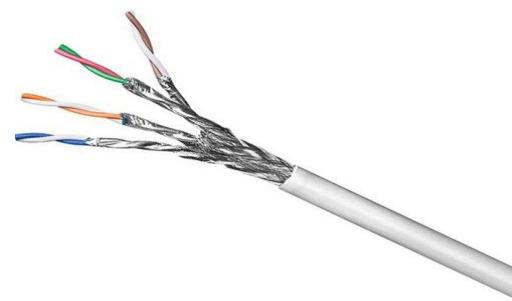
- Fiber optic



# Part 1\_Network Media ( Hardware )

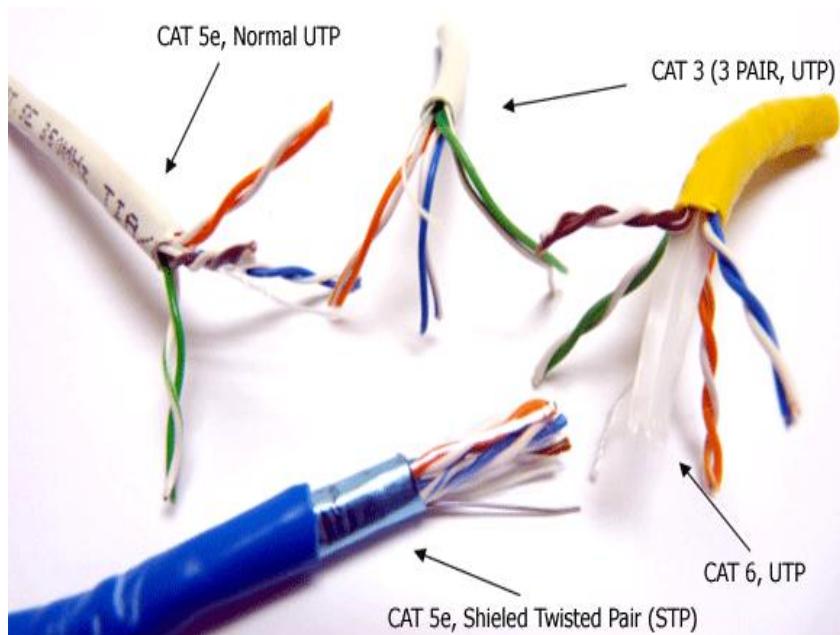
## Network Transmission Media -Twisted pair cable

- Most widely used (Ethernet networks)
- Two basic types
  - STP
    - Shielded twisted pair
    - Protected
    - Hard to install
  - UTP
    - Unshielded twisted pair
    - Most common
    - Easy to install
    - Less expensive
    - Effectected By electromagnetic interference
- Use RJ-45 connectors
- Crimper tool attach the twisted pair cable to RJ-45



# Part 1\_Network Media ( Hardware )

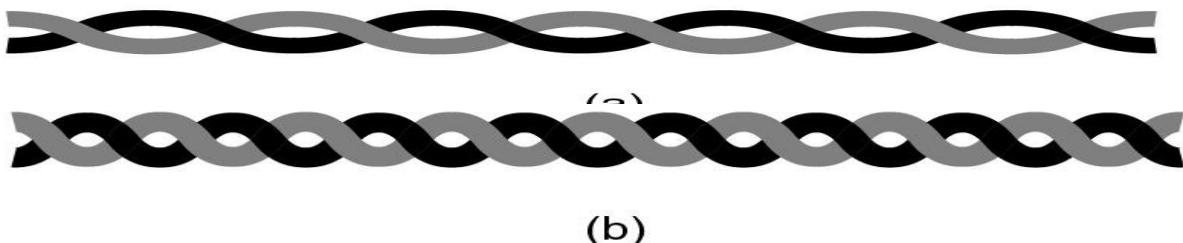
## UTP Categories



(a) Category 3 UTP.

(b) Category 5 UTP.

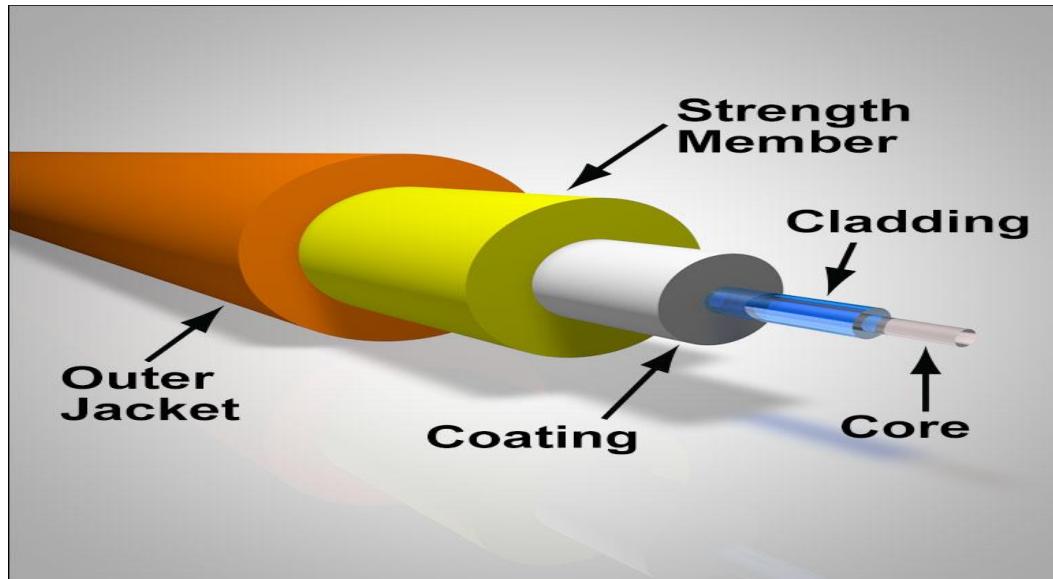
Type	Use
Category 1	Voice Only (Telephone Wire)
Category 5	Data to 100 Mbps (Fast Ethernet)
Category 5e	Data to 1 Gbps (Giga Ethernet)
Category 6	Data to 1 – 10 Gbps (Giga Ethernet)



# Part 1\_Network Media ( Hardware )

## Fiber optic

- Fiber optic cabling is composed of the following components:
  - The core that carries the signals. It is made of plastic or glass
  - The cladding maintains the signal in the center of the core as the cable bends.



# Part 1\_Network Media ( Hardware )

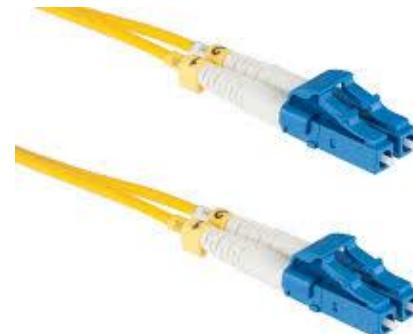
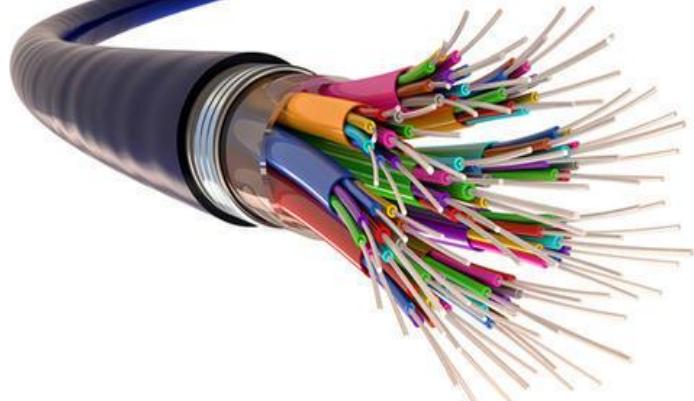
## Fiber Optic advantages

- **Advantages**

- Faster than twisted pair and coaxial
- Send data as light pulses over glass medium
- Free of electromagnetic interference
- Highly resistance to Eavesdropping
- Support extremely high data transfer rate
- Allow greater cable distances without repeater

- **Disadvantages**

- Expensive
- Hard to install





## Wireless Media

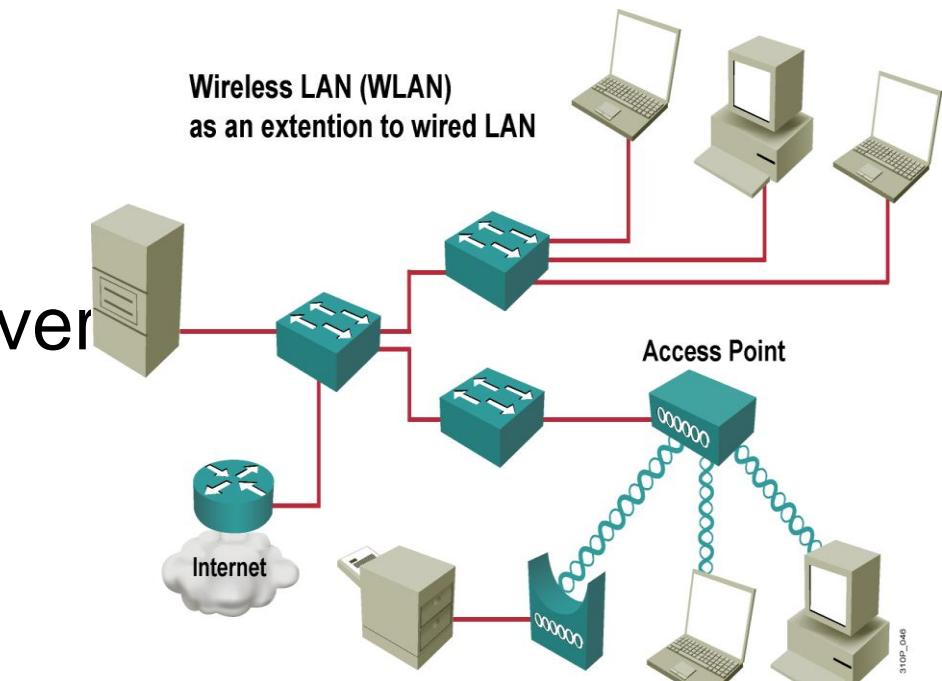
- Flexible (Used in areas where it is hard to install cables )
- Used in wireless LANs
- Hybrid environment is one which wireless components communicate with a network that use cables



# Part 1\_Wireless Communication



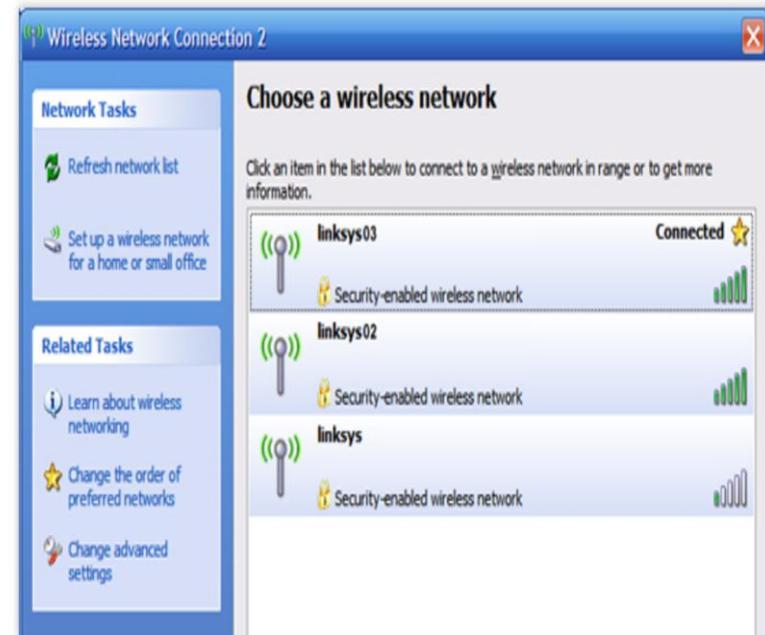
- Transmits data over the air vs. data over the wire
- Looks like a wired network to the user
- Defines physical and data link layer
- Uses MAC addresses
- The same protocols/applications run over LANs.
  - IP (network layer)
  - Web, FTP, SNMP (applications)



# PART 1\_WIRELESS COMMUNICATION

## Service Set Identifier (SSID)

- Unique identifier that client devices use to distinguish between multiple wireless networks in the same vicinity (separate WLANs)
- Alphanumeric, case-sensitive entry from 2 to 32 characters long.
- The SSID is configured on the AP and can be either **broadcasted** to the outside world or **hidden**.
- The SSID must match on client and access point.
- Access point broadcasts one SSID in beacons.
- Client cannot be configured without SSID.





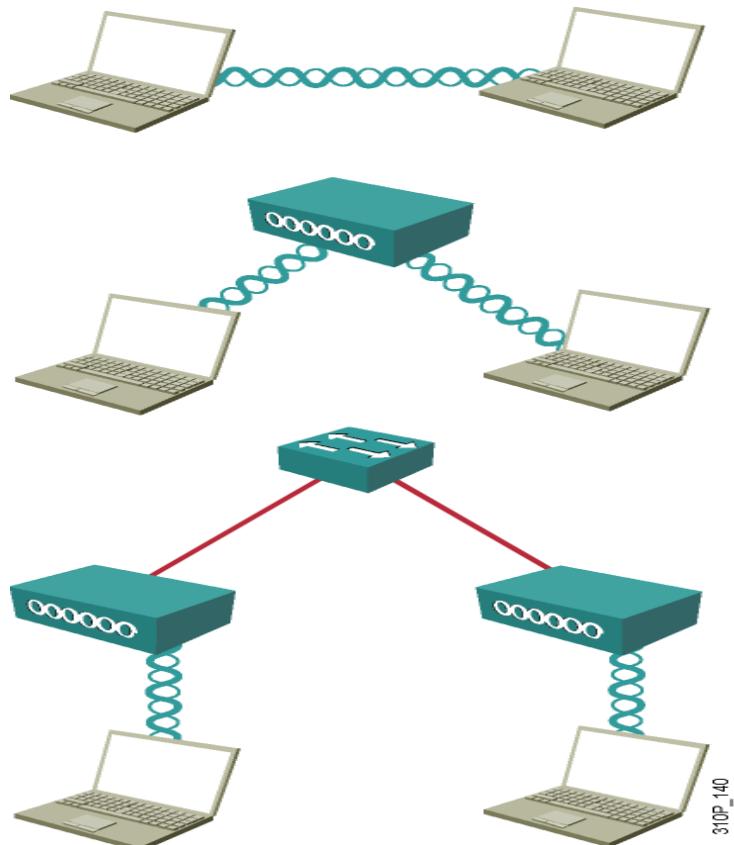
## Service Modes

### Independent Mode:

- Mobile clients connect directly without an intermediate access point.
- Ad hoc mode

### Infrastructure Mode:

- Mobile clients use a single access point for connecting to each other or to wired network resources.



# PART 1\_WIRELESS COMMUNICATION



- **Advantages**

- Provide the **ability to work anywhere** within range of your access points
- **Extends the range of your network without running additional wires**

- **Disadvantages**

- Introduces serious **security concerns**
- provides **much less bandwidth** than wired devices

# Thank You

