Tikrit University

COLLAGE OF COMPUTER SCIENCE AND MATHEMATICS

Computer Networking

Networks Physical Topologies

4th stage

Lecturer 2

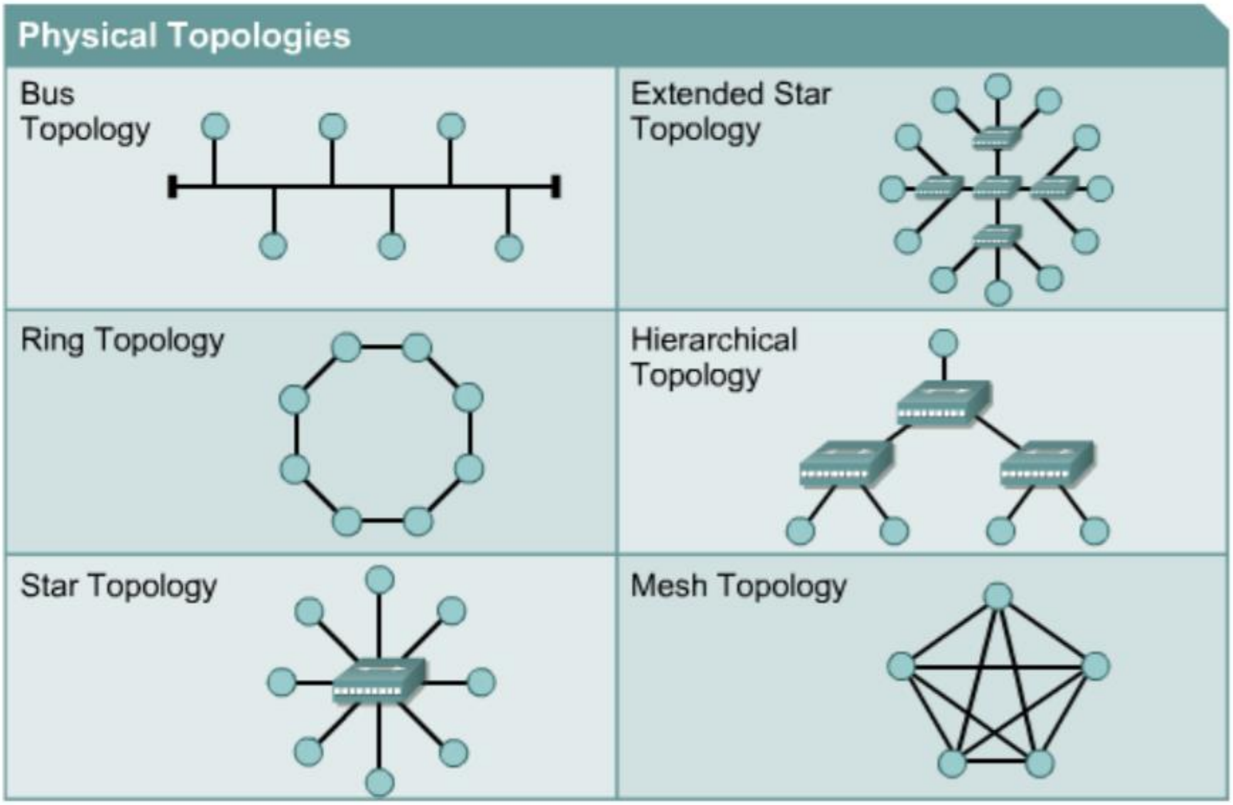
Majid Hamid Ali

2023- 2024

1- Physical Topology and Logical Topology

Physical topology: The term physical topology refers to the way in which a network is laid out physically. The actual layout of the wire or media. Two or more devices connect to a link; two or more links form a topology.

Logical topology: Defines how the hosts access the media to send data. Shows the flow of data on a network.



1. Bus Topology:

A networking topology that connects networking components along a single cable or that uses a series of cable segments that are connected linearly. A network that uses a bus topology is referred to as a “bus network.” Bus networks were the original form of Ethernet networks, using the 10Base5 cabling standard. Bus topology is used for:

- Small work-group local area networks (LANs) whose computers are connected using a thinnet cable
- Trunk cables connecting hubs or switches of departmental LANs to form a larger LAN
- Backboning, by joining switches and routers to form campus-wide networks

Advantages:

- Easy to install
- Costs are usually low
- Easy to add systems to network
- Great for small networks

Disadvantages:

- out of date technology.
- include difficult reconnection and fault isolation
- Can be difficult to troubleshoot.
- Unmanageable in a large network
- If cable breaks, whole network is down

2. Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally, in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Advantages:

- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a bus topology under heavy network load
- Does not require network server to manage the connectivity between the computers

Disadvantage:

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Network adapter cards and MAU's a Multistation Access Unit are much more expensive than Ethernet cards and hubs
- Much slower than an Ethernet network under normal load

3. Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To connect n nodes in Mesh topology, we require n(n-1)/2 duplex mode links.

Advantages:

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. Robust, if one link becomes unusable, it does not incapacitate the entire system.
3. Advantage of privacy or security.
4. point-to-point links make fault identification and fault isolation easy; Traffic can be routed to avoid links with suspected problems.

Disadvantage:

1. Required high amount of cabling and the number of I/O ports.
2. the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
3. the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

4. Star Topology:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

Advantages:

1. Less Expensive than Mesh topology.
2. In a star topology, each device needs only one link and one I/O port to connect it to any number of other devices. This factor also makes it easy to install and reconfigure.

3. Less Cabling, Addition and Deletion involves only one connection between the devices and the Hub or Switch.
4. Easy for Fault identification and fault isolation. If one link fails, only that link is affected. All
5. other links remain active.

Disadvantage:

One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

An extended star topology links individual stars together by connecting the hubs or switches.

A hierarchical topology is similar to an extended star. However, instead of linking the hubs or switches together, the system is linked to a computer that controls the traffic on the topology.

Logical Topology:

The logical topology of a network determines how the hosts communicate across the medium. The two most common types of logical topologies are **broadcast and token passing**.

The use of a **broadcast topology** indicates that each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to use the network. It is first come, first serve. Ethernet works this way as will be explained later in the course.

The second logical topology is token passing. In this type of topology, an electronic token is passed sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself. Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface (**FDDI**). A variation of Token Ring and **FDDI** is Arcnet. Arcnet is token passing on a bus topology.

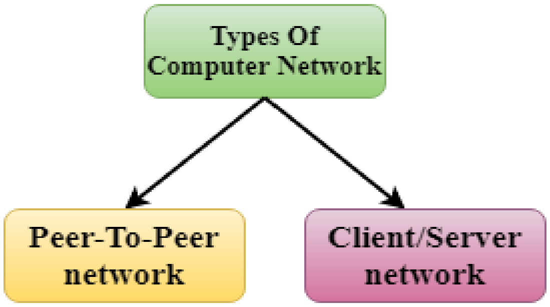
Difference between Physical and Logical Topology :

Physical Topology	Logical Topology
Depicts physical layout of network.	Depicts logistics of network concerned with transmission of data.
The layout can be modified based on needs.	There is no interference and manipulation involved here.
It can be arranged in star, ring, mesh and bus topologies.	It exists in bus and ring topologies.
This has major impact on cost, scalability and bandwidth capacity of network based on selection and availability of devices.	This has major impact on speed and delivery of data packets. It also handles flow control and ordered delivery of data packets.
It is actual route concerned with transmission.	It is a high-level representation of data flow.
Physical connection of the network.	Data path followed of the network.

2- Computer Network Architecture

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

The two types of network architectures are used:



- Peer-To-Peer network
- Client/Server network

Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

1. Point-to-Point

A **point-to-point connection** provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When we change television channels by infrared remote control, we are establishing a point-to-point connection between the remote control and the television's control system.

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

Advantages Of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

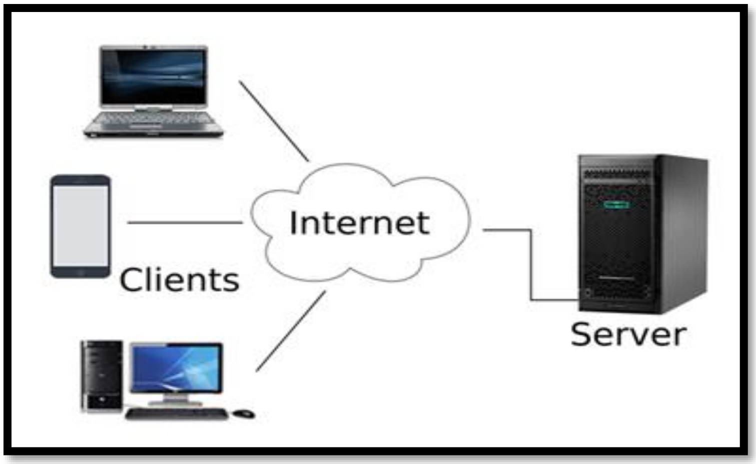
- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

2. Client/Server Network

The term client-server refers to a popular model for computer networking that utilizes client and server devices each designed for specific purposes. The client-server model can be used on the Internet as well as local area networks (LANs). Examples of client-server systems on the Internet include Web browsers and Web servers, FTP clients and servers, and DNS.

In a client/server arrangement, network services are located on a dedicated computer called a server. The server responds to the requests of clients. The server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services. Most network operating systems adopt the form of a client/server relationship. Typically, desktop computers function as clients and one or more computers with additional processing power, memory, and specialized software function as servers.

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages Of Client/Server network:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

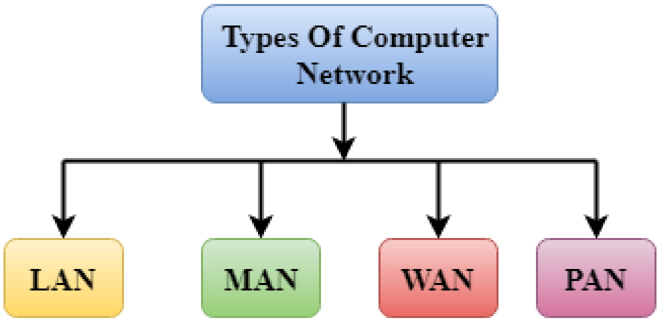
Peer-to-Peer Networks vs Client/Server Networks	
Peer-to-Peer Networks	**Client/Server Networks**
❖ Easy to set up	❖ More difficult to set up
❖ Less expensive to install	❖ More expensive to install
❖ Can be implemented on a wide range of operating systems	❖ A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking
❖ More time consuming to maintain the software being used (as computers must be managed individually)	❖ Less time consuming to maintain the software being used (as most of the maintenance is managed from the server)
❖ Very low levels of security supported or none at all. These can be very cumbersome to set up, depending on the operating system being used	❖ High levels of security are supported, all of which are controlled from the server. Such measures prevent the deletion of essential system files or the changing of settings
❖ Ideal for networks with less than 10 computers	❖ No limit to the number of computers that can be supported by the network
❖ Does not require a server	❖ Requires a server running a server operating system
❖ Demands a moderate level of skill to administer the network	❖ Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system

3- Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:

- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)



1. Local Area Network (LAN)

The term LAN refers to a local network or a group of interconnected network that are under the same administrative control. In the early days of networking, LANS are defined as small networks that existed in a single physical location. While LANs can be a single network installed in a home or small office, the definition of LAN has evolved to include interconnected local networks consisting of many hundreds of hosts, installed in multiple buildings and locations.

LANs are designed to:

Operate within a limited geographic area. Allow Multi-access to high bandwidth media.

LANs consist of the following components:

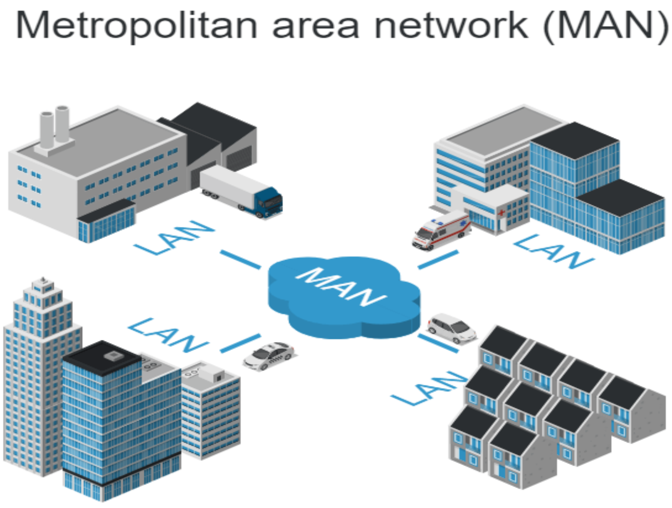
1. Computers
2. Network interface cards
3. Peripheral devices
4. Networking media
5. Network devices

LANs allow businesses to locally share computer files and printers efficiently and make internal communications possible. A good example of this technology is email. LANs manage data, local communications, and computing equipment. Some common LAN technologies include the following:

- Ethernet
- Token Ring
- FDDI

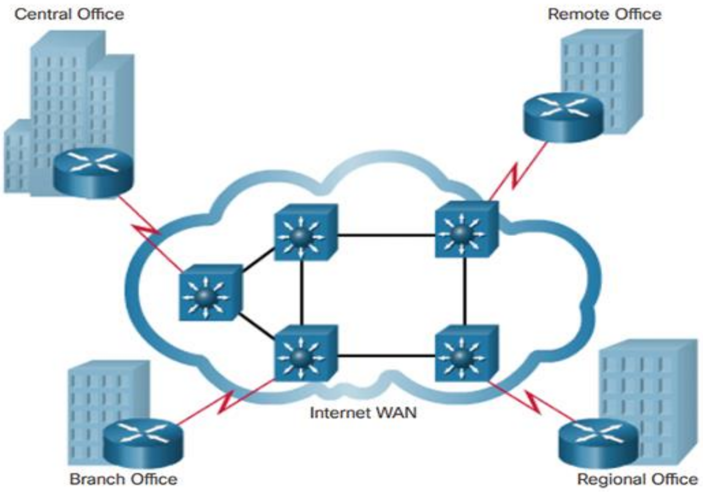
2. MAN:

is a network that spans a city. The network consists of various buildings interconnected via either wireless or fiber optics backbones. A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus. A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet.



3. WAN:

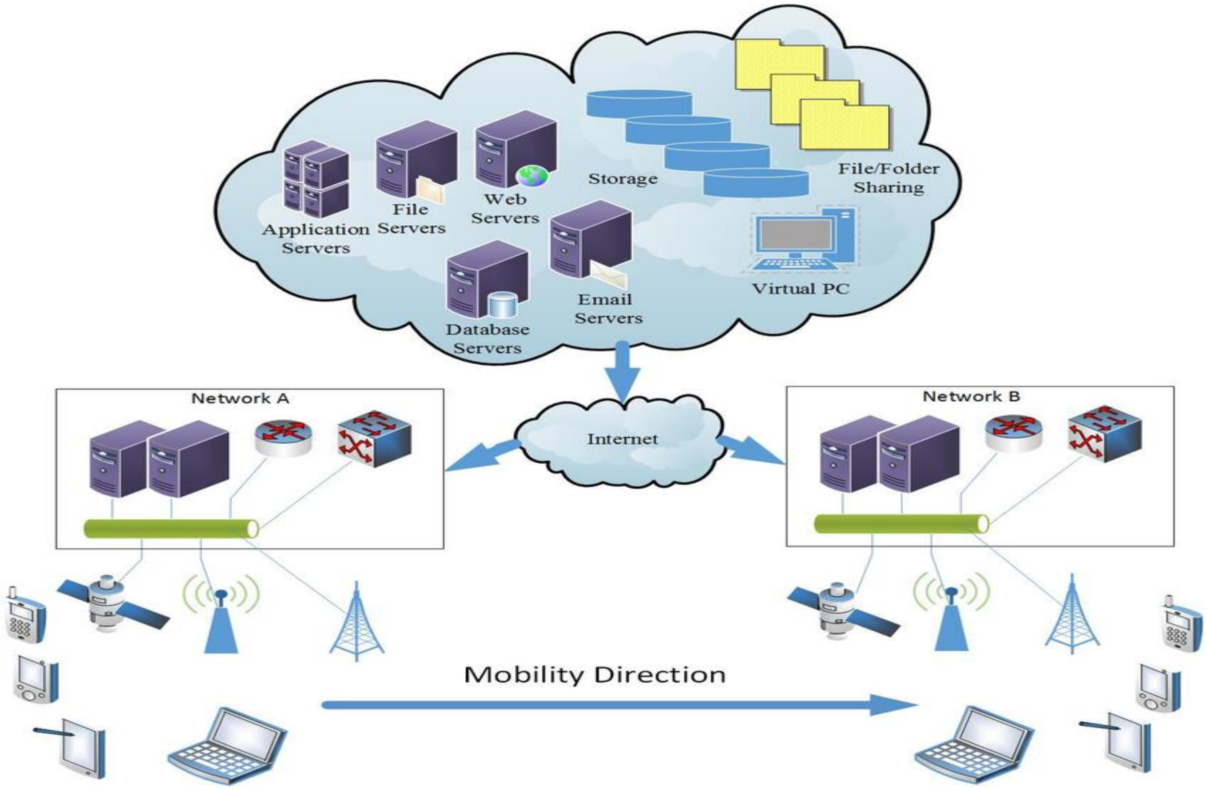
A network that spans broader geographical area than a local area network over public communication network. WANs interconnect LANs, which then provide access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs provide instant communications across large geographic areas. Collaboration software provides access to real-time information and resources and allows meetings to be held remotely. WANs have created a new class of workers called telecommuters. These people never have to leave their homes to go to work.



4. Intranet:

A private TCP/IP internetwork within an organization that uses Internet technologies such as Web servers and Web browsers for sharing information and collaborating. Intranets can be used to publish company policies and newsletters, provide sales and marketing staff with product information, provide technical support and tutorials, and just about anything else you can think of that fits within the standard Web server/Web browser environment.

Intranet Web servers differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization. Intranets are designed to permit users who have access privileges to the internal LAN of the organization. Within an intranet, Web servers are installed in the network. Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data.



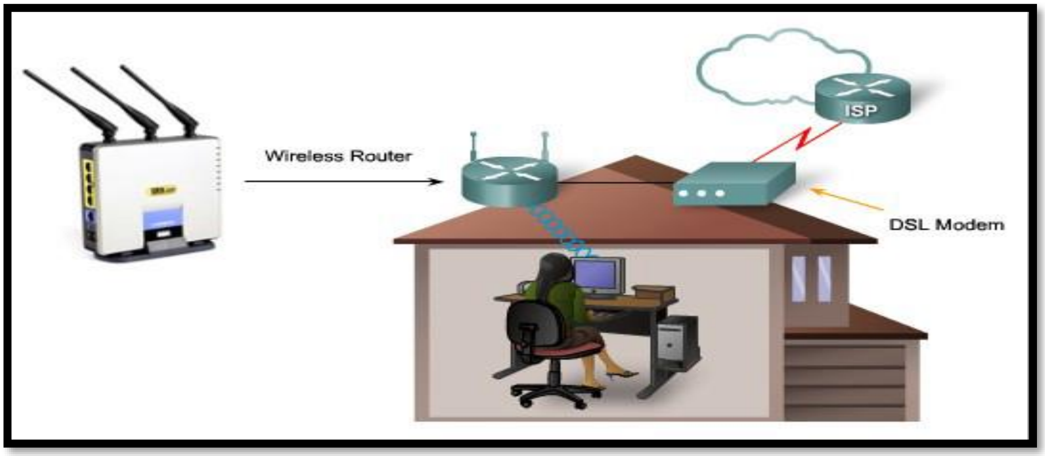
4- Wireless LAN:

The infrastructure-less network where, there is no required of any physical cable for network connection. In wireless LAN each client computer is connected to the Access Point through which they can share the file and access to the Internet.

These days People are becoming more mobile and want to maintain access to their business LAN resources from locations other than their desks. Workers in the office want to take their laptops to meetings or to a co-worker's office. When using a laptop in another location, it is inconvenient to rely on a wired connection.

- RF does not have boundaries, such as the limits of a wire in a sheath. The lack of such a boundary allows data frames traveling over the RF media to be available to anyone that can receive the RF signal.

- RF is unprotected from outside signals, whereas cable is in an insulating sheath. Radios operating independently in the same geographic area but using the same or a similar RF can interfere with each other.
- RF transmission is subject to the same challenges inherent in any wave-based technology, such as consumer radio. For example, as you get further away from the source, you may hear stations playing over each other or hear static in the transmission. Eventually, you may lose the signal altogether. Wired LANs have cables that are of an appropriate length to maintain signal strength.
- RF bands are regulated differently in various countries. The use of WLANs is subject to additional regulations and sets of standards that are not applied to wired LANs.



Advantages of Wireless

Allows for wireless remote access

The network can be expanded without disruption to current user

Disadvantages

Potential security issues associated with wireless transmissions

Limited speed in comparison to other network topologies

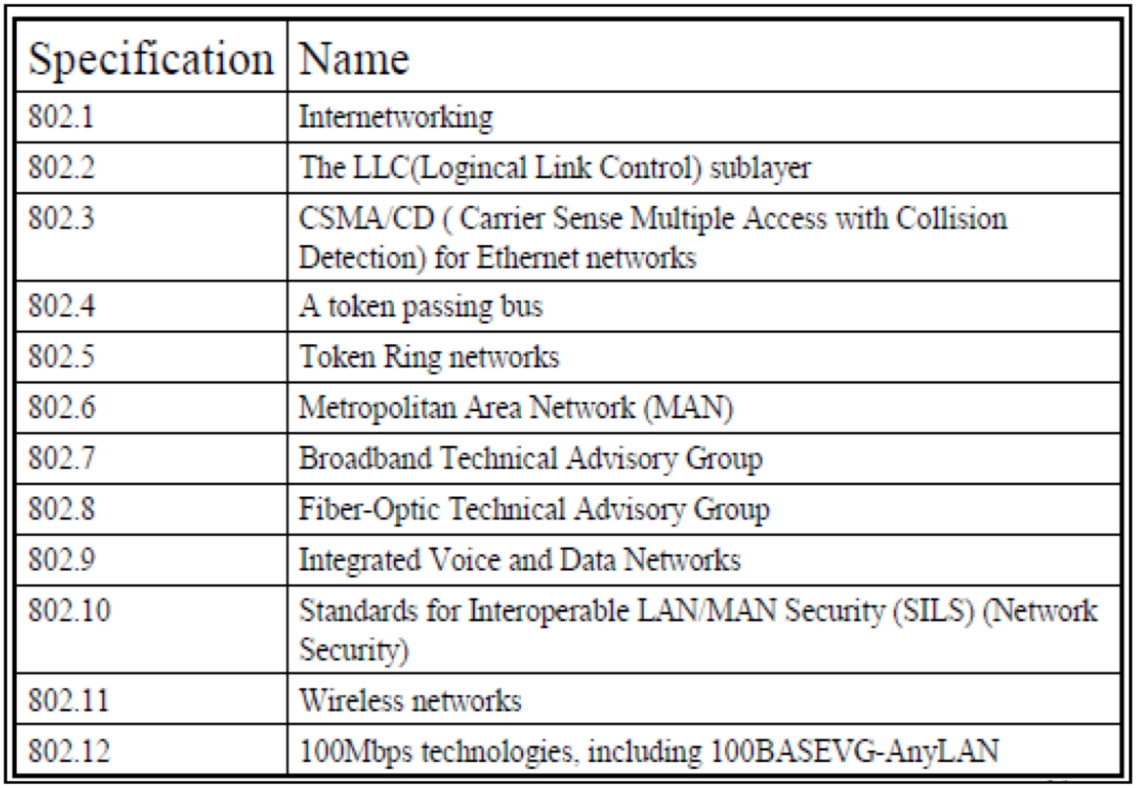
IEEE and Networking standards:

- Institute of Electrical and Electronic Engineers (IEEE) developed a series of networking standards
- Networking technologies developed by manufacturers are compatible
- Cabling, networking devices and protocols are all interchangeable under the banner of a specific IEEE.

Example of protocols or IEEE standards:

1- 802.3 IEEE Ethernet standard

- Defines characteristics for Ethernet networks.
- New additions: 802.3u for Fast Ethernet, 802.3z for Gigabit Ethernet, referred to as 802.3x., 802.3ac 10gbits/s, in 2009
- Speed: Original 10Mbps, Fast Ethernet 100Mbps, Gigabit Ethernet 1000Mbps
- Topology: bus or star.
- Media: Coaxial and twisted pair cabling, also fiber optic cable.
- Access method: CSMA/CD



Specification	Name
802.1	Internetworking
802.2	The LLC(Logincal Link Control) sublayer
802.3	CSMA/CD (Carrier Sense Multiple Access with Collision Detection) for Ethernet networks
802.4	A token passing bus
802.5	Token Ring networks
802.6	Metropolitan Area Network (MAN)
802.7	Broadband Technical Advisory Group
802.8	Fiber-Optic Technical Advisory Group
802.9	Integrated Voice and Data Networks
802.10	Standards for Interoperable LAN/MAN Security (SILS) (Network Security)
802.11	Wireless networks
802.12	100Mbps technologies, including 100BASEVG-AnyLAN

IEEE standard for some network topologies

2- Wireless Standards - 802.11b 802.11a 802.11g and 802.11n

• Specifies the characteristics of wireless LAN Ethernet networks.

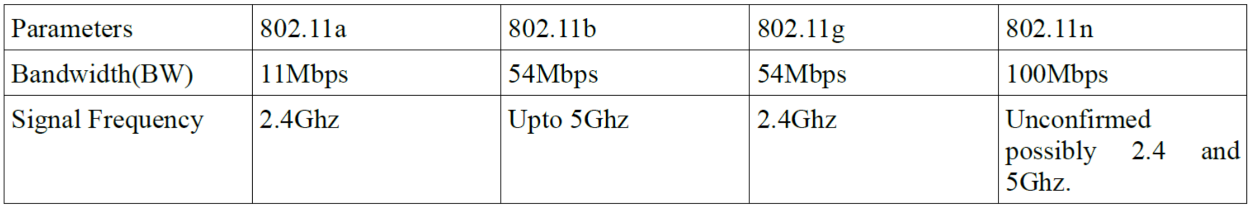
– Special devices are called wireless access points to allow communication.

– Also connect to wired networks to create wireless portions of entire networks.

– Access method: Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), a variation of CSMA/CD.

– Topology: physical wireless, logical bus

• Protocols: (a) 802.11b 1999 2.4GHz, 11Mbits/s, (b) 802.11g 2003 2.4GHz, 54 Mbits/s, (c) 802.11n 2008 2.4G,5GHz, 248Mbits/s



Parameters	802.11a	802.11b	802.11g	802.11n
Bandwidth(BW)	11Mbps	54Mbps	54Mbps	100Mbps
Signal Frequency	2.4Ghz	Upto 5Ghz	2.4Ghz	Unconfirmed possibly 2.4 and 5Ghz.

802.11a:

- **Pros of 802.11a** - fast maximum speed; regulated frequencies prevent signal interference from other devices
- **Cons of 802.11a** - highest cost; shorter range signal that is more easily obstructed

802.11b:

- **Pros of 802.11b** - lowest cost; signal range is good and not easily obstructed
- **Cons of 802.11b** - slowest maximum speed; home appliances may interfere on the unregulated frequency band

802.11g:

- **Pros of 802.11g** - fast maximum speed; signal range is good and not easily obstructed
- **Cons of 802.11g** - costs more than 802.11b; appliances may interfere on the unregulated signal frequency.

802.11n:

- **Pros of 802.11n** - fastest maximum speed and best signal range; more resistant to signal interference from outside sources

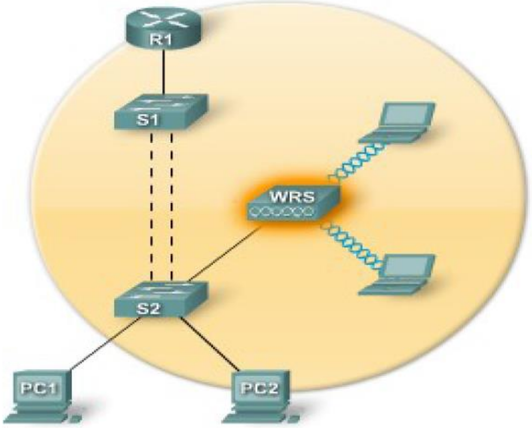
- **Cons of 802.11n** - standard is not yet finalized; costs more than 802.11g; the use of multiple signals may greatly interfere with nearby 802.11b/g based networks.

WLAN VS LAN:

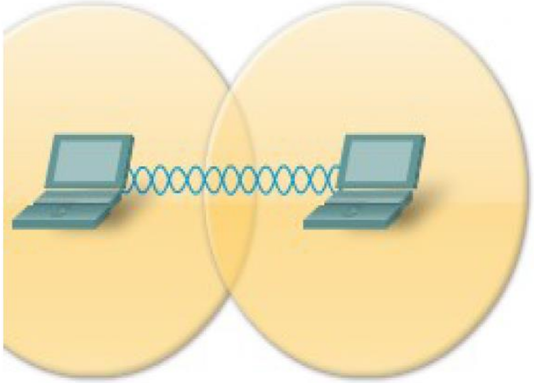
Characteristics	**802.11 Wireless LAN**	**802.3 Ethernet LANS**
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance (CSMA/CA)	Collision Detection(CSMA/CD)
Availability	Anyone with a radio NIC in range of an Access point	Cable connection required
Signal interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

Wireless Topologies:

1. BSS (Basic Service Set). (in the presence of a Control Module often called "Base Station" or Access points.
2. Ad-hoc or Peer-to-Peer (When there is no Control Module)



BSS Topology



Adhoc Topology

BSS:

Access points provide an infrastructure that adds services and improves the range for clients. A single access point in infrastructure mode manages the wireless parameters and the topology is simply a BSS.

Ad-Hoc:

Wireless networks can operate without access points; this is called an ad hoc topology. Client stations which are configured to operate in ad hoc mode configure the wireless parameters between themselves. The IEEE 802.11 standard refers to an ad hoc network as an independent BSS (IBSS).