UNIT 6
WIRED AND WIRELESS LOCAL AREA NETWORK

CONTENTS

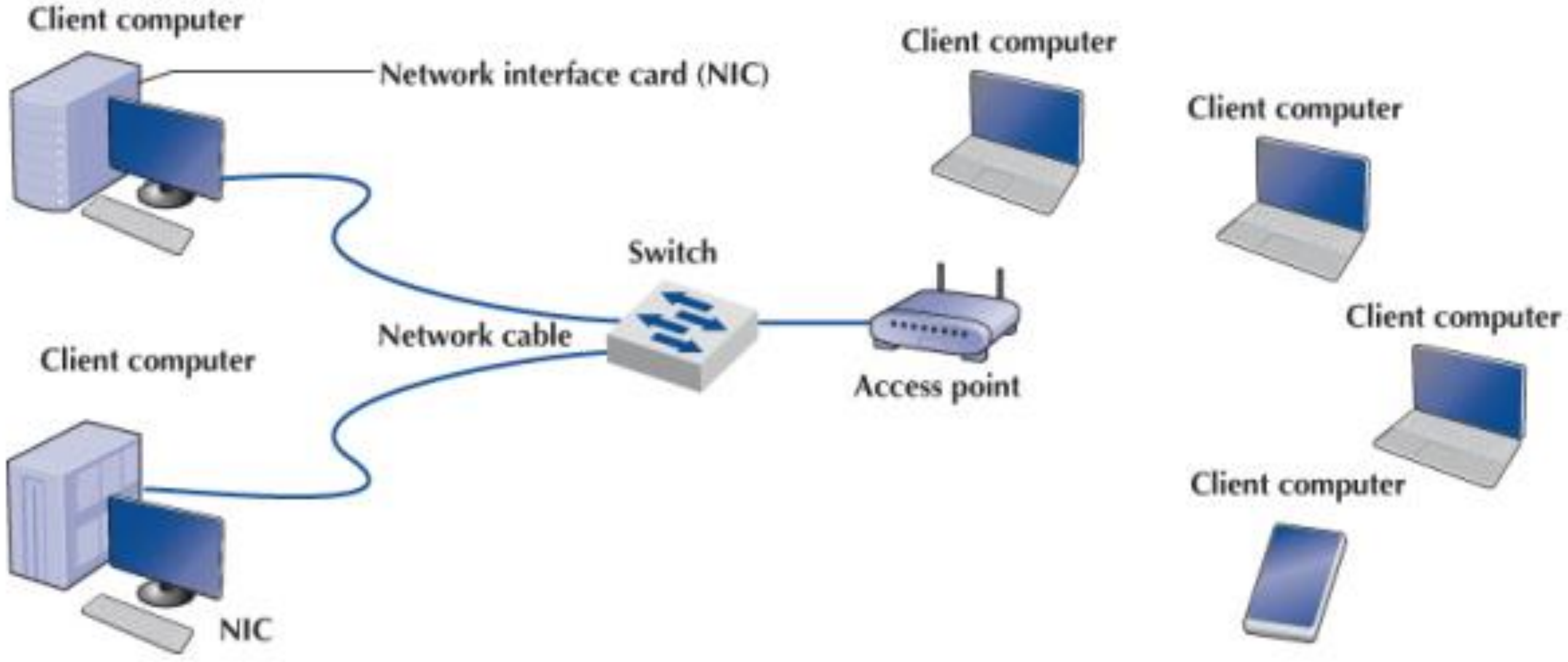
- Introduction; LAN Components (Network Interface Cards, Network Circuits, Network Hubs, Switches, and Access Points, Network Operating Systems); Wired Ethernet (Topology, Media Access Control, Types of Ethernet); Wireless Ethernet (Topology, Media Access Control, Wireless Ethernet Frame Layout, Types of Wireless Ethernet, Security); The Best Practice LAN Design (Designing User Access with Wired Ethernet, Designing User Access with Wireless Ethernet, Designing the Data Center, Designing the e-Commerce Edge, Designing the SOHO Environment); Improving LAN Performance (Improving Server Performance, Improving Circuit Capacity, Reducing Network Demand).

INTRODUCTION

- The first major network architecture component is the local area networks (LANs) that provide users access to the network. Most large organizations have numerous wired and wireless LANs connected by backbone networks.
- The fundamental components of a LAN, along with two technologies commonly used in LANs—traditional wired Ethernet (IEEE 802.3), which is commonly used to connect desktop computers, and wireless Ethernet (IEEE 802.11, commonly called Wi-Fi), which often is used to connect laptop computers and mobile devices.

LAN Components

- There are several components in a traditional LAN as shown in figure. The first two are the client computer and the server. The other components are network interface cards (NICs), network circuits, hubs/switches/access points, and the network operating system.



- **Network Interface Cards (NIC):**
- A NIC is circuit board or a card that allows computers to communicate over a network via cables or wirelessly. It is also called as LAN adaptor, network adaptor or network card. Enable clients, servers, printers and other devices to transmit and receive data over the network.
- It operates on physical layer and data link layer of OSI model. Every network adaptor is assigned a unique 48-bit Media Access Control (MAC) address, which is stored in ROM to identify themselves in a network or a LAN.
- Typically network adaptor has RJ45 or BNC or both sockets for connecting and a LED to show up it is active and transmitting the data. It connects to a network via cables like CAT5, Co-axial, fiber-optics etc. and wirelessly by a small antenna.

- **Network Circuits:**
- Each computer must be physically connected by network circuits to the other computers in the network.
- **Wired LANs:** Most LANs are built with unshielded twisted-pair (UTP) cable, shielded twisted-pair (STP) cable, or fiber-optic cable. Many LANs use UTP cable. Its low cost makes it very useful. STP is only used in special areas that produce electrical interference, such as factories near heavy machinery or hospitals near MRI scanners. Fiber-optic cable is even thinner than UTP wire and therefore takes far less space when cabled throughout a building. It is also much lighter, weighing less than 10 pounds per 1,000 feet. Because of its high capacity, fiber-optic cabling is perfect for Backbone Networks, although it is beginning to be used in LANs.

- **Wireless LANs (WLANs)** use radio transmissions to send data between the NIC and the access point (AP). Most countries (but not all) permit WLANs to operate in two frequency ranges: the 2.4 and 5 GHz range. These same frequency ranges can be used by cordless phones and baby monitors, which means that your WLAN and your cordless phone may interfere with each other. Under ideal conditions, the radio transmitters in the NICs and APs can transmit 100–150 meters (300–450 feet). In practice, the range is much shorter as walls absorb the radio waves. The other problem is that as the distance from the AP increases, the maximum speed drops, often very dramatically.
- When we design a WLAN, it is important to ensure that the APs don’t interfere with each other. If all APs transmitted on the same frequency, the transmissions of one AP would interfere with another AP.
- Therefore, each AP is set to transmit on a different channel, very much like the different channels on your TV. Each channel uses a different part of the 2.4 or 5 GHz frequency range so that there is no interference among the different channels. When a computer first starts using the WLAN, its NIC searches all available channels within the appropriate frequency range and then picks the channel that has the strongest signal.

- **Network Hubs, Switches, and Access Points:**
- Hub is a connecting device in which various types of cables are connected to centralize network traffic through a single connecting point. Hub with multiple ports is used to connect topologies, segments of LAN and to monitor network traffic. It manages and controls the send and receive data to and from the computers. Hub works on the physical layer of OSI or TCP/IP model. To avoid collision of data CSMA/CD protocol is used and protocol varies depending upon the vendor.
- The types of hubs are as follows:

Active Hub:

- Can store, amplify, split and retransmit the received signals.
- Requires additional electronic circuit for performing different functions.
- It does work of repeater to amplify the signal, so it is also called as repeater.

Passive Hub:

- Can only forward received signal without amplifying it.
- It doesn't content any additional electronic circuit.

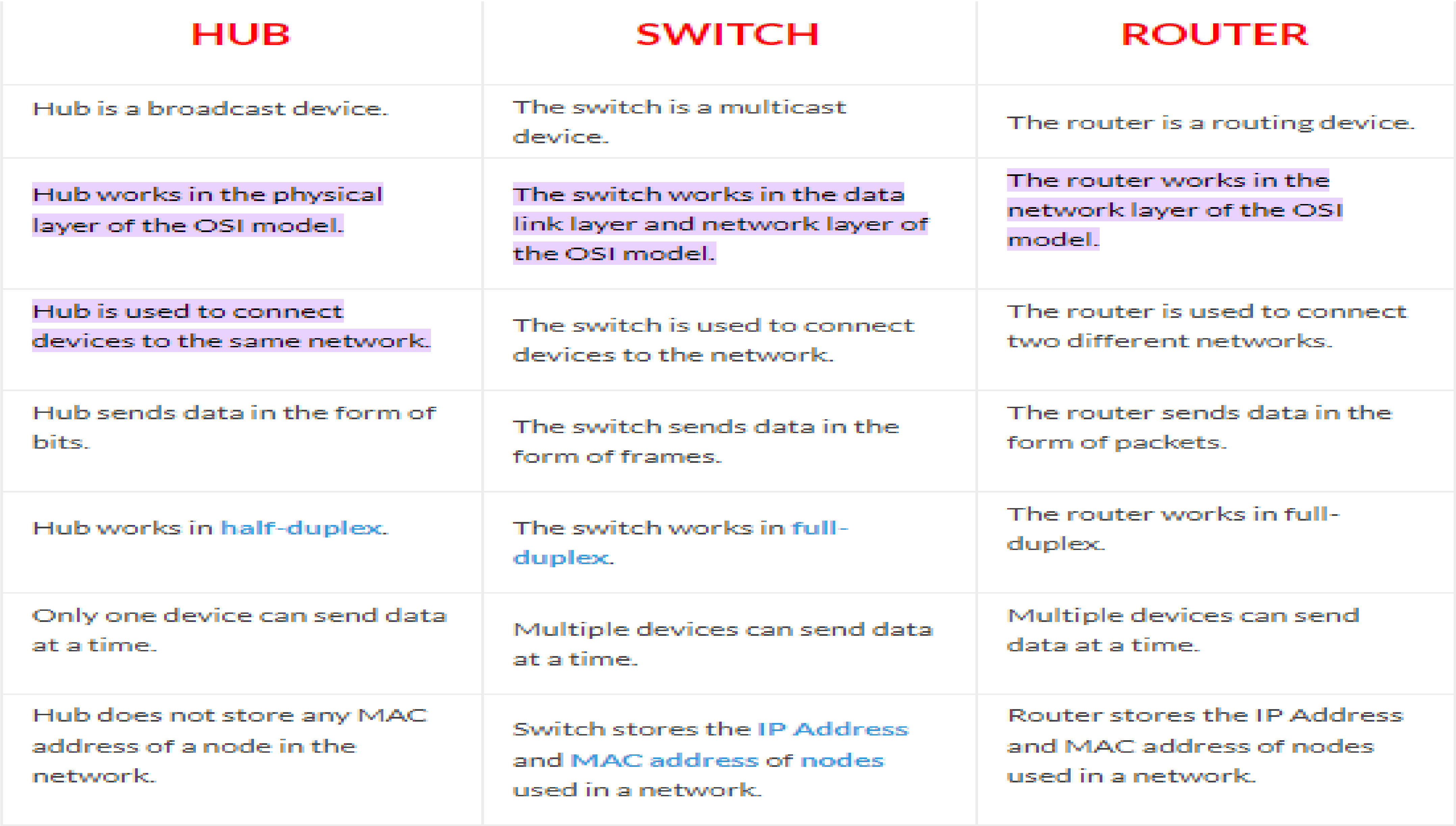
Intelligent Hub:

- Performs functions of both active and passive hub.
- Quickly routes the signals between the ports of hub.
- Also performs different functions of router and bridge.
- So, it is called as intelligent hub.

- **Switch:**
- Switch is a multiple LAN connecting device, which takes incoming data packet from any multiple input ports and passes the data packet to specific output port.
- It works same as hub but does its work very efficiently.
- It uses MAC address information to switch forward the data packets to a particular destination device. By monitoring the network traffic, it can learn where the particular addresses are located.
- It operates at one or more OSI model layers mainly the data link layer. Switch helps to minimize the collision of data packets and provides better security and better utilization of limited bandwidth.

- It uses two different methods for switching the packets:

1. In cut-through method switch examines the header of the packet and decides, where to pass the packet before it receives the whole packet. Increases the chances of errors without verifying the data integrity.
2. In store and forward method switch reads the entire packet in its memory and checks for error before transmitting the packet. This method is slower and time consuming but error free.



HUB	SWITCH	ROUTER
Hub is a broadcast device.	The switch is a multicast device.	The router is a routing device.
Hub works in the physical layer of the OSI model.	The switch works in the data link layer and network layer of the OSI model.	The router works in the network layer of the OSI model.
Hub is used to connect devices to the same network.	The switch is used to connect devices to the network.	The router is used to connect two different networks.
Hub sends data in the form of bits.	The switch sends data in the form of frames.	The router sends data in the form of packets.
Hub works in half-duplex.	The switch works in full-duplex.	The router works in full-duplex.
Only one device can send data at a time.	Multiple devices can send data at a time.	Multiple devices can send data at a time.
Hub does not store any MAC address of a node in the network.	Switch stores the IP Address and MAC address of nodes used in a network.	Router stores the IP Address and MAC address of nodes used in a network.

- **Access Point:**
- While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the Data Link layer, and it can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another. It allows wireless-capable devices, such as laptops, smartphones, and tablets, to connect to a wired network or the internet. Access points are essential components in the deployment of wireless networks and are often used to extend the coverage and reach of an existing wired network.

- Some key features and functions of access points are:
- **Wireless Connectivity:** An access point provides wireless connectivity, allowing devices equipped with Wi-Fi adapters to connect to the network without the need for physical cables. It acts as a bridge between wired and wireless networks.
- **SSID (Service Set Identifier):** Each access point is associated with an SSID, which is a unique name that wireless devices used to identify and connect to a specific wireless network. Users select the SSID when connecting to the Wi-Fi network.
- **Authentication and Encryption:** Access points typically support various security protocols, including WPA3, WPA2, and WEP, to secure the wireless network. Users must enter a pre-shared key or password to authenticate and access the network.
- **Network Address Translation (NAT):** Some access points include NAT functionality allowing multiple devices connected to the access point to share a single public I address, useful for home networks with limited IP addresses from the Internet Servic Provider (ISP).

- **DHCP Server:** Many access points have built-in DHCP (Dynamic Host Configuration Protocol) servers that automatically assign IP addresses to connected devices, simplifying network configuration for users.
- **Management Interface:** Access points can be configured and managed through web-based interfaces or dedicated management software. Administrators can set network parameters, security settings, and monitor the status of connected devices.
- Power over Ethernet (PoE): Some access points support PoE, allowing them to receive power and data through a single Ethernet cable. This feature simplifies installation, especially in locations where power outlets are not readily available.

- **Network Operating Systems (NOS):**
- The network operating system (NOS) is the software that controls the network. Every NOS provides two sets of software: one that runs on the network server(s) and one that runs on the network client(s).
- The server version of the NOS provides the software that performs the functions associated with the data link, network, and application layers and usually the computer’s own operating system.
- The client version of the NOS provides the software that performs the functions associated with the data link and the network layers and must interact with the application software and the computer’s own operating system.
- Most NOSs provide different versions of their client software that run on different types of computers, so that Windows computers, for example, can function on the same network as Apple computers. In most cases (e.g., Windows and Linux), the client NOS software is included with the operating system itself.

- **NOS Server Software:**
- The NOS server software enables the file server, print server, or database server to operate. In addition to handling all the required network functions, it acts as the application software by executing the requests sent to it by the clients (e.g., copying a file from its hard disk and transferring it to the client, printing a file on the printer, executing a database request, and sending the result to the client). NOS server software replaces the normal operating system on the server. By replacing the existing operating system, it provides better performance and faster response time because a NOS is optimized for its limited range of operations. The most commonly used NOS are Windows Server and Linux.
- **NOS Client Software:**
- The NOS software running at the client computers provides the data link layer and network layer. Most operating systems today are designed with networking in mind. For example, Windows provides built-in software that will enable it to act as a client computer with a Windows Server.

- One of the most important functions of a NOS is a directory service. Directory services provide information about resources on the network that are available to the users, such as shared printers, shared file servers, and application software. A common example of directory services is Microsoft’s Active Directory Service (ADS).
- **Network Profiles:**
- A network profile specifies what resources on each server are available on the network for use by other computers and which devices or people are allowed what access to the network. The network profile is normally configured when the network is established and remains in place until someone makes a change. In a LAN, the server hard disk may have various resources that can or cannot be accessed by a specific network user (e.g., data files and printers). Furthermore, a password may be required to grant network access to the resources.

Wired Ethernet

- Almost all LANs installed today use some form of Ethernet. Ethernet was originally developed by DEC, Xerox, and Intel but has since become a standard formalized by the IEEE as IEEE 802.3. The IEEE 802.3 version of Ethernet is slightly different from the original version but the differences are minor. Likewise, another version of Ethernet has also been developed that differs slightly from the 802.3 standard. Ethernet is a layer 2 protocol, which means it operates at the data link layer. Every Ethernet LAN needs hardware at layer 1, the physical layer, that matches the requirements of the Ethernet software at layer 2.

- **Topology:**
- Topology refers to the physical or logical layout of a network. It defines the way different nodes are placed and interconnected with each other. Alternately, Topology may describe how the data is transferred between these nodes. There are two types of network topologies: physical and logical. Physical topology emphasizes the physical layout of the connected devices and nodes much like a physical data flow diagram (DFD) or physical entity relational diagram (ERD), while the logical topology focuses on the pattern of data transfer between network nodes much like a logical DFD or logical ERD. Types of Topology:

1. Bus Topology (Hub based)
2. Ring Topology
3. Star Topology (switch based)
4. Mesh Topology
5. Hybrid Topology

Bus Topology:

- A bus network uses a single conduit (channel) called bus or backbone to which all the network nodes and peripheral devices are attached.
- Each node is connected in series to a single cable.
- At the cable’s start and end points, a special device called a terminator is attached. A terminator stops the network signals so they do not bounce back down the cable.
- In a bus topology, the cable is arranged in a long straight line and each computer attached to the cable directly or by using a short drop cable.
- A bus topology is passive, each computer is only responsible for traffic directly addressed to it. The nodes don’t actively move each signal along, so any one computer can go down and it won’t affect the whole network.
- The way the stations share the single communication medium is similar to the way people share multiple extensions on the same phone line (listen to see if the line is in use; if so try again later; if not talk.

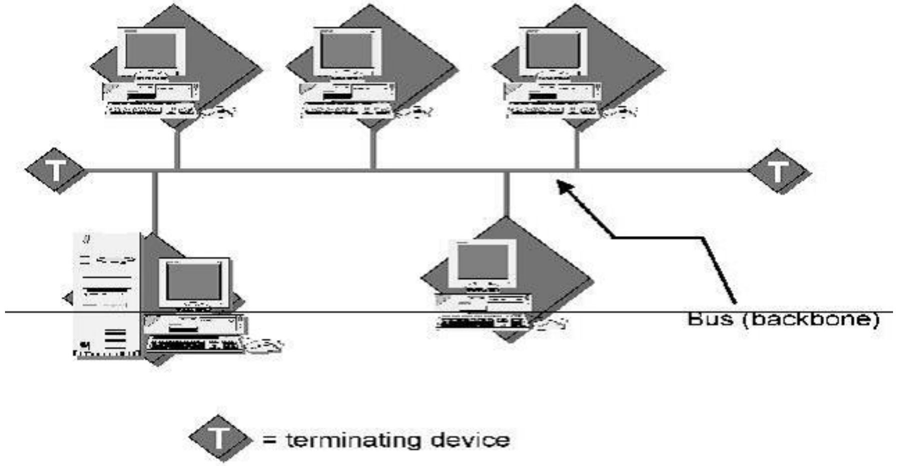
Advantages:

- Easy to implement and extend.
- Well suited for temporary networks that must be set up in a hurry.
- Typically the least cheapest topology to implement.
- Failure of one station does not affect others.

Disadvantages:

- Difficult to administer/ troubleshoot.
- Limited cable length and number of stations.
- A cable break can disable the entire network.
- Maintenance cost may be higher in the long run.
- Performance degrades as additional computers are added.

Examples: ARCnet (Attached Resource Computer Network), Ethernet



- **Ring Topology:**
- The ring topology connects the nodes of the network in a circular chain, with each chain connected to the next.
- The final node in the chain connects to the first to complete the ring.
- With this methodology, each node examines data sent through the ring.
- The stations are attached to the ring and share the ring by passing **token** that specifies whose turn it is.
- If the token is not addressed to the node examining it, the node passes it along the next node in the ring.
- It's an active topology; each computer has to take responsibility for moving the data along.
- For fault tolerance, some systems uses a dual ring. One ring is the primary method, and other is used as backup. Data goes in one direction in the primary ring, and opposite direction in the secondary ring. So, if there's a failure, messages can backup and go around the block to avoid the problem area.

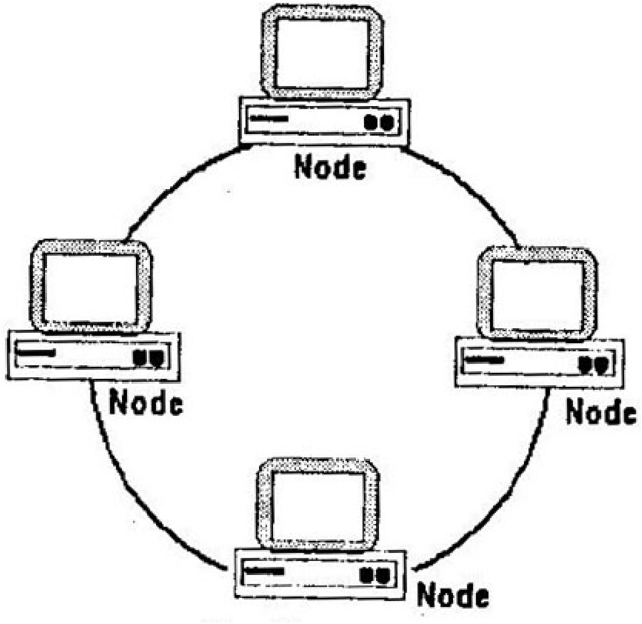
Advantages:

- No loss in signal quality because each computer retransmits the signal.
- Easy to install.
- Easy to troubleshoot, because it’s easy to locate the fault areas.
- No need to terminate cable.

Disadvantages:

- Unless you have a dual ring, which is expensive, a single failed station can bring down the whole network.
- It’s hard to reconfigure large rings.
- It uses more cable than the bus topology.
- As with all networks, there are limitations in the size of the ring and number of devices.

Examples: IBM Token Ring and Fiber Distributed Data interface (FDDI)



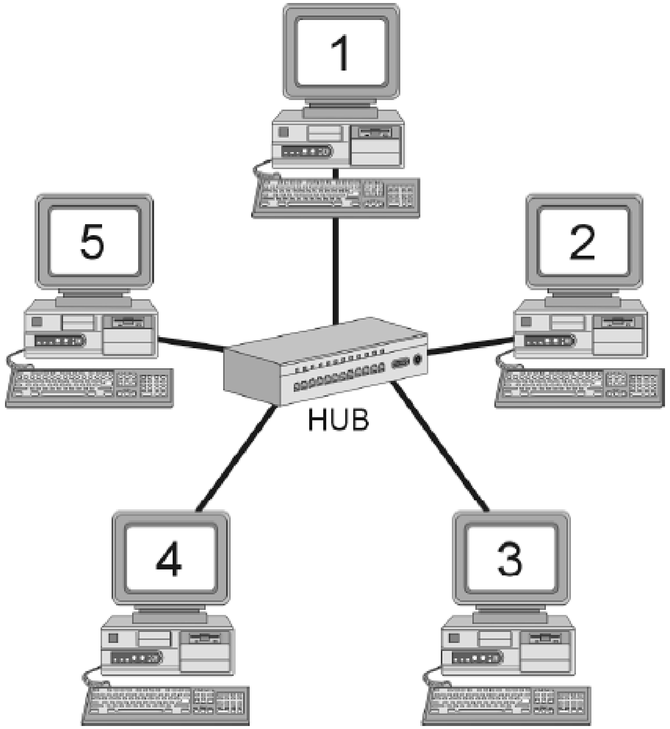
- **Star Topology:**
- In star network, a device called a hub is placed in the center of the network, i.e. all nodes are connected to the central hub and communicate through it.
- Groups of data are routed through the hub and sent to all the attached nodes, thus eventually reaching their destinations.
- In this topology, the cables go out from the hub in all directions. Most hubs are active, and can monitor traffic and regenerate each signal. Other hubs are passive and act only as connection points. The computers in topology are all passive.
- Now, here’s the good example of where the apparent physical topology doesn’t have to match the logical topology. Some networks look like stars because they are connected to a hub. But inside the hub the connections go from one to another in a straight line, like a bus. It’s a bus topology, but that’s not visible from outside the hub.

Advantages:

- It’s quite inexpensive
- Its easy to troubleshoot.
- If there’s a media failure, it only affects one computer.
- Its easy to reconfigure, just plug and unplug devices.

Disadvantages:

- Data transmission rates are low.
- There aren’t any de jure (by law) standards.
- It requires a lot of cable.
- Its somewhat difficult to install, you have to find paths to run all that cable to the hub.



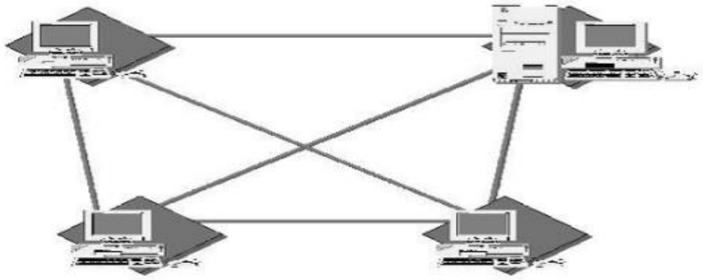
- **Mesh Topology:**
- The mesh topology is the least used network and the most expensive to implement.
- In a mesh environment, a cable runs from every computer to every other computer.
- If you have four computers, you must have six cables- three coming from each computer to the other computers.
- Devices are connected with many interconnections between network nodes.

Advantages:

- Great reliability. Data can never fail to be delivered; if one connection goes down, there are other ways to route the data to its destination.

Disadvantages:

- Requires lots of cable and connections.
- Impractical for most workplace environments.



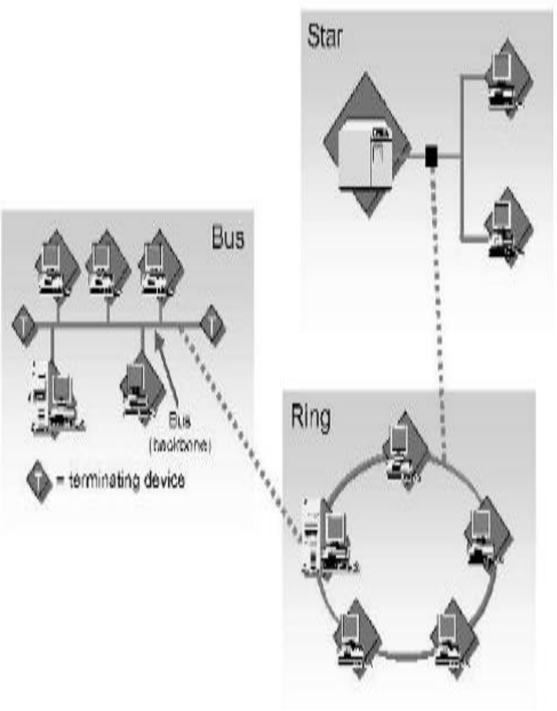
- **Hybrid Topology:**
- In reality, network topologies might combine characteristics from more than one of these standard patterns. This is usually because a functioning network is really a combination of several smaller networks. Networks that combine more than one topology are called hybrid networks. It is very hard to design and implement the hybrid topology.
- It is used in large wide area networks because each topology has its own strengths and weaknesses, several different types can be combined for maximum effectiveness.

Advantages:

- A company can combine the benefits of several different types of topologies.
- Workgroup efficiency and traffic can be customized.

Disadvantages:

- Devices on one topology cannot be placed into another topology without some hardware changes.

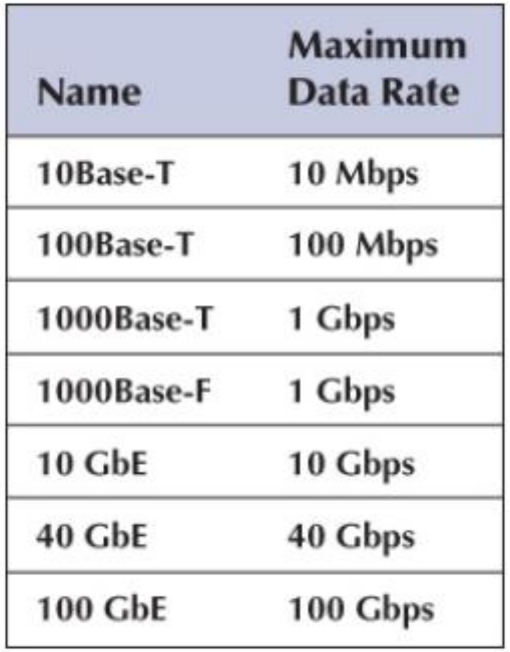


- **Media Access Control:**
- Media Access Control (MAC) protocols are a set of rules and procedures used in network communication to control how devices on a shared network medium access and transmit data. MAC protocols are essential for coordinating access to the transmission medium, ensuring that multiple devices can share it efficiently and avoid data collisions. Here are some common MAC protocols used in various network technologies:
- **Ethernet MAC (CSMA/CD):** Ethernet, one of the most widely used LAN technologies, uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) MAC protocol. In CSMA/CD, devices listen to the network to detect if it's busy (carrier sense)before attempting to transmit. If a collision is detected (two devices transmitting simultaneously), a backoff and retry mechanism is employed to prevent further collisions.
- **Ethernet MAC (CSMA/CA):** In wireless Ethernet networks (Wi-Fi), the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol is used. CSMA/CA avoids collisions by requesting permission (Clear to Send, or CTS) from the access point before transmitting, reducing the chances of collisions compared to CSMA/CD.

- **Token Ring:** Token Ring networks use a MAC protocol where devices communicate in a circular, token-passing manner. A token is continuously passed around the network, and only the device holding the token is allowed to transmit data. This deterministic approach minimizes collisions and is especially suitable for time-sensitive applications.
- **CSMA/CA in Wi-Fi:** Wi-Fi networks use a variant of CSMA/CA optimized for wireless communication. Devices listen for clear channels and send Request to Send (RTS) and Clear to Send (CTS) packets to reserve channel access. This reduces the chances of collisions in wireless environments.
- **Token Bus:** Similar to Token Ring, Token Bus networks use a token-passing MAC protocol. However, Token Bus networks are organized as a linear bus topology, with devices attaching to the bus.
- **Token-Passing in FDDI**: Fiber Distributed Data Interface (FDDI) is a high-speed LAN technology that uses a token-passing MAC protocol for data transmission. Devices connected to an FDDI network pass a token to gain access to the network medium.

- **Time Division Multiple Access (TDMA):** TDMA is commonly used in cellular networks. It divides time into slots, and each device is allocated specific time slots to transmit data. This ensures efficient use of the shared medium and avoids collisions.
- **Carrier Sense Multiple Access (CSMA):** The basic concept of CSMA is used in various networking technologies. Devices listen to the network to determine if it's clear before transmitting. There are variations of CSMA, including CSMA/CD (used in Ethernet) and CSMA/CA (used in Wi-Fi).
- **Aloha Protocols:** Aloha and its variants (Pure Aloha and Slotted Aloha) are MAC protocols used in early radio-based networks. Devices transmit data at any time in the case of Pure Aloha and within specific time slots in the case of Slotted Aloha. These protocols have high collision rates but were influential in the development of later MAC protocols.

- **Types of Ethernet:**
- Table summarizes the many different types of Ethernet in use today. The 10Base-T standard revolutionized Ethernet and made it the most popular type of LAN in the world. Today, 100Base-T and 1000Base-T are the most common forms of Ethernet.
- Other types of Ethernet include 1000Base-F (which runs at 1 Gbps and is sometimes called 1 GbE), 10 GbE (10 Gbps), 40 GbE (40 Gbps), and 100 GbE (100 Gbps). They can use Ethernet's traditional half-duplex approach, but most are configured to use full duplex. Each is also designed to run over fiber-optic cables, but some may also use traditional twisted-pair cables (e.g., Cat 5e).
- For example, two common versions of 1000Base-F are 1000Base-LX and 1000Base-SX, both of which use fiber-optic cable, running up to 440 and 260 meters, respectively; 1000Base-T, which runs on four pairs of category 5 twisted-pair cable, but only up to 100 meters; and 1000Base-CX, which runs up to 24 meters on one category 5 cable. Similar versions of 10 and 40 GbE that use different media are also available.



Name	Maximum Data Rate
10Base-T	10 Mbps
100Base-T	100 Mbps
1000Base-T	1 Gbps
1000Base-F	1 Gbps
10 GbE	10 Gbps
40 GbE	40 Gbps
100 GbE	100 Gbps

- Some organizations use 10/100/1000 Ethernet, which is a hybrid that can run at any of these three speeds; 10/100/1000 NICs and switches detect the signal transmitted by the computer or device on the other end of the cable and will use 10 Mbps, 100 Mbps, or 1 Gbps, depending on which the other device uses.

Wireless Ethernet

- Wireless Ethernet (commonly called Wi-Fi) is the commercial name for a set of standards developed by the IEEE 802.11 standards group. A group of vendors selling 802.11 equipment trademarked the name Wi-Fi to refer to 802.11 because they believe that consumers are more likely to buy equipment with a catchier name than 802.11.
- Wi-Fi is intended to evoke memories of Hi-Fi, as the original stereo music systems in the 1960s were called. The 802.11 family of technologies is much like the Ethernet family. They reuse many of the Ethernet 802.3 components and are designed to connect easily into Ethernet LANs. For these reasons, IEEE 802.11 is often called wireless Ethernet. Just as there are several different types of Ethernet (e.g., 10Base-T, 100Base-T, and 1000Base-T), there are several different types of 802.11.

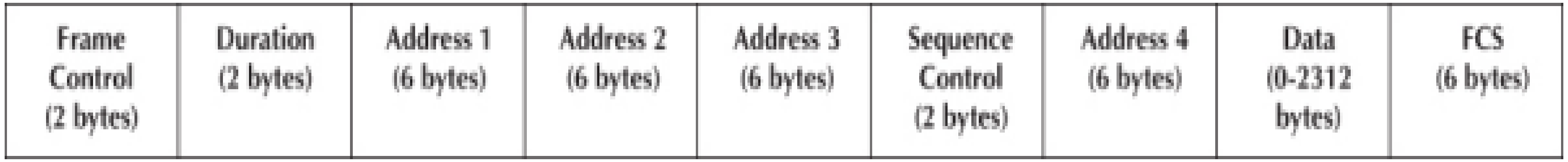
- **Topology:**
- The logical and physical topologies of Wi-Fi are the same as those of hubbased Ethernet: a physical star and a logical bus. There is a central AP to which all computers direct their transmissions (star), and the radio frequencies are shared (bus) so that all computers must take turns transmitting.

- **Media Access Control:**
- The Media Access Control (MAC) protocol for wireless Ethernet, also known as Wi-Fi, is a set of rules and procedures that govern how wireless devices access and transmit data over a shared wireless medium. Unlike wired Ethernet (e.g., Ethernet over twisted-pair cables), wireless Ethernet operates over the air using radio frequency (RF) signals. Some key components and principles of the MAC protocol for Wi-Fi are:
- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):** Wi-Fi networks use CSMA/CA as the fundamental MAC protocol. CSMA/CA is designed to prevent collisions that can occur in the absence of physical cables where devices can't directly detect collisions as they do in wired Ethernet (CSMA/CD).
- **Channel Selection and Clear Channel Assessment (CCA):** Wireless devices listen to the RF environment to determine if the communication channel is busy (carrier sense). If a channel is clear, the device can initiate data transmission. This process helps avoid collisions.

- **Request to Send/Clear to Send (RTS/CTS):** To further reduce the likelihood of collisions, some Wi-Fi devices use an optional mechanism called Request to Send (RTS) and Clear to Send (CTS). Before transmitting data, a device sends an RTS frame requesting permission to transmit. If it receives a CTS frame in response, it knows the channel is clear for data transmission.
- **Distributed Coordination Function (DCF):** DCF is the most commonly used access method in Wi-Fi networks. It employs a backoff mechanism, where devices select random backoff times before attempting to transmit. This helps distribute access fairly and prevent multiple devices from contending for the channel simultaneously.
- **Contention Windows:** The duration of the backoff is randomized based on a contention window. Shorter contention windows are used for devices that have experienced fewer collisions or are closer to the access point, allowing them to gain quicker access.
- **Interframe Spacing (IFS):** Different types of frames (e.g., data, acknowledgment) are separated by specific interframe spacing values. For example, after a data frame, thereis usually a short IFS before the acknowledgment frame to avoid collisions.

- **Wireless Network Infrastructure:** Wi-Fi networks typically have wireless access points (APs) that manage the RF medium and coordinate communication between devices. APs are responsible for selecting channels, managing network parameters, and controlling which devices can access the network. SSID (Service Set Identifier): Each Wi-Fi network is identified by a unique SSID. Devices scan for available SSIDs and choose which network to connect to based on the SSID they select.
- **Authentication and Encryption**: Wi-Fi networks often use security protocols like WPA3 or WPA2 to authenticate and encrypt data, ensuring that unauthorized device cannot access the network or decipher transmitted information.
- **Quality of Service (QoS):** Wi-Fi networks can implement QoS mechanisms prioritize specific types of traffic (e.g., voice or video) to ensure they receive the necessary bandwidth and low latency.
- **Roaming:** Wi-Fi devices can roam between access points as they move within a wireless network's coverage area. This seamless handover requires coordination between APs.
- **Wireless Standards:** Wi-Fi networks adhere to IEEE 802.11 standards, such 802.11ac, 802.11n, and 802.11ax, which define the rules and specifications for wire communication.

- **Wireless Ethernet Frame Layout**
- An 801.11 data frame is illustrated in Figure. We notice two major differences when we compare the 802.11 frame to the 802.3 frame used in wired Ethernet.



Frame Control (2 bytes)	Duration (2 bytes)	Address 1 (6 bytes)	Address 2 (6 bytes)	Address 3 (6 bytes)	Sequence Control (2 bytes)	Address 4 (6 bytes)	Data (0-2312 bytes)	FCS (6 bytes)

- First, the wireless Ethernet frame has four address fields rather than two like the wired Ethernet. These four address fields are source address, transmitter address, receiver address, and destination address. The source and destination address have the same meaning as in wired Ethernet. However, because every NIC has to communicate via an AP (it cannot directly communication with another NIC), there is a need to add the address of the AP and also any other device that might be needed to transmit the frame. To do this, the transmitter and received address fields are used.

- Second, there is new field called sequence control that indicates how a large frame is fragmented—split into smaller pieces. Recall that in wired networks this is done by the transport layer, not the data link layer. Moving the segmentation to the data link layer for wireless makes the transmission transparent to the higher layers. The price, however, is less efficiency because of the size of the frame and thus also a higher error rate.

- **Types of Wireless Ethernet:**
- Wi-Fi is one of the fastest changing areas in networking. There are six versions of Wi-Fi; all but the last two or three versions are obsolete but may still be in use in some companies. All the different types are backward compatible, which means that laptops and APs that use new versions can communicate with laptops and APs that use older versions. However, this backward compatibility comes with a price. These old laptops become confused when other laptops operate at high speeds near them, so when an AP detects the presence of a laptop using an old version, it prohibits laptops that use the newer versions from operating at high speeds. Thus, one old laptop will slow down all the other new laptops around it.

- These wireless Ethernet types are based on the IEEE 802.11 family of standards and include:
- **802.11a:** This standard operates in the 5 GHz frequency band and offers high data rates. It was one of the first Wi-Fi standards to provide faster speeds but has limited range compared to some other standards.
- **802.11b:** Operating in the 2.4 GHz frequency band, 802.11b was one of the earliest and most widely adopted Wi-Fi standards. It provides data rates of up to 11 Mbps. However, it has limited bandwidth and may be susceptible to interference from other devices operating in the same frequency range.
- **802.11g:** Also operating in the 2.4 GHz band, 802.11g offers data rates of up to 54 Mbps, making it significantly faster than 802.11b. It is backward compatible with 802.11b, which facilitated its adoption.
- **802.11n:** This standard operates in both the 2.4 GHz and 5 GHz bands and offers data rates of up to 600 Mbps. 802.11n introduced multiple-input multiple-output (MIMO) technology, which enhances performance and range. It also improved signal quality and reliability.

- **802.11ac:** Also known as Wi-Fi 5, 802.11ac operates exclusively in the 5 GHz band and offers data rates of up to several gigabits per second. It introduced advanced features such as wider channels and beamforming, significantly improving network performance and capacity.
- **The IEEE 802.11ad:** It is often referred to as WiGig, is a wireless communication standard designed to provide extremely high data rates and very short-range wireless connectivity in the 60 GHz frequency band. It was developed to support high-speed data transfer, wireless displays, and short-range applications where data rates are critical.
- **802.11ax:** Commonly referred to as Wi-Fi 6, this standard operates in both 2.4 GHz and 5 GHz bands and offers data rates exceeding 10 Gbps. Wi-Fi 6 introduces technologies like Orthogonal Frequency Division Multiple Access (OFDMA) and Target Wake Time (TWT), which improve network efficiency and capacity. Wi-Fi 6 is designed for high-density environments and is more energy-efficient.

- **802.11ay:** This standard operates in the 60 GHz frequency band and provides extremely high data rates (tens of gigabits per second). It is designed for very short-range, high-speed wireless communication, often used for specific applications like wireless displays and high-speed data transfers.
- **802.11ah:** Also known as Wi-Fi HaLow, 802.11ah operates in the sub-1 GHz frequency range, providing extended range and coverage, making it suitable for low-power, long-range applications like IoT devices and smart home networks.
- **802.11af:** This standard, often called "White-Fi," operates in unused TV spectrum (TV white spaces) and provides extended range and coverage. It's suitable for rural broadband access and other long-range applications.

- **Security:**
- Wireless Ethernet (Wi-Fi) security is essential to protect your wireless network from unauthorized access, data breaches, and other security threats. Implementing strong security measures helps maintain the confidentiality, integrity, and availability of your network and its data. Moreover, wireless intrusion detection and prevention systems also enable protection of a wireless network by alerting the wireless network administrator in case of a security breach. Some key aspects of wireless Ethernet security are:
- **Encryption:** Use encryption protocols to secure the data transmitted over the wireless network. The two primary encryption standards for Wi-Fi are WPA2 (Wi-Fi Protected Access 2) and WPA3. Avoid using WEP (Wired Equivalent Privacy), as it is not as secure.
- **Wired Equivalent Policy (WEP):** WEP was developed for wireless networks and approved as a Wi-Fi security standard in September 1999. WEP was supposed to offer the same security level as wired networks, however there are a lot of well-known security issues in WEP, which is also easy to break and hard to configure. Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

- **Wi-Fi Protected Access (WPA):** This wireless security protocol precedes the WEP. Hence, it is designed to deal with the flaws that are found with the WEP protocol. Most modern WPA applications use a pre-shared key (PSK), most often referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP) for encryption. WPA Enterprise uses an authentication server for keys and certificates generation.
- **Wi-Fi Protected Access 2 (WPA2):** The WPA2 (also called 802.11i), a successor to WPA, comes with enhanced features and encryption abilities. For instance, the WPA2 uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) instead of (TKIP). This replacement feature is known to be efficient in encrypting data. Hence, WPA2 is considered the best wireless security protocol. At this time the main vulnerability to a WPA2 system is when the attacker already has access to a secured Wi-Fi network and can gain access to certain keys to perform an attack on other devices on the network.
- **Wi-Fi Protected Access 3 (WPA3):** This one is a recent wireless protocol. It is enhanced in terms of encryption abilities and keeping hackers at bay from both private and public networks. WPA3 will protect against dictionary attacks by implementing a new key exchange protocol. WPA3's expanded encryption for public networks also keeps Wi-Fi users safe from a vulnerability they may not realize exists in the first place. In fact, if anything it might make Wi-Fi users feel too secure.

- **MAC Filtering:** Enable MAC address filtering to restrict access to authorized devices only. Each device's unique MAC address is added to an access control list (ACL) to grant or deny network access.
- **Network Authentication:** Use strong and unique network authentication credentials, such as Wi-Fi passwords (pre-shared keys or PSKs), to prevent unauthorized access. Consider using long and complex passwords or passphrases that are difficult to guess.
- **Change Default Passwords**: Change default passwords for Wi-Fi routers and access points to eliminate the risk of attackers using default credentials to gain access.
- **Hidden SSID**: Consider hiding the SSID (Service Set Identifier), which is the name of your Wi-Fi network. Although this does not provide strong security, it can make your network less visible to casual users.
- **Two-Factor Authentication (2FA):** Some Wi-Fi routers and access points support two-factor authentication for network access. This adds an extra layer of security by requiring a second form of authentication in addition to a password.

- **Firewalls:** Enable the built-in firewall on your wireless router or access point to block unauthorized incoming traffic and protect your network from external threats.
- **Firmware Updates:** Regularly update the firmware of your wireless router and access points. Manufacturers release updates to patch security vulnerabilities and enhance network security.
- **Network Segmentation:** Use network segmentation to separate different types of devices (e.g., IoT devices, personal computers, work devices). This limits the potential damage if one segment is compromised.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Implement IDS and IPS solutions to monitor and protect your network against unusual or malicious activities. Logging and Monitoring: Enable logging and monitoring of network activities to detect suspicious behavior and security incidents.
- **Physical Security:** Physically secure your wireless networking equipment to prevent unauthorized access. Place routers and access points in secure locations, Regular Audits: Periodically audit your network security to ensure that security measures are up to date and effective.
- **Security Best Practices:** Follow best practices for security, including keeping software and operating systems updated, using strong passwords, and educating users about security risks.

The Best Practice LAN Design

- This section focuses on the design of wired and wireless LANs that provide network access to users. The data center and e-commerce edge also use LANs.
- The past few years have seen major changes in LAN technologies (e.g., gigabit Ethernet and high-speed wireless Ethernet). As technologies have changed and costs have dropped, so too has our understanding of the best practice design for LANs.
- One of the key questions facing network designers is the relationship between Wi-Fi and wired Ethernet. The data rates for Wi-Fi have increased substantially with the introduction of each new version of 802.11, so they are similar to the data rates offered by 100Base-T wired Ethernet. The key difference is that 100Base-T wired Ethernet using switches provides 100 Mbps to each user, whereas Wi-Fi shares its available capacity among every user on the same AP, so as more users connect to the APs, the network gets slower and slower.
- Wi-Fi is considerably cheaper than wired Ethernet because the largest cost of LANs is not the equipment, but in paying someone to install the cables.

- Most organizations today install wired Ethernet to provide access for desktop users and install Wi-Fi as overlay networks. They build the usual switched Ethernet networks as the primary LAN, but they also install Wi-Fi for laptops and mobile devices. Some organizations have begun experimenting with Wi-Fi by moving groups of users off the wired networks onto Wi-Fi as their primary network to see whether Wi-Fi is suitable as a primary network.
- Today, we still believe the best practice is to use wired Ethernet for the primary LAN, with Wi-Fi as an overlay network. However, this may change.
- A network (usually a WLAN) used to supplement a primary network (usually a wired LAN) is called overlay networks.
- Designing a Local Area Network (LAN) that is efficient, secure, and scalable requires careful planning and adherence to best practices. LAN design is an ongoing process, and staying updated with evolving technologies and security threats is essential. Regularly review and adapt your network design to meet changing business requirements and cybersecurity challenges. Here are some key considerations and best practices for LAN design:

- **Needs Assessment:** Start by understanding the specific requirements of your organization. Consider factors such as the number of users, the types of applications, data transfer rates, and future growth expectations.
- **Topology Selection:** Choose an appropriate network topology based on your organization's needs. Common topologies include star, bus, ring, mesh, and tree. The star topology is often recommended for its ease of management and scalability.
- **Redundancy:** Implement redundancy in critical network components, such as switches and routers, to ensure high availability. This can involve deploying redundant hardware and using protocols like HSRP (Hot Standby Router Protocol) or VRRP (Virtual Router Redundancy Protocol).
- **Scalability:** Design the LAN to accommodate future growth. Use modular and expandable components to make it easier to add devices or expand the network as needed.
- **Segmentation:** Divide the LAN into segments or VLANs (Virtual LANs) to improve network performance, enhance security, and isolate traffic. VLANs can be created based on departments, functions, or security requirements.

- **Quality of Service (QoS):** Implement QoS mechanisms to prioritize network traffic. This ensures that critical applications, such as VoIP or video conferencing, receive the necessary bandwidth and low latency. Subnetting: Properly plan IP addressing and subnetting to avoid IP address conflicts and efficiently manage IP resources.
- **Security:** Prioritize network security. Utilize firewalls, intrusion detection and prevention systems, access control, and encryption to protect against unauthorized access, data breaches, and threats. Regularly update security measures to address new vulnerabilities.
- **Authentication and Authorization:** Implement strong user authentication mechanisms, such as RADIUS or LDAP, to ensure that only authorized users can access the network resources.
- **Access Control:** Control access to network resources through user-based and role-based access controls. Limit access to sensitive data and applications based on user permissions.
- **Backup and Disaster Recovery:** Establish backup and disaster recovery procedures to ensure data and network services are recoverable in case of unexpected events.

- **Monitoring and Management:** Deploy network management tools to monitor network performance, detect issues, and manage network components. Regularly review logs and alerts to identify and address network problems proactively.
- **Cable Management:** Properly organize and label network cables to simplify troubleshooting and maintenance. Use cable management solutions to keep cables neat and prevent physical damage.
- **Documentation:** Maintain detailed network documentation, including network diagrams, configurations, and hardware specifications. This documentation is invaluable for troubleshooting and planning upgrades.
- **Regular Maintenance:** Schedule routine maintenance tasks, such as updating firmware and software, applying security patches, and testing network performance.
- **Employee Training**: Educate employees about network security best practices to reduce the risk of security breaches resulting from human errors.
- **Compliance:** Ensure that your network design and operation comply with relevant industry regulations and data protection standards (e.g., GDPR, HIPAA).
- **Consult Experts:** Consider consulting with network professionals or experts for complex network design or significant upgrades to ensure best practices are followed.

Designing User Access with Wired Ethernet

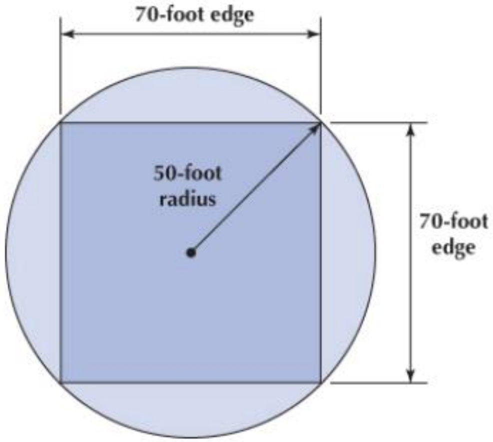
- Many organizations today install switched 100Base-T or 1000Base-T over category 5e wiring for their wired LANs. It is relatively low cost and fast.
- In the early days of LANs, it was common practice to install network cable wherever it was convenient. Little long-term planning was done. The exact placement of the cables was often not documented, making future expansion more difficult—you had to find the cable before you could add a new user.
- With today’s explosion in LAN use, it is critical to plan for the effective installation and use of LAN cabling. The cheapest point at which to install network cable is during the construction of the building; adding cable to an existing building can cost significantly more.
- Indeed, the costs to install cable (i.e., paying those doing the installation and additional construction) are usually substantially more than the cost of the hubs and switches, making it expensive to reinstall the cable if the cable plan does not meet the organization’s needs. Most buildings under construction today have a separate LAN cable plan, as they have plans for electrical cables. Each floor has a data wiring closet that contains one or more network hubs or switches. Cables are run from each room on the floor to this wiring closet.

- Designing user access with wired Ethernet involves planning and configuring the network infrastructure to provide secure, reliable, and efficient connectivity for end-users. It begins with determining the specific access requirements, such as the number of users, their locations, and the types of devices they'll be using.
- Once these requirements are identified, the network can be designed to accommodate them. This includes selecting the appropriate network topology, cabling, and switches to ensure seamless connectivity. Security is a critical aspect, and access controls, such as user authentication and authorization, should be implemented to restrict network access to authorized personnel.
- Quality of Service (QoS) mechanisms can be applied to prioritize critical applications and services. Regular maintenance and monitoring are essential to ensure that the network operates optimally and to address any issues promptly. An effective wired Ethernet user access design provides a stable and secure foundation for users to connect to the network, facilitating their productivity and the efficient operation of the organization.

Designing User Access with Wireless Ethernet

- Selecting the best practice wireless technology is usually simple. You pick the newest one, cost permitting. Today, 802.11ac is the newest standard, but in time, there will be a new one.
- Designing the physical WLAN is more challenging than designing a wired LAN because the potential for radio interference means that extra care must be taken in the placement of APs to ensure that their signals do not overlap.
- With the design of LANs, there is considerable freedom in the placement of switches, subject to the maximum limits to the length of network cables. In WLANs, however, the placement of the APs needs to consider both the placement of other APs and the sources of interference in the building.
- The physical WLAN design begins with a site survey. The site survey determines the feasibility of the desired coverage, the potential sources of interference, the current locations of the wired network into which the WLAN will connect, and an estimate of the number of APs required to provide coverage. WLANs work very well when there is a clear line of sight between the AP and the wireless computer. The more walls there are between the AP and the computer, the weaker the wireless signal becomes. The type and thickness of the wall also has an impact; traditional drywall construction provides less interference than does concrete block construction.

- An AP with an omnidirectional antenna broadcasts in all directions. Its coverage area is a circle with a certain radius. Wi-Fi has a long range, but real-world tests of Wi-Fi in typical office environments have shown that data rates slow down dramatically when the distance from a laptop to the AP exceeds 50 feet.
- Therefore, many wireless designers use a radius of 50 feet when planning traditional office environments, which ensures access high quality coverage. It is also expensive, because many APs will need to be purchased. Costs may be reduced by using a longer radius (e.g., 100 feet), so that fewer APs are needed, but this may result in slower data rates.
- One may design wireless LANs using this 50-foot-radius circle, but because most buildings are square, it is usually easier to design using squares. Figure shows that a 50-foot radius translates into a square that is approximately 70 feet on each edge. For this reason, most designers plan wireless LANs using 50- to 75-foot squares, depending on the construction of the building: smaller squares in areas where there are more walls that can cause more interference and larger squares in areas with fewer walls.



Design parameters for Wi-Fi access point range

- When designing a wireless LAN, it is important to ensure that the APs don’t interfere with each other. If all APs transmitted on the same frequency, the transmissions of one AP would interfere with another AP where their signals overlapped—just like what happens on your car radio when two stations are in the same frequency. Therefore, each AP is set to transmit on a different channel, very much like the different channels on your TV.
- Suppose you had a conference room or classroom that needed several APs to provide adequate Wi-Fi for everyone who will use it. You could put several APs in the same room and set them on different channels so their signals did not interfere with each other. One challenge is managing the number of users on each AP. Laptops and mobile phones connect to the AP with the strongest signal, which means most will connect to the same AP. If too many users connect to one AP, it will get very busy and Wi-Fi speeds will be slow, while the other APs in the room will be only lightly used. This occurs because standard APs are autonomous and do not talk to each other. Each AP only responds to the devices that request access to it.

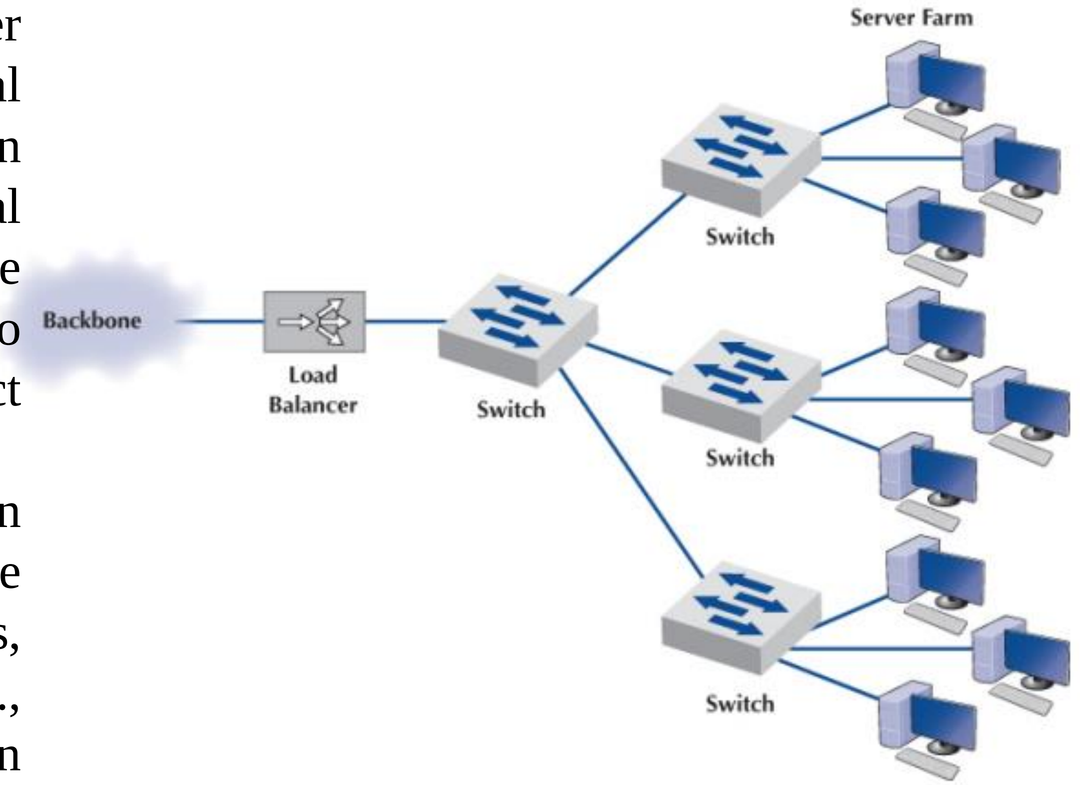
- Most large companies install managed APs that are different than the SOHO APs we install in our homes and apartments. Managed APs are wired into a Wi-Fi Controller (rather than a normal hub or switch). They report what devices are attached to them and how busy they are to the controller, which balances traffic across the APs it manages. If a laptop connects to a very busy AP when there are less busy APs nearby, the controller will instruct the AP to deny access to the laptop and the laptop will automatically try to connect to the next AP it sees. As a result, the number of devices connected to each AP and the amount of traffic each receives is balanced across the set of APs managed by the controller, and overall network performance improves.
- After the initial design is complete, a site survey is done using a temporary AP and a computer or device that can actually measure the strength of the wireless signal. The temporary AP is installed in the area as called for in the initial design, and the computer or device is carried throughout the building measuring the strength of the signal. Actually measuring the strength of the signal in the environment is far more accurate than relying on estimated ranges.

- Design becomes more difficult in a multistory building because the signals from the APs travel up and down as well as in all horizontal directions. The design must include the usual horizontal mapping but also an added vertical mapping to ensure that APs on different floors do not interfere with one another. Because floors are usually thicker than walls, signals travel further horizontally than vertically, making design a bit more difficult. It becomes even more difficult if your set of floors in a large office tower is surrounded by APs of other companies. You have to design your network not to interfere with theirs.

Designing the Data Center

- The data center is where the organization houses its primary servers. In most large organizations, the data center is huge because it contains the data center as well as the campus backbone switches and the enterprise edge.
- Designing the data center requires considerable expertise, because most data on a network flow from or to the data center. In all large-scale networks today, servers are placed together in server farms or clusters, which sometimes have hundreds of servers that perform the same task. Yahoo.com, for example, has more than a thousand Web servers that do nothing but respond to Web search requests. In this case, it is important to ensure that when a request arrives at the server farm, it is immediately forwarded to a server that is not busy—or that is the least busy.
- A special device called a load balancer or load balancing switch acts as a router at the front of the server farm. All requests are directed to the load balancer at its IP address. When a request hits the load balancer, it forwards it to one specific server using its IP address. Sometimes a simple round-robin formula is used (requests go to each server one after the other in turn); in other cases, more complex formulas track how busy each server actually is. If a server crashes, the load balancer stops sending requests to it, and the network continues to operate without the failed server. Load balancing makes it simple to add servers (or remove servers) without affecting users. You simply add or remove the server(s) and change the software configuration in the load balancing switch; no one is aware of the change.

- Server virtualization is somewhat the opposite of server farms and load balancing. Server virtualization is the process of creating several logically separate servers (e.g., a Web server, an email server, and a file server) on the same physical computer. The virtual servers run on the same physical computer but appear completely separate to the network (and if one crashes, it does not affect the others running on the same computer).
- Some operating systems enable virtualization natively, which means that it is easy to configure and run separate virtual servers. In other cases, special purpose virtualization software (e.g., VMware) is installed on the server and sits between the hardware and the operating systems; this software means that several different operating systems can be installed on the same physical computer.



Network with load balancer

- A storage area network (SAN) is a LAN devoted solely to data storage. When the amount of data to be stored exceeds the practical limits of servers, the SAN plays a critical role. The SAN has a set of high-speed storage devices and servers that are networked together using a very high speed network. When data are needed, clients send the request to a server on the LAN, which obtains the information from the devices on the SAN and then returns it to the client.
- The devices on the SAN may be a large set of database servers or a set of network-attached disk arrays. In other cases, the devices may be network attached storage (NAS) devices. A NAS is not a general-purpose computer, such as a server that runs a server operating system (e.g., Windows and Linux); instead, it has a small processor and a large amount of disk storage and is designed solely to respond to requests for files and data. NAS can also be attached to LANs, where they function as fast file servers.

Designing the e-Commerce Edge

- The e-commerce edge contains the servers that are designed to serve data to customers and suppliers, such as the corporate Web server. The e-commerce edge is essentially a smaller, specialized version of the data center. It contains all the same equipment as the data center (e.g., load balancer, SAN, and UPS), but this equipment supports access by users external to the organization. It is often connected directly to the Internet access part of the network via a very-high-speed circuit as well as the campus backbone.
- The e-commerce edge often has different security requirements than the servers in the data center intended for use by employees inside the organization because the e-commerce edge is primarily intended to serve those external to the organization.
- Designing the e-Commerce edge involves creating a robust and customer-centric digital storefront, enabling businesses to connect with online shoppers, manage transactions, and deliver an exceptional shopping experience. It starts with a deep understanding of the specific needs of your e-commerce operation, including the range of products or services you offer and your expected customer base. Your e-commerce website or application serves as the digital face of your business, requiring a user-friendly design optimized for both desktop and mobile devices to ensure a seamless shopping experience. Implementing a Content Delivery Network (CDN) is vital to optimize content delivery, reduce latency, and accelerate page loading times.

- A reliable web hosting provider is crucial to ensure high uptime and consistent performance. Scalability is a key consideration, as your e-commerce platform should easily handle fluctuations in traffic and business growth. Security measures are paramount to protect customer data, transactions, and the integrity of the platform. This includes the use of SSL/TLS encryption, firewalls, and intrusion detection systems. Payment gateways and inventory management systems must be seamlessly integrated to offer secure payment options and real-time stock information. Effective order management and personalized recommendations are essential to cater to customers' preferences and provide a personalized shopping experience.
- Furthermore, the site should be mobile-optimized, as mobile commerce continues to grow in significance. Robust customer support channels, such as live chat, email, and phone support, coupled with an efficient ticketing system, can streamline customer inquiries. Regular testing and analysis of user experience helps identify and rectify performance issues. E-commerce analytics tools offer insights into customer behavior and sales trends, driving informed decision-making. Security and regulatory compliance are crucial aspects, ensuring the platform aligns with industry standards and data protection regulations. By designing the e-commerce edge, businesses can effectively reach customers, enhance their online shopping experience, and ensure secure and efficient operations in the digital marketplace.

Designing the SOHO Environment

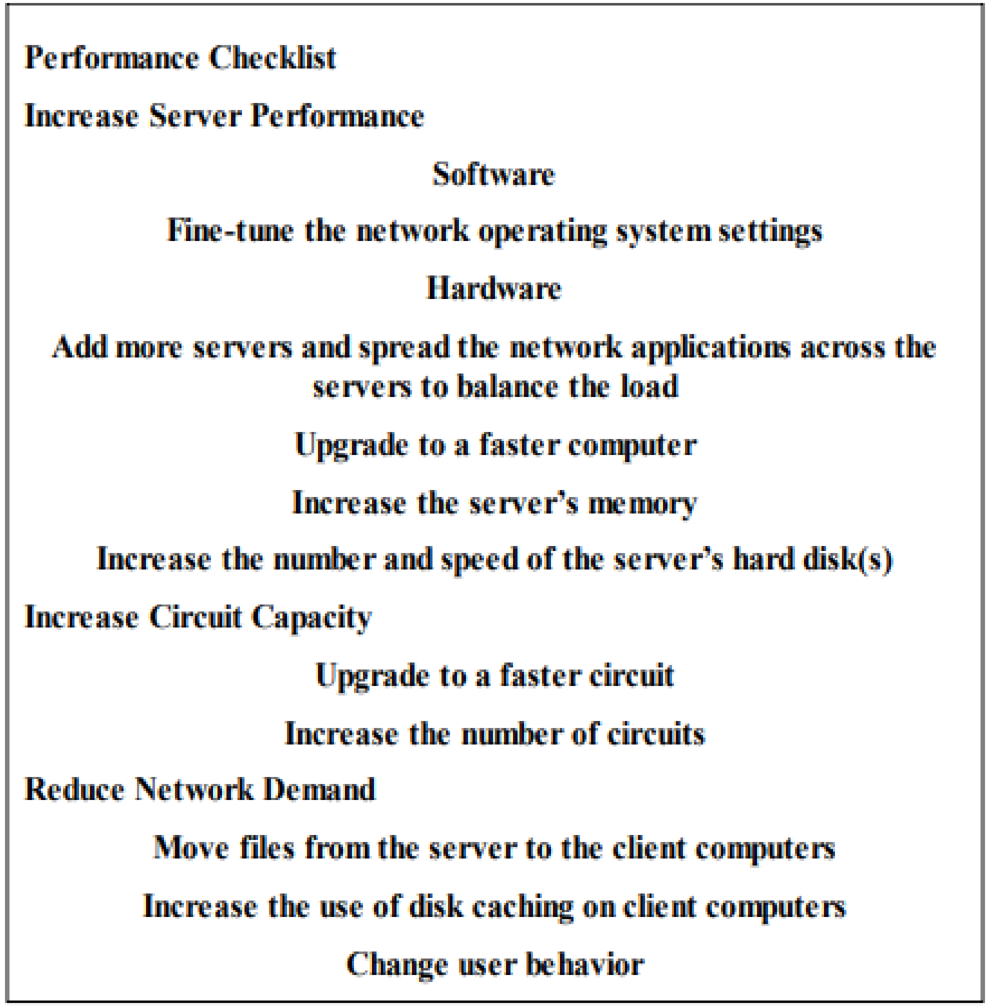
- Designing a Small Office/Home Office (SOHO) environment entails crafting a workspace that is both functional and efficient, whether you're running a small business or working from home. To get started, a thorough needs assessment is crucial, identifying the specific requirements of your work. Consider the number of users and the nature of the tasks at hand, and then plan your physical space accordingly. Selecting the right furniture, equipment, and computer hardware is key; opt for ergonomic solutions that boost productivity and comfort.
- Establish a robust networking infrastructure with a reliable internet connection, taking into account your online activities. Security measures, including firewalls and antivirus software, should be in place to protect your digital assets, and a solid data backup strategy is essential. Ensure your software and applications align with your work tasks, and consider implementing a professional voice communication system and video conferencing tools for effective collaboration. Don't forget about file organization, physical and cybersecurity, and ergonomic considerations for your workspace's comfort.
- Ultimately, designing a SOHO environment means creating a tailored and secure space that supports your work needs and adapts to the ever- changing demands of your small business or home-based profession. Regular maintenance and cybersecurity practices will help maintain a productive and secure SOHO environment.

- Installing cables for wired Ethernet is expensive, so most SOHO designs use wireless Ethernet. Sometimes a house is big enough that one WAP won’t cover the entire building and the outdoor area. Powerline networking is an old technology that is making a comeback for exactly this situation.
- Powerline networking provides Ethernet over the existing electrical power wires in your house at rates up to 1 Gbps. The powerline adapters convert the traditional wired Ethernet signal that runs over Cat 5e cables into a signal that can travel over the electrical powerwires.

Improving LAN Performance

- When LANs had only a few users, performance was usually very good. Today, however, when most computers in an organization are on LANs, performance can be a problem. Performance is usually expressed in terms of throughput (the total amount of user data transmitted in a given time period) or in response time (how long it takes to get a response from the destination). In this section, we discuss how to improve throughput. We focus on dedicated-server networks because they are the most commonly used type of LANs, but many of these concepts also apply to peer-to-peer networks.
- To improve performance, you must locate the bottleneck, the part of the network that is restricting the data flow. Generally speaking, the bottleneck will lie in one of two places. The first is the network server. In this case, the client computers have no difficulty sending requests to the network server, but the server lacks sufficient capacity to process all the requests it receives in a timely manner. The second location is a network circuit, either the access LAN, the building backbone, the campus backbone, or the circuit into the data center. In this case, the server (or more likely, a server farm) can easily process all the client requests it receives, but a circuit lacks enough capacity to transmit all the requests to the server.

- The first step in improving performance, therefore, is to identify whether the bottleneck lies in a circuit or the server. To do so, you simply watch the utilization of the server during periods of poor performance. If the server utilization is high (e.g., 80–100%), then the bottleneck is the server; it cannot process all the requests it receives in a timely manner. If the server utilization is low during periods of poor performance, then the problem lies with a network circuit; some circuits cannot transmit messages as quickly as necessary.
- Most organizations focus on ways to improve the server and the circuits to remove bottlenecks. These actions address only the supply side of the equation—that is, increasing the capacity of the LAN as a whole. The other way to reduce performance problems is to attack the demand side: reduce the amount of network use by the clients, which we also discuss. Figure provides a performance checklist.



Performance Checklist

Increase Server Performance

Software

Fine-tune the network operating system settings

Hardware

Add more servers and spread the network applications across the servers to balance the load

Upgrade to a faster computer

Increase the server's memory

Increase the number and speed of the server's hard disk(s)

Increase Circuit Capacity

Upgrade to a faster circuit

Increase the number of circuits

Reduce Network Demand

Move files from the server to the client computers

Increase the use of disk caching on client computers

Change user behavior

Improving Server Performance

- Improving server performance can be approached from two directions simultaneously: software and hardware.
- **Software:**
- The NOS (Network Operating Software) is the primary software-based approach to improving network performance. Some NOSs are faster than others, so replacing the NOS with a faster one will improve performance. Each NOS provides a number of software settings to fine-tune network performance. Depending on the number, size, and type of messages and requests in your LAN, different settings can have a significant effect on performance. The specific settings differ by NOS but often include things such as the amount of memory used for disk caches, the number of simultaneously open files, and the amount of buffer space.
- **Hardware**
- One obvious solution if your network server is overloaded is to buy a second server (or more). Each server is then dedicated to supporting one set of application software (e.g., one handles email, another handles the financial database, and another stores customer records). The bottleneck can be broken by carefully identifying the demands each major application software package places on the server and allocating them to different servers.

- Sometimes, however, most of the demand on the server is produced by one application that cannot be split across several servers. In this case, the server itself must be upgraded. **The first place to start is with the server's CPU.** Faster CPUs mean better performance. If you are still using an old computer as a LAN server, this may be the answer; you probably need to upgrade to the latest and greatest. Clock speed also matters: the faster, the better. Most computers today also come with CPU-cache (a very fast memory module directly connected to the CPU). Increasing the cache will increase CPU performance.
- **A second bottleneck is the amount of memory in the server.** Increasing the amount of memory increases the probability that disk caching will work, thus increasing performance.
- **A third bottleneck is the number and speed of the hard disks in the server.** The primary function of the LAN server is to process requests for information on its disks. Slow hard disks give slow network performance.
- The obvious solution is to buy the fastest disk drive possible. Even more important, however, is the number of hard disks. Each computer hard disk has only one read/write head, meaning that all requests must go through this one device.

- By using several smaller disks rather than one larger disk (e.g., five 200 gigabyte disks rather than one 1 terabyte disk), you now have more read/write heads, each of which can be used simultaneously, dramatically improving throughput. A special type of disk drive called RAID (redundant array of inexpensive disks) builds on this concept and is typically used in applications requiring very fast processing of large volumes of data, such as multimedia. Of course, RAID is more expensive than traditional disk drives, but costs have been shrinking. RAID can also provide fault tolerance.

Improving Circuit Capacity

- Improving the capacity of a circuit means increasing the volume of simultaneous messages the circuit can transmit from network clients to the server(s). One obvious approach is simply to buy a bigger circuit. For example, if you are now using a 100Base-T LAN, upgrading to 1000Base-T LAN will improve capacity. Or if you have 802.11n, then upgrade to 802.11ac. You can also add more circuits so that there are two or even three separate high-speed circuits between busy parts of the network, such as the core backbone and the data center. Most Ethernet circuits can be configured to use full duplex, which is often done for backbones and servers.
- Another approach is to segment the network. If there is more traffic on a LAN than it can handle, you can divide the LAN into several smaller segments. Breaking a network into smaller parts is called network segmentation. In a wired LAN, this means adding one of more new switches and spreading the computers across these new switches. In a wireless LAN, this means adding more APs that operate on different channels. If wireless performance is significantly worse than expected, then it is important to check for sources of interference near the AP and the computers such as Bluetooth devices and cordless phones.

Reducing Network Demand

- One way to reduce network demand is to move files to client computers. Heavily used software packages that continually access and load modules from the network can place unusually heavy demands on the network.
- Although user data and messages are often only a few kilobytes in size, today's software packages can be many megabytes in size. Placing even one or two such applications on client computers can greatly improve network performance (although this can create other problems, such as increasing the difficulty in upgrading to new versions of the software).
- Most organizations now provide both wired and wireless networks, so another way to reduce demand is to shift it from wired networks to wireless networks, or vice versa, depending on which has the problem. For example, you can encourage wired users to go wireless or install wired Ethernet jacks in places where wireless users often sit.

- Because the demand on most LANs is uneven, network performance can be improved by attempting to move user demands from peak times to off-peak times. For example, early morning and after lunch are often busy times when people check their email. Telling network users about the peak times and encouraging them to change their habits may help; however, in practice, it is often difficult to get users to change. Nonetheless, finding one application that places a large demand on the network and moving it can have a significant impact (e.g., printing several thousand customer records after midnight).