Unit 6
Wired and Wireless Local Area Networks

Introduction

Most large organizations have numerous wired and wireless LANs connected by backbone networks. These LANs also provide access to a variety of servers and the Internet.
In this chapter, we discuss the fundamental components of a LAN, along with two technologies commonly used in LANs—traditional wired Ethernet (IEEE 802.3) that is commonly used to network desktop computers and wireless Ethernet (IEEE 802.11, commonly called Wi-Fi) that often is used to network laptop computers and mobile devices.

Why use a LAN?

There are two basic reasons for developing a LAN**: information sharing and resource sharing**.

Information sharing refers to having users access the same data files, exchange information via email, or use the Internet. For example, a single purchase order database might be maintained so all users can access its contents over the LAN. The main benefit of information sharing is improved decision making, which makes it generally more important than resource sharing.

Resource sharing refers to one computer sharing a hardware device (e.g., printer, an Internet connection) or software package with other computers on the network to save costs. For example, suppose we have 30 computers on a LAN, each of which needs access to a word processing package. One option is to purchase 30 copies of the software and install one on each computer. This would use disk space on each computer and require a significant amount of staff time to perform the installation and maintain the software, particularly if the package were updated regularly. An alternative is to install the software on the network for all to use. This would eliminate the need to keep a copy on every computer and would free up disk space.

LAN Components

There are several components in a traditional LAN as shown in figure below. The first two are the client computer and the server. Clients and servers have been discussed earlier. The other components are **Network Interface Cards (NICs), Network Circuits, Hubs, Switches, Access Points, and the Network Operating System**.

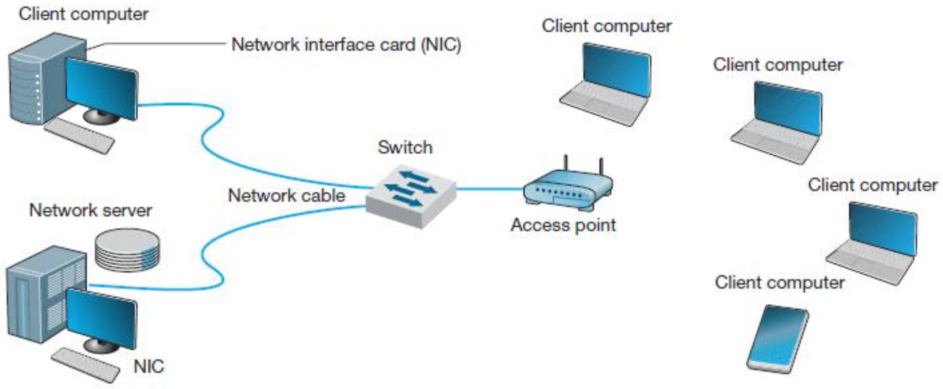
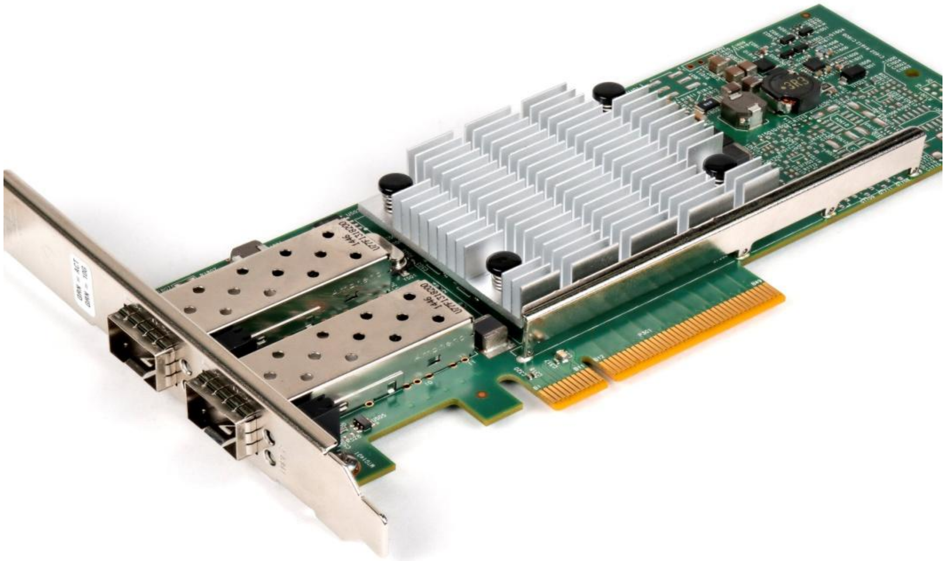


Fig: Local Area Network

Network Interface Cards

The **network interface card (NIC)** is used to connect the computer to the network cable in a wired network and is one part of the physical layer connection among the computers in the network. In a wireless network, the NIC is a radio transmitter that sends and receives messages on a specific radio frequency. Virtually all desktop computers have a wired NIC built in, while virtually all laptops have both a wired NIC and a wireless NIC. You can purchase a wireless NIC for a desktop computer (often as a USB device). NIC is a circuit board or a card often called as LAN adaptor, network adaptor or network card. Every Network adaptor is assigned a unique 48-bit MAC address, which is stored in ROM to identify themselves in a network or a LAN.



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),** or **fiber-optic cable**. Many LANs use UTP wire. 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 also is much lighter, weighing less than 10 pounds per 1,000 feet. Because of its high capacity, fiber-optic cabling is perfect for BNs, although it is beginning to be used in LANs.

Wireless LANs WLANs use radio frequencies or infrared to send data eliminating the requirement of wires. Most countries (but not all) permit WLANs to operate in two frequency ranges: the 2.4 GHz range and the 5 GHz range. These same frequency ranges can be used by cordless phones and baby monitors, which means that WLAN and cordless phone may interfere with each other. Under ideal conditions, the radio transmitters in the NICs and Access Points (AP) 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**.

Network Hubs, Switches, and Access Points

Network **hubs** and **switches** serve two purposes. First, they provide an easy way to connect network cables. A hub or a switch can be thought of as a junction box, permitting new computers to be connected to the network as easily as plugging a power cord into an electrical socket. Each connection point where a cable can be plugged in is called a **port.** Each port has a unique number. Switches can be designed for use in Small Office, Home Office (SOHO) environments or for large enterprise environments.

Simple hubs and switches are commonly available in 4-, 8-, 16-, and 24-port sizes, meaning that they provide anywhere between 4 and 24 ports into which network cables can be plugged. When no cables are plugged in, the signal bypasses the unused port.

When a cable is plugged into a port, the signal travels down the cable as though it were directly connected to the hub or switch. Some switches also enable different types of cables to be connected and perform the necessary conversions (e.g., twisted-pair cable to coaxial cable, coaxial cable to fiber-optic cable).

Second, hubs and switches act as repeaters. Signals can travel only so far in a network cable before they attenuate and can no longer be recognized. All LAN cables are rated for the maximum distance they can be used (typically 100 meters for **twisted-pair cable**, and 400 meters to several kilometers for fiber-optic cable).

A wireless **access point (AP)** is a radio transceiver that plays the same role as a hub or switch in wired Ethernet LANs. It enables the computers near it to communicate with each other and it also connects them into wired LANs, typically using 100Base-T.An AP works at 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. All NICs in the WLAN transmit their frames to the AP and then the AP retransmits the frames over the wireless network or over the wired network to their destination. Therefore, if a frame has to be transmitted from one wireless computer to another, it is transmitted twice, once from the sender to the AP and then from the AP to the destination.

Q. Explain Hub, types of hub, switch, Access Point and key features of Access Point.

Network Operating Systems

The **network operating system (NOS)** is the software that controls the network. It provides the necessary functionality and services for multiple devices and users to communicate, share resources, and access information within a network.

Every NOS provides two sets of software (components): 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.

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 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. windows client Operating Systems (Windows 10, windows 11), macOS, FTP Clients (FileZilla, WinSCP), Email Clients (Microsoft Outlook, Mozilla Thunderbird, Apple Mail) etc are NOS client software.

Characteristics of NOS

1. Network Management
2. User Authentication
3. File and Print Sharing
4. Directory Services
5. Security
6. Data backup and recovery
7. Network monitoring and troubleshooting
8. Scalability
9. Interoperability

Q. Explain the characteristics of NOS.

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.** 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. Ethernet is compatible with a variety of layer 3 protocols but is commonly used with TCP/IP.

Topology

Topology is the basic geometric layout of the network—the way in which the computers on the network are interconnected. It is important to distinguish between a logical topology and a physical topology. A **logical topology** is how the network works conceptually, much like a logical data flow diagram (DFD) or logical entity relation diagram (ERD) in systems analysis and design or database design. A **physical topology** is how the network is physically installed, much like a physical DFD or physical ERD. It includes: **Bus Topology, Ring Topology, Tree Topology, Star Topology, Ring Topology, Mesh Topology, and Hybrid Topology.**

Media Access Control

When several computers share the same communication circuit, it is important to control their access to the media. If two computers on the same circuit transmit at the same time, their transmissions will become garbled. These collisions must be prevented, or if they do occur, there must be a way to recover from them. This is called **media access control. Some MAC protocols used in network technologies are:**

1. **Carrier Sense Multiple Access with Collision Detection (**CSMA/CD): Ethernet uses a contention-based media access control technique called **Carrier Sense Multiple Access with Collision Detection (CSMA/CD).** CSMA/CD, like all contention-based techniques, is very

simple in concept: wait until the circuit is free and then transmit. Computers wait until no other devices are transmitting, then transmit their frames. Ethernet's CSMA/CD protocol can be termed "ordered chaos." As long as no other computer attempts to transmit at the same time, everything is fine. However, it is possible that two computers located some distance from one another can both listen to the circuit, find it empty, and begin simultaneously. This simultaneous transmission is called a **collision.** The two frames collide and destroy each other.

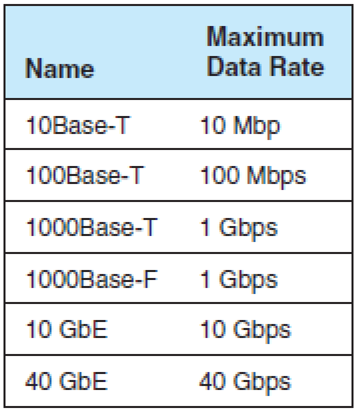
2. **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):** The performance of pure CSMA is improved by modifying CSMA to be less greedy on the channel which results CSMA/CA. It tries to avoid collision before they happen rather than listen and detect collision. All the stations before they transmit must wait an amount of time called an intra-frame space (IFS). Some applications have short IFS while other has long IFS. If two applications want to transmit at the same time then the application with the short IFS will go first. A station wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel. When the channel is clear a station sends a signal telling all other stations not to transmit and sends its data. CSMA/CA optionally is supplemented by the exchange of request to send (RTS) packet send by the sender S and a clear to send (CTS) packet by the intended receiver, alerting all nodes within the range of the sender, receiver or both to keep quiet for the duration of the main packet. This is known as IEEE 802.11 RTS/CTS exchange.
3. **Token Ring:** This is done by passing a token which is a short electronic message giving permission to transmit data. Only the computer holding the token can transmit. The token is passed around the network in a pre-determined sequence. This method is efficient in high traffic and eliminates collisions.
4. **Aloha Protocols:** Aloha can be pure Aloha or slotted Aloha. In pure aloha, this protocol allows every system to send a frame if it is ready to send. The slotted ALOHA protocol involves dividing the time intervals into discrete slots and each slot interval corresponds to the time period of one frame.

Types of Ethernet

Figure below summarizes the many different types of Ethernet in use today. It was the **10Base-T** standard that revolutionized Ethernet and made it the most popular type of LAN in the world. **100Base-T** is the most common form of Ethernet today.

Other types of Ethernet include: **1000Base-T** and 1000Base-F (which run at 1 Gbps and are sometimes called **1 GbE**), **10 GbE** (which runs at 10 Gbps), and **40 GbE** (which runs at 40 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 5, Cat 5e). Two common versions of 1000Base-F are *1000Base-LX* and *1000Base-SX*, which both use

fiber-optic cable, running up to 440 meters and 260 meters, respectively; *1000Base-T*, which runs on four pairs of category 5 twisted-pair cable, but only up to 100 meters2; and *1000Base-CX*, which runs up to 24 meters on one category 5 cable. Similar versions of 10 GbE and 40 GbE that use different media are also available.



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

Fig: Types of ethernet

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. 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**.

Topology

The logical and physical topologies of Wi-Fi are the same as those of hub-based 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

Media access control in Wi-Fi is **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA),** which is similar to the contention-based CSMA/CD approach used by Ethernet. With CSMA/CA, computers listen before they transmit and if no one else is transmitting, they proceed with transmission. Detecting collisions is more difficult in radio transmission than in transmission over wired networks, so Wi-Fi attempts to avoid collisions to a greater extent than traditional Ethernet. CSMA/CA has two media access control approaches. However, before a computer can transmit in a WLAN is must first establish an **association** with a specific AP, so that the AP will accept its transmissions.

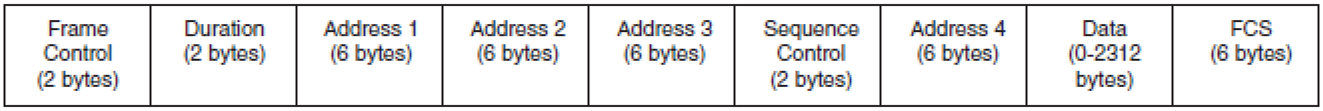
Associating with an AP Searching for an available AP is called ***scanning*** and NIC can engage in either **active or passive scanning**. During **active scanning,** a NIC transmits a special frame called **probe frame** on all active channels on its frequency range. When an AP receives a probe frame, it responds with a probe response that contains all the necessary information for a NIC to associate with it. A NIC can receive several probe responses from different APs. It is up to the NIC to choose with which AP to associate with. This usually depends on the speed rather than distance from an access point. Once a NIC associates with an access point they start exchanging packets over the channel that is specified by the access point. During **passive scanning,** the NIC listens on all channels for a special frame called **beacon frame** that is sent out by an access point. The beacon frame contains all the necessary information for a NIC to associate with it. Once a NIC detects this beacon frame it can decide to associate with it and start communication on the frequency channel set by the access point.

i. **Distributed Coordination Function** The first media access control method is the **distributed coordination function (DCF)** (also called **physical carrier sense** method because it relies on the ability of computers to physically listen before they transmit). With DCF, each frame in CSMA/CA is sent using stop-and-wait ARQ. After the sender transmits one frame, it immediately stops and waits for an ACK from the receiver before attempting to send another frame. When the receiver of a frame detects the end of the frame in a transmission, it waits a fraction of a second to make sure the sender has really stopped transmitting, and then immediately transmits an ACK (or a NAK). The original sender can then send another frame, stop and wait for an ACK, and so on. While the sender and receiver are exchanging frames and ACKs, other computers may also want to transmit. So when the sender ends its transmission, you might ask why doesn't some other computer begin transmitting before the receiver can transmit an ACK? The answer is that the physical carrier sense method is designed so that the time the receiver waits after the frame transmission ends before sending an ACK is significantly less time than the time a computer must listen to determine that no one else is transmitting before initiating a new transmission. Thus, the time interval between a frame and the matching ACK is so short that no other computer has the opportunity to begin transmitting.

ii. **Point Coordination Function** The second media access control technique is called the **point coordination function (PCF)** (also called the **virtual carrier sense** method). Not all manufacturers have implemented PCF in their APs. DCF works well in traditional Ethernet because every computer on the shared circuit receives every transmission on the shared circuit. With this approach, any computer wishing to transmit first sends a **request to transmit (RTS)** to the AP, which may or may not be heard by all computers. The RTS requests permission to transmit and to reserve the circuit for the sole use of the requesting computer for a specified time period. If no other computer is transmitting, the AP responds with a **clear to transmit (CTS),** specifying the amount of time for which the circuit is reserved for the requesting computer. All computers hear the CTS and remain silent for the specified time period.

Controlled-access methods provide poorer performance in low-traffic networks because computers must wait for permission before transmitting rather than just waiting for an unused time period. However, controlled-access techniques work better in high-traffic WLANs because without controlled access there are many collisions.

Wireless Ethernet Frame Layout



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)

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 access point (it cannot directly communication with another NIC), there is a need to add the address of the access point and also any other device that might be needed to transmit the frame. To do this, the transmitter and received address fields are used. 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.

Types of Wireless Ethernet

Wi-Fi is one of the fastest changing areas in networking. There are four types of Wi-Fi but one, the latest version (802.11n) is dominant today. The other three versions are obsolete, but may still be in use in some companies.

i. **802.11a:** IEEE **802.11a** is an obsolete, legacy technology, and no new products are being developed. Under perfect conditions, it provides eight channels of 54 Mbps each with a maximum range of 50 meters or 150 feet. Speeds of 20 Mbps at 50 foot ranges are more common in the face of interference such as drywall or brick walls.

ii. **802.11b**: IEEE **802.11b** is another obsolete, legacy technology. Under perfect conditions, it provides three channels of 11 Mbps each with a maximum range of 150 meters or 450 feet, although in practice both the speed and range are lower.

iii. **802.11g:** IEEE **802.11g** is another obsolete, legacy technology, but many organizations still use it. Under perfect conditions, it provides three channels of 54 Mbps each with a maximum range of 150 meters or 450 feet, although in practice both the speed and range are lower.

iv. **802.11n:** IEEE **802.11n** is the latest version of Wi-Fi that most firms use (or are in the process of installing). Under perfect conditions, it provides three channels of about 200 Mbps each with a maximum range of 150 meters or 450 feet, although in practice both the speed and range are lower. It is also possible to configure APs to use different frequency ranges to provide fewer channels that run at higher speeds up to 600 Mbps each.

Security

Security is important to all networks and types of technology, but it is especially important for wireless networks. With a WLAN, anyone walking or driving within the range of an AP (even outside the offices) can begin to use the network. There can occur unauthorized access, data breaches and other security threats

Implementing strong security measures helps to maintain confidentiality, integrity and availability. Some key aspects of wireless Ethernet security are:

i. **Encryption:** there should be the use of encryption protocols to secure the data transmitted over the wireless network. The two primary technique of encryption for Wi-Fi are WPA2 (Wi-Fi Protected Access 2) and WPA3. WEP (Wired Equivalent Privacy) is not much secured for Wi-Fi.

ii. **WEP** One wireless security technique is **wired Equivalent Privacy (WEP).** With WEP, the AP requires the user to have a *key* in order to communicate with it. All data sent to and from the AP is encrypted so that it can only be understood by computers or devices that have the key. If a computer does not have the correct WEP key, it cannot understand any messages transmitted by the access point and the access point will not accept any data that is not encrypted with the correct key. WEP has security issues which is easy to break and hard to configure and is abandoned by Wi-Fi alliance in 2004.

iii. **WPA**: **Wi-Fi Protected Access (WPA)** is a newer, more secure type of security. WPA works in ways similar to WEP and EAP: every frame is encrypted using a key, and the key can be fixed in the AP like WEP or can be assigned dynamically as users login like EAP (Extensible Authentication Protocol). With **Extensible Authentication Protocol (EAP),** the WEP keys are produced dynamically. The difference is that the WPA key is longer than the WEP key and thus is harder to break. More importantly, the key is changed for *every* frame that is transmitted to the client. Each time a frame is transmitted, the key is changed.

iv. **Wi-Fi Protected Access 2 (WPA2): WPA 2** (also called **802.11i**) is the newest, most secure type of WLAN security. It uses EAP to obtain a master key—in other words, the user logs in to a login server to obtain the master key. Armed with this master key, the user's computer and the AP negotiate a new key that will be used for this session until the users leaves the WLAN. 802.11i uses the Advanced Encryption Standard (AES) as its encryption method.

v. **Wi-Fi Protected Access 3 (WPA3):** This is recent wireless protocol. It is enhanced in terms of encryption abilities and keeping hackers at bay from both private and public networks. WPA3 expanded encryption for public networks and keep Wi-Fi users safe from vulnerability.

vi. **MAC Address Filtering:** With **MAC address filtering,** the AP permits the owner to provide a list of MAC addresses (i.e., layer-2 addresses). The AP only processes frames sent by computers whose MAC address is in the address list; if a computer with a MAC address not in the list sends a frame, the AP ignores it. Unfortunately, this provides no security against a determined hacker.

vii. **Network Authentications**

viii. Change default Passwords

ix. Hidden SSID

x. Firewalls

xi. Intrusion Detection/ Prevention Systems

xii. Regular Audits

The Best Practice LAN Design

Designing a Local Area Network (LAN) that is efficient, secure and scalable requires careful planning and adherence to best practices. LAN designing is ongoing process and staying updated with the evolving technologies and security threat is essential. Some key considerations for best practice for LAN design are:

i. Needs Assessments: Organizations requirements need to be understood. The factors such as number of the users, the types of applications, data transfer rates and future growth expectations.

ii. Topology Selection: topology should be selected on the basis of organizations need.

iii. Redundancy: Redundancy should be implemented in critical network components such as switches, router which ensures higher availability.

iv. Scalability: Design LAN to accommodate future growth. There should be the use of modular and expandable components.

v. Segmentation: Divide LAN into segments or VLAN to improve network performance, enhance security and isolate traffic.

vi. Subnetting:

vii. Security

viii. Authentication and Authorization

ix. Access Control

x. Backup and Disater Recovery

xi. Monitoring and Management

xii. **Cable Management**
xiii. **Regular Maintenance**
xiv. **Documentation**
xv. **Employee Training**
xvi. **Consult Experts**

1. Designing User Access with Wired Ethernet

It involves planning and configuring the network infrastructure to provide secure, reliable and efficient connectivity for end users. It includes determining the requirements such as number of users, locations, types of devices that will be used. Also it should include appropriate network topology, cabling and switches to ensure seamless connectivity. Security, access controls such as user authentication and authorization should be implemented.

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. 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 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 telephone cables and electrical cables. Each floor has a telecommunications wiring closet that contains one or more network hubs or switches. Cables are run from each room on the floor to this wiring closet.

2. Designing User Access with Wireless Ethernet

It involves creating a network infrastructure that provides convenient and reliable wireless connectivity for users and devices. 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 access points. 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 access points needs to consider both the placement of other access points as well as 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.

Also implementing a robust security framework is a top priority to protect network and sensitive data. It includes encryption, secure authentication methods and access controls. Regular monitoring and management tools are necessary to ensure network performance and detect and address issues. The design should also be scalable to accommodate future growth. Overall, a well designed wireless Ethernet network delivers flexibility and mobility to users with security and reliability.

3. Designing the Data Center

Designing the data center is a complex and critical process that plays a vital role in the operation of organizations, ranging from small businesses to large enterprises. A well designed data center ensures the efficient and reliable storage, processing and management of an organizations infrastructure and data.

A critical starting point in designing a data center is conducting a comprehensive needs assessment. It involves understanding the organizations specific requirements both present and future. It includes evaluating volume of data, computing and storage needs and expected growth over time.

Location selection is also important. Factors such as accessibility, proximity to users and environmental considerations must be taken into account. A security measure is also important to ensure the safety and confidentiality of sensitive information. Firewalls, intrusion detection/ prevention are necessary.

Also the data structure layout, infrastructure, power supply is also crucial. Raised flooring, efficient rack placement, continuous power supply for continuous operation is necessary. Standard cabling system should be maintained for efficient data transfer and connectivity.

In conclusion, designing a data center is a complex. A well designated data center serves as the backbone of an organization. Regular monitoring, maintenance, updates and security are vital to ensure the continued success of data center.

4. Designing the e-Commerce Edge

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 **Control 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 is 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 enquiries. Regular testing and analysis of user experience helps identify and rectify performance issues. E- Commerce analytics tools offers insights into customer behavior and sales trends, driving informed decision-making. Security and regulatory compliance are crucial aspect, ensuring the platform aligns with industry standards and data protection regulations. By designing the ecommerce edge, businesses can effectively reach customers, enhance online shopping experience, and ensures secured and efficient operations in the digital market place.

.

5. **Designing the SOHO Environment**

   Designing a small office/ home office environment entails crafting a workspace that is both functional and efficient, whether running a small business or working from home. This requires assessment such as identifying the specific requirement of work. Number of users, nature of task at hand, selecting right furniture, equipment and computer h/w is key task for boosting productivity and comfort. A robust networking infrastructure with reliable internet connection is necessary. Security measures including firewalls and antivirus software should be used to protect digital assets, and a solid data backup strategy is essential. Ensure the software and applications aligned with the work task, and consider implementing a professional voice communication system and video conferencing tools for effective collaboration. Don't forget about file organization, physical and cyber security, and ergonomics considerations for the work place comfort. Ultimately, designing a SoHO environment means crating a tailored and secured space that supports the work need and adapts to the ever- changing demands of small business or home based profession. Regular maintenance and cyber security practices will hhelp maintain a productive and secured SOHO environment.

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). Here 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, the **bottleneck** must be located**,** the part of the network that is restricting the data flow. The bottleneck will lie in one of two places. The first is the **network server**. The second location is the **network circuit**.

i. Improving Server Performance

Improving server performance can be approached from two directions simultaneously: **software and hardware**.

Software The NOS 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 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 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. 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. By using several smaller disks rather than one larger disk (e.g., five 200 gigabyte disks rather than one 1 terabyte disk). 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. Several vendors sell special-purpose network servers that are optimized to provide extremely fast performance. Many of these provide RAID and use **symmetric multiprocessing (SMP)** that enables one server to use up to 16 CPUs. Such servers provide excellent performance but cost more (often $5,000 to $15,000).

ii. Improving Circuit Capacity

Improving the capacity of the 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 there is use of a 100Base-T LAN, upgrading to 1000Base-T LAN will improve capacity. Or if you have 802.11g, then upgrade to 802.11n.

The other 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 switched. In a wireless LAN, this means adding more access points 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.

iii. 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 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 upon 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