UNIT 14 LIMITED ACCESS COMPUTER NETWORKS

Structure

14.1 INTRODUCTION

Nowadays practically every business, no matter how small, uses computers to handle various transactions. As business grows it often needs several people to input and process data simultaneously and in order to achieve this it is necessary that all the computers are networked. Computer networks are simply a group of computers connected by cables or other media and enabled by relevant software such that they can share data and resources.

Computers can be arranged in a network using various topologies like star, ring, bus, mesh etc. Each topology has its own merits and demerits. It is necessary to use some special hardware components to make the computers 'converse' with each other. To achieve information exchange at the hardware level, some standards need to be set up which decide on the format of the information being exchanged like where the address of receiver is to be placed, where the actual information is placed etc. This is achieved by the local area network (LAN) protocols. Most common of these protocols are Ethernet and token ring.

In this unit you will be learning about all these aspects of network functioning. In Sec.14.2 you will learn the classification of computer networks, which essentially depends on the physical spread of the network. Different hardware components required for computer networking are discussed in Sec.14.3. Various network topologies are discussed in Sec.14.4 and the protocols going with these topologies are discussed in Sec.14.5. In Sec.14.6 we briefly discuss the two main architectures of computer networks viz. client/server and peer to peer.

Objectives

After studying this unit you should be able to:

- describe the different types of networks and the advantages and disadvantages of each;

- differentiate between LAN, MAN and WAN;
- specify the hardware components required to achieve computer connectivity with a network;
- compare the different network topologies; and
- describe the frame format in Ethernet and token ring protocols.

14.2 TYPES OF COMPUTER NETWORKS

A Computer network is a group of two or more computer systems linked together such that they can share information and resources. There are many types of computer networks, including **Local-area networks (LANs); Metropolitan-area networks (MANs)** and **Wide-area networks (WANs).** Computers on a network are sometimes called **nodes**. Computers and devices that allocate resources for a network are called **servers**.

a. LAN

LAN is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programmes, and it is also able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, scanners as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. There are many different types of LANs, Ethernet being the most common for PCs.

Chat is a process of exchanging text messages on the Internet in real-time. This is a synchronous type of information sharing where the users are simultaneously accessing the session. There is a fast data transfer, since it is basically in the text mode and hence even slow telephone lines can be used to carry out a chat session.

The following characteristics differentiate one LAN from another:

Topology: The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line or in star configuration.

Protocols: The rules and encoding specifications for sending data. The protocols also determine whether the network uses a peer-to-peer or client/server architecture.

Media: Devices can be connected by twisted-pair wire, coaxial cables, or optical fibre cables. Some networks do without connecting media altogether, communicating instead via radio waves.

LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

b. MAN

MAN stands for Metropolitan Area Network. It is a data network designed for a town or city. In terms of geographic breadth, MANs are larger than local area networks (LANs), but smaller than wide area networks (WANs). MANs are usually characterised by very high speed connections using optical fibre cable or other digital media.

c. WAN

WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Computers connected to a wide area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

14.3 HARDWARE FOR COMPUTER COMMUNICATION

In order that the computers 'talk' to each other i.e. are able to exchange information, certain additional components are necessary to be installed in the machine. In this section we take a brief review of these special hardware components. These components are connected on the serial or parallel or USB port of the computer.

a. Network Interface Card (NIC)

It is also known as *network adapter*. It is a printed circuit board that plugs into the computer (personal computers, workstations and servers) and controls the exchange of data between the machines. A typical interface card is shown in Fig. 14.1. The network adapter provides services at the data link level of the network, which is also known as the access method.

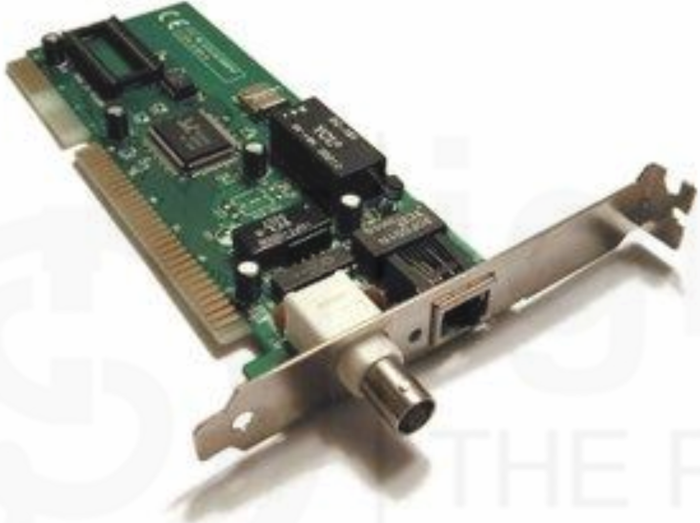

Fig. 14.1: Network interface card

The most common network adapters are Ethernet and Token Ring, as you will learn later in this unit. Sometimes, the Ethernet adapter is built into the motherboard of the computer.

Transmission media, such as twisted pair, co-axial cable or optical fibre interconnect all the adapters in the network.

b. Modem

MODEM is an acronym for modulator-demodulator. A modem is a device that enables a computer to transmit data over telephone lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms as depicted in Fig. 14.2.

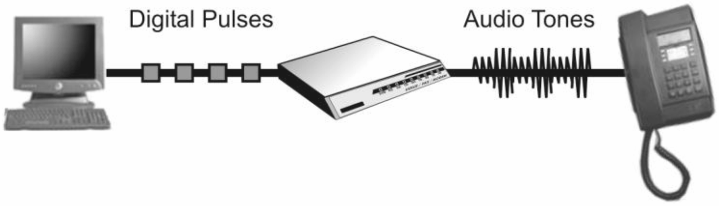

Fig. 14.2: Modem

Fortunately, there is one standard interface for connecting external modems to computers on serial port called RS-232. Consequently, any external modem can be attached to any computer that has an RS-232 port, which almost all personal computers have. There are also modems that come as an expansion board that you can insert into a vacant expansion slot on the computer motherboard. These are sometimes called onboard or internal modems.

While the modem interfaces are standardised, a number of different protocols for formatting data to be transmitted over telephone lines exist. Most modems have built-in support for the more common protocols. At slow data transmission speeds at least, most modems can communicate with each other. At high transmission speeds, however, the protocols are less standardised.

Aside from the transmission protocols that they support, the following characteristics distinguish one modem from another:

bps: How fast the modem can transmit and receive data. The speed of the modem is measured in terms of bits per second (bps). The fastest modems run at 57,600 bps, although they can achieve even higher data transfer rates by compressing the data. Obviously, the faster the transmission rate, the faster you can send and receive data. However, note that you cannot receive data any faster than it is being sent. If, for example, the device sending data to your computer is sending it at 2,400 bps, you must receive it at 2,400 bps. It does not always pay, therefore, to have a very fast modem. In addition, some telephone lines are unable to transmit data reliably at very high rates.

Voice/data: Many modems support a switch to change between voice and data modes. In data mode, the modem acts like a regular modem. In voice mode, the modem acts like a regular telephone. Modems that support a voice/data switch have a built-in loudspeaker and microphone for voice communication.

Auto-answer: An auto-answer modem enables your computer to receive calls in your absence. This is only necessary if you are offering some type of computer service that people can call in to use.

Data compression: Some modems perform data compression, which enables them to send data at faster rates. However, the modem at the receiving end must be able to decompress the data using the same compression technique.

Flash memory: Some modems come with flash memory, which is erasable, programmable ROM (EPROM), rather than conventional ROM. Because of this, the communications protocols can be easily updated if necessary.

c. Repeater

Repeater is a communications device that amplifies or regenerates the data signal in order to extend the transmission distance. Available for both analog and digital signals, it is used extensively in long distance transmission. It is also used to tie two LANs of the same type together. The term *Repeater* may also sometimes refer to a multiport repeater, which is a hub.

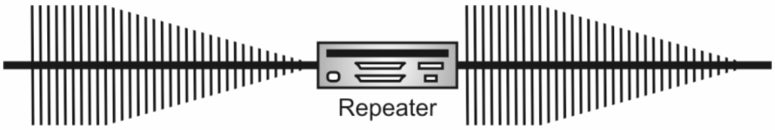

Fig. 14.3: Repeater

d. Bridge

Bridge is a device that connects two LAN segments together, which may be of similar or dissimilar types, such as Ethernet and Token Ring as shown in Fig. 14.4. A bridge can also be inserted into a network to segment it and keep traffic contained within the segments to improve performance.

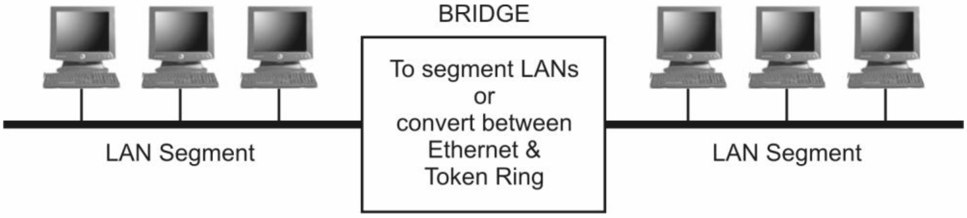

Fig. 14.4: Bridge connecting two LAN segments

Bridges learn from experience and build and maintain address tables of the nodes on the network. By monitoring which station acknowledged receipt of the address, they learn which nodes belong to the segment.

Bridges with more than two ports (multiport bridges) perform a switching function. Today's LAN switches are really multiport bridges that can switch at full wire speed.

Transparent Bridge is a common type of network bridge, in which the host stations are unaware of its existence in the network. A transparent bridge learns which node is connected to which port through experience by examining which node responds to each new station address that is transmitted. Ethernet uses this type of bridge, also called an adaptive bridge.

e. Hub

A hub is a central connecting device in a network that joins communication lines in a star configuration as shown in Fig. 14.5. Passive hubs are just connecting units that add nothing to the data passing through them. Active hubs, also sometimes called multiport repeaters, regenerate the data bits in order to maintain a strong signal.

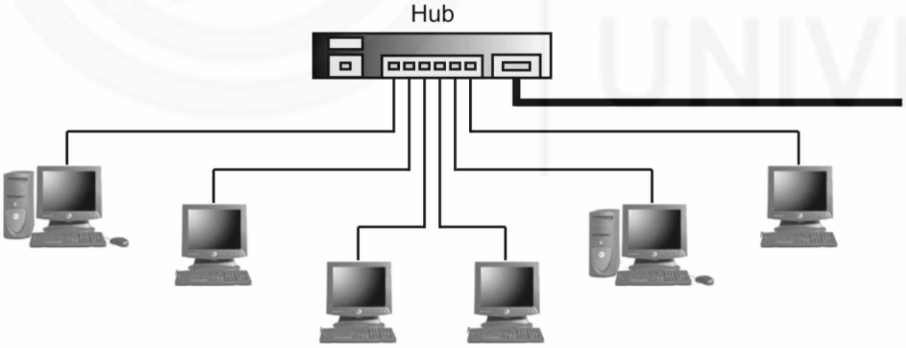

Fig. 14.5: Hub

In Token Rings standard, the hub is called MAU (Multi-station Access Unit). Multiple media hubs interconnect different types of Ethernet media (twisted pair, co-axial cable and optical fibre) and can bridge between Ethernet, Token Ring, and other topologies. Switching hubs provide Ethernet switching.

Hubs have become very intelligent, modular and customisable, allowing for the insertion of bridging, routing and switching modules all within the same unit. A hub can even host a CPU board and network operating system, turning the hub into a file server or some type of network control processor that performs complex functions as networks grow.

f. Router

Router is a device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another as seen in Fig. 14.6. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.).

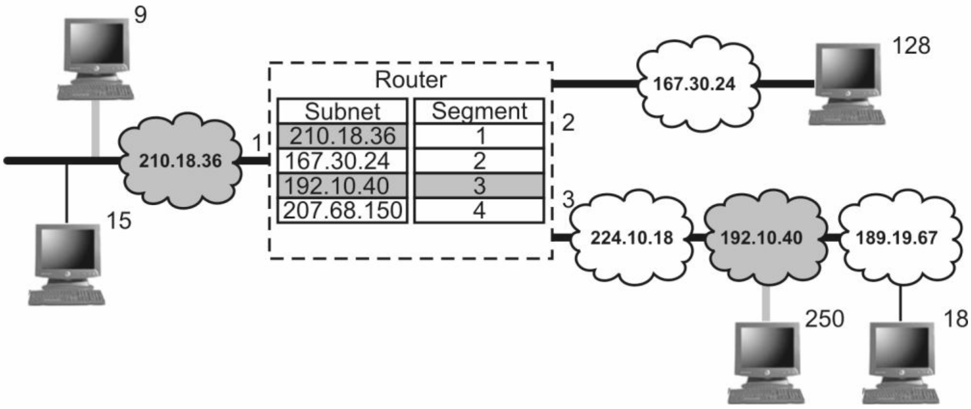

Fig. 14.6: Router connecting between 210.18.36.9 and 192.10.40.250 terminals

Routers are used to segment LANs in order to balance traffic within workgroups and to filter traffic for security purposes and policy management. Routers are also used at the edge of the network to connect remote offices. Multiprotocol routers support several protocols such as IP, IPX, AppleTalk and DECnet.

Routers can only route a message that is transmitted by a routable protocol such as IP or IPX. Messages in non-routable protocols, such as NetBIOS and LAT cannot be routed, but they can be transferred from LAN to LAN via a bridge. Because routers have to inspect the network address in the protocol, they do more processing and add more overhead than a bridge or switch.

Routers serve as a backbone, interconnecting all networks in the enterprise. This architecture strings several routers together via a high-speed LAN topology such as Fast Ethernet or Gigabit Ethernet about which you will learn later in this unit. Routers are also the backbone of the Internet, which spans the planet.

g. Gateway

Gateway is a computer that performs protocol conversion between different types of networks or applications as depicted in Fig. 14.7. For example, in this figure, an ISDN system is connected to a LAN. Now, you know that ISDN handles different kind of information and services (like computer data, telephone calls, fax messages). Hence the protocols used for ISDN are different than the ones used for LAN (TCP/IP or OSI). To provide the inter-conversion of the protocols, gateways are used.

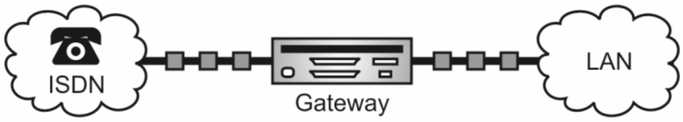

Fig. 14.7: Gateway

Gateways perform complete conversions from one protocol to another rather than simply support one protocol from within another. Sometimes routers can implement gateway functions. In electronic mail or messaging, gateway converts messages between two different messaging protocols.

h. Switch

In networks, switch is a device that filters and forwards packets between LAN segments.

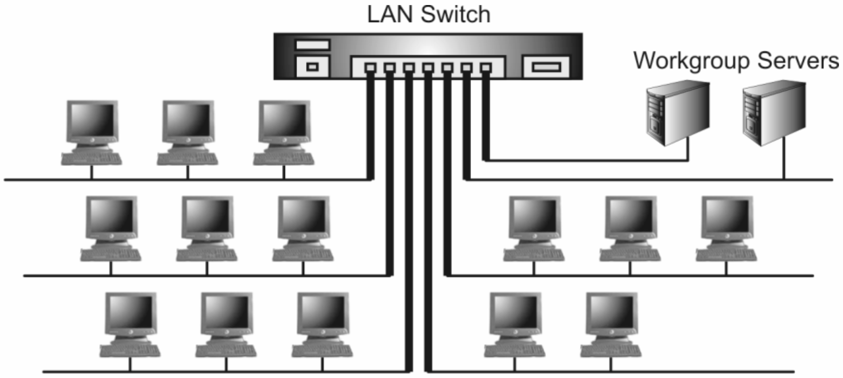

Fig. 14.8: Switch

LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs. Please don't confuse these switches with the standard switches available on devices like power on/off switch.

i. Firewall

Firewall is a method for keeping a network secure by establishing access control policies among networks. They can block information from entering a network or from getting out of that network as depicted in Fig. 14.9. You will notice that in this figure, the firewall stops the entry of packets from the foe site (dark packets) and allows only the friendly (white) packets to reach the user.

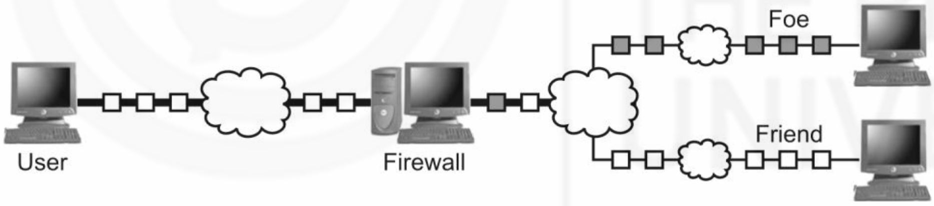

Fig. 14.9: Firewall

A firewall can be implemented in a single router that filters out unwanted packets, or it may use a combination of technologies in routers and hosts. Firewalls are widely used to give users access to the Internet in a secure fashion as well as to separate a company's public Web server from its internal network. They are also used to keep internal network segments secure. For example, a research or accounting subnet might be vulnerable to snooping from within.

Following are the types of techniques used individually or in combination to provide firewall protection.

Packet filter blocks traffic based on IP address and/or port numbers. It is also known as a *screening router*.

Proxy server serves as a relay between two networks, breaking the connection between the two.

IP Address is the sequence of numbers used to identify any computer attached to the Internet. You will learn about the IP addresses in the next unit.

Network address translation (NAT) hides the IP addresses of client stations in an internal network by presenting one IP address to the outside world. It performs the data transfer back and forth.

Stateful inspection tracks the transaction in order to verify that the destination of an inbound packet matches the source of a previous outbound request.

All these hardware elements are necessary for establishing a computer network however; just having the hardware in place is not enough. The computer should be supported by necessary software and standard protocols in order to achieve the dialogue between the machines. The most popular common rules (protocols/ standards) of information exchange on computer are open system interconnection (OSI) and transmission control protocol/internet protocol (TCP/IP) models. You will learn about them in the next unit.

Spend
3 *Min.*

SAQ 1

Which of the above discussed hardware components are essential for establishing contact within a local area network?

After learning about the essential hardware components require for networking of computers, let us now discuss the different configurations in which the computers in a network can be connected. These physical arrangements of networked computers are called *topologies*.

14.4 NETWORK TOPOLOGY

A network topology describes the configuration of a network (how the network components are connected together). There are four main topologies.

14.4.1   Star

The star topology uses a central hub through which all computers are connected. The peripherals attached to any of these computers or to the central hub are accessible to all users connected to this topology. In a computer network, the central hub is the host computer, and at the end of each connection is a terminal as shown in Fig. 14.10.

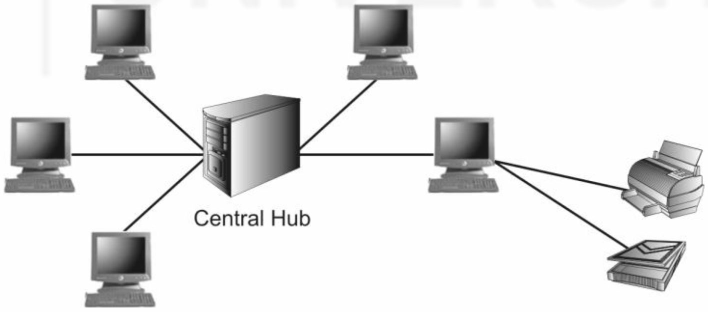

Fig. 14.10: Star Topology

A star network uses a significant amount of cable since each terminal computer is wired back to the central hub, even if two terminals are side-by-side several hundred metres away from the host. All routing decisions in case of star topology are made by the central hub.

An advantage of the star topology is that a failure in one of the terminals does not affect any other terminal; however, failure of the central hub affects the whole network. This type of topology is frequently used to connect terminals to a large time-sharing host computer.

14.4.2 Ring

The ring topology connects computer terminals (workstations) in a closed loop. Each terminal is connected to two other neighbouring terminals in a ring as shown in Fig. 14.11. Data is transmitted around the ring in one direction only; each station passing on the data to the next station till it reaches its destination.

The information travels around the ring from one workstation to the next. Each packet of data sent on the ring is prefixed by the address of the station to which it is being sent. When a packet of data arrives, the workstation checks to see if the packet address is the same as it's own. If it is, it grabs the data in the packet. If the packet does not belong to it, it sends the packet to the next workstation in the ring.

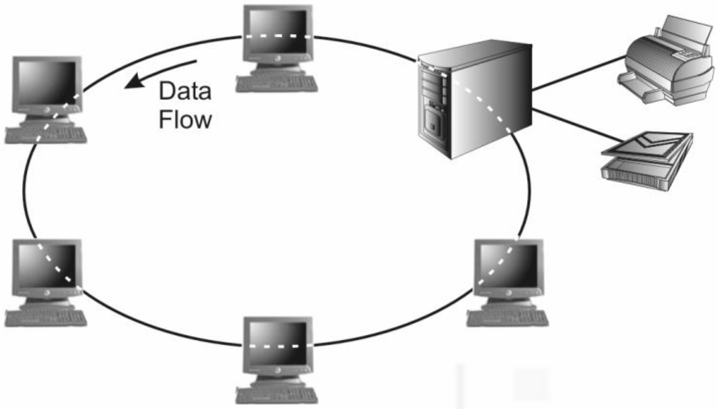

Fig. 14.11: Ring Topology

In ring topology, faulty workstations can be isolated from the ring. When the workstation is powered on, it connects itself into the ring. When power is off, it disconnects itself from the ring and allows the information to bypass the workstation. Though individual workstations can be isolated from the ring, any break in the ring causes the entire network to fail.

The common implementation of this topology is token ring as you will learn in the later section.

14.4.3 Bus

The term *Bus* is used for a set of connections carrying data/address inside the computer as well as for cable connecting computer terminals.

The bus topology connects workstations using a single common cable called **bus**. Each workstation is connected to the next workstation via this cable as shown in Fig. 14.12

The common implementation of this topology is Ethernet. A message transmitted by one workstation is heard by all the other workstations. Care has to be taken to see that only one workstation sends data on the bus at a time. This requires a special coordination of workstations.

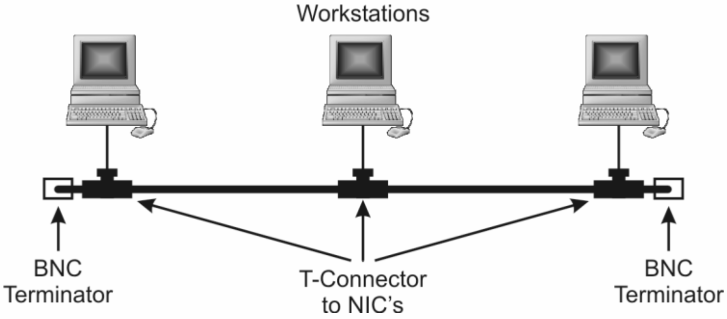

Fig.14.12: Bus Topology

Since all workstations share the same cable for the sending and receiving information, the cabling costs of bus systems is the least of all the different topologies. Each end of the cable is terminated using a special terminator. A fault in the bus cable causes the whole network to fail.

14.4.4 Mesh

The mesh topology connects all computers to each other as shown in Fig. 14.13. The cable requirements are high, but there are redundant paths built in. Any failure of one computer allows all others to continue, as they have alternative paths to other computers.

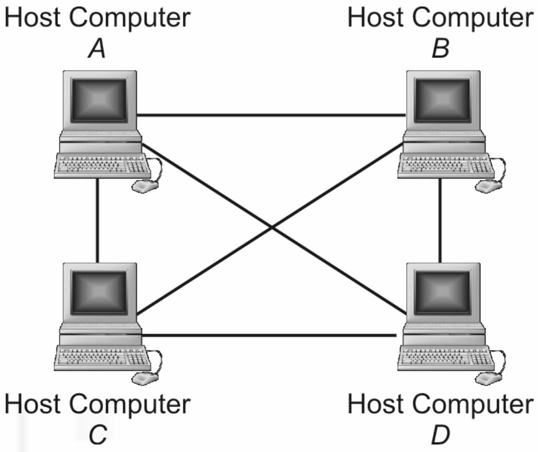

Fig. 14.13: Mesh Topology

Mesh topologies are used in critical connection of host computers (typically telephone exchanges).

Spend
2 *Min.*

SAQ 2

Among the topologies discussed which one is the most rugged and which one is most cost effective?

After learning the physical layout of various topologies, let us discuss now the protocols governing these LANs.

14.5 LAN PROTOCOLS

A protocol is a common set of rules and conventions that helps in establishing communication between computer terminals. Since there are more than one computer, which may like to transmit data on a network at a time, unless there are some rules to regulate this transfer, there would be chaos on the network. The LAN protocol allows two computers attached to same network to share information. The main function of any protocol is to establish necessary conventions like who gets priority of information transmission etc. Two main protocols used in computer communication on LAN are Ethernet (bus topology) and token ring (ring topology).

14.5.1 Ethernet

Ethernet protocol was invented by Bob Metcalf and was later developed by Xerox Corporation in 1970s. In 1980s it became the most widely used protocol and became IEEE standard in 1985.

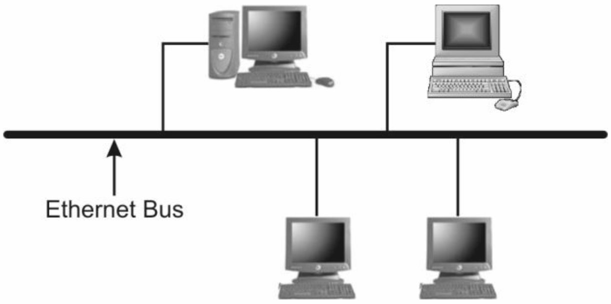

Fig. 14.14: Ethernet Protocol

Ethernet is the most widely used LAN access method, which is defined by the IEEE 802.3 standard.

The data rates of main Ethernet standards in use are defined for operation over optical fibre and twisted-pair cables:

- 10 Mbps - 10Base-T Ethernet (IEEE 802.3)
- 100 Mbps - Fast Ethernet (IEEE 802.3u)
- 1000 Mbps - Gigabit Ethernet (IEEE 802.3z)
- 10-Gigabit - 10 Gbps Ethernet (IEEE 802.3ae)

A detailed list of the Ethernet designations in given in Appendix A.

The Ethernet system consists of three basic elements:

1. The physical medium used to carry protocol signals between computers;
2. A set of medium access control (MAC) rules embedded in each Ethernet interface that allow multiple computers to fairly arbitrate access to the shared Ethernet channel; and
3. An Ethernet frame that consists of a standardised set of bits used to carry data over the system.

Each Ethernet equipped computer operates independent of all other stations on the network; there is no central controller. All stations attached to an Ethernet are connected to a shared signalling system, also called the medium. To send any data, first it is broken into small packets. These packets are put into a frame which consists of fields. Each field has a separate function and fixed size (number of bits). The packet is placed in the data/information field of the frame. Its size is determined by the packet size as indicated in Fig.14.15. The size of the data field is kept in such a way that the total frame does not become too unwieldy to handle or too small.

After each frame transmission, all stations on the network must contend equally for the next frame transmission opportunity. Access to the shared channel is determined by the medium access control (MAC) incorporated in the Ethernet interface located in each station. The medium access control mechanism is based on a system called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

A typical Ethernet MAC frame structure is shown in Fig. 14.15.

- **Preamble (PRE)-** 7 bytes. The PRE is an alternating pattern of ones and zeros that tells receiving stations that a frame is coming and provides a means to synchronise the frame-reception portions of receiving physical layers with the incoming bit stream.

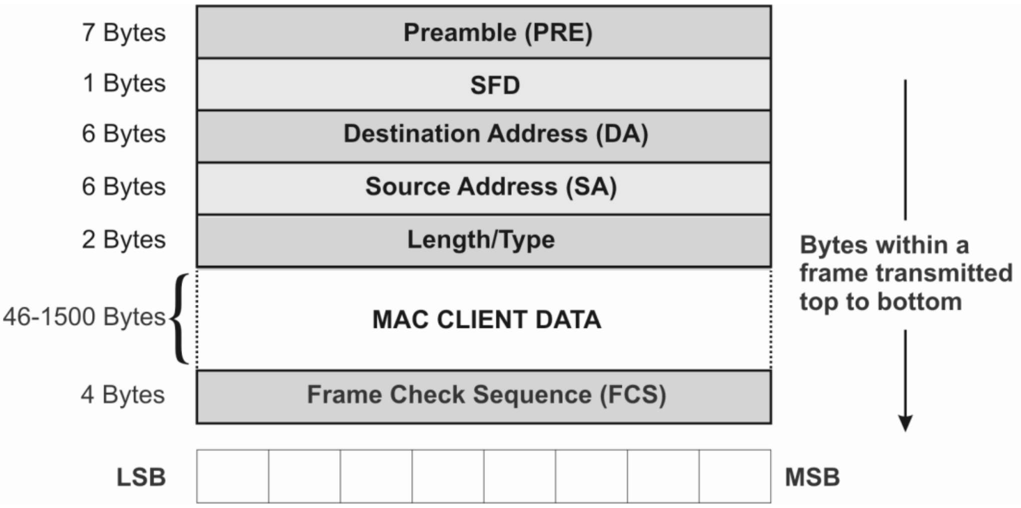

Fig. 14.15: Basic IEEE 802.3 Ethernet MAC frame format for 10/100 Mbps

- **Start-of-frame delimiter (SFD)-** 1 byte. The SFD is an alternating pattern of ones and zeros, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address.
- **Destination address (DA)-** 6 bytes. The DA field identifies which station should receive the frame.
- **Source addresses (SA)-** 6 bytes. The SA field identifies the sending station.
- **Length/Type-** 2 bytes. This field indicates either the number of MAC client data bytes that are contained in the data field of the frame or the frame type ID if the frame is assembled using an optional format.
- **Data-** Is a sequence of *n* bytes ($46 \leq n \leq 1500$) of any value.
- **Frame check sequence (FCS)-** 4 bytes. This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames.

As each Ethernet frame is sent onto the shared signal channel, all Ethernet interfaces look at the destination address. If the destination address of the frame matches with the interface address of one of the terminals, the frame will be read entirely and be delivered to that computer. All other network interfaces will stop reading the frame when they discover that the destination address does not match their own address.

When it comes to how signals flow over the set of media segments that make up an Ethernet system, it helps to understand the topology of the system. The signal topology of the Ethernet is also known as the logical topology, to distinguish it from the actual physical layout of the media cables. The logical topology of an Ethernet provides a single channel (or bus) that carries Ethernet signals to all stations. Multiple Ethernet segments can be linked together to form a larger Ethernet LAN using a signal amplifying and retiming device called a repeater. You must remember here that in the Ethernet system every segment must have two ends and there should not be any loop path.

14.5.2 Token Ring

Token Ring is a LAN protocol defined in the IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbour. Permission to transmit is granted by a message (token) that circulates around the ring as shown in Fig. 14.16.

Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has some information to send, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network, which means that other stations wanting to transmit must wait. Therefore, data collisions cannot occur in Token Ring networks.

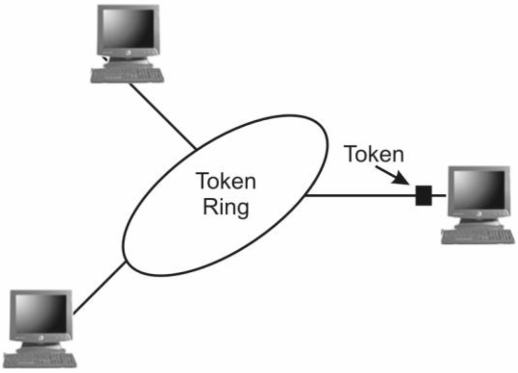

Fig. 14.16: Token Ring

The information frame circulates in the ring until it reaches the intended destination station, which copies the information for further processing. The information frame continues to circle the ring and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination. After this the token is released in the ring, indicating that the ring is free for next data transfer.

Unlike Ethernet CSMA/CD networks, token-passing networks are deterministic, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting. This feature and several reliability features make Token Ring networks ideal for applications in which delay must be predictable and robust network operation is important.

Structure of a typical token ring frame is shown in Fig. 14.17.

SD	AC	FC	DA	SA	RI	INFO	FCS	ED	FS

Fig. 14.17: Token ring frame format

- SD/ED-Starting Delimiter / Ending Delimiter. Both the SD and ED are single byte long and have specific Manchester code violations in certain bit positions so that the start and end of a frame can never be accidentally recognised in the middle of other data.
- AC - Access control field contains the Priority fields (1 byte).
- FC - Frame control field indicates whether the frame contains data or control information (1byte).
- DA - Destination station address (6 bytes).
- SA - Source (station) address (6 bytes).
- RI - Field with routing control, route descriptor and routing type information (variable length from 0 to 30 bytes).

- INFO - The Information field is of variable length.
- FCS - Frame check sequence (4 byte).
- FS - Frame Status contains bits that may be set on by the recipient of the frame to signal recognition of the address and whether the frame was successfully copied (1 byte).

Spend
4 *Min*.

SAQ 3

With a diagram explain how a token ring protocol can be implemented in case of star topology.

14.6 NETWORK ARCHITECTURE

Depending on the architecture used, networks can be classified as Client/Server or Peer-to-Peer.

14.6.1 Client/Server Architecture

Client/server architecture is one in which the client (personal computer or workstation) is the requesting machine and the server is the supplying machine, both of which are connected via a local area network (LAN) or wide area network (WAN) (Refer Fig. 14.18). Since the early 1990s, client/server has been the buzzword for building applications on LANs in contrast to centralised mini- and main-frames with dedicated terminals.

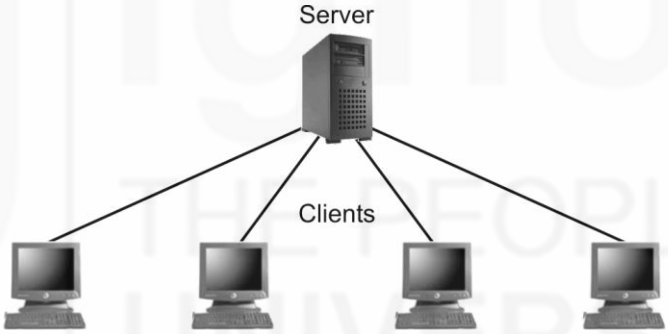

Fig. 14.18: Client/server LAN Architecture

Any PC of the present generation can work as a server.

The client contains the user interface and may perform some or all of the application processing. Servers can be high-speed microcomputers, minicomputers or even mainframes. Usually the intelligence capacity of these servers is much higher than that of client machines. A database server maintains the databases and processes requests from the client to extract data or update the database. An application server provides additional business processing for the clients.

The term client/server is sometimes used to contrast a peer to peer network, in which any client can also act as a server. In that case, client/server means nothing more than having a dedicated server. However, client/server architecture means more than dedicated servers. Simply downloading files from or sharing programmes and databases on a server is not a true client/server architecture. True client/server implies that the application was originally designed to run on a network and that the network infrastructure provides the same quality of service as traditional mini- and main-frame information systems.

As you know, the computer is a very versatile machine and can perform several functions. Sometimes we require a limited function from a computer, for which we can make a limited function chip (CPU) to perform only that limited job. Such machines are function specific and much cheaper than the complete functionality computer. For only storing data which can be retrieved when required by any client terminal, such low capacity computers can be used as server. Depending on the server intelligence, the client/server configurations can be classified as

- non-client/server;
- two tier client/server; and
- three tier client/server.

Non-Client/Server:

In non-client/server architecture, the server is nothing more than a remote disk drive like shown in Fig. 14.19. The user's machine does all the processing. If many users routinely perform lengthy searches, this can bog down the network, because for each client the entire database has to be passed over the net. At 1,000 bytes per record, a 10,000 record database requires 10MB of data to be transmitted.

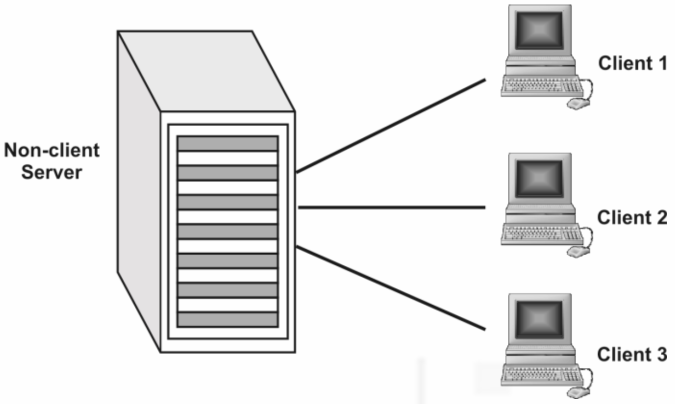

Fig. 14.19: Non-client/server

Two-Tier Client/Server:

Two-tier client/server is really the foundation of client/server. The database processing is done in the server. The search request is generated by the client and sent to the server. The data base management system on the server searches locally and returns only matching records. If 50 records met the criteria, only 50kB would be transmitted. This reduces traffic in the LAN.

Three-Tier Client/Server:

Many applications lend themselves to centralised processing. If they contain proprietary algorithms, security is improved. Upgrading is also simpler. Sometimes, programmes are just too demanding to be placed into every client PC. In three-tier client/server architecture the *user interface*, the *functional process logic (business rules)* and *data storage/access* are developed and maintained as independent modules, most often on separate platforms. Such architecture allows any of the three tiers to be upgraded or replaced independently e.g. change of operating system will only affect the user interface code.

14.6.2 Peer to Peer Architecture

A type of network in which each workstation has equivalent capabilities and responsibilities is called peer to peer network. Here each workstation acts as both a client and a server. There is no central repository for information and there is no central server to administer the net. Data and resources are distributed throughout the network, and each user is responsible for sharing data and resources connected to their system. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer to peer networks are generally simpler and less expensive, but they usually do not offer the same performance under heavy loads.

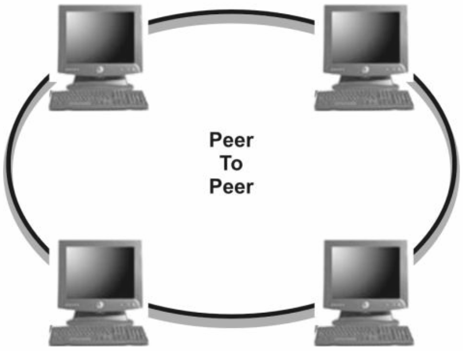

Fig. 14.20: Peer to Peer Architecture

Spend
2 *Min.*

SAQ 4

On Internet you access the information from various web sites. Which architecture is used in Internet?

Let us now summarise the points you learnt in this Unit.

14.7 SUMMARY

- The components necessary to achieve connectivity between machines are: network interface card (NIC), modem, repeater, bridges, hub, gateway and routers. The firewalls are used to protect the machines from any unauthorised access.
- There are various types of LAN topologies (arrangement of computers in a network) like ring, star, bus, mesh etc.
- Ethernet and token ring are the most common LAN protocols which define the frame format in which data transfer takes place from one machine to others in a network.
- The main network architecture in use are: client/server and peer to peer. The Internet uses client/server architecture.

14.8 TERMINAL QUESTIONS

Spend 20 *Minutes*

1. In your house, if you want to connect the computers kept in different rooms by a network, what considerations will you make to choose a proper topology?
2. What hardware components are a must to establish a contact with the world-wide network?
3. Why is it not necessary to devise collision detection in token ring protocol?
4. Give examples of peer to peer network applications you may have come across.

14.9 SOLUTIONS AND ANSWERS

Self Assessment Questions

1. NIC; Repeater (for large distance network); Passive Hub; Switch; Firewall (to protect any unauthorised outside entry into the network).
2. Mesh topology is rugged and reliable since break in any cable link will not affect operation of any terminal. However cost of cabling here is extremely high. Bus topology can save on cable costing.

3.

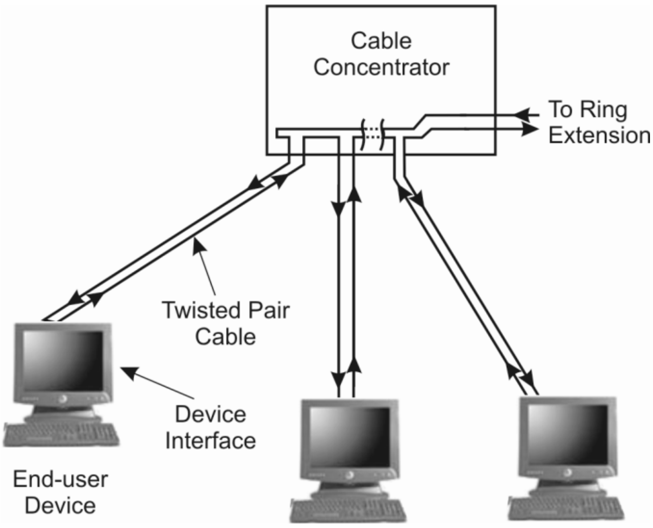

Fig. 14.21: Star wiring topology supporting token ring protocol

4. Internet uses client/server architecture.

Terminal Questions

1. Number of terminal, length of cabling, hardware components required (like hub, repeaters), speed of data communication required are typical considerations while choosing any network topology. It also depends on the software required to operate these systems.

2. NIC, Modem, Router and Gateway.

3. Refer to Sec. 14.5.2.

4. There are many applications like file sharing programmes, which work in peer to peer mode. The prominent examples have been the song sharing programme like Napster, Grokster, which allowed computer users to exchange songs from one machine to another without having a central server. However, due to issues like copyright violations, these applications have been stopped now. Another example of peer to peer network is distributed computing, about which you will learn in Unit 16.

Reference Material:

1. *Computer Networks* by Tanenbaum, A.S; (IV Edition) (Prentice Hall of India.)
2. *Introduction to Data Communication and Networking* by Forouzani, Behrouz; (IV Edition) (Tata McGraw-Hill)
3. *Data Communications and Networks*, by Godbole, Achyut; (Tata McGraw-Hill)
4. www.ieee.org/
5. www.webopedia.com/
6. www.wikipedia.org/

APPENDIX A: Ethernet Designations

IEEE 802.3 specifies a series of standards for telecommunication technology over Ethernet local area networks. The following chart details the different Ethernet types and how they differ from one another.

10Base-2	10 Mbps base band Ethernet over coaxial cable with a maximum distance of 185 metres. Also referred to as *Thin Ethernet* or *Thinnet* or *Thinwire*.
10Base-5	10 Mbps base band Ethernet over coaxial cable with a maximum distance of 500 metres. Also referred to as *Thick Ethernet* or *Thicknet* or *Thickwire*.
10Base-36	10 Mbps base band Ethernet over multi-channel coaxial cable with a maximum distance of 3,600 metres.
10Base-F	10 Mbps base band Ethernet over optical fibre.
10Base-FB	10 Mbps base band Ethernet over two multi-mode optical fibres using a synchronous active hub. Maximum distance 200 metres.
10Base-FL	10 Mbps base band Ethernet over two optical fibres and can include an optional asynchronous hub. Maximum distance 200 metres.
10Base-FP	10 Mbps base band Ethernet over two optical fibres using a passive hub to connect communication devices. Maximum distance 1000 metres.
10Base-T	10 Mbps base band Ethernet over twisted pair cables with a maximum length of 100 metres.
10Broad-36	10 Mbps base band Ethernet over three channels of a cable television system with a maximum cable length of 3,600 metres.
10Gigabit Ethernet	Ethernet at 10 billion bits per second over optical fibre. Multimode fibre supports distances up to 300 metres; single mode fibre supports distances up to 40 kilometres.
100Base-FX	100 Mbps base band Ethernet over two multimode optical fibres.
100Base-T	100 Mbps base band Ethernet over twisted pair cable.
100Base-T2	100 Mbps base band Ethernet over two pairs of Category 3 or higher unshielded twisted pair cable.
100Base-T4	100 Mbps base band Ethernet over four pairs of Category 3 or higher unshielded twisted pair cable.
100Base-TX	100 Mbps base band Ethernet over two pairs of shielded twisted pair or Category 4 twisted pair cable.
100Base-X	A generic name for 100 Mbps Ethernet systems.
1000Base-CX	1000 Mbps base band Ethernet over two pairs of 150 shielded twisted pair cable.
1000Base-LX	1000 Mbps base band Ethernet over two multimode or single-mode optical fibres using long wave laser optics.
1000Base-SX	1000 Mbps base band Ethernet over two multimode optical fibres using shortwave laser optics.
1000Base-T	1000 Mbps base band Ethernet over four pairs of Category 5 unshielded twisted pair cable.
1000Base-X	A generic name for 1000 Mbps Ethernet systems.

Source**:** www.ieee.org/