Unit 7 Communication System Concepts

Structure:

7.1 Introduction

In the previous unit you have learnt about operating system concepts. In this unit you are going to learn about communication system concepts. This unit introduces the fundamental concepts of communication in computer networks. We will first look at constituent network components and various network types, and then describe a reference model for network protocol architectures We will also discuss the components of internet.

Objectives:

- explain the basic elements of data communication
- explain the different types of network topologies
- explain different network types
- discuss on OSI reference model

- discuss on TCP/IP model
- describe the components of internet

7.2 Basic elements of communication system

To understand communication systems, we need to look at its parts.This section explains to you the meaning of communication systems and the functions of various blocks of communication system block diagram.

Communication Systems:

Communication System is a system or facility capable of providing information transfer between persons or equipment's. The elements used in communication system make communication simpler and faster. The three important elements of communication system are:

- Transmitter
- Transmission channel
- Receiver

The terms "signal" and "message" will be used interchangeably. This is because the signal, like the message, is a physical embodiment of information.

Basic Block Diagram of a Communication System:

Block diagram is a diagram of a communication system shown in figure 7.1 consists of information source, transmitter, channel and receiver blocks. The detailed explanation of the blocks is discussed below.

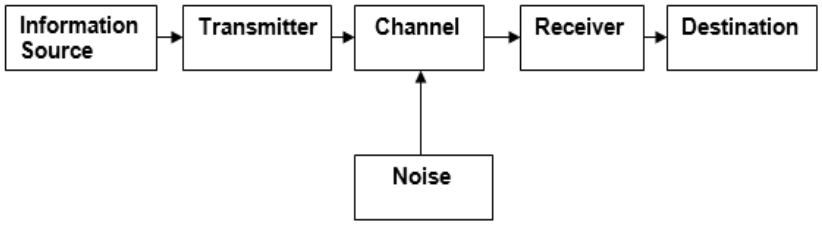

Fig. 7.1: Basic Block Diagram of Communication System

Information source: Information source is one in which information is generated. Source of information may be analog or digital. Source of information may be for example, human brain originating ideas and changes in the physical environment. If this information or message is not in the

electrical form, then it has to be converted into electrical form. This is done by using a suitable input transducer which converts the message into electrical signal then it is fed to the transmitter. For example, input transducer could be a microphone which converts sound into electrical signal. This can be used in case the information source produces voice signal.

Transmitter: The device which is used to adapt the information into another signal which is capable of passing on to a suitable medium is called transmitter. The information signal involves a process called modulation and coding.

Channel: The medium which carriers the information signal is called transmission channel or simply channel. That is, the medium which the information coming from a transmitter actually propagates or travels to a particular receiver. This channel is used for sending the information from one place to another place. Some of the transmission channels are:

- Couple of wires
- coaxial cable
- Radio wave
- Laser beam
- Fiber optic

While transmission each transmission channel produces some loss of energy. It is because when the distance increases cause the decrease in energy.

Noise: Unwanted signal called noise gets added to the message signal in the channel and causes distortion to the message signal. In other words, this noise signal disturbs, interferes and affects the wanted signal in the communication process. The noise is generally normal in communication process. We cannot prevent it but we can minimize it.

Receiver: The device which converts the suitable information into original message is called receiver. The receiver gets information produced by the transmitter and produces the actual data. Some operations performed by receiver are:

- Amplification of signal
- Demodulation
- Decoding

The decoding is the reversing process performed by transmitter.

Destination is one in which we get the original form of the information. It converts electrical signal into its original message. For example, destination could be an output transducer like loud speaker which converts the recovered original signal in the electrical form into sound waves.

Self Assessment Questions

1. _____ is used to convert the information into another signal which is capable of passing on to a suitable medium.
2. The device which converts the suitable information into original message is called _____.

7.3 Data Communication

Data communication is the transfer of data or information between a source and a receiver, the source transmits the data and the receiver receives it. The distance over which data moves within a computer may vary from a few thousandths of an inch, as is the case within a single IC chip, to as much as several feet along the backplane of the main circuit board. Over such small distances, digital data may be transmitted as direct, two-level electrical signals over simple copper conductors. Except for the fastest computers, circuit designers are not very concerned about the shape of the conductor or the analog characteristics of signal transmission.

Data Communications concerns the transmission of digital messages to devices external to the message source. "External" devices are generally thought of as being independently powered circuitry that exists beyond the chassis of a computer or other digital message source. As a rule, the maximum permissible transmission rate of a message is directly proportional to signal and inversely proportional to channel noise. It is the aim of any communications system to provide the highest possible transmission rate at the lowest possible power and with the least possible noise.

Basic elements of data communication are discussed below:

Data and signals – A signal is an electric current or electromagnetic field used to convey data from one place to another. The simplest form of signal is a direct current (DC) that is switched on and off; this is the principle by which the early telegraph worked. More complex signals consist of an

alternating-current (AC) or electromagnetic carrier that contains one or more data streams.

Data is superimposed on a carrier current or wave by means of a process called modulation. Signal modulation can be done in either of two main ways: analog and digital. Data can be analog or digital. The term analog data refers to information that is Continuous; digital data refers to information that has discrete states. For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous.

Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.

Digital data take on discrete values. For example, data are stored in computer memory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

Analog and digital signals – Like the data they represent, signals can be either analog or digital. An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0.

Periodic and non-periodic signals – Both analog and digital signals can take one of two forms: periodic or non-periodic. A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A non-periodic signal changes without exhibiting a pattern or cycle that repeats over time.

7.3.1 Data Transmission methods

There are three methods of data transfer. These methods are discussed below:

- **Simplex communication:** In this type, data transfer occurs in only one direction, i.e., either from source to destination or destination to source machines.
- **Half-duplex communication:** In this type, data transfer occurs in either directions, but not simultaneously.
- **Full-duplex communication:** In this type, data transfer occurs in either direction simultaneously. The protocol must also determine the number of logical channels per connection along with their individual priorities. Many networks provide at least two logical connections per channel, one for normal data, and one for urgent data.

7.3.2 Data Transmission Medium

Transmission media is the physical path between the transmitter and receiver. It can be guided or unguided.

Guided & unguided transmission medium

Guided media provides a guided (by a solid medium) path for propagation of signals such as twisted pairs, coaxial cables, optical fibers etc. *Unguided media* employ an antenna for transmitting through air, vacuum or water. This form of transmission is referred to as wireless transmission. For example Broadcast radio, satellite etc.

Selection of transmission Media depends on the characteristics and quality of data transmission which are in turn determined by characteristics of the medium and signal. For guided media the medium itself in determining the limitations of transmission. For Unguided media Bandwidth (BW) width of the signal produced at the transmitting antenna is more important than characteristics of the transmission characteristics.

In general, signals at lower frequencies are Omni directional (all directions) and at higher frequencies are directional (focused). The key concern in design of data transmission system is Data Rate and Distance: The greater the data rate and distance, the better transmission system.

Factors used to determine data rate and distance are:

- ***Bandwidth (BW):*** Greater the BW of the signal, higher the data rate that can be achieved.

- ***Transmission impairment:*** These limit the distance. Twisted pair suffers more impairment than coaxial cable which in turn suffers more than optical fiber.
- ***Interference:*** Overlapping frequency bands can distort/wipeout a signal.

  It is of more concern for unguided media than guided.

  For guided it can be caused due to nearby cables. Proper shielding of cables can minimize this problem.
- ***Number of receivers:*** Point to point links is used or a shared link is used with multiple attachments.

  In a shared link, each attachment introduces some attenuation and distortion on the line limiting the distance and/or data rate.
- For guided media the transmission capacity depends on data rate or BW and depends critically on the distance (whether medium is p-p or multipoint)

7.3.3 Network Topologies

Topology is a term used to define the way in which computers are connected in network. The physical topology of a network denotes to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations. Each topology is suited to specific tasks and has its own advantages and disadvantages.

Network Topologies are logical layouts of the network. The term "logical" used here marks a great significant. That means network topology depends not on the "physical" layout of the network.

The choice of topology is dependent upon

- Type and number of equipment being used
- Planned applications and rate of data transfers
- Required response times
- Cost

It is to find the most economical and efficient way to connect all the users to the networks resources while providing adequate capacity to handle user demands, maintain system reliability and minimize delay. Many topologies do exist but most commonly there are 4 types of basic topologies used for networking computers which are discussed below.

1) Bus topology

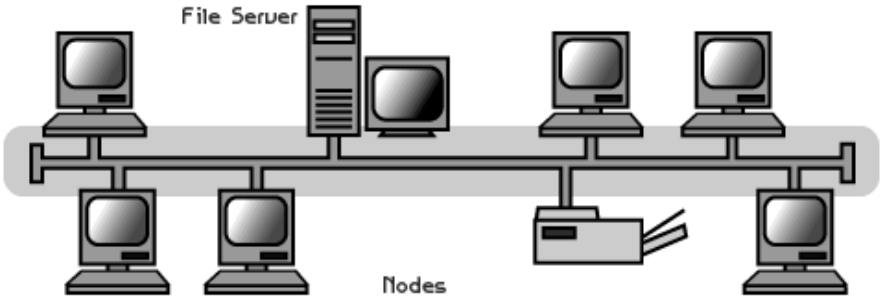

Fig. 7.2: Bus topology

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints is called the 'bus'. That is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network virtually simultaneously. It consists a single main cable connects each node. The bus topology is as shown in Figure 7.2.

The network OS keeps track of unique electronic address for each node, and manages the flow of information a single cable is dedicated to all the information traffic, performance can be slow at times. This topology is often bound in client/server systems (example file server: dedicated solely to the distribution of data files). This topology is most commonly used, as it can be easily expandable as the network grows.

Advantages of a linear bus topology:

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a linear bus topology:

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

2) Ring topology

The type of network topology in which each of the nodes of the network is connected to two other nodes in the network and with the first and last nodes being connected to each other, forming a ring. Ring topology looks something like shown in Figure 7.3. In this the nodes are connected in a circle using cable segments. Each node is physically connected only to two others.

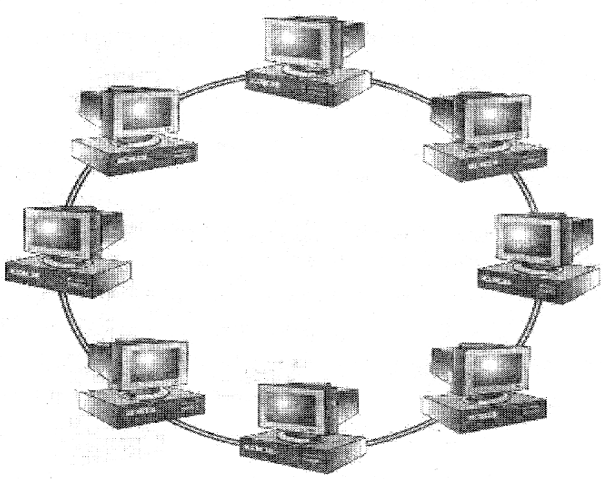

Fig. 7.3: Ring topology

All data that is transmitted between nodes in the network travels from one node to the next node in a circular manner and the data generally flows in a single direction. Performance can be faster. Found in peer-to-peer networks.

Advantages

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

Disadvantages

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Much slower than an Ethernet network under normal load

3) Star topology

A star topology is designed with each node connected directly to a central network hub or concentrator as shown in Figure 7.4. Data on a star network passes through the hub or concentrator before continuing to its destination. The hub or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

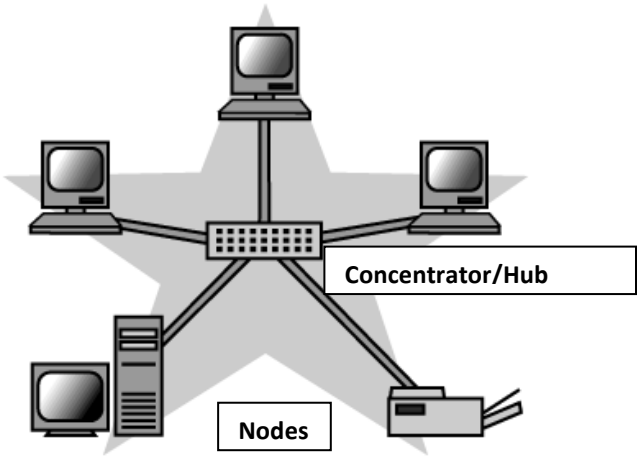

Fig. 7.4: Star topology

Advantages of a star topology:

- Easy to install and wire.
- No disruptions to the network then connecting or removing devices.
- Easy to detect faults and then remove faulty parts.
- Has the advantage of minimum data traffic along the cables (node to server)

Disadvantages of a star topology:

- It requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- Star topology is more expensive than linear bus topology because of the cost of concentrators.
- It Requires an extremely powerful (and expensive) file server, plus additional cable.

4) Tree topology

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable is as shown in Figure 7.5. Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

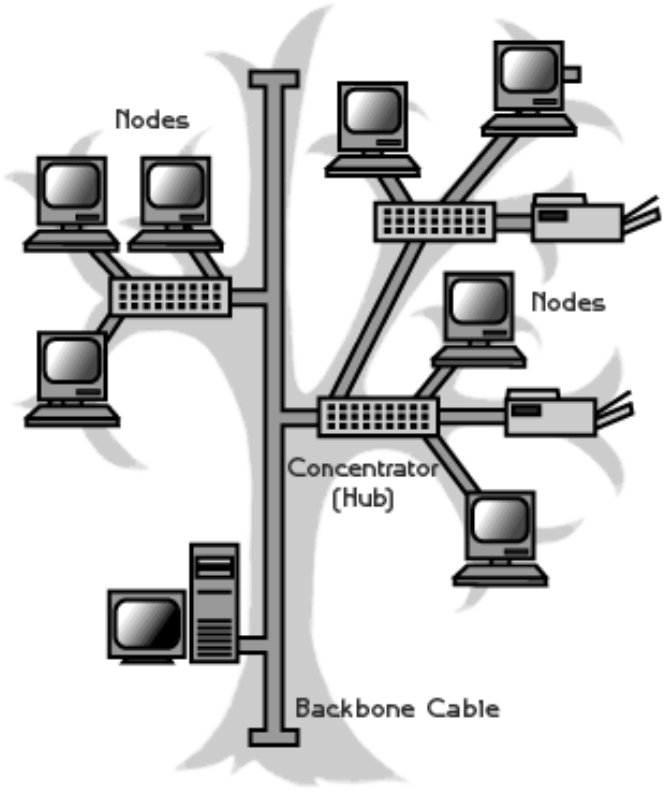

Fig. 7.5: Tree topology

Advantages of a tree topology:

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a tree topology:

- The type of cabling used limits overall length of each segment.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

7.4 Network Types

A computer network is a collection of computers and a device interconnected by communications channels that facilitate communications among users and allows users to share resources. Networks may be classified according to a wide variety of characteristics. A computer network allows sharing of resources and information among interconnected devices.

One way to categorize the different types of computer network designs is by their scope or scale. For historical reasons, the networking industry refers to nearly every type of design as some kind of *area network*. Common examples of area network types are:

1) LAN (Local Area Network)

These are the networks that connect computers and resources together in a building or buildings close together. The computers share resources such as hard-drives, printers, data, CPU power, fax/modem, applications, etc. They usually have distributed processing – means that there are many desktop computers distributed around the network and that there is no central processor machine (mainframe). Fig. 7.6 shows a typical Local area network.

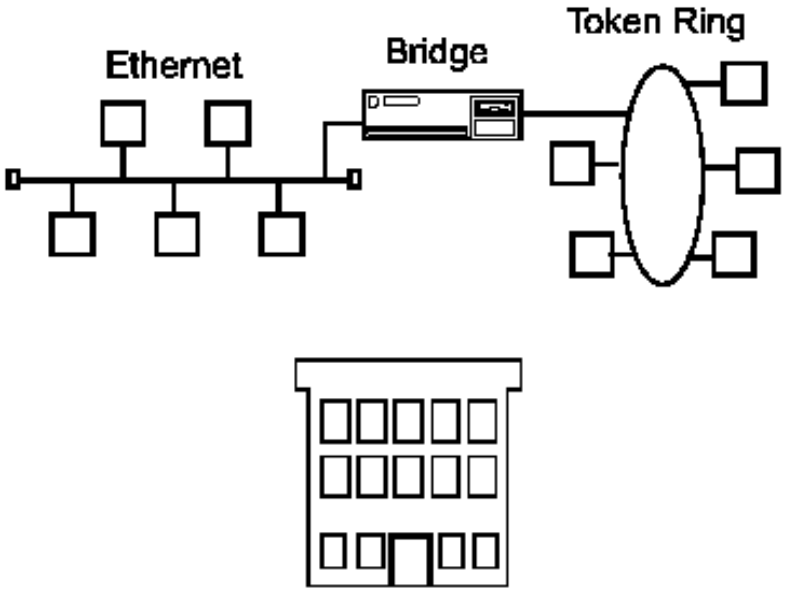

Fig. 7.6: Local area Network

Location: In a building or individual rooms or floors of buildings or connecting nearby buildings together like a campus wide network like a college or university.

2) MAN (Metropolitan Area Network)

These types of networks connect LANs together within a city. In the fig. 7.7, we see that telecommunication services provide the connection (storm clouds) between networks. Local telecommunication services provide the external connection for joining networks across cities. The main criteria for a MAN are that the connection between the LANs is through a local exchange carrier (the local phone company).

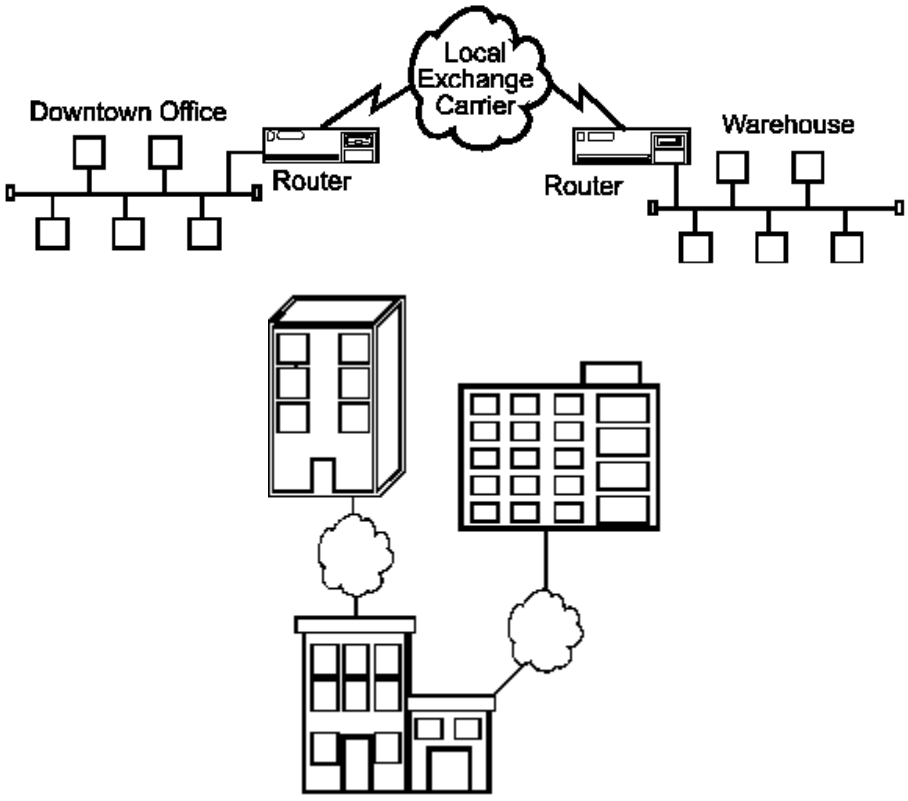

Fig. 7.7: Metropolitan Area Network

Location: Separate buildings distributed throughout a city.

Examples of companies that use MANs are universities, colleges, grocery chains, gas stations, department stores and banks.

The protocols that are used for MANs are quite different from LANs except for ATM which can be used for both under certain conditions.
Examples of MAN protocols are:

- RS-232, V.35
- X.25 (56kbps), PADs
- Frame Relay (up to 45 Mbps), FRADs
- Asynchronous Transfer Mode (ATM)
- ISDN (Integrated Services Digital Network) PRI and BRI
- Dedicated T-1 lines (1.544 Mbps) and Fractional T-1
- T-3 (45 Mbps) and OC-3 lines (155 Mbps)
- ADSL (Asymmetrical Digital Subscriber Line)
- xDSL (many different types of Digital Subscriber Lines)

3) WAN (Wide Area Networks)

This communication system links LANs between cities, countries and continents. The main difference between a MAN and a WAN is that the WAN uses Long Distance Carriers rather than Local Exchange carriers. Otherwise the same protocols and equipment are used as a MAN. Fig. 7.8 shows this type of network.

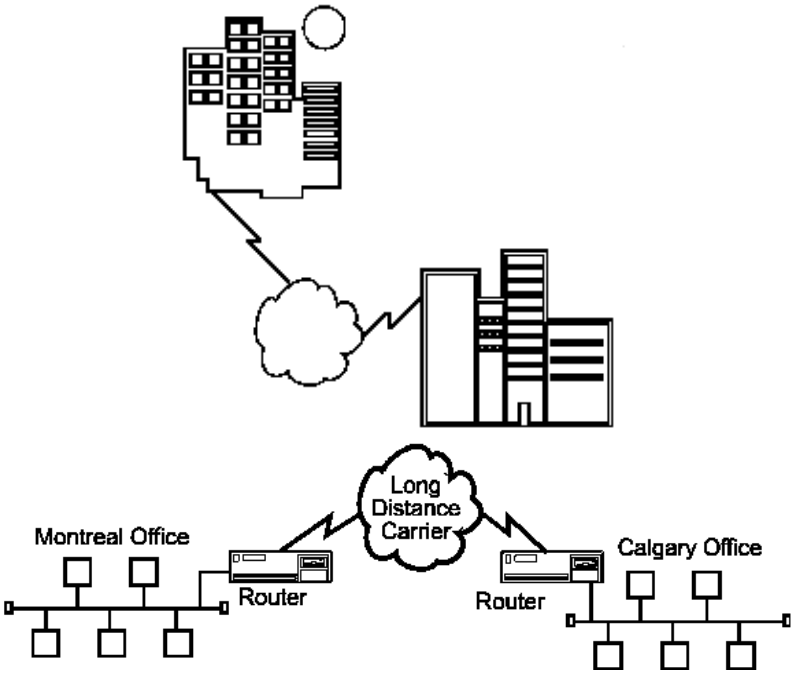

Fig. 7.8: Wide Area Network

Location: City to city, across a country or across a continent.

Wide Area Networks (WANs) connect LANs together between cities or across a country. The TransCanada Pipeline has a WAN that stretches from Alberta in the Western Provinces of Canada to Boston on the Eastern United States seaboard. The pipeline goes from Alberta to Ontario then through the States and ends up in Boston. The maintenance and control of the network resides in Calgary, Alberta.

Self Assessment Questions

3. Which type of network connects computers and resources together in a building or buildings close together?
4. Which type of networks connects LANs together within a city?
5. Which type of Networks connects LANs together between cities or across a country?
6. Star topology requires less cable length than a linear topology. (True/ False).
7. In bus topology it is difficult to identify the problem if the entire network shuts down. (True/False).

7.5 OSI Reference Model

The layered model that dominated data communications and networking literature before 1990 was the ***Open Systems Interconnection (OSI)*** model. Everyone believed that the OSI model would become the ultimate standard for data communications, but this did not happen. The TCP/IP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

Layered Architecture:

The OSI Model is composed of seven ordered layers:

- Layer 1 – The Physical Layer
- Layer 2 – The Data Link Layer
- Layer 3 – The Network Layer
- Layer 4 – The Transport Layer
- Layer 5 – The Session Layer
- Layer 6 – The Presentation Layer
- Layer 7 – The Application Layer

Figure 7.9 below shows the layers involved when a message is sent from device A to device B. As the message travels from one device to another, it may pass through several intermediate nodes or devices. These intermediate nodes or devices usually involve only the first three layers of the OSI model.

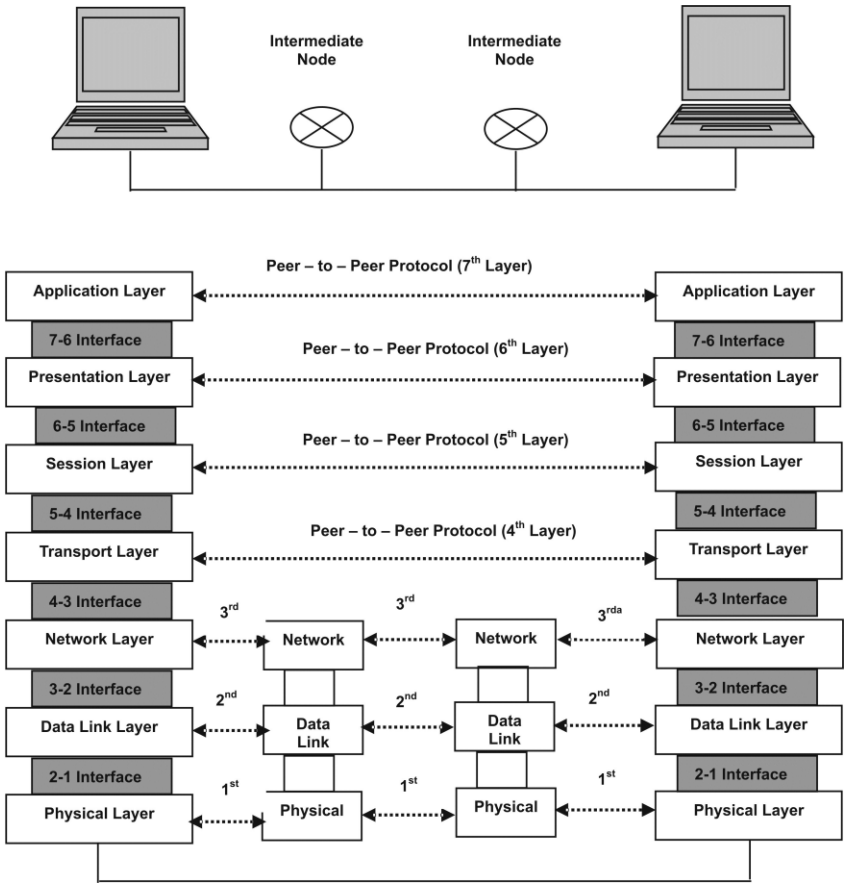

Fig. 7.9: The OSI Model

7.5.1 Layers in the OSI model

Let's discuss the functions of all the 7 layers of OSI model.

1) **Physical layer:** This layer manages the functions required to carry a bit stream over a physical medium. It deals with the electrical and mechanical specifications of the interface and transmission medium. It defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

2) **Data link layer:** This layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (to the Network layer). It is also responsible for other functions such as framing, error control, flow control, physical addressing, and access control mechanisms.
3) **Network layer:** This layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). The Data Link Layer oversees the delivery of the packet between two systems on the same network (links); the network layer ensures that each packet gets from its point of origin to its final destination. If two systems are attached to the same link, there is no need for the network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Other responsibilities of the Network layer include logical addressing, and routing.
4) **Transport layer:** This layer is accountable for process-to-process delivery of the entire message. A process is an application program running on the host. The Network layer oversees the source-to-destination delivery of individual packets; it does not recognize the relationship between those packets. It treats each packet independently, as though each piece belonged to a separate message, whether or not it does, The Transport layer, also ensures that the whole message arrives intact and in order, overseeing both error and flow control at the source-to-destination level.
5) **Session layer:** This layer acts as the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.
6) **Presentation layer:** This layer is anxious with the syntax and semantics of the information exchanged between two systems. The specific responsibilities of this layer include Translation, Encryption, and Compression.
7) **Application layer:** This layer enables the user, whether human or software to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed

information services. Specific services offered by the Application layer include: Provision of Network Virtual terminals, File transfer, access, and management, mail services, and Directory Services.

7.5.2 Data transmission in OSI model

The sending process has some data it wants to send to the receiving process. It gives the data to the application layer, which then attaches the application header, AH (which may be null), to the front of it and give the resulting item to the presentation layer.

The presentation layer may transform this item in various ways, where they are actually transmitted to the receiving machine. On the machine various headers are stripped off one by one as the message propagates up the layers until it finally arrives at the receiving process.

The key idea throughout is although actual data transmission is vertical, each layer is programmed as though it were really horizontal.

Network models

Computer networks are created by different entities. Standards are needed so that these heterogeneous networks can communicate with one another. The two best known standards are the OSI model and the Internet model. The OSI model defines a seven-layer network; the Internet model defines a five-layer network.

Self Assessment Questions

8. _____ layer coordinates the functions required to carry a bit stream over a physical medium.
9. _____ layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks.
10. _____ layer is responsible for process-to-process delivery of the entire message.

7.6 Transmission Control Protocol/Internet Protocol Model

TCP/IP (Transmission Control Protocol/Internet Protocol) is the simple communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other

computer that you may send messages to or get information from also has a copy of TCP/IP. Most of the networking software, TCP/IP is modeled in layers. This layered representation leads to the term protocol stack, which denotes to the stack of layers in the protocol suite. It can be used for positioning (but not for functionally comparing) the TCP/IP protocol suite against others, such as Systems Network Architecture (SNA) and the Open System Interconnection (OSI) model. Functional comparisons cannot easily be extracted from this, because there are basic variances in the layered models used by the different protocol suites.

By dividing the communication software into layers, the protocol stack allows for division of labor, ease of implementation and code testing, and the ability to develop alternative layer implementations. Layers communicate with those above and below via concise interfaces. In this regard, a layer provides a service to the layer directly above it and makes use of services provided by the layer directly below it. For example, the IP layer provides the ability to transfer data from one host to another without any guarantee to reliable delivery or duplicate suppression. Transport protocols such as TCP make use of this service to provide applications with reliable, in-order, data stream delivery.

Figure 7.10 shows how the TCP/IP protocols are modeled in four layers.

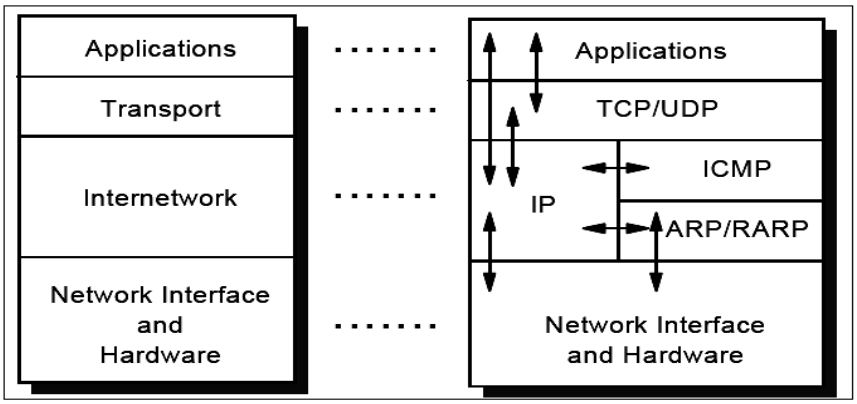

Figure 7.10: The TCP/IP protocol stack: Each layer represents a package of functions.

These layers include:

(i) Application layer: The application layer is provided by the program that uses TCP/IP for communication. An application is a user process cooperating with another process usually on a different host (there is also a benefit to application communication within a single host). Examples of applications include Telnet and the File Transfer Protocol (FTP). The interface between the application and transport layers is defined by port numbers and sockets.

(ii) Transport layer: The transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer. Multiple applications can be supported simultaneously. The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides connection-oriented reliable data delivery, duplicate data suppression, congestion control, and flow control. Another transport layer protocol is the User Datagram Protocol (UDP). It provides connectionless, unreliable, best-effort service. As a result, applications using UDP as the transport protocol have to provide their own end-to-end integrity, flow control, and congestion control, if desired. Usually, UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

(iii) Internetwork layer: The internetwork layer, also called the *internet layer* or the *network layer*, provides the "virtual network" image of an internet (this layer shields the higher levels from the physical network architecture below it). Internet Protocol (IP) is the most important protocol in this layer. It is a connectionless protocol that does not assume reliability from lower layers. IP does *not* provide reliability, flow control, or error recovery. These functions must be provided at a higher level. IP provides a routing function that attempts to deliver transmitted messages to their destination. A message unit in an IP network is called an *IP datagram*. This is the basic unit of information transmitted across TCP/IP networks. Other internetwork-layer protocols are IP (Internet protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol), ARP **(**Address Resolution Protocol)**,** and RARP (Reverse Address Resolution Protocol).

(iv) Network interface layer: The network interface layer, also called the *link layer* or the *data-link layer*, is the interface to the actual network hardware. This interface may or may not provide reliable delivery, and may

be packet or stream oriented. In fact, TCP/IP does not specify any protocol here, but can use almost any network interface available, which illustrates the flexibility of the IP layer. Examples are IEEE 802.2, X.25 (which is reliable in itself), ATM, FDDI, and even SNA. TCP/IP specifications do not describe or standardize any network-layer protocols; they only standardize ways of accessing those protocols from the internetwork layer.

A more detailed layering model is included in Figure 7.11.

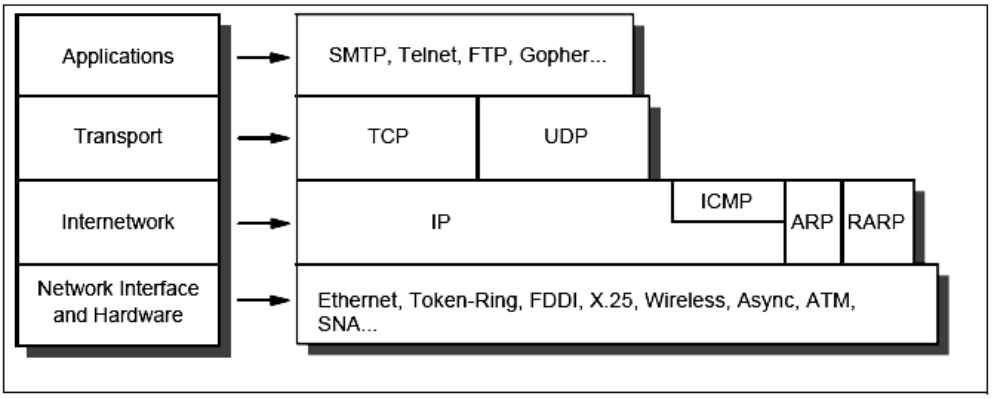

Figure 7.11: Detailed Architectural Model

7.7 Internet

Internet is a worldwide network of networks. It is also the network of networks that connects millions computers (called hosts). The Internet is the virtual space in which users send and receive email, login to remote computers (telnet), browse databases of information (gopher, World Wide Web, WAIS), and send and receive programs (ftp) contained on these computers.

7.7.1 Web browsers

A Web browser is referred as an application that provides access to a Web server. Depending on the implementation, browser capabilities and thus structures vary. A Web browser, at a minimum, consists of a Hypertext Markup Language (HTML) interpreter and HTTP client that are used to retrieve HTML Web pages. Besides this basic requirement, many browsers also support FTP, NNTP (Network News Transfer Protocol), e-mail (POP and SMTP clients), among other features, with an easy-to-manage graphical interface. Fig. 7.12 illustrates a basic Web browser structure.

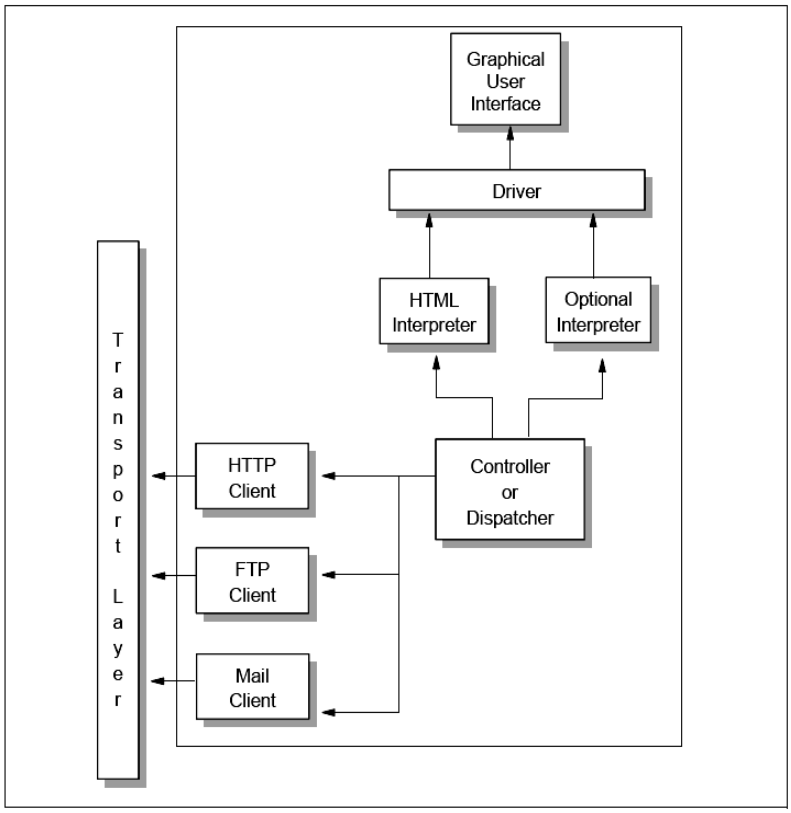

Fig. 7.12: Structure of a Web Browser

As with many other Internet facilities, the Web uses a client/server processing model. The Web browser is the client component. Examples of Web browsers include Mozilla Firefox, Netscape Navigator, and Microsoft Internet Explorer® Web browsers are responsible for formatting and displaying information, interacting with the user, and invoking external functions, such as Telnet, or external viewers for data types that Web browsers do not directly support. Web browsers have become the “universal client” for the GUI workstation environment, in much the same way that the ability to emulate popular terminals such as the DEC VT100 or IBM 3270 allows connectivity and access to character-based applications on a wide variety of computers. Web browsers are widely available for all popular GUI workstation platforms and are inexpensive.

7.7.2 Web servers

Web servers are responsible for servicing requests for information from Web browsers. The information can be a file retrieved from the server's local disk, or it can be generated by a program called by the server to perform a specific application function. There are a number of public-domain Web servers available for a variety of platforms, including most UNIX variants, as well as personal computer environments such as Microsoft Windows. Some well-known public domain servers are CERN, NCSA httpd, and Apache servers.

CERN Servers -

NCSA httpd Servers - The CERN httpd (also known as W3C httpd) is a generic public domain full-featured hypertext server which can be used as a regular HTTP server. The server is typically running on port 80 to serve hypertext and other documents but it can also serve as a proxy -- a server on a firewall machine -- that provides access for people inside a firewall to the outside world. When running as proxy httpd may be configured to do caching of documents resulting in faster response times.

Apache Servers

Apache, a public-domain open source Web server established by a loosely-knit group of programmers. The first version of Apache, based on the NCSA httpd Web server, was developed in 1995. Core development of the Apache Web server is performed by a group of about 20 volunteer programmers, called the Apache Group. However, because the source code is freely available, anyone can adapt the server for specific needs, and there is a large public library of Apache add-ons. In many respects, development of Apache is similar to development of the Linux operating system. The original version of Apache was written for UNIX, but there are now versions that run under OS/2, Windows and other platforms.

Self Assessment Questions

11. A _____ is referred to as an application that provides access to a Web server.
12. _____ is responsible for servicing requests for information from Web browsers.

7.7.3 Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol is a protocol designed to allow the transfer of Hypertext Markup Language (HTML) documents. HTML is a tag language used to create hypertext documents. Hypertext documents include links to other documents that contain additional information about the highlighted term or subject. Such documents can contain other elements apart from text, such as graphic images, audio and video clips, Java applets, and even virtual reality worlds (which are described in VRML, a scripting language for that kind of elements).

Nowadays, both HTTP 1.0 and HTTP 1.1 are stable specifications; therefore, World Wide Web Consortium has closed the HTTP activity after its goal of creating a stable and weakness-free HTTP standard has been achieved.

1. Overview of HTTP

HTTP is based on request-response activity. A client, running an application called a browser, establishes a connection with a server and sends a request to the server in the form of a request method. The server responds with a status line, including the message's protocol version and a success or error code, followed by a message containing server information, entity information, and possible body content.

An HTTP transaction is divided into four steps:

1) The browser opens a connection.
2) The browser sends a request to the server.
3) The server sends a response to the browser.
4) The connection is closed.

On the Internet, HTTP communication generally takes place over TCP connections. The default port is TCP 80, but other ports can be used. This does not preclude HTTP from being implemented on top of any other protocol on the Internet or on other networks. HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used. Except for experimental applications, current practice requires that the connection be established by the client prior to each request and closed by the server after sending the response. Both clients and servers should be aware that either party can close the connection prematurely, due to user action, automated timeout, or program failure, and should handle such

closing in a predictable and desirable fashion. In any case, the closing of the connection by either or both parties always terminates the current request, regardless of its status.

In simple terms, HTTP is a stateless protocol because it does not keep track of the connections. To load a page including two graphics, for example, a graphic-enabled browser will open three TCP connections: one for the page and two for the graphics. Most browsers, however, are able to handle several of these connections simultaneously. This behavior can be rather resource-intensive if one page consists of a lot of elements, as quite a number of Web pages do. HTTP 1.1, as defined in RFC 2616, alleviates this problem to the extent that one TCP connection will be established per type of element on a page, and all elements of that kind will be transferred over the same connection respectively. These deviates from HTTP 1.0 by making the connections persistent.

HTTP operation

In most cases, the HTTP communication is initiated by the user agent requesting a resource on the origin server. In the simplest case, the connection is established through a single connection between the user agent and the origin server, as shown in the following figure 7.13.

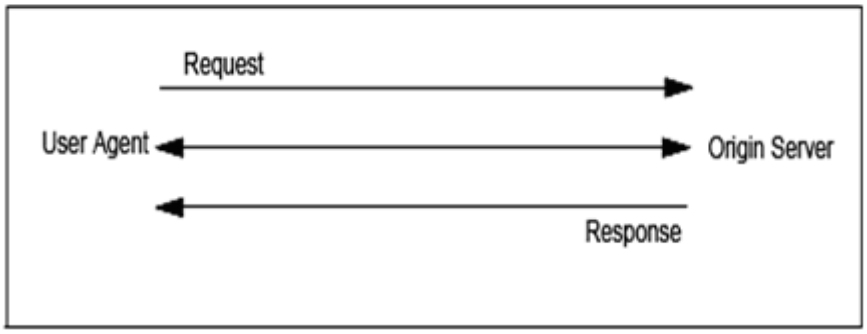

Fig. 7.13: HTTP: Single client/server connection

In some cases, there is no direct connection between the user agent and the origin server. There is one (or more) intermediary between the user agent and origin server, such as a proxy, gateway, or tunnel. Requests and responses are evaluated by the intermediaries and forwarded to the destination or another intermediary in the request-response chain.

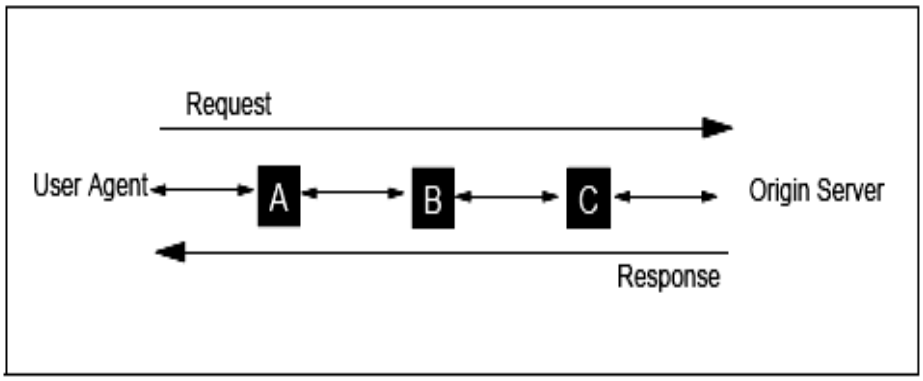

Fig. 7.14: HTTP: Client/server connection

A proxy can handle the content of the data and therefore modify the data accordingly. When a request comes to a proxy, it rewrites all or part of the message and forwards the message to the next destination. A gateway receives the message and sends the message to the underlying protocols with an appropriate format. A tunnel does not deal with the content of the message; therefore, it simply forwards the message as it is.

Proxies and gateways in general, can handle the caching of HTTP messages. This can dramatically reduce the response time and IP traffic in the network. Because tunnels cannot understand the message content, they cannot store cached data of HTTP messages. In the previous figure (Fig. 7.14), if one of the intermediaries (A, B or C) employs an internal cache for HTTP messages, the user agent can get a response from the intermediary if it is previously cached from the origin server in the response chain. Fig. 17.15 illustrates that A has a cached copy of an earlier response from the origin server in the response chain. Therefore, if the server response for the request is not already cached in the user agent's internal cache, it can directly be obtained from A.

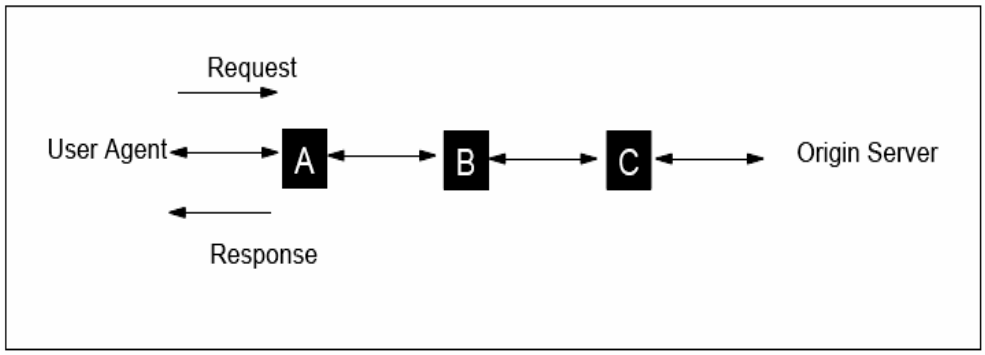

Fig. 7.15: HTTP: Cached server response

Caching is not applicable to all server responses. Caching behavior can be modified by special requests to determine which server responses can or cannot be cached. For this purpose, server responses can be marked as non-cachable, public or private (cannot be cached in a public cache).

Self Assessment Questions

13. HTTP is a stateless protocol because _____.
14. The HTTP communication is initiated by the _____ requesting a resource on the origin server.

7.7.4 World Wide Web (WWW)

The World Wide Web is an architectural frame work for accessing linked documents spread out over millions of machines all over the internet. Its popularity stems from the fact that:

- It has colorful graphical interface that is easy to users to use.
- It provides an enormous wealth of information on almost every conceivable subject.

Architectural overview

The Web consists of a vast, world wide collection of documents called *Web pages* often called simply *pages*. Each page may contain links to other pages anywhere in the world. The idea of having one page point to another is now called hypertext, invented by a visionary M.I.T professor of electrical engineering Vannevar Bush, in 1945, long before the Internet was invented.

A collection of useful, related resources, interconnected via hypertext links, is what has been called a 'web' of information. Making it available on the Internet created what Tim Berners-Lee first called the World Wide Web in

1990. The term "www" is commonly found at the beginning of Web addresses because of the long-standing practice of naming Internet hosts (servers) according to the services they provide.

Pages are viewed with a program called browser. The most popular ones are Internet explorer and Netscape navigator. The browser fetches the page requested, interprets the text and formatting commands on it, and displays the page properly formatted on the screen. Typically Web page starts with a title, contains some information, and ends with email address of the page maintainer.

Strings of text that are links to other pages is called hyperlink. Hyperlinks are often highlighted by underlining, or displaying them in special color or both.

Common Uniform Resource Locator

URL scheme is open-ended in the sense that it is straight forward to have browsers use multiple protocols to get at different kinds of resources. Some common URLs are listed in table 7.1.

Table 7.1: Common Uniform Resource Locator

Name	Used for	Example
http	Hypertext (HTML)	http://www.cs.vu.nl/~ast/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
news	Newsgroup	news:comp.os.minix
news	News article	news:AA0134223112@cs.utah.edu
gopher	Gopher	gopher://gopher.tc.umn.edu/11/Libraries
mailto	Sending e-mail	mailto:JohnUser@acm.org
telnet	Remote login	telnet://www.w3.org:80

1) The *http* protocol is the webs native language, the one spoken by web servers. HTTP stands for hypertext transfer protocol.
2) The ftp is file transfer protocol is used to access files. It is more power than HTTP. For example, it allows user on machine A to transfer a file from machine B to machine C.
3) The *file* protocol is allows to access a local file as a web page. It is similar to FTP but does not require server.

4) Two forms of *news* protocol the first one specifies a news group and can be used to get a list of articles from a preconfigured news site. The second one requires an identifier of a specific news article to be given. The browser then fetches the given article from its preconfigured news site using the Network News Transfer Protocol (NTTP)
5) The *gopher* protocol was used by the Gopher system. It was an information retrieval scheme conceptually similar to the Web. It supported only text and not images.
6) The *mailto* protocol allows users to send email from a Web browser.
7) The *telnet* protocol is used to establish an online connection to remote machines.

Self Assessment Questions

15. What does the Web consists of?
16. State true or false: Each page may contain links to other pages any where in the world.
17. The idea of having one page point to another is now called _____.

7.7.5 Internet Protocol Addressing

IP addresses are represented by a 32-bit unsigned binary value. It is usually expressed in a dotted decimal format. For example, 9.167.5.8 is a valid IP address. The numeric form is used by IP software. The mapping between the IP address and an easier-to-read symbolic name, for example, myhost.ibm.com, is done by the ***Domain Name System (DNS)***.

To identify a host on the Internet, each host is assigned an address, the *IP address*, or in some cases, the *Internet address*. When the host is attached to more than one network, it is called *multihomed* and has one IP address for each network interface. The IP address consists of a pair of numbers:

IP address = <network number><host number>

IP addresses are 32-bit numbers represented in a *dotted decimal* form (as the decimal representation of four 8-bit values concatenated with dots). For example, 128.2.7.9 is an IP address with 128.2 being the network number and 7.9 being the host number. Next, we explain the rules used to divide an IP address into its network and host parts.

The binary format of the IP address 128.2.7.9 is:

10000000 00000010 00000111 00001001

IP addresses are used by the IP protocol to uniquely identify a host on the Internet (or more generally, any internet). Strictly speaking, an IP address identifies an interface that is capable of sending and receiving IP datagrams. One system can have multiple such interfaces. However, both hosts and routers must have at least one IP address, so this simplified definition is acceptable. IP datagrams (the basic data packets exchanged between hosts) are transmitted by a physical network attached to the host. Each IP datagram contains a *source IPaddress* and a *destination IP address*. To send a datagram to a certain IP destination, the target IP address must be translated or mapped to a physical address. This might require transmissions in the network to obtain the destination's physical network address.

Class-based IP addresses

The first bits of the IP address specify how the rest of the address should be separated into its network and host part. The terms *network address* and *netID* are sometimes used instead of network number. Similarly, the terms *host address* and *hostID* are sometimes used instead of host number.

There are five classes of IP addresses as shown in Figure 7.16.

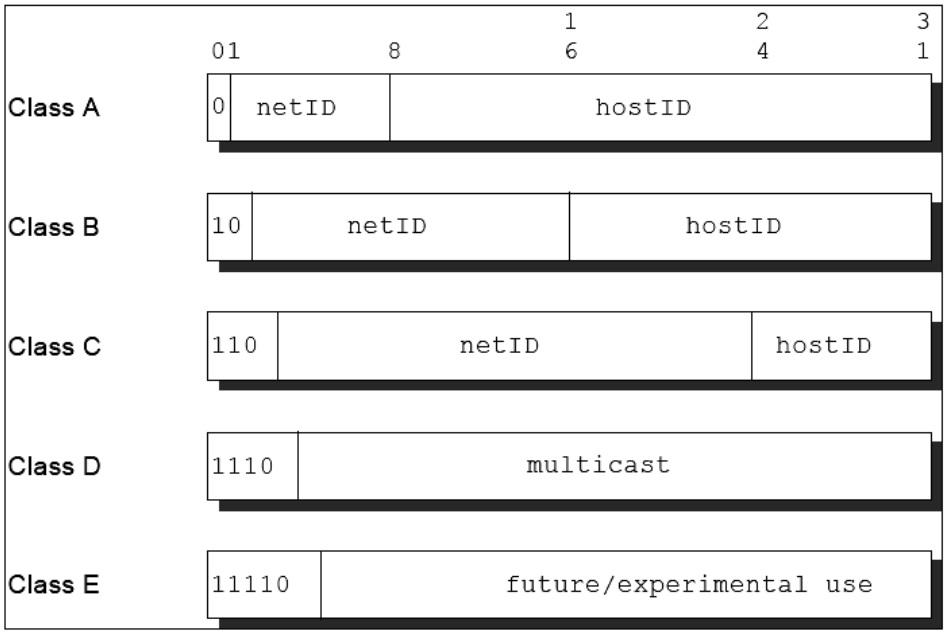

Fig. 7.16: Assigned classes of IP addresses

Where:

Class A addresses: These addresses use 7 bits for the <network> and 24 bits for the <host> portion of the IP address. This allows for 2^7-2 (126) networks each with 2^{24}-2 (16777214) hosts – a total of more than 2 billion addresses.

Class B addresses: These addresses use 14 bits for the <network> and 16 bits for the <host> portion of the IP address. This allows for 2^{14}-2 (16382) networks each with 2^{16}-2 (65534) hosts – a total of more than 1 billion addresses.

Class C addresses: These addresses use 21 bits for the <network> and 8 bits for the <host> portion of the IP address. That allows for 2^{21}-2 (2097150) networks each with 2^8-2 (254) hosts – a total of more than half a billion addresses.

Class D addresses: These addresses are reserved for multicasting (a sort of broadcasting, but in a limited area, and only to hosts using the same Class D address).

Class E addresses: These addresses are reserved for future or experimental use.

Class A address is suitable for networks with an extremely large number of hosts. Class C addresses are suitable for networks with a small number of hosts. This means that medium-sized networks (those with more than 254 hosts or where there is an expectation of more than 254 hosts) must use Class B addresses. However, the number of small- to medium-sized networks has been growing very rapidly. It was feared that if this growth had been allowed to continue unabated, all the available Class B network addresses would have been used by the mid-1990s. This was termed the **IP address exhaustion problem**.

The division of an IP address into two parts also separates the responsibility of selecting the complete IP address. The network number portion of the address is assigned by the RIRs. The host number portion is assigned by the authority controlling the network. As shown in the next section, the host number can be further subdivided: This division is controlled by the authority that manages the network. It is not controlled by the RIRs.

7.8 Summary

In this unit you learnt about the various concepts of Communication.

Let's recap the important points covered in the unit:

- Communication System is a system or facility capable of providing information transfer between persons or equipment's.
- Data Communications concerns the transmission of digital messages to devices external to the message source.
- A signal is an electric current or electromagnetic field used to convey data from one place to another.
- Topology is a term used to define the way in which computers are connected in network. The physical topology of a network denotes to the configuration of cables, computers, and other peripherals.
- A star topology is designed with each node connected directly to a central network hub or concentrator.
- A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable.
- The layered model that dominated data communications and networking literature before 1990 was the *Open Systems Interconnection (OSI)* model.
- Network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
- Transport layer is accountable for process-to-process delivery of the entire message.
- Most of the networking software, TCP/IP is modeled in layers. This layered representation leads to the term protocol stack, which denotes to the stack of layers in the protocol suite.
- The internetwork layer, also called the *internet layer* or the *network layer*, provides the "virtual network" image of an internet (this layer shields the higher levels from the physical network architecture below it).
- A Web browser is referred as an application that provides access to a Web server. Depending on the implementation, browser capabilities and thus structures vary.
- The Hypertext Transfer Protocol is a protocol designed to allow the transfer of Hypertext Markup Language (HTML) documents.

7.9 Terminal Questions

1. Explain basic elements of communication system.
2. What is data communication?
3. Briefly explain data & signal.
4. Write a short note on data transmission medium.
5. Briefly explain various network types.
6. What is OSI reference model?

7.10 Answers

Self Assessment Questions

1. Transmitter
2. Receiver
3. LAN
4. MAN
5. WAN
6. False
7. True
8. Physical
9. Network
10. Transport
11. Browser
12. Web server
13. It does not keep track of the connections
14. User agent
15. Web pages
16. True
17. Hypertext

Terminal Questions

1. Communication System is a system or facility capable of providing information transfer between persons or equipment's. (Refer section 7.2)
2. Data Communications concerns the transmission of digital messages to devices external to the message source. (Refer section 7.3)
3. A signal is an electric current or electromagnetic field used to convey data from one place to another. The simplest form of signal is a direct current (DC) that is switched on and off; this is the principle by which the early telegraph worked. (Refer section 7.3)

4. Transmission media is the physical path between the transmitter and receiver. It can be guided or unguided. (Refer section 7.3.2)
5. One way to categorize the different types of computer network designs is by their scope or scale. (Refer section 7.4)
6. The layered model that dominated data communications and networking literature before 1990 was the Open Systems Interconnection (OSI) model.

References:

- Absolute Beginner's Guide to Computer Basics By Michael Miller, Que Publishing, 2007
- Alex Leon & Mathews Leon, “Fundamentals of Information Technology”, Leon Techworld, 2009.
- Computer Concepts Basics By Dolores Wells, Course Technology, 2009
- Computer fundamentals: architecture and organization By B. Ram, New Age International, 2000
- Data and Computer Communications (9th Edition) by William Stallings (Aug 13, 2010)
- P. K. Sinha & Priti Sinha, “Computer Fundamentals”, BPB Publications, 2004.
- Vikas Gupta, “Comdex Computer Kit”, Wiley Dreamtech, Delhi, 2004
- V. Raja Raman, “Introduction to Computers”, PHI, 1998.
- Windows XP: the complete reference By John R. Levine, Margaret Levine Young, Osborne/McGraw-Hill, 2001.

E-References

- www.webopedia.com/TERM/N/network.html
- searchnetworking.techtarget.com/definition/network
- www.howstuffworks.com
- www.personal.kent.edu
- www.searchcio-midmarket.techtarget.com