UNIT 9 COMMUNICATION PROTOCOLS AND NETWORK ADDRESSING

Structure

9.0 OBJECTIVES

After going through this Unit, you will be able to understand and appreciate:

- What are protocols;
- Difference between computing and communication protocols;
- Need for communication protocols;

- Difference between connection-oriented and connectionless protocols;
- Basic packet transfer protocols like IP, TCP and UDP;
- Most widely used network computing architecture: Client-Server;
- File transfer and remote login application protocols like FTP and Telnet;
- Convergent cell switching in ATM networks;
- Fast routing technique using labels: MPLS;
- Numbering schemes used for landline and mobile phones;
- How network computers are addressed world over;
- Details of IPv4 addressing scheme;
- IPv6 features briefly; and
- Web access protocols for both wired and wireless networks.

9.1 INTRODUCTION

Quest for new knowledge is the central theme of human existence. All of us, whether we realise or not, are in the process of acquiring new knowledge all the time. When we ask a question, we are seeking knowledge. When we answer a query, we give information to the person posing the question. When a person assimilates the given information, we say that the person has acquired knowledge. Knowledge is spread via information that is communicated from one person to another in some form: oral, writing etc. Thus, knowledge, information and information communication are three entities that are closely inter-related.

It is often said that we are in the information age. In the last about six decades, information in the world has been growing at an exponential rate, i.e. doubling every 10 years. Information Communication Technology (ICT) has grown leaps and bound in the last 30 - 40 years. Instant transfer of information from one part of the world to any other part is a reality today. Underlying this development is the convergence of computer and communication technologies. This convergence process started in late 1960s and has led to the development of worldwide computer network that is now known popularly as **Internet.** A large number of home and office local area networks (LANs) and innumerable personal computers all over the world have been interconnected to form Internet. Hence, it aptly said that Internet is a **network of networks.** Information travels in the form of data packets on Internet and hence it is also called a **data network.** Data packets are of fixed length, say 2048 bytes, i.e. 2" bytes. Long messages are broken into as many packets as required before transmission. Because of packet-based transmission, the Internet also carries the nomenclature **Packet Data Network** (PDN). Since Internet is an open public network, another related nomenclature that is used sometimes is **Packet Switched Public Data network** (PSPDN). Internet is not limited to its presence only on the land but is also in ships at the seas and in planes in the air.

United Nations today has 192 countries of the world as its members. Almost all these countries have Internet connection in place. About 200,000 LANs are connected to the Internet. Over 1.5 billion people, i.e. a quarter of the world population has access to Internet. With the evolution of Internet, our life-style is changing. A number of our day-to-day activities are being carried out on the Internet. Clearly, the society is evolving towards a networked community with electronic information as the central commodity.

One might term the society of the 21st century as the **Networked Electronic Information Society** (NEIS). It is a society in which activities are centred on networks and the main commodity on the networks is electronic information in digital form.

It is important to realise that with alt its massive presence, Internet is still evolving. Today's Internet services are predominantly text and data oriented with only sprinkles of graphics, still pictures and slow motion video. Experience shows that Internet is slow for many network applications. Internet is basically designed for data transport. Real time services like voice and video transmissions experience serious quality problems. The key to the solution of current Internet problems lies in building **Global Information Infrastructure** (GII) that would have adequate capacity and efficiency to support full-scale services including high quality audio and motion video and high-resolution graphics envisioned for NEIS.

Information exchange between computers that are connected to a massive worldwide network cannot happen without standard procedures and sets of rules that govern such an exchange. A comprehensive collection of such standard sets of rules and procedures are called **communication protocols.** Furthermore, every entity on the Internet needs to be identified uniquely. This is done by assigning a **network address** to each entity. Communication protocols and network addressing are the subject matter of this unit.

9.2 WHAT ARE PROTOCOLS?

Let us start understanding protocols. The word protocol has different connotation under different circumstances. In governments, protocol means a strict official procedure in state affairs and diplomatic occasions. For example, in India the President is the Head of the State and there are protocols that govern his/her participation in state functions. These protocols specify how and where the President will be seated, who would accompany him/her, how would the dignitaries be introduced etc. In other words, they specify the accepted code of behaviour in particular situations. They may cover aspects about appearance (dress code), ways of greeting, conversation, and eating manners. All these rules help people successfully communicate and work together.

In inter-governmental dealings, the word protocol is used to denote the original draft of a diplomatic document containing especially terms of a treaty agreed to in a conference and signed by the parties concerned. You might have heard of Kyoto Protocol, a document that spells out the terms to be adhered to by the signatories for controlling and reducing carbon emissions in the world.

In science, a formal record of scientific experimental observations is often called a protocol. Procedures for carrying out scientific experiments or a record of the course of any medical treatment are also known as protocols.

The word protocol is used extensively in computers and communications as well. In computers, protocols deal with interaction between processes, exchange of messages etc. A process, as you may know, is a program in execution. In communication, protocols deal with signalling, switching, routing, forwarding, error control, monitoring, and recovery procedures in the exchange and transmission of information across entities in a network. A fundamental difference between the two is as follows. While computing protocols define rules for communication among processes within a computer, the communication protocols define rules for communication among computers. Both of them, however, deal with exchange of information. Protocols are generally software programs that implement the rules for communication. Some protocol functions are implemented in hardware, particularly those dealing with the movement of bits and bytes. In Section

9.3, we briefly discuss computing protocols and study communication protocols in greater detail in later sections.

9.3 COMPUTING PROTOCOLS

Computing and communication protocols together define sets of rules and procedures that govern all the information management functions. With electronic information being the central commodity in NEIS, information management functions become the core of technological capability in networks. There are seven functions of electronic information management that are important:

1) Generation
2) Acquisition
3) Storage
4) Retrieval
5) Processing
6) Transmission
7) Distribution

Computing and communication protocols govern all these functions. In general, information is generated by human thought process, human acts and by happenings in nature. Human intellectual activity is creative and intuitive and hence may not be amenable to protocols. Whether technology generates information is a debatable point. When data is processed in a computer, the output is considered as information. In that sense, it may be said that computers generate information. But the basic data comes from nature or human activity. However, machine generation of information can be governed by protocols.

Among the other functions, storage, retrieval and processing fall in the realm of computing protocols. The remaining functions, viz. acquisition, transmission and distribution fall in the class of communication protocols. Transmission and distribution functions may be collectively called as information *dissemination.* Transmission refers to bulk transfer between two main points. Distribution refers to transfer to end points like user computers or terminals.

Computing protocols are relatively a recent development. As you are aware, information processing, storage and retrieval are functions performed by application processes. You are familiar with applications like word processing, spread sheet, power point presentation and data base management. Computing protocols deal with information storage, retrieval and exchange among these applications. For example, how do we import information from word files into spreadsheets or vice versa? Or how do we import information from word files to power point presentation slides and vice versa? Computing protocols are being evolved to make such imports fairly easy. Some of the well-known computing protocol functions include message passing, process synchronisation and process switching, simple object access and object communication and data portability.

The idea of computing protocols is to encourage what are known as open systems design. Open systems follow industry standards and are capable of running on variety of platforms. For example, open office is an innovation in computing protocols. Many Java products use open computing protocols. Microsoft has recently announced a

number of open computing protocols and has made them available in public domain. Open computing protocols offer greater opportunity and choice for freelance developers as they conform to industry standards. In contrast, closed protocols are proprietary in nature and are vendor specific.

Interoperability in computer systems is the main goal of computing protocols. By interoperability we mean the ability of different applications to interwork with each other using common data. User does not have to reformat and copy data from one application to another. Interoperability principles include:

- Ensuring open connections
- Promoting data portability
- Enhancing support for industry standards
- Driving open approach across competitors.

Although the open approach is currently limited to application packages from the same vendor, increasingly computing protocols are addressing issues for interoperability across different vendor products and platforms. Interoperability concept is also applicable to networked computers.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

1) Differentiate between computing and communication protocols.

.....

.....

.....

.....

9.4 COMMUNICATION PROTOCOLS: GENERAL CONCEPTS

Communication protocols deal with all aspects of communication functions that are required for information exchange among computers in a network or across networks. They are designed especially in the context of Internet. We have already discussed in Unit 8 the protocols that are used for information exchange in LANs. On the Internet, communication related functions include:

- Breaking up messages into packets
- Packet sequencing and reassembly
- Synchronisation or handshaking for information exchange
- Signalling: start and end of messages
- Switching: routing or forwarding of messages towards their respective destinations
- Connectionless and connection oriented transfers

- Message encapsulation and de-capsulation
- Format conversion
- Error detection and correction
- Setting up and termination of sessions
- Recover from unexpected loss of connection.

We discuss each one of the above functions in order in the following paragraphs.

Packet formation: As mentioned earlier, in data networks information is transferred in the form of packets. Packets are of fixed length with an upper bound on the size. For example, the maximum size of a packet in Ethernet is 1500 bytes. User messages longer than the maximum permissible packet size need to be broken into multiple packets.

Packet sequencing: As explained in Unit 8, routers take forwarding decisions independently for each packet. Even static routing algorithms may have more than one route defined for the same destination. Depending upon the path taken, the packets may arrive out of sequence at the destination. If the packets belong to the same message, they cannot be delivered to the user program unless they are properly sequenced. The concerned communication protocol needs to perform this function of sequencing the packets of the same message in proper order. Breaking up a message into multiple packets at the source and reassembling them at the destination are complementary functions performed by communication protocols.

Synchronisation: A packet transmission cannot start unless the receiving station is ready. The sending and the receiving stations exchange handshake signals and synchronise their transfer process. Handshake signals are like sending a query 'Are you ready?' and receiving a response like 'OK, go ahead'. The synchronisation process includes agreeing on transfer speeds and the required buffer sizes. When the transfer is in progress, the receiving station may want a pause for reasons like buffer full. Handshake signals are exchanged to enforce 'pause' and 'resume' actions.

Signalling: Once synchronisation is achieved, the actual transmission starts. At this stage, the sending station must signal to the receiving station the start of the packet. This is usually done by sending 'start of text (STX)' bit pattern. Similarly, the end of the packet is indicated by 'end of text (ETX)' bit pattern.

Routing: We have discussed this function in detail in Unit 8.

Transfer modes: There are two fundamental ways in which information transfer takes place in our life: connectionless and connection oriented. These transfers are analogous to postal communication and telephone communication respectively. In postal system, we write a letter, post the same and expect it to reach the addressee. The postal system delivers on the best-of-efforts basis. While the letters are delivered most of the time, some get lost somewhere. In telephone communication a connection is first established between the parties concerned and then the communication takes place.

Encapsulation: Consider a packet traversing six routers before reaching the destination. Let the source station and the first four routers be on the same network. The last two routers and the destination station belong to another incompatible network. The fourth router will now have to encapsulate the user packet to make it compatible to the destination network. Encapsulation is like putting one envelope (user packet) into another and writing the addresses differently on the outer envelop. At the destination, the outer

envelope (encapsulated packet) is discarded and the original information obtained. This is termed as de-capsulation.

Format conversion: Sometimes when moving packets between incompatible networks, pack formats may have to be changed. An example is moving packets between Ethernet and Token ring LANs, which calls for format conversion.

Error handling: Errors occur in data transmission. These have to be detected and corrective action taken. Error detecting codes are used to detect errors. There are two basic techniques available for error recovery. One is when an error is detected in a packet, it is discarded and the sending station is requested to retransmit the packet. This technique is called automatic repeat request (ARQ). Handshake mechanism is used to request retransmission of the packet. The other is to use forward error correction codes (FEC) that are capable of both detecting and correcting errors at the receiving end.

Sessions: A variety of tasks are performed on the networks by establishing sessions between a server and a client computer. Online search of databases, remote job entry, remote login to a time sharing system and fie transfer between two systems are examples of different types of sessions. Different sessions have different requirements. For example, a dialogue may be two-way simultaneous or one-way alternating. A large file transfer session may call for establishing roll back points to recover from connection failures. Session protocols perform functions required to establish, successfully execute and terminate properly different types of sessions.

Packet loss: It is not unusual to experience unexpected loss of connections in networks. You might have had this experience while accessing Internet. Some Internet browsers including Microsoft's Internet Explorer have provision to resume a session that was terminated unexpectedly, say due to a power failure. Many communication protocols have features to recover from unexpected connection failures. This is particularly so in sessions related protocols.

In this section, we have studied the general features that are required in communication protocols. In the next section, we look at the details of some of the commonly used communication protocols.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

2) We use signalling as a matter of fact in our daily life. Give any four examples of such signalling.

3) Is SMS a connectionless or connection oriented service?

4) When you are typing on a computer terminal, you make a mistake. Then you correct it. Which one of the techniques, ARQ or FEC you are using? Give reasons.

5) Many word processing packages have auto correct features. Which one of the techniques, ARQ or FEC is used there? Give reasons.

.....

.....

.....

.....

9.5 COMMON COMMUNICATION PROTOCOLS

The field of ICT is replete with protocols. Hundreds of protocols have been defined for various purposes. Many are very specialised, some are rarely used and some are defunct. You are already familiar with computing and communication protocols. There are other classes of protocols such as *data (bits & bytes) transmission protocols, routing protocols, access protocols, services protocols* and *applications protocols.* As a user of networks, you need to be concerned with only about a dozen protocols. This is much like a language dictionary having over 100,000 words and the average vocabulary of a person being about 4000 words.

Extensively used communication protocols include:

- Internet Protocol (IP)
- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
- File Transfer Protocol (FTP)
- Remote Login Protocol (Telnet)
- Internet Control Message Protocol (ICMP)
- Dynamic Host Configuration Protocol (DHCP)
- Post Office Protocol 3 (POP3)
- Simple Mail Transfer Protocol (SMTP)
- Internet Message Access Protocol (IMAP)
- Cell Switching Protocols (ATM)
- Muti Protocol Label Switching (MPLS)
- HyperText Transfer Protocol (HTTP)
- Wireless Application Protocol (WAP)
- Lightweight Transport Protocol (LTP)
- General Packet Radio Service (GPRS)
- Simple Network Management Protocol (SNMP)

Of the above, the first three protocols, viz. IP, UDP and TCP are basic protocols used by a variety of Internet services and applications. We discuss them in Section 9.6. FTP and Telnet are most extensively used service or application level Internet protocols. A large number of applications on the Internet use what is known as Client-Server architecture. FTP and Telnet and web browsers also use this architecture. We present this architecture in Section 9.7. We discuss FTP and Telnet in Section 9.8.

Routers use ICMP to report any abnormal event on the network. An example of an abnormal event that a router may discover is the outage of the network in some segment. Such an event may be reported to all other routers on the network as welt as the to the network management centre. ICMP is also used to monitor the functioning of Internet. ICMP, however, is not discussed in this course. DHCP is used for managing IP address allocation in local networks. This is an advanced protocol meant for network

administrators and as such we do not discuss the same. POP3, SMTP and IMAP are all e-mail related protocols. They are not discussed in this unit.

At the data transmission level, viz. transfer of bits and bytes a new convergent switching technique has emerged in the 1990s. This technique is known as cell switching and the associated transfer mode is called Asynchronous Transfer Mode (ATM). There is a set of protocols associated with ATM. We present an introduction to ATM in Section 9.9.

Multi Protocol Label Switching (MPLS) is router-based technique for routing IP packets fast. An introduction is given to MPLS in Section 9.10.

HTTP is the widely used web access protocol designed to work with desktop and laptop computers. WAP and LTP are wireless access protocols designed to work with small portable devices like mobile phones. These protocols are discussed in Section 9.14.

A related protocol is GPRS that is used to send packets over slow-speed wireless links. GPRS is not discussed here. SNMP is discussed in Unit 11 that deals with network management.

9.6 BASIC COMMUNICATION PROTOCOLS: IP, UDP, TCP

9.6.1 Internet Protocol (IP)

Internet protocol (IP) is fundamental to the operation of Internet. All services on the Internet use IP for sending or receiving packets. No computer can be connected to the Internet without the IP running on it. Hence all computer operating systems like Windows provide IP bundled with them. IP software is usually memory resident. IP specifies exactly how a packet must be formed and how an Internet router should deal with the packet.

Packet and packet switching are generic terms used in a variety of contexts in ICT. For example, a network not conforming to Internet standards may use packet switching and define its own packet structure. In order to distinguish from other packets and to uniquely identify IP packets, the term *IP datagram* or simply *datagram* is used. We use the term datagram to mean an IP packet in this course module.

Although IP is a communication protocol defining datagram formats and transfer details, it serves an important purpose that goes almost unnoticed. Once on the Internet, a user can create and send datagrams to any computer on the Internet irrespective of where the destination computer is located. The user is unmindful of the presence of different component networks and a host of routers that interconnect them. Thus, IP makes a network of networks appear as one giant seamless data network.

An important aspect of IP is that it delivers datagrams on the best-of-efforts basis. The delivery is not guaranteed. The central idea in IP design has been internetworking and fast transfer of datagrams and not aspects like recorded delivery. Such aspects are taken care of higher-level protocol like TCP that we discuss later.

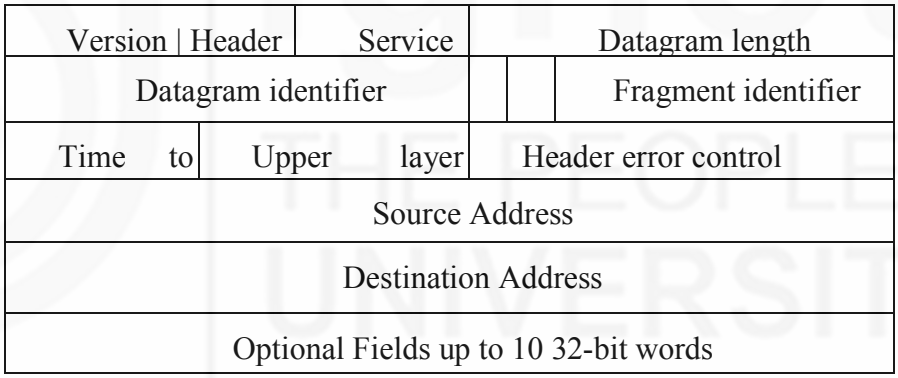
In general, a packet has the structure shown in Fig. 9.1. We use the term payload to denote the sum total of data handed over to IP for transmission. The payload may be pure user data or user data encapsulated with other information by any of the communication protocols.

The datagram header has a mandatory fixed length part and an optional variable length part as shown in Fig. 9.1(b). The fixed length is 20 bytes and the variable length can be up to 40 bytes making the maximum size of the header as 60 bytes. The different fields of the fixed part are illustrated in Fig. 9.1 (c) where each row is 32-bit or 4 bytes long. The source and destination addresses are 32-bit each corresponding to IPv4 address format.

IP addresses have two versions: Version 4 and Version 6 abbreviated as IPv4 and IPv6 respectively. IPv4 uses 32-bit address and IPv6 128-bit. IPv4 has been in use for a very long time, over 30 years, and most of the computers on the Internet have IPv4 addresses as of now. IPv6 has been introduced recently. Over the years, IPv6 is expected to replace IPv4 addresses. IP addresses are discussed in detail in Sections 9.13. The 'version' field in the header specifies the version to which the header belongs. Version information in each datagram permits the coexistence of different versions and smooth transition from one version to another.

(a) A Generalised Packet format

(b) Datagram header Darts



(c) Mandatory Fields of IPv4 datagram header

Fig. 9.1: IPv4 datagram formats

The maximum size of IP datagrams can be up to 64 k bytes including the header and the text part. But rarely such a big size is used. Different networks are allowed to set their own limit for the maximum size of the datagram well below the theoretical limit of 64 k. This maximum size set by a network is called the *maximum transfer unit* (MTU) of that network. This provision further complicates processing of datagrams. If a datagram is delivered to a network with a size greater than the MTU of the network, then the datagram needs to be fragmented for transportation within that network and reassembled at the exit point of that network. In such a case, we need a provision to identify the datagram and its fragments. IP header fields, datagram identifier* and 'fragment identifier' in Fig. 9.1(c) are provided for this purpose. While reassembling the fragments, IP must know the original protocol from which the fragments came. This is specified in the field 'Upper layer protocol'. The one-bit 'M' field when set to 'V implies 'More fragments to come'. This bit is set to '1' in all but the last fragment. The last fragment will have this bit set to '0'. There may be certain applications where fragmentation may not be acceptable. The one-bit 'D' field, if set to '1' would mean Do not fragment'. In such cases, the route will be so chosen that no fragmentation occur.

You may recall that sometimes packets may wander indefinitely without getting delivered to the destination due to routing errors. The field Time to live' is used to exercise control over such malfunctioning. The field 'service type' addresses issues like priority etc. Other fields in the header are self-explanatory.

9.6.2 User Datagram Protocol (UDP)

UDP provides connectionless service at the user level. It uses IP for this purpose. In that sense, UDP is a higher-level protocol when compared to IP. Here, a user submits his/her entire message to UDP with a request for transfer to the specified destination. User message is a payload for UDP. In turn, UDP encapsulates this with its own header and passes the same to IP as payload. User datagrams are different from IP datagrams. User datagrams do not conform to IP standard. They are just chunks of information of any size. UDP encapsulates the user datagram with its own header to form UDP datagram. UDP may split a user datagram into multiple UDP datagrams conforming to IP standards.

UDP datagram is shown in Fig 9.2. Now let us see as to why UDP adds its own header to the user data. Many application processes or users on a computer may use UDP simultaneously. Hence, UDP needs to maintain an identity of individual process and its corresponding destination process. This information is kept in its header in the form of source and destination port numbers so that the datagram may be delivered to the correct destination process along with the source identification. In Fig. 9.2 each row is 4 bytes long. With two rows the UDP header is 8-bytes long. The port fields in the header identify the source and destination processes or applications.

Source Port	Destination Port
UDP Length	UDP Error
UDP Data or payload	

.

Fig. 9.2: UDP datagram structure

Each port field is 16-bit long. The destination port value is used to deliver the user datagram to the correct application. The destination application may use the source port value for sending a response to the source application. The port address feature is the one that distinguishes UDP from IP. Otherwise, the functional capability of UDP is the same as that of IP. As in the case of IP, UDP messages may be lost, duplicated and delivered out of sequence.

The value of the UDP length field specifies the total length of the datagram including data part and the header. The use of UDP error control field is optional. This field is used only for the header portion of the PDU, i.e. the error control is done only for the header. The UDP does not perform error control at the datagram level. This must be taken care of at the application level. The payload supplied by the user or an application program follows the header. The entire UDP datagram with its header and user data becomes the payload for IP.

UDP, being a connectionless service functions on the best-of-efforts basis. There is no delivery acknowledgement in UDP. There is no guarantee of delivery. But it is used extensively like the postal system. The protocol is simple, efficient and fast. There are a large number of applications where occasional non-delivery is acceptable. If the underlying network is reliable, UDP is very effective.

9.6.3 Transmission Control Protocol (TCP)

TCP is a connection-oriented service. It uses IP and is at a higher level. In fact, UDP and TCP are at the same level. TCP is guaranteed delivery service. TCP provides reliable and error free communication. It achieves this in four ways:

1) Detects errors in datagrams and uses ARQ technique for error recovery

2) Recognises duplicate datagrams and discards all but one

3) Detect lost datagrams and retransmit the same

4) Sequences datagrams received out of sequence

You are already familiar with error detection and the use of automatic repeat request. As you aware that some routing algorithms send out multiple copies of datagrams to achieve robustness. TCP checks for duplicate datagrams and accepts only the error free copy received first. Detection of lost datagrams is done using acknowledgement and timer mechanisms. Receipt of every datagram is acknowledged by the destination. At the time of sending a datagram the source initiates a timer with a value within which the acknowledgement must be received. If the timer expires and no acknowledgement has been received, the source concludes that the datagram is lost and despatches another copy. By adopting the above said four mechanisms TCP is able to provide reliable and error free transmission.

TCP being a connection-oriented service establishes a connection between two communicating programs before data transfer begins. The service progresses in four phases as in the following:

- Source requests TCP for a connection by giving the destination identity. TCP contacts the destination
- Destination responds with a positive acknowledgement
- Data transfer takes place
- Connection terminated

This is very much like what happens in a telephone conversation. Much as the way we use both telephone and postal systems extensively in our daily life, both TCP and UDP are used extensively on the Internet. Since TCP and IP are closely interlinked, vendors bundle both the software routines as part of the operating system. This is why you always hear of TCP/IP together.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

6) How many fields are there in the mandatory portion of IP header?

7) Why is fragmentation required while transferring IP datagrams?

8) What action is expected of a router if the field 'D' is set to '1' in the IP header?

9) What purpose the port fields in UDP header serve?

10) How does TCP detect lost datagrams?

.....

.....

.....

.....

9.7 CLIENT-SERVER ARCHITECTURE

As mentioned earlier, FTP, Telnet and Web browsers are based on client-server architecture. Client-Server architecture is the most widely used form of computation on data networks. It has evolved from interactive computing model that was prevalent in the 1960s and 1970s. In interactive computing, a user interacts with a mainframe computer via a terminal that may be dumb or smart. The interaction model follows a master-slave approach. The mainframe computer acts as the master and the terminal as the slave. The slave terminal is under the complete control of the master computer.

With the advent of personal computers and data networks, the master-slave model of interaction has given way to **peer-to-peer interaction model.** Peer-to-peer interaction permits arbitrary communication among computers on the network. No distinction is made among the computers. A PC may contact another PC or a large mainframe as easily. Similarly, a mainframe computer can contact another mainframe or a PC. Distributed computing has become the norm. Distributed computing means any form of computation between two or more computers communicating over network.

Computers called **servers** that provide different types of services are on the networks. The services are accessible to other computers that are treated as **clients** of the service-providing computers. This model of interaction is known as the **client-server architecture.** A computer on the network may act both as a server and a client. When it provides service, it is a server and when it accesses the services of another computer, it is a client. We may thus say that the client-server architecture is a form of distributed computing with peer-to-peer interaction.

The client-server configuration is depicted in Fig 9.3. There are two machines and a network in the configuration: a server machine, a client machine and a data network.

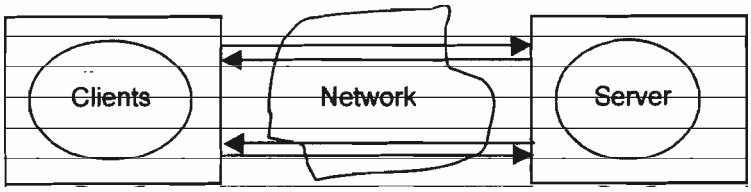


Fig. 9.3: Client -Server configuration

The server and the client interact via the data network. The server provides a set of information and computational services that are availed by remote clients. As shown in Fig. 9.3, usually many clients access one server simultaneously. It must be noted that the server and client machines do not actually interact. It is the server program and the client program that interact although we normally speak of server and client interaction. Support for multiple clients is possible only because of program-to-program interaction. A server creates as many processes of the same program as there are clients logged on to it. Use of multiprogramming and time-sharing features of the server operating system makes this possible. The server machine is one, but the instances of a server application program are many. This is how many users access one web site simultaneously. Client-server interaction may take place at one of the following three levels:

1) Human - Server Program

2) Human - Human

3) Client Program - Server Program

The first case is the most popular one with human client and a machine server. A typical example is that of user accessing information from a server, say searching a database. An example of the second case is student - teacher chat session. In online learning, student is tutored by a teacher. The student is the client and the teacher is the server. Timed periodic file transfer or email transfer between two or more machines are examples of the third case.

In all client-server interactions, it the client that always initiates a session. The server is ready and waiting without doing anything. When a client request comes, the server program responds. This is like a shopkeeper ready to sell with his shop open but the actual transaction takes place only when a customer arrives. The server service must be available on 24 x 7 (24 hours a day, 7 days a week).

Server systems are generally more powerful than client systems. They fall in one of the following categories:

- PC servers
- Workstation servers
- Mainframe servers

PC servers typically use standard 32-bit microprocessors. They have large RAM and hard disk capacity. They are ruggedised for continuous uninterrupted running with backup power systems and cooling systems where required. PC servers must have an operating system that can handle multiple users, as many client PCs may connect to the server at a time. Such operating systems are known as *network operating system (NOS)*. Some of the popular NOS are MS Windows NT, Windows 2003, Novell Netware and Linux. All the servers are designed to support simultaneous access from many clients.

Workstation servers use high power or custom designed microprocessors. They are generally 64-bit or 128-bit microprocessor based systems. Workstation servers run under Unix like operating system that has a rich set of tools for supporting a wide variety of applications. Unix is a more reliable and secure operating system when compared to Windows. Linux is a recent addition to the world of operating systems and is considered a suitable substitute for both Unix and Windows. Linux is available in the open software domain. Some predict that in future, both PCs and workstations may run Linux instead of Windows or Unix. However, experience so far has not shown this to be true.

Mainframe computer based servers are even more reliable and powerful than Unix workstation servers. Mainframe based servers are often called enterprise servers to convey the fact that they are more powerful than PC servers or workstation servers.

Client systems are of two types:

- Desktop personal computers
- Mobile stations

The most popularly used desktop systems are Intel microprocessor based computers running Microsoft's Windows operating system. Such systems are sometimes called

Wintel systems signifying Windows operating systems and Intel microprocessor. The other class of desktop personal computer is Apple Macintosh. Mobile stations may be smart cellular phones (like Blackberry or iPOD), notebook computers and personal digital assistants or tablet PCs etc.

One of the powerful features of client-server architecture is its **scalability.** An application may start on a low-end PC and move in steps to a large PC, workstation and mainframe as the number of users rises. Interestingly, the upgradatton may happen without the user ever being aware of it.

In client-server architecture all applications have two program parts: a server program part and a client program part. The server program part is responsible for providing the specified services and the client part enables access to the services. Hence, anyone developing applications that would run on a network needed to develop both server and client parts of the software. The client software needs to be distributed to all client machines that may be spread all over the world. For example, you cannot access a server site that stores PDF (portable document format) files without an Acrobat Reader that is the client software for accessing PDF databases. In the early days, new server applications used custom-designed client software. Soon, it was obvious that roiling out client software to thousands of users all around the world is rather time consuming and expensive. With the arrival of World Wide Web (WWW), most of the network applications are designed to be **web-enabled** so that browsers now available with most of the PCs can access the applications without having to have special client software. In other words, the client software is embedded in the browsers. Two of the well-known browsers are Internet Explorer from Microsoft and Netscape Navigator from Netscape Communications.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

11) What are the differences between interactive computing and client-server computing models?

12) Can we say that Internet uses peer-to-peer communication? Why?

13) What mechanisms are used to support multiple clients on the same server?

.....

.....

.....

.....

9.8 APPLICATION LEVEL COMMUNICATION PROTOCOLS: FTP, TELNET

9.8.1 File Transfer Protocol (FTP)

FTP is used to transfer files from one computer to another on the Internet. FTP works in an interactive mode. A repertoire of FTP commands is available for interaction. A user invokes FTP client application on his/her computer as the first step. The user then enters the identity of the remote computer from which files are to be transferred using

'open' command of FTP. The FTP client then invokes TCP to establish connection with the remote computer. Once the connection is established, FTP server is activated at the remote computer.

At the next step, the user is authorised to access the remote computer by inputting a valid user name and password. A valid user account is required for this purpose. When the authorisation is successful, the user may examine and select a file on the remote computer by using the list command 'Is'. He/She then uses FTP 'gef command to transfer the file to his/her own computer. FTP client allows a user to transfer a file to the remote computer from the local computer as well. For this purpose, user invokes the 'send' command of FTP. The FTP client application is closed by 'bye' command.

FTP recognises only two types of files: text and binary. Any non-text file is treated as binary file. Examples include audio, computer programs, spread sheets and graphics data. Text files have to be strictly according to one of the standard character encoding schemes like ASCII or EBCDIC. If in doubt about the nature of the fife, it is best to specify binary format. Binary format will transfer a text file as well successfully. However, transfer of text files is more efficient and faster. Where known, it is a good idea to specify 'text' as the file type. However, If an incorrect type is specified, the resulting file may be malformed.

There are server systems on the Internet, which make available files to general public. Examples include servers providing government circulars or legal judgements. Such public files can be accessed without the user having an account on the server. FTP client makes this possible by providing an account called anonymous' with password as 'guest'.

Since FTP application runs on client-server model, the FTP server must run under multiprogramming and time-sharing operating system to enable multiple clients to access the server simultaneously.

9.8.2 Remote Login (Telnet)

Telnet allows an Internet user to log into a remote time-sharing computer and access and execute programs on the remote machine. For this purpose, the user invokes a Telnet client on his/her machine and specifies the identity of the remote machine. Telnet client makes a connection to the remote computer using TCP. Once the connection is established, the remote computer (Telnet server program) takes over the user's display and issues a login command. The user follows the regular login procedure by giving his/her account name and password. From then on the user computer behaves exactly like a terminal on the remote system. When the user logs out, the remote computer breaks the Internet connection and the Telnet client on the local machine exits automatically.

Remote login is a general access feature. The generality makes it a powerful tool on the Internet. It enables the programs on the remote computer accessible without having to make any changes to the programs themselves. The installation of the Telnet server on the time-sharing system is ail that is required. The telnet client and server together make the user computer appear as a standard terminal on the remote system. Hence, no changes are required as far as the application on the remote system is concerned. In view of this generality, different arbitrary brand of computers can be connected to the remote system. In effect, any computer on the Internet can become a Telnet client to any Telnet server on the Internet. Unlike FTP or e-mail, Telnet allows the user to interact dynamically with the remote system. Due to this, Telnet service is very popular.

Telnet sessions may run into occasional problems. The application program on the

remote computer may malfunction or freeze. The local computer then hangs. We need a mechanism to come out of this situation. Remember that during a Telnet session, two programs are running: one the program on the remote computer and the other the Telnet client on the local machine. Telnet makes a provision to switch between these two programs. Once a Telnet session is established, every keystroke by the user is passed on to the remote computer. A special combination keystroke, like *Ctrl* +], is reserved to revert to the local program. The Telnet client examines every keystroke of the user before passing on the same to the remote machine. If the special combination key is pressed, it stops communication with the remote machine and allows communication with the local client program. The user can then terminate connection with the remote computer, close the Telnet client and resume local operations.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

14) Let the IGNOU LIS course modules be available on a fictitious FTP server called "cm.lis@Jgnou.ac.in". Write down the FTP commands and responses to download this unit to your computer.

.....

.....

.....

.....

9.9 SWITCHING LEVEL CONVERGENCE PROTOCOL: ATM

There are three major forms of switching techniques used in telecommunication and networks:

1) Circuit Switching

2) Packet Switching

3) Cell Switching

Circuit switching is the oldest technique used in telephone networks and has been in existence for over 120 years. Packet switching is about 50 years old used in data networks like the Internet. Cell switching is the most recent one evolved during mid 1990s used in new telecommunication infrastructure.

Before we proceed to discuss these techniques, definitions of two terms are in order: *channel* and *circuit.* A *channel* is defined as an information pipe with some specified characteristics like bandwidth, capacity, level of attenuation and noise immunity. A channel is a one-way link. A *circuit* is a two-way link and comprises two channels that enable two-way information flow between two entities. The two channels of a circuit need not have the same characteristics. If they do, then the circuit is said to be *symmetric.* Otherwise, the circuit is said to be *asymmetric.* Some authors tend to use the term *channel* to mean a physical medium. This is incorrect. A physical medium like optical fibre may carry several thousand information channels in a multiplexed mode.

Circuit switching is connection oriented. A circuit comprising two channels for two-way communication is established between the two communicating entities before the information transfer begins. The circuit is established using dedicated physical resources. The physical resource may be copper wires, optical fibres, radio or satellite links or a combination of these media. The circuit remains dedicated for the communicating pair until it is released, it is unavailable to any other communication need while dedicated to the communicating pair.

The main advantage of circuit switching is that once the circuit is established there is a direct connection between the communicating entities and the network is transparent to them. The information flows smoothly over the circuit from one end to another. The information is delivered in proper sequence and there is no possibility of out of sequence delivery. There is no delay caused by network elements like routers. The main disadvantage of circuit switching is that the scarce network resources remain dedicated for the entire duration of the information transfer phase and are heavily under utilised. Be it a telephonic conversation or computer interaction, mere are pauses during the session and the dedicated resources remain idle during the pauses.

In packet switching, messages are split as packets at the source and delivered to the network. *The* network transports the packets to the destination. Packet switched networks adopt two different approaches for transporting packets from the source to the destination:

- Datagram approach
- Virtual circuit approach

You are already familiar with datagram transport and the associated problems of out-of-sequence arrival at the destination and datagram losses. Virtual circuit approach was conceived to take advantage of in-sequence delivery of circuit switching while better utilizing the physical resources. The virtual circuit approach draws upon the idea of circuit estabtishment as in circuit switching. Instead of establishing a dedicated circuit, it establishes a fixed route from the source to destination. Since the packets follow the fixed route, they are delivered in order to the destination. Need for re-sequencing does not arise.

Virtual circuit makes routing more efficient and reduce the header overhead. As soon as a virtual circuit (fixed route) is established between a communicating pair, the same is given a unique identifier called *virtual circuit number* (VCN). The VCN defines the source and destination addresses, the message and the route. Hence, VCN together with the packet number uniquely identifies the packet. VCN plus packet number is much smaller in size when compared to the elaborate identification described earlier. Thus the header size and the transmission overhead are reduced significantly. Routing is also made simpler as the VCN is used to index a table to find out the outgoing link. There is no analysis of destination address and route determination.

Although virtual circuit concept is a major step forward, it still suffers from possible loss of packets and non-smooth flow of information. Since routers are involved, queues may build up and packets may be discarded. Dynamic variation in queue lengths may result in packets being delivered with different delay times thus interrupting smooth flow and affecting real time services.

Cell switching is the most recent switching technique evolved during 1990s. The main objective of cell switching has been to minimise the problems experienced in virtual circuit switching. This is done in two ways:

- To redefine the packet as a cell that is very small in size
- To leap forward in the speeds of virtual circuit switching.

Cell switching is designed to cause minimal network delay ensuring at the same time efficient utilisation of network resources. You are aware of MTU and the associated problem of possible segmentation and reassembly. This problem is completely avoided in cell switching. The entire infrastructure uses a standard cell size of 53 bytes. The cell has 48 bytes of payload and 5 bytes of header. Now let us understand the merits of cell switching. Ceil switching is built on a very reliable and ultra fast network infrastructure. The reliable technology almost rules out cell tosses. Even if a cell or two is lost very rarely, the effect is unnoticeable in real time services like voice and video. The small size of the cell makes the loss imperceptible to hearing or viewing. In data services of course, recovery is required.

Cell switching uses virtual circuit principle. The cells are guaranteed to be delivered in sequence. Virtual circuit reduces switching overheads significantly and makes switching extremely fast. For this reason, cell switching is sometimes called **fast packet switching.**

The networks that use cell switching are called **Asynchronous Transfer Mode (ATM)** networks. The reason for this is that the cells of a particular message are not switched in a fixed time frame say every millisecond. They are switched as they arrive. The arrival is a mixed bag of cells from different messages or services. They are switched in the order in which they arrive. Consecutive cells do not necessarily belong to the same message or service. In other words, the cells of a message or service are not continuous or synchronous in time. Hence, the term asynchronous transfer is used. Asynchronous transfer ensures effective utilisation of the network resources. The resources are not dedicated to one service.

In contrast, in the conventional circuit switched networks the information transfer is continuous and synchronous. In synchronous transfers, information pieces arrive in fixed time frame, say one byte every microsecond. In ATM, the cell arrival is not time synchronous. The time gap between the arrivals of two consecutive cells of the same message is not fixed but a variable one. However, the variability is very small because of the high-speed switching of ATM. For all practical purposes, the services perceive synchronous arrival. ATM is a technique that marks the convergence of both circuit and packet switching. Hence, ATM protocols are often referred to as convergence protocols.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

15) Why is cell switching superior to circuit and packet switching?

.....

.....

.....

.....

9.10 MULTI PROTOCOL LABEL SWITCHING: MPLS

As you know, virtual circuit makes routing more efficient and reduce the header overhead by using VCN. The VCN uniquely defines the source and the destination, the message and the route. Use of VCN reduces the header size and the transmission overhead.

Routing is made simpler as the VCN is used to index a table to find out the outgoing link. Multi Protocol Label Switching (MPLS) is an attempt to bring VCN concept to IP packets. Here, an IP packet is assigned a label that uniquely identifies the destination. In fact, the IP packet is encapsulated with the label header. The label is then used to index into a table to find out the outgoing link to be used for forwarding the packet. There is no examination of the destination address every time. This greatly simplifies routing overhead and makes the IP packets move faster through the network. This is particularly useful where large volume data transfers are involved as in the case FTP service.

MPLS is a router-based solution to improve the router efficiency. This is not a protocol that runs on any user machine. User machines run only the conventional communication protocols like TCP and FTP. We need MPLS-capable routers to implement MPLS. Only MPLS-capable routers can assign labels and handle MPLS packets. There are two ways in which the labels are assigned to IP packets: data-driven and control-driven assignments.

In data-driven assignment, when a packet enters a MPLS-capable router, it contacts the next MPLS-capable router and asks for a label for the destination address. The next MPLS-capable router in turn connects to the next one and the process is continued until the destination router is reached. Thus a fixed route is formed for all packets to the same destination. The first router now encapsulates the IP packet with the label supplied by the next router and forwards the packet. From then on, the label is used for routing. The name mufti protocol is used to signify the fact that the MPLS-capable routers can forward IP packets from a variety o f protocols like TCP and FTP.

In control-driven assignment, a destination router creates labels for all its host computers and passes them to its neighbours. The neighbours in turn create labels and contact other neighbours. The process is continued until all the routers acquire the path. Thereafter, the label is used for routing.

9.11 TELEPHONE AND MOBILE NUMBERING

Every entity in any network needs to be uniquely identified. Otherwise, the entity cannot be accessed. In telephone and mobile networks the entity is a phone instrument and it is number that uniquely identifies the entity. In Internet, the entity is a computer and it is IP address that uniquely identifies the entity. Although it is called an address, IP address is also a number. At the user level, the addresses are specified by string of characters on the Internet, (e.g. ignou.com). In a sense, similar character addressing is also available in telephone networks by way of directories where one looks up the number corresponding to a name. The addressing or numbering scheme follows a structure. We discuss the telephone and mobile addressing schemes in this section and the IP addresses in Section 9.13.

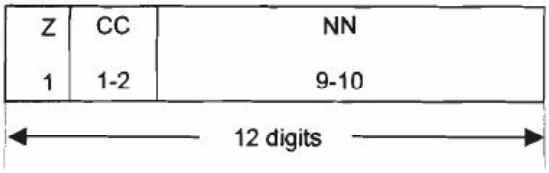
9.11.1 Landline Telephone Numbering

Telephone numbering worldwide follows an international standard set by International Telecommunications Union (ITU). The details are specified in the standards E.160 - E.163 of ITU. In ITU parlance, the numbering scheme is called **numbering plan.** As per the plan, the world is divide into 9 zones with each zone being identified by a zone code as indicated in Table 9.1. The zone names in Table 9.1 are representative. For exact delineation, one is advised to refer to the standards. Europe is given two codes, as there are many countries there.

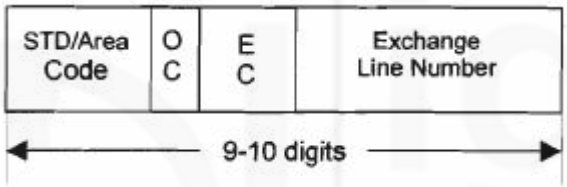
Table 9.1: World zones for telephone numbering

Zone	Code	Zone	Code
North America	1	Australia	6
Africa	2	Russia	7
Europe 1	3	Far East	8
Europe 2	4	South Asia	9
South America	5	-	-

The structure of the number is illustrated in Fig. 9.4. The maximum size of the number is 12 digits. The first digit is the zone number. The remaining 11 digits are divided between



(a) International telephone number



(b) National telephone number

EC = Exchange code OC = Operator code

Fig. 9.4: Telephone Number Structure

country code (CC) and the national number (NN). The country code is one or two digits. With the zone code added, effectively the country code is 3-digit long. In common usage, zone code is not mentioned separately. It is included as part of country code. For example, the country code for India is mentioned as '91'. But to be precise, one should say that the zone code for India is '9' and the country code is '1'. Together they make '91'. The country code is kept to be of variable length. The general principle adopted is that the countries with large population are assigned short codes of two digits (1 zone + 1 country). The countries with smaller population are assigned longer codes of three digits (1 zone + 2 country). For example, in zone 9, Maldives has a 3-digit country code '960'. With just over 200 countries in the world this coding would work for millenniums to come, in fact, forever. Countries with large population like India get 10 digits for national number and smaller countries tike Maldives nine digits. Ten digits provide for a maximum of 10 billion connections. For India with a population of 1.2 billion, this is adequate for times to come. You may appreciate that the telephone numbering plan has been designed with farsightedness.

National telephone number has four parts in it as shown in Fig. 9.4(b). Subscriber Trunk dialling (STD) code may be further subdivided as one digit region code within the country and one or more digits of sub area codes within the region. In India, eight regions have been identified for telephone numbering. These are numbered 1 - 8 as shown in Table 9.2. The region descriptions are indicative and actual area covered is as per Department of Telecommunications guidelines.

Table 9.2: Indian regions for telephone numbering

Region	C	Region	C
Delhi, NCR, Haryana, Punjab	**1**	U.P. & Bihar	**5**
Mumbai, Maharashtra,	**2**	Orissa	**6**
Kolkata & North East	**3**	Central	**7**
Tamil Nadu & Kerala	**4**	Karnataka &	**8**

The sub area codes are kept to be of variable length. The general principle adopted is that the sub areas with large population are assigned short codes of two digits (1 region + 1 sub area). The sub areas with smaller population are assigned longer codes of three or more digits. For example, Delhi has a code '11' and Noida '120'. Similarly, Mumbai has a code '22' whereas Bopal, a town near Ahemadabad has the code '2707'.

Operator code (OC) is used when there is more than one service provider in an area. Until the early 90s, India had only the state operator, the Department of Telecommunications, providing telecom services in the country. But now telecom is opened up to private operators. We generally have more than one operator in major cities and towns. The operator code is used to identify the different service providers.

Every service provider has more than one telephone exchange in a city. Exchange code (EC) identifies the telephone exchange to which the subscriber is connected. Usually two or three digits are provided for EC. If the number of exchanges exceeds 99, we need three digits. This is the case in cities like Delhi and Mumbai. In smaller cities and towns, only two digits may be used.

The last part of the national telephone number is the line number assigned to the subscriber in the telephone exchange to which he/she is connected. Exchanges are usually designed to support 1000 or 10,000 subscribers. Accordingly, the line number may have 3 or 4 digits.

9.11.2 Mobile Phone Numbering

Technically speaking, there is no reason as to why mobile phone numbering could not follow the same numbering plan as the landline phone numbering. After all, the mobile is another telephone instrument except that it works on radio technology instead of landline (electrical or optical cable) technology. In fact, initially mobile phones in the United States used the same numbering scheme as the landlines. But, commercial considerations have led to a different scheme of numbering for mobile phones. In the beginning, the cost of mobile technology was relatively higher when compared to the landline technology. Mobile service providers needed to charge the customers higher. You may be aware that in the initial days of mobile communications, the incoming calls to mobile phones used to attract incoming call charges and the outgoing calls used to cost about six times the landline charges. The charge differential being so high, users needed to know whether they are calling a mobile phone or a landline phone. Further, roaming feature of mobile phones and the associated charging policies made the distinct identification of mobiles phones necessary. Hence, the need arose to distinguish a mobile phone from a landline phone. Thus was bom a different numbering scheme for mobile phones.

In general the series of numbers starting with '9' was reserved all over the world for future use while the landline numbering plan was evolved. When mobile technology

came up and a need arose for distinguishing mobile phone numbering, it was decided to use the '9' series for mobile numbering. As you have learnt, India has 10-digit national number with its country code being '91'. The 10-digit national number starting with '9' was allotted to mobile phones. The '9' series provides for one billion numbers and it was considered adequate to meet the needs of mobile users in India, particularly because the cost being high not much penetration was expected. But, the history proved otherwise.

India has over 500 million mobile users in the country as of June 2010. Close to 750 million mobile numbers have already been allotted. If the rate of growth in mobile users continues at the present rate, we would run out of mobile number space soon. Hence, Telecommunications Regulatory Authority of India (TRAI) has opened up unused '8' series numbers for mobile users. An interesting fact is that India has only about 450 landline users and the growth rate here is not very significant. Considering this, it is likely over a period of time that number space for landline users may be reduced and the space thus freed may be allotted to mobile users. However, it is important to note that the potential for high-speed applications is much higher in the case of landline communications. This is because the radio bandwidth is limited whereas the landline bandwidth is unlimited.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

16) What is the maximum number of telephone numbers (both landline and mobile together) that can be assigned using the 10-digit national number?

17) Identify the different components of the international telephone number 911129534336.

.....

.....

.....

.....

9.12 NUMBER PORTABILITY

Number portability is a feature that allows a telephone user to retain his telephone number permanently. It is like the PAN (Permanent Account Number) allotted by the Income Tax Department or the Social Security Number assigned to individuals in the United States. Such numbers remain permanent for the lifetime of the individual irrespective of where the individual lives or works with. The number portability feature implements a similar concept. Imagine that you are given a telephone number once in your lifetime and that number remains valid for your complete lifespan. Would that not be very interesting? Number portability attempts to do just that. However, we have a long way to go in this regard.

Number portability needs to be considered in three situations from the users' point of view:

- Change of location
- Change of operator or service provider

- Change of service from landline to mobile or vice versa

Accordingly, three kinds of number portability are discussed from the telecom network point of view:

- Location portability
- Operator portability
- Service portability

Location portability implies that if a user moves his residence or place of work from one locality to another in the same city or moves from one city to another, his/her telephone number does not change. Both intra-city and inter-city movements have to be taken care of.

Operator portability implies that if a user moves from one operator to another, say from Airtel to Vodafone, his/her telephone number does not change. You may recall that the national number has a field (OC) that identifies the service provider. When number portability is introduced, OC may lose significance and may just be used by the old operator to redirect the call to the new operator.

Service portability implies that a user may move from one form of service to another and yet retain the original number. At present, three forms of service are available: landline telephone, mobile phone and voice-over-IP. Service portability must ensure mobility of the user among all these three services.

So far our discussions were limited to one portability requirement at a time. Portability requirements may occur in combinations as well. The following combinations may arise:

- Location + operator portability. A user may shift from one city to another and may want to change the operator also at the same time.
- Location + service portability. A user may shift from one city to another and may want to change from one form of service to another at the same time.
- Operator + service portability. A user may want to change the operator and the service as well.
- Location + Operator + Service portability. All aspects being changed at the same time.

Major changes may be required in the telecommunication equipments for implementing number portability. Hence, although number portability is being talked about for many years now, its implementation is not wide spread.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

18) A mobile user moves from the city of Hyderabad to Mangudi, a village in Tamil Nadu, which does not have mobile network coverage but has landline connectivity. What portability aspects would come into picture in this case?

.....

.....

.....

.....

9.13 IP ADDRESSING: IPV4, IPV6

As explained earlier, every entity in a network needs to be uniquely identified. Otherwise, the entity cannot be accessed. In telephone and mobile networks the entity is a phone instrument and it is number that uniquely identifies the entity. In Internet, the entity is a computer and it is IP address that uniquely identifies the entity. Although it is called an address, IP address is also a number. An IP datagram cannot be delivered to the destination unless the destination is uniquely and unambiguously identified and IP address does exactly that. Computers connected to the Internet are called **hosts** and hence the term host address is used extensively.

There are two versions of IP addresses under active use. The most widely used one is defined in Version 4 of Internet Protocol abbreviated as **IPv4.** IPv4 has been in successful use for about 30 years and it uses a 32-bit address. With 32 bits we can uniquely address 2^{32} hosts, i.e. approximately 4 billion (4×10^9) hosts. Remember that the world has a population of over 6 billion. If everyone were to have a computer in this world, we would not have enough IP addresses to assign to each one of these. Further, the IP address is a structured one having different address formats. Structuring has the effect of reducing the effective address space to a much smaller number than 4 billion. With the rapid growth of Internet over the last 30 years we are now on the brink of running out of addresses for new machines. It is in this context, a new version of IP, Version 6 abbreviated as **IPv6** has been recently standardised and is being introduced on internet. Addresses in IPv6 are 128 bits long. With 128 bits we can have approximately 256×10^{36} unique addresses. Such an address space is unlikely to run out in the foreseeable future and must serve the mankind at least for a few millenniums. The two addresses, IPv4 and IPv6 are interoperable and would coexist for many decades to come. IP addresses are assigned and managed by a non-profit corporation called *Internet Corporation for Assigned Names and Numbers* (ICANN) to ensure uniqueness in naming and numbering hosts. In this Unit, we discuss IPv4 in detail and IPv6 briefly. Readers interested in more details of IPv6 may refer to Further Reading material listed at the end of this unit.

IPv4 address is structured reflecting the objectives of Internet. You may recall that Internet is a network of networks. Hence, at the level of ICANN, the main interest concerns networks rather than hosts. ICANN, through its agents around the world assigns addresses to networks that contain many hosts. As you are aware, each network is connected to the Internet via a **router** or a **layer-3 switch.** The router has an Internet network address and is capable of forwarding datagrams towards destination networks. On its own network, it distributes the datagrams to the respective hosts. The host addresses are assigned by the respective network owners and maintained on the router.

For the purpose of assigning network addresses by ICANN, the networks are classified under three categories: large, medium and small signifying the number of hosts on the network. Corresponding to three network categories, there are three address classes: **Class A, Class B** and **Class C** respectively. The general structure of IPv4 address has three fields as shown in Fig. 9.5. Class A provides for large, Class B for medium and Class C for small networks. The 'Class' field is of variable length of 1 - 3 bits. A one-bit class field with a value '0' specifies Class A addresses. The 2-bft field with value '10' and the 3-bit field with value '110' specify Class B and C addresses respectively. Often, the class field and the network number field together are called **network address** and the host field as **host address.** We also use the same convention in this unit.

Class	Network No.	Host

Fig. 9.5: IPv4 Address structure

In Class A address, 7-bit pattern following the first bit specifies the network number. Seven bits provide for $2^7 = 128$ bit patterns. Two of the 7-bit patterns are reserved for special purposes. They are all zeros '0000000' and all ones '1111111' patterns. The all zeros pattern implies the local network in which the host itself is located. The all ones pattern is used for loop back testing of protocols and applications. That leaves us with 126 Class A networks world over. The remaining 24 bits are used for host addresses supporting up to 16 million hosts on each network. With 16 million hosts on a single network, Class A represents the largest possible network on the Internet using IPv4 addresses.

In Class B address, 14-bit pattern following the first two bits specifies the network number. Leaving out the special patterns mentioned above, this means that up to $(2^{14} - 2) = 16,382$ medium sized networks may exist on the Internet. Much as in the case of network addresses, special patterns are reserved for similar purposes in host addresses as well. Taking this into consideration, each medium sized network may have up to $(2^{16} - 2) = 64$ k hosts.

In Class C address, 21-bit pattern following the first three bits specifies the network number. Leaving out the special patterns mentioned above, this means that up to $(2^{21} - 2)$ H" 2 million small sized networks may exist on the Internet and each such network may have up to $(2^8 - 2) = 254$ hosts. Class C networks are ideally suited for small organisations. They are used extensively. Some small organisations may have more than 254 hosts, say ranging from 300 to 1000, but may not have as many as 16 k hosts to warrant a Class B address. This, in fact is the case with organisations like universities, research laboratories and large corporate houses. In such cases, the organisation is allotted as many Class C addresses as needed. For example, three Class C addresses can support up to 762 (3×254) hosts. This approach of using multiple Class C addresses helps in conserving Class B addresses. If Class B addresses were to be assigned to such organisations, the address space would remain heavily under utilised.

In addition to the above three primary classes of addresses, there are two special categories of addresses, Class D & E. Class D address is used for multicasting and Class E is reserved for future use. Multicasting is the distribution of datagrams to many hosts that have the same address group. Note that broadcasting is the distribution of datagrams to all the hosts. Hence, multicasting can be called as 'limited broadcasting'.

For the sake of convenience and clarity, the 32-bit IPv4 addresses are presented in a dotted decimal notation. The addresses are viewed as four bytes (32 bits) and the decimal value of each byte is written with periods separating them. As you know, an 8-bit pattern can have values ranging from 0 —255. An example address in decimal notation is 183.41.235.7. The equivalent binary address is 10110111 00101001 11101011 00000111. With experience, it is felt that a hexadecimal representation would have served the purpose of clarity much better. As you know, hexadecimal representation uses a base of 16 using symbols 0 through 9 and A, B, C, D, E and F. The hexadecimal representation of this address is B7.29.EB.07.

Consider the case of an organisation that has 9,000 hosts. We would need to allocate a Class B address for this organisation to avoid allocating too many Class C addresses. Recall that one Class B address can support up to 16,382 computers. In this case, 7,382 addresses are wasted because the same network address cannot be used for

another organisation. This is yet another example of how address space remains unutilised. The net result is the loss of address space. It was realised, though rather late, that a large segment of address space remains unused in IP class based address structure. While address space remained unused with the existing users, addresses for new users were becoming unavailable. A class definition with incremental number of hosts would have been far better. By the time this realisation came, the damage had been done. In order to contain further damage, Internet management introduced a classless addressing mechanism known as **Classless Inter Domain Routing** (CIDR) in late 1990s. The basic idea behind CIDR is to allocate the remaining IP addresses in blocks of contiguous addresses without any class consideration. With CIDR, an organisation can seek provision for hosts in powers of 2 such as 256, 512,1024, 2048 and so on. While network address length is fixed in Class A, B, C networks as 8, 16, 24 bits respectively, in CIDR the network address length may lie in the range of 8 - 31 bits theoretically. In practice, however, the range is 12 - 24. Note that the network address length of 8, 16, and 24 in CIDR automatically correspond to Class A, B and C networks respectively.

While CIDR makes more efficient utilisation of IP address space, it needed major changes in the routers all over the Internet, as the algorithm for routing has to undergo a sea change to handle both classed and classless addresses. Routing was relatively simpler and the router configuration was small with classed addressing. With CIDR the situation has changed. Routers have to maintain a much larger database including information about the length of the network address field. This is kept in a 32-bit field called **subnet mask** by setting as many higher order bits of the subnet mask to T as the length of the network address. For example, if the network address length is 20 bits, the subnet mask in binary notation is 11111111 11111111 11110000 00000000 and in decimal notation is 255.255.240.0. In decimal notation 255 means all the 8 bits of the byte, are set to '1' and 240 implies that four higher order bits of the byte are set to '1'. Therefore, twenty higher order bits of the subnet mask are set to '1' in this case.

IPv4 addressing is a classical example of how ad hoc and non-visionary decisions at the global level can turn out to be messy. It is worth noting that such a mess has never occurred in other fields like telephone and ISDN numbering. One of the major drawbacks of Internet is that many such shortsighted decisions exist and more and more ad hoc solutions are being found. This is clearly due to the lack of rigorous standardisation process such as the ones followed in ISO and ITU.

The introduction of CIDR and the concept of subnet mask led to a slight modification to the decimal notation for the IP address. Since the network address is now of variable length, its length is indicated by a number at the end of decimal notation after placing a 7. Example of new notation is 183.241.060.000/23. Here the network address is of length 23 bits. The subnet mask is 255.255.254.0

Let us now briefly discuss IPv6 addresses. As mentioned earlier, IPv6 addresses are 128 bits long. This is a very large address space, i.e. $2^{128} = 10^{38}$, i.e. approximately 10^{28} times the world population. This number is large enough to probably address almost every little thing on the earth. Therefore, it is impossible that this number space will ever get exhausted, certainly not for many millenniums. It is expected that in future items like refrigerators, air conditioners, cars, buses, ships, airplanes, and even bicycles will all be assigned IPv6 addresses so that they can be controlled and guided from the Internet.

IPv6 addresses are structured along the IPv4 addresses. The address space being very large, over 20 classes of addresses have been proposed. Five significant changes have been introduced in IPv6:

1) Large address space provided by 128-bit addresses

2) Flexible multiple header format. There is one base header that is mandatory and is of fixed size of 40 bytes. More extension headers can be introduced optionally.

3) Improved control options

4) Permits pre-allocation of resources

5) Provision for protocol extension.

There are only five fields in the fixed header portion other than the source and the destination addresses. These are *version, flow label, payload length, next header* and *hop limit.* You may recall that Ipv4 header has 11 fields in its header excluding the source and destination address.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

19) What are the lengths of network addresses in Class A, B, and C IP addresses?

20) How many hosts can be supported in one Class C address? Explain.

21) Write the following binary IP address in decimal and hexadecimal notations: 00011100 10101000 1100110011 00001100. What class of IP address is this? What is the network number (decimal) in this address?

22) Write the subnet mask in binary for /22 Classless address suffix?

23) How many hosts can be supported in classless address with suffix /27?

.....

.....

.....

.....

9.14 WEB COMMUNICATION PROTOCOLS: HTTP, WAP, LTP

As you are aware, World Wide Web (WWW) or simply Web is very popular on the Internet. These days, a large number of business houses, government agencies and many individuals have their own web sites. The number of web sites is growing day by day. Many business houses are currently upgrading their web sites to facilitate electronic commerce. In this context, it is necessary for you to learn about the communication protocol used for web access. Before we discuss the protocol let us briefly review the basics of web.

The concept of Web started in 1989 in France. In 1994, a consortium called World Wide Web Consortium (W3C) was established. W3C now has many countries as its members and is responsible for development and standards for Web and its access. From the users' point of view, web is a collection of documents scattered all over the world that are accessible over the Internet. The documents are often referred to as web pages. These documents are **hypertexts** as they contain embedded links to other

documents. Embedded links are in the form of Uniform Resource Locator (URL) that contains three parts: a resource name, the identification of the server in which the resource is located and the protocol that can be used to access the resource. In effect, URL is unique identifier for a specific resource on the Internet anywhere in the world. An embedded URL is called **hyperlink.**

Web pages are of two types: static and dynamic. Static web pages are designed using a language called *Hypertext Markup Language* (HTML) that allows a developer to place text, graphics, sound, video and hyperlinks in a web page Being a mark up language, HTML defines how documents are to be formatted. In the process, it mixes the contents and format information. This poses serious problems while editing the pages. To overcome this deficiency, two new languages called *extensible Mark up Language* (XML) and *extensible Style Language* (XSL) have been developed. XML sets standards for structuring the contents and XSL for formatting the pages. Thus, the content and formatting are separated. These languages are being used increasingly these days.

As you are aware, web access is based on the client-server architecture that was discussed in Section 9.7. The web browser that acts as the client sends a web page request using URL and the server responds by returning the requested document. It is often necessary for the server to keep track of the user preferences for presenting information. The server does this by storing what are called **cookies** on the clients system. Cookies are short strings of data that a server sends along with a web page and uses the same later for meeting user preferences. The user, however, has the option of blocking cookies being stored on his/her system.

The protocol used for communication between the web browser client and the server is called *Hypertext Transfer Protocol* (HTTP). For secure applications, *Secure Hypertext Transfer Protocol* (HTTPS) is used. HTTPS is discussed in Unit 12 on Network Security. We discuss HTTP below.

HTTP is used universally to access web services all over the Internet. It specifies how a client may send requests to servers and how the servers may respond. The requests are sent in the form of ASCII (American Standard Code for Information Interchange) strings and the responses are received in the form of Multipurpose Internet Mail Extension (MIME) format. HTTP establishes a TCP connection on Port 80 of the server and uses the same for sending requests and receiving responses. More than one request may be sent without waiting for the responses. This is called pipelining of requests.

The first word of the ASCII string is one of the reserved words that specify the operation requested. For example, the reserved word GET signifies a read request for a web page and PUT for storing a page. PUT operation calls for authentication of the user. The authentication information usually follows the PUT request. The information that follows the operational request is called **request header** and need to be specified in a particular format.

In HTTP parlance, these operational requests are called **methods.** Other methods include POST, DELETE, and TRACE etc. POST is used append information to an existing page. It is used in the case of notice and news boards. POST method requires authentication so that only authorised users can post notice or news. DELETE is a request for removing the web page and obviously requires authentication. TRACE is a request for echoing the message that is being sent. This is used for diagnostic purposes.

The response from the server begins with a 3-digit status word that informs the client whether the request was successfully processed or not. It also indicates the reason in

the case of unsuccessful processing. Typical failure messages include 'no content found', 'page not found', 'page removed' and 'forbidden page' etc.

With the advent of digital wireless access to Internet, considerable interest was generated in making small portable devices like mobile phones access web using wireless finks. Two access protocols **Wireless Application Protocol (WAP)** and **Lightweight Transport Protocol (LTP)** were developed for this purpose. These protocols were optimally designed to work with low bandwidth wireless links and wireless devices with a slow CPU, small amount of memory and a small screen. Obviously, such restrictions do not apply to desktop or laptop PCs. The device and link capability dictated the design of wireless protocols. In designing HTTP, these restrictions were not there. Over the time, the handsets have been made very powerful and wireless communication links have also become faster. The latest example in this category is iPhone4 from Apple Corporation. Accordingly, the later versions of WAP and LTP are also more sophisticated.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

24) How do the design considerations differ for wireless web access protocols when compared with HTTP?

.....

.....

.....

.....

9.15 SUMMARY

This unit has dealt with two distinct but closely related aspects: Internet communication protocols and network addressing. Protocols are generally software programs that implement the rules and procedures for communication. Some protocol functions are implemented in hardware too. There are protocols for computing purposes as well. Computing protocols are relatively a recent development. They define rules for information exchange among processes within a computer. Communication protocols define rules for exchange of information among computers. They deal with all aspects of communication functions that are required for information exchange among computers in a network or across networks.

An overview discussion of the communication protocols in Section 9.4 brings out their general functionalities like breaking messages into packets, packet sequencing and reassembly, message encapsulation and de-capsulation, error detection and correction and loss recovery. A list of commonly used communication protocols is given in Section 9.5. Then, the basic or fundamental protocols without which Internet cannot function are discussed in detail. They include IP, TCP and UDP. Internet Protocol (IP) is responsible for transporting packets from source to destination. Transmission Control Protocol (TCP) provides assured quality services that ensure errorless and lossless data transmission. User Datagram Protocol (UDP) is a low overhead, fast and simple protocol that delivers user messages on best-of-efforts basis.

The unit then covers Client-Server architecture that is fundamental to running remote applications on the Internet. It is the most widely used form of computation model on data networks. It has evolved from interactive computing model of yesteryears. Thereafter, two application level protocols that use client-server model for communication are discussed. File Transfer Protocol (FTP) is used for transferring files from one computer to another on the Internet. FTP works in an interactive mode using a repertoire of commands. Remote login protocol (Telnet) allows an Internet user to log into a remote time-sharing computer and access and execute programs on the remote machine.

The unit then focuses on two switching level communication protocols ATM and MPLS. Asynchronous Transfer Mode (ATM) is the new communication protocol used in basic telecommunication infrastructure. It uses the principle of cell switching that combines the advantages of both circuit and packet switching techniques. ATM is extremely reliable and fast. Routers use Multi Protocol Label Switching (MPLS) to speed up the process of routing packets across networks.

The unit then turns its attention to addressing entities uniquely on the networks. First, the numbering plans for telephone and mobile networks are discussed. Both international numbering and national numbering in India are elaborated. Another important issue, viz. number portability is then discussed. Number portability needs to be considered at three levels: Location portability, Operator portability and Service portability.

Addressing in data networks is then discussed. Version 4 of IP address (IPv4) is discussed in detail bringing out its limitations and merits. Developments in IPv6 are then briefly presented.

Finally, the unit discusses the web communication protocols. The universally used HyperText Transfer Protocol (HTTP) is described in detail. Brief features of wireless web protocols Wireless Application Protocol (WAP) and Lightweight Transfer Protocol (LTP) are then presented.

9.16 ANSWERS TO SELF-CHECK EXERCISES

1) Computing protocols define rules for communication among processes within a computer. Communication protocols define rules for communication among computers connected to the same or different networks.

   Computing protocols are concerned with storage, retrieval and processing functions of information management. Communication protocols are concerned with acquisition, transmission and distribution functions of information management.

2) Examples of signalling from our daily life:

   - A bus conductor's whistle to stop and start the bus
   - Flagging of a sport event like running race
   - Indicator lights in cars
   - Caller tunes in mobile phones.

3) Small Messaging Service is a connectionless service. One prepares a message and sends it across expecting it to be delivered. The service is provided on the best-of-efforts basis.

4) ARQ is the technique used here. You observe (detect) an error, erase (discard) it and input the right character (retransmit).

5) FEC is the technique here. The package detects the error and corrects it automatically. There is no retransmission by the user. This is forward correction at the receiving end.

6) Thirteen including source and destination addresses.

7) Internet is a network of networks. Each component network has its own maximum transfer unit (MTU) defined. If a datagram is delivered to a network with a size greater than the MTU of the network, then the datagram needs to be fragmented for transportation within that network and reassembled at the exit point of that network.

8) There are certain applications that cannot run with fragmentation. For such applications, the 1-bit 'D' field is set to '1'. This would mean 'Do not fragment'. If a router finds this bit set to '1', it must route the datagram via such networks that have MTU equal to or greater than the datagram size. Then no fragmentation will occur.

9) The port fields in UDP header identify the source and destination processes or applications. Using the information in these fields, UDP is able to deliver the datagram to the correct destination application. The source port identifies the source application that is sending the datagram, tf the destination so desires, it can send a reply datagram to the source application by using the source port address.

10) In TCP, detection of lost datagrams is done using acknowledgement and timer mechanisms. Receipt of every datagram is acknowledged by the destination. At the time of sending a datagram the source initiates a timer with a value within which the acknowledgement must be received. If the timer expires and no acknowledgement has been received, the source concludes that the datagram is lost and dispatches another copy.

11) In interactive computing, a user interacts with a mainframe computer via a terminal that may be dumb or smart. The interaction model follows a master-slave approach. The mainframe computer acts as the master and the terminal as the slave. The slave terminal is under the complete control of the master computer.

12) In client-server architecture, a computer on the network may act both as a server and a client. When it provides service, it is a server and when it accesses the services of another computer, it is a client. During interaction, the client is not under the control of the server. Client can do its own computing. Both the client and the server act independently and hence share the status of being peers. We may thus say that the client-server architecture is a form of distributed computing with peer-to-peer interaction.

13) Yes. Internet uses peer-to-peer communication. Any computer can contact any other computer. No computer is under the control of another. All computers are considered autonomous and can function independently. Hence, we say Internet uses peer-to-peer communication.

14) Machines do not communicate in client-server interaction. The interaction is between the server program and client program running on the server machine and the client machine respectively. As many instances of server program are activated as there are clients accessing the service. One instance is dedicated to one client. This is made possible by using the multi-programming and time-sharing features of the server operating system.

ftp>open

(to) cm.lis@ignou.ac.in

Connected to cm.lis@ignou.ac.in

LIS Course Module Services at IGNOU

cm.lis@ignou.ac.in FTP server ready

Name: yourusername

Password:……..

Login OK

ftp> Is

PORT command successful.

Opening ASCII mode data connection for file list

Block 1: Basics of ICT

Block 2: Middleware Technologies

Block 3: Network Fundamentals

Block 4: Internet Tools and Services

Transfer complete

Xxx bytes received in xx seconds

ftp> Is Block 3: Network Fundamentals

PORT command successful.

Opening ASCII mode data connection for file list

Unit 8: Topology

Unit 9: Communication Protocols and Network Addressing

Unit 10: Protocol Architecture

Unit 11: Network Applications and Management

Unit 12: Network Security

Transfer complete

Xxx bytes received in xx seconds

ftp> get

(remote file): Block 3: Network Fundamentals/ Unit 8: Topology

(local-file): mydocuments/topology

PORT command successful.

Opening ASCII mode data connection for file list

Transfer complete

Local: mydocuments/topology

Xxx bytes received in xx seconds

ftp>bye Goodbye.

15) In packet switching, there are problems like out-of-sequence arrival at the destination and datagram losses. There is also the problem of segmentation and reassembly due to maximum transfer unit (MTU) limitation. Routing overheads are high in packet switching. In circuit switching, physical resources remain dedicated leading to their inefficient use. Cell switching overcomes these problems.

Cell switching is designed to cause minimal network delay ensuring at the same time efficient utilisation of network resources. The physical resources do not remain dedicated.

Cell switching is built on a very reliable and ultra fast network infrastructure. The reliable technology almost rules out cell losses. Even if a cell or two is lost very rarely, the effect is unnoticeable in real time services like voice and video. The small size of the cell makes the loss imperceptible to hearing or viewing. In data services of course, recovery is required.

Cell switching uses virtual circuit principle. The cells are guaranteed to be delivered in sequence. Virtual circuit reduces switching overheads significantly and makes switching extremely fast. It is for these reasons that cell switching is superior to both packet and circuit switching.

16) 10-digit national number can support 10^{10} i.e. 10 billion numbers.

17) The 12-digit international telephone number given is '911129534336'. Here '91' stands for country code for India. The country code may further be subdivided as zone code '9' and country code within the zone as '1'. Next '11' stands for area code for Delhi. The area code may be further subdivided as region code as '1' and sub area code within the region as '1'. The following digit '2' stands for operator code, which in this case is MTNL. Digits '953' is the exchange code and '4336' is the exchange line number for the subscriber. The combination '29534336' is called the subscriber number.

18) Since the user is moving location, location portability is required. Since the user is a mobile subscriber and there is no mobile coverage available in the new place, service portability is required. It is assumed the operator is the same in the new place. Otherwise, operator portability is also required.

19) The lengths of network addresses in Class A, B, and C IP addresses are 8, 16, 24 bits respectively.

20) Class C address has 8 bits for host address. With 8 bits $2^8 = 256$ hosts can be supported. But the host addresses of all zeros and all ones are reserved for special purposes. Hence, a maximum of 254 hosts can be supported in Class C address.

21) The given binary address is '00011100 10101000 11101001 00001101'. Its decimal equivalent is 28.168.233.13. Hexadecimal equivalent is 1C.A8.E9.0D. This is Class C address as the most significant digit is zero. Seven bits following the first digit gives the network number which in this case is '0011100' and is 28 in decimal.

22) The subnet mask in binary for /22 Classless address suffix '11111111 11111111 11111100 00000000'

23) Classless address suffix is /27. This means 5 bits are available for host address. Leaving out the special reserved patterns of all zeros and all ones, we can have $(2^5 - 2) = 30$ hosts.

24) HTTP is designed for desktop and laptop and other high-end computers like servers. Here, there are no limitations of memory, computing power and screen size. It also assumes the availability of high-speed data links of at least 64 kbps. The emphasis on HTTP design is flexibility and powerful features. On the other hand, wireless protocols have to work with small portable devices like mobile phones. Here, the screen size is small, the available memory is very low and the CPU is not powerful. Data link speeds may be as low as 1.2 kbps or even less. Hence, the emphasis on WAP and LTP is high efficiency with essential minimal features only.

9.17 KEYWORDS

Client-Server : A computing and communication model used extensively in Internet

Connectionless : A service or protocol that commences information transfer without establishing a connection with the destination

Connection-oriented : A service or protocol that establishes a connection between the source and destination before information transfer commences

DHCP : Dynamic Host Configuration Protocol

Encapsulation : The process of covering a packet with another layer of header with a different format

Error control : The process of detecting and correcting errors

FTP : File Transfer Protocol

HTTP : HyperText Transfer Protocol

ICT : Information Communication Technology

ICMP : Internet Control Message Protocol

IMAP : Internet Message Access Protocol

Interoperability : Ability of different applications to interwork with each other using common data

IP : Internet Protocol

IPv4 : IP Version 4 using 32-bit addresses

IPv6 : IP Version 6 using 128-bit addresses

LTP : Lightweight Transport Protocol

NEIS : Networked Electronic Information Society

Open Protocols : Protocols that follow industry standards and are capable of running on a variety of platforms

POP3 : Post Office Protocol Version 3

Protocol : A set of rules and procedures for information exchange between computers and applications

SMTP	:	Simple Mail Transfer Protocol
SNMP	:	Simple Network Management Protocol
TCP	:	Transmission Control Protocol
Telnet	:	Remote Login Protocol
UDP	:	User Datagram Protocol
WAP	:	Wireless Application Protocol.

9.18 REFERENCES AND FURTHER READING

Black, U. *Computer Networks: Protocols, Standards and Interfaces*. 2nd Edition. New Delhi: Prentice Hall of India, 1999. Print

Homer, Douglas E. *The Internet*. New Delhi: Prentice Hall of India, 2000. Print

Homer, Douglas E. *Internetworking with TCP/IP*, Volume I. 3rd Edition. New Delhi: Prentice Hall of India, 2001. Print

Lin, Yi-Bing. *Wireless and Mobile Network Architectures*. Singapore: John Wiley & Sons (Asia), 2001. Print

Mansfield, Kenneth C and Antonakos, James L. *An Introduction to Computer Networking*. New Delhi: Prentice Hall of India, 2002. Print

Panko, R. R. *Business Data Networks and Telecommunications*. 4th Ed. New Delhi: Prentice Hall of India, 2002. Print

Stallings, W. *Data and Computer Communications*. 5th Ed. New Delhi: Prentice Hall of India, 2000. Print

Tanenbaum, A. S. *Computer Networks*. 4th Ed. New Delhi: Prentice Hall of India, 2002. Print

Viswanathan, Thiagarajan. *Telecommunications Switching Systems and Networks*,. New Delhi: Prentice Hall of India, 2010. Print