Uttar Pradesh Rajarshi Tandon
Open University

Bachelor of Computer Application

BCA-1.13

Computer Network

Uttar Pradesh Rajarshi Tandon
Open University

Bachelor of Computer Application

BCA-1.13

Computer Network

Block

1

History of Internet and WWW

Course Design Committee

Dr. Ashutosh Gupta — **Chairman**
Director (In-charge)
School of Computer & Information Sciences
UPRTOU, Prayagraj

Prof. R. S. Yadav — **Member**
Department of Computer Science and Engineering
MNNIT-Allahabad, Prayagraj

Ms Marisha — **Member**
Assistant Professor (Computer Science)
School of Science, UPRTOU, Prayagraj

Mr. Manoj Kumar Balwant — **Member**
Assistant Professor (Computer Science),
School of Sciences, UPRTOU, Prayagraj

Course Preparation Committee

Dr. Maheshwari Prasad Singh — **Author**
Assistant Professor, Department of CSE
NIT Patna

Dr. Rajiv Mishra — **Editor**
Associate Professor, Department of CSE
IIT Patna

Dr. Ashutosh Gupta (Director in Charge)
School of Computer & Information Sciences
UPRTOU, Prayagraj

Mr. Manoj Kumar Balwant — **Coordinator**
Assistant Professor (Computer Science),
School of Sciences, UPRTOU, Prayagraj

ISBN : 978-93-83328-18-5

Printed and Published by Dr. Arun Kumar Gupta Registrar, Uttar Pradesh Rajarshi Tandon Open University, 2019.

[TESLA-006]
BCA-1.13/4

Printed By: Chandrakala Universal Pvt. Ltd. 42/7 Jawahar Lal Neharu Road, Prayagraj.

BLOCK INTRODUCTION

This is the first block on Computer Networks named as Computer Network Basics and Services. As name of this block indicate that this block will introduce computer network along with some basics. This block has four units namely, Introduction of Computer Network, OSI and TCP/IP Model, The Physical Layer and ISDN and Switching Techniques.

We will begin the first unit on introduction of Computer Networks. This unit presents basics of Computer networks along with Network Hardware. It also explains different types of computer networks likes Local Area networks, Metropolitan Area networks, Wide Area networks. It also explains basics of Wireless networks. This unit also has concept of Internetworks. You will also understand Network Software. In the second unit, the most important part of computer network that is protocol stack has been discussed. Mainly it will discuss two different types of protocol stacks namely OSI reference model, and TCP/IP model. This unit presents design and issues of layers of protocol stack. With the help of the protocol stack you will also understand interface and services. With the help of protocol stack, you will understand that how communication is being performed in order to transfer the packet from one device to another device. It explains Connection oriented and Connection less Services. In the third unit, the first layer of protocol stack that is Physical layer is being discussed. This unit discussed guided and unguided media which works at Physical layer. It also introduces base band and broadband in details. In the last, the fourth unit introduced the basics of switching. This unit focused on ISDN services. This unit also tells about Switching Message, and Packet Circuit switching. This unit also focused on the working of multiplexing like TDM, and FDM. It also introduces ATM, and X.25. As you study the material, you will understand the concept with the help of figures, tables, wherever required. Each unit has been describes using many sections. Every unit has summary and review questions in the end. These questions will help you to review yourself.

UNIT-1 INTRODUCTION TO COMPUTER NETWORK

Structure

1.0 INTRODUCTION

Computer network can be defined as a cluster of computer systems and other computing hardware equipment, connected together by communication links to facilitate resource-sharing and communication among a wide range of users. In today's world data is distributed across the globe. Computer networks are therefore needed to connect users to systems far away from their locations, such that the data on those systems can be accessed. An organization/business may have offices scattered on a huge geographical location. To interconnect theses offices, so that they can exchange information among each other, we need to establish networks.

The rest of the unit is organized as follows. Section 1.1 lists the objectives of the unit. Section 1.2 discusses the basics of computer networks. Sections 1.3 and 1.4 explain the network hardware and network software respectively. Section 1.5 captures the summary of the unit and section 1.6ends the unit with some terminal questions for students to work out.

1.1 OBJECTIVES

After end of this unit, you should be able to understand:

- The basics of computer networks and various network topologies
- Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), etc.
- Network layers, protocols and interfaces

1.2 COMPUTER NETWORKS [1]

Data communication is the exchange of data between two devices through a common medium. A data communications system is a combination of physical equipment (hardware) and software (program), necessary for the communication to take place. Basically a data communications system has five components – Message, Sender, Receiver, Medium and Protocol.

1.2.1 Data communications system

A data communications system has five components as shown in Figure 1.1 below.

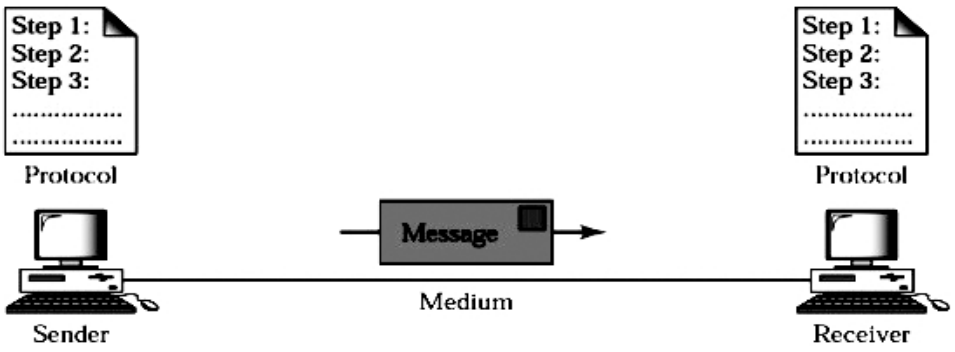


Figure 1.1: Five components of data communication [2]

Message: It is the information (data) that is to be communicated. The data can be in form of text, audio, image, video etc. - or a mixture of any of these.

Sender: It is the device that communicates the message. It can be a telephone handset, computer, a television set, a video camera, etc.

Receiver: It is the device that accepts the message from sender. It can be a telephone handset, computer, a television set, a video camera, etc.

Medium: It is the physical route through which the receiver receives a message from the sender. It can be a wired medium like coaxial cable, twisted-pair cable or fiber-optic cable. It can even be a wireless medium like radio wave, micro wave or infrared. All these media types have been discussed in unit 3.

Protocol: Data communication is manages by a set of rules known as protocol. It represents a contract between the devices that communicates.

The effectiveness of a data communications system depends on three basic characteristics:

Delivery: The system must deliver data to the correct destination and not to any other user or device.

Accuracy: The system must deliver the data correctly. The data should not have been changed in transit.

Timeliness: The data must be delivered within the stipulated time by the systems. Data that arrives late may not be of any use to the receiver.

1.2.2 Direction of Data Flow [3]

Communication can be done in either of the three modes - Simplex, Half Duplex or Full Duplex as shown in Figure 1.2.

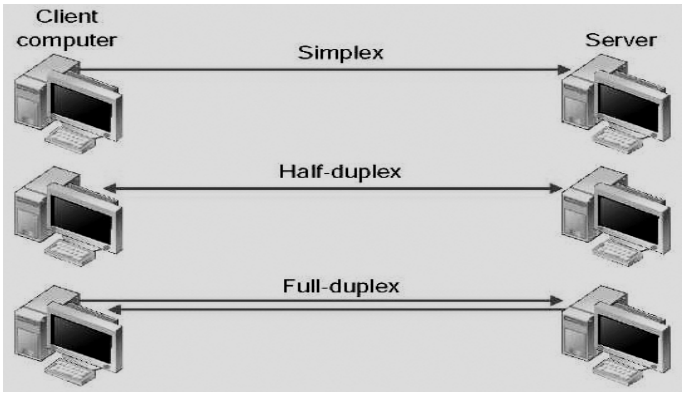


Figure 1.2: Data transmission modes: Simplex, Half Duplex and Full Duplex [3]

Simplex: In this mode message transmission is unidirectional. It means that only of the two devices connected through a channel can send the message; the other can only listen (receive). For example, the keyboard is an input device and the monitor is an output device.

Half Duplex: In this mode each device can both send and receive, but not at the same period. When one device is transferring, the other can only accept the message, and vice versa. For example, in radio broadcasting and TV, information moves only from the transmitter site to multiple receivers.

Full Duplex: In this mode both devices can transmit and receive simultaneously. Either of the two techniques can be implemented - Two physical paths are used for communication, one for sending and the other for receiving; or the channel capacity is divided between the two devices so that each device can use the channel as per requirement. For example, when two people are having a telephonic conversation, both can listen and talk at the same time.

1.2.3 Network criteria

A network is a set of devices that are connected to each other through communication links. Devices in a network can share information with each other. Various hardware (printers, scanners etc.) and software resources (files) can also be shared between the devices. Every network

should be able to fulfill certain number of criteria. Some of these criteria are:

Performance: Criteria for performance include both transmission time and response time. Transmission time is the overall time required by a message to travel from one computer to another. Response time is the time intervened between request and its response.

Reliability: Reliability is defined by the rate of failure, the time taken by a link to recover from a failure, and the network's strength in a catastrophe.

Security: Network security includes preventing the data from being accessed by unapproved sources, shielding it from modification or harm and employing mechanisms to recover data from data losses and breaches.

1.2.4 Physical Structures

For communication to take place, two devices must be associated in some way to the same channel at the same time. There are two kinds of connections: point-to-point and multipoint [4].

Point-to-Point: A dedicated link between two devices is known as point-to-point connection. The entire link capacity is kept reserved for communication of those two dedicated devices only. For example, when a television channels is changed by infrared remote control, a point-to-point connection is established between the television's control system and the remote control. Figure 1.3a shows a point-to-point link between two devices.

Multipoint: When more than two specific devices share a single link then it is known as multipoint (also called multi-drop) connection. A *spatially shared* connection one when several devices can use the link simultaneously. Whereas a *timeshared* connection is when users take turns. Figure 1.3b shows a multipoint link between many devices.

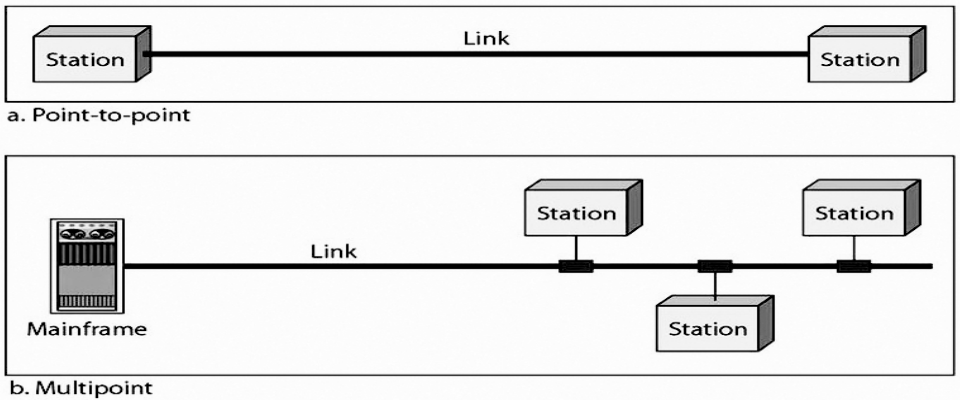


Figure 1.3: Types of connection: (a) point-to-point (b) multipoint [4]

The geometric depiction of the connection of all the links and connecting devices (generally known as nodes) to one another is represented by topology of a network. There are five topologies, four among them is

elementary topologies. They are: bus, star, mesh and ring. And hybrid topology is the combination of any elementary topology.

Bus topology

It is the multipoint topology. One long wire in a network behaves as a backbone link for the entire device. Drop lines and tapes are used to connect the nodes to the bus cable. Figure 1.4 shows the connections in a bus topology. Advantages of a bus topology include ease of installation and less cabling than mess and star topologies. Disadvantages include difficulty in adding new devices and fault isolation.

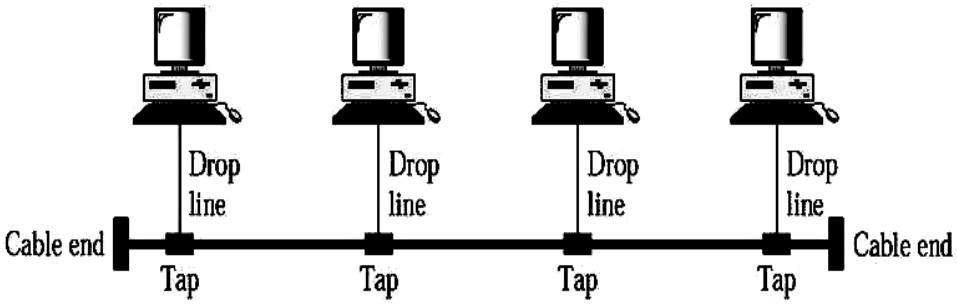


Figure 1.4: A bus topology connecting four stations [1]

Star topology

In a star topology, there is a central controller called hub. Remaining devices in the network are linked to hub through a dedicated point-to-point link. The devices are not linked directly to each other. If one device needs to communicate to another, it sends the message to the central controller, which then communicates the message to the dedicated receiver (other connected device in a network). Figure 1.5 shows the connections in a star topology. Advantages of a star topology include easy installation and reconfiguration, network robustness (if one link fails, only that link is affected) and easy fault identification and isolation. Disadvantages include the dependency of network on the hub (if the hub goes down, the whole system is dead) and more cabling than ring and bus topologies.

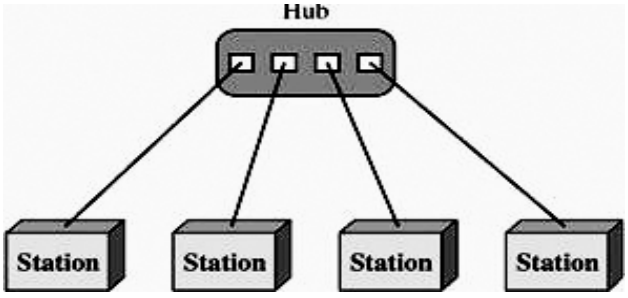


Figure 1.5: A star topology connecting four stations [1]

Mesh topology

In a mesh topology, there is a dedicated point-to-point link among every devices. The word *dedicated* means that the channel transports traffic only

between the devices that it connects. To connect n nodes, physical links required are n(n-1). However, if each physical link permits transmission in both directions (duplex mode), it can be halved in numbers. Thus, the total number of physical links required now, is n(n-1)/2. Advantages of a mesh topology include network robustness, privacy and security (each message can only be seen by the intended recipient because of the dedicated link) and easy fault identification and isolation. Disadvantages include more cabling as compared to all other topologies, difficulty in installation and reconnection and expensiveness (more hardware needed for network setup). Figure 1.6 shows the connections in a mesh topology.

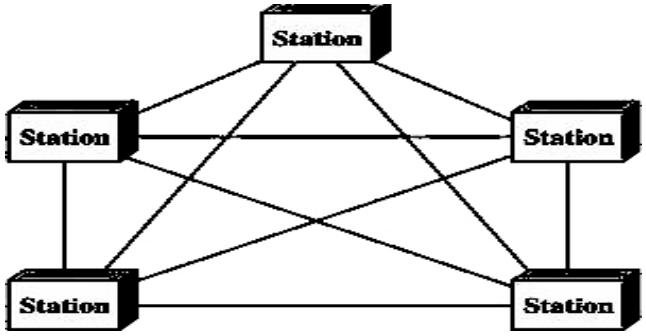


Figure 1.6: A mesh topology connecting five devices [1]

Ring topology

In a ring topology, a dedicated point-to-point connection exists only for the two devices that are on either side of a device. A signal traverse from device to device in one direction along the ring, until it reaches the destination. A repeater is incorporated with each device in the ring. When a device obtains a signal anticipated for other device, it regenerates the bits with help of repeater and passes them along. Figure 1.7 shows the connections in a ring topology. Advantages of a ring topology include easy installation and reconfiguration and easy fault isolation. A disadvantage can be a unidirectional traffic. Also a discontinuity in the ring can deactivate the whole network. This flaw can be resolved by means of a switch or a dual ring accomplished of closing off the discontinuity.

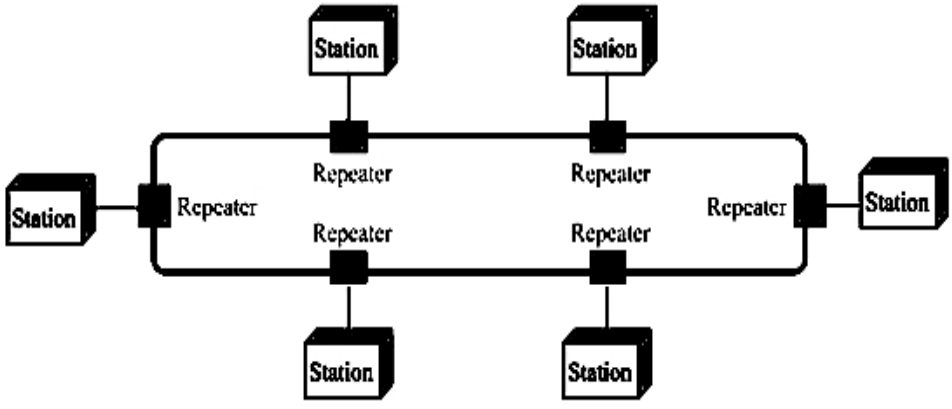


Figure 1.7: A ring topology connecting six stations [1]

Hybrid topology:

Hybrid networks is the combination of any two or more elementary topologies such that the resultant topology (network) does not demonstrates any one of the existing elementary topologies (e.g. star, bus, ring, etc.). It is produced only when two or more different standard network topologies are combined. Hybrid example may be: star bus network and star ring network. Figure 1.8 shows a star bus network which has a star backbone with three bus networks.

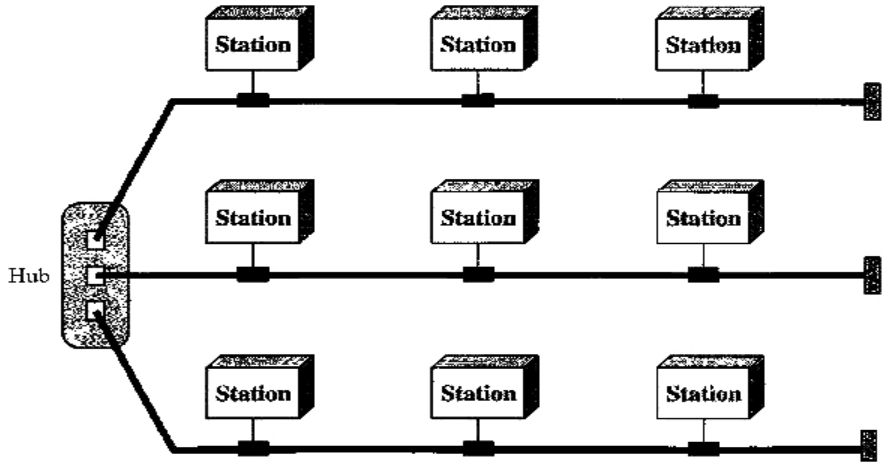


Figure 1.8: A hybrid topology: a star backbone with three bus networks [1]

CHECK YOUR PROGRESS

1. Discuss the communication model for networking in detail.
2. Describe different type of topologies used in computer networks.
3. Differentiate between simplex, half duplex and full duplex.

1.3 NETWORK HARDWARE [1]

The classification of a network can be identified by the geographical area it spans. An important classification metric can be distance because different technologies are used at different scales. The major types of networks in the increasing order of scale are – Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN). Internetwork discussed later, is the connection of two or more networks. The world-wide Internet is the best example of an internetwork.

Local Area Network (LAN)

It is usually a privately possessed network and connects the nodes (devices) in a single house, campus or office. Based on the requirements of an organization and the type of equipment used, a LAN can formed simply by using two Personal Computers (PCs) and a printer in somebody's office or home; or it can spread all through a company and

includes video and audio peripherals. Currently, size of LAN is limited to few kilometers only. Figure 1.9 below shows the connections in a typical LAN where workstations, file servers and print servers are connected to each other through a common transmission medium. Some devices are connected to the transmission medium directly and some are connected through a hub (a networking device that takes message from a node and relays it to all other nodes) or a switch (a networking device that takes message from a node and forwards it only to the intended receiver). Hubs and switches have been discussed in detail in unit 8 along with some other networking devices.

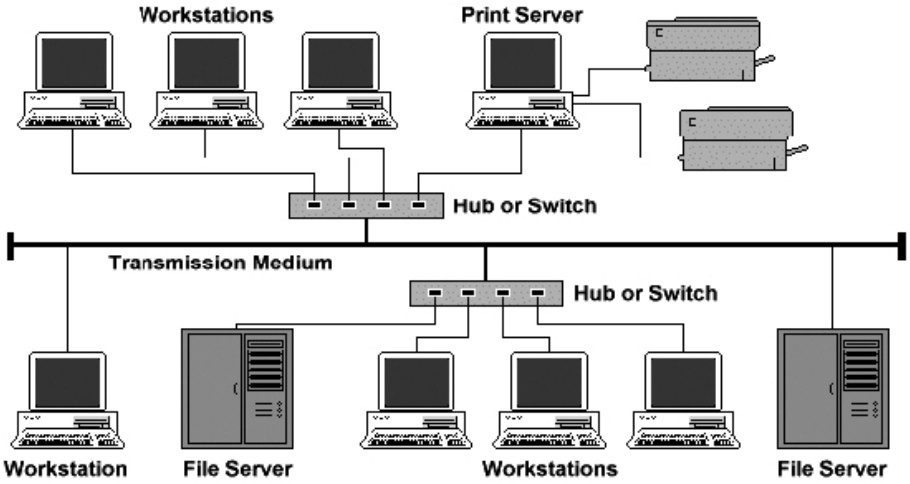


Figure 1.9: A typical local area network[5]

LANs are intended to allow resources sharing between PCs or terminals. The resources to be shared can comprise of software (e.g., an application program), hardware (e.g., a printer), or data. An example of a LAN, for many corporate environments, linking of a workgroup of task-related systems (accounting PCs or engineering workstations). One computer may behave as a server to clients, if given a large capacity disk drive. Server may store important software in it and this can be utilized whenever needed by the whole group.

The LAN size may be identified by imposing limitations on the number of users authorized to access the OS (operating system) or by restricting the number of users per software copy. In addition to size, transmission media and topology are the other distinguishing factors that differentiate LAN from other networks. In general, one type of transmission medium is used by a given LAN at a time. The common topologies used in LAN are ring, bus and star. Earlier LANs had 4 to 16 megabits per second (Mbps) as the data rates. However, in today's time, data speeds are normally 100 or 1000 Mbps.

Metropolitan Area Network (MAN)

A MAN is a network whose size varies between a LAN and a WAN network. Normally the area inside town or a city is covered under this. It is designed for users who require a high-speed connection, generally to the Internet, and have endpoints extended over a part of city or a city. Few examples of MAN can be a part of the cellular phone company network

that can offer a high-speed Digital Subscriber Line (DSL- a technology for bringing high- bandwidth information to homes and small businesses over ordinary copper telephone lines) connected to the customer or the cable TV network, today used for high-speed data connection to the Internet (originally was designed for cable TV). Figure 1.10 below is an example of a MAN. In this figure both Internet and television signals are being fed into the centralized **cable headend** for consequent delivery to people's homes.

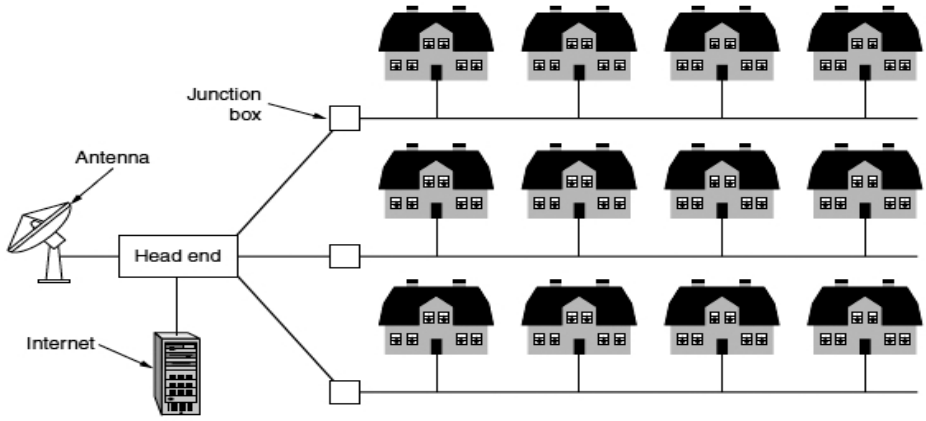


Figure 1.10: A metropolitan area network based on cable TV [6]

Wide Area Network (WAN)

A WAN allows communication over a large geographic areas that may comprise a country, a continent, or even the whole world. The transmission can be comprised of data, audio, image, and video information. A WAN can be as simple as a dial-up line that connects a home computer to the Internet or as complex as the backbones that connect the Internet. We normally refer to the first as a point-to-point WAN and second as a switched WAN. Figure 1.11a shows a Switched WAN that connects the end systems, which generally include a router (internetworking connecting device) that links to another LAN or WAN.

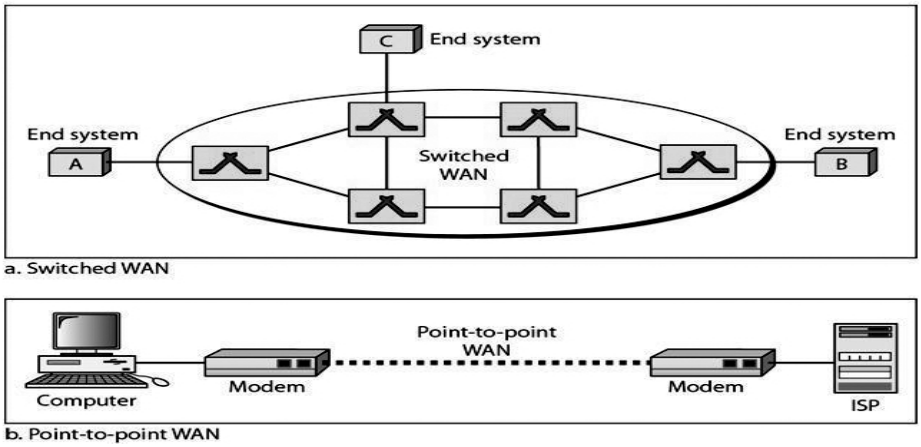


Figure 1.11: WANs: a switched WAN and a point-to-point WAN [7]

Figure 1.11b shows a point-to-point WAN that is generally a line rented from a cable TV or telephone provider that joins a home computer or a small LAN to an ISP (Internet service provider - a company that provides Internet services, including personal and business access to the Internet). This is mostly used to give Internet access.

Internetworks

In today environment, it is very infrequent to see a LAN, a MAN or a WAN in segregation. They are linked to one another to form internetworks or internet. For example, there are two offices of an organization, one situated on the east shore and the other on the west shore. The west shore office has a LAN network with bus topology the other east shore has a LAN network with star topology. The head of the organization lives anywhere in the middle and wants to have control over the organization from there only. To connect these three networks, a backbone WAN is used with a switched WAN. Further, three point-to-point WANs are required to connect these LANs to the switched WAN. The connection may be established by using either a cable modem line or a high-speed DSL line as shown in Figure 1.12.

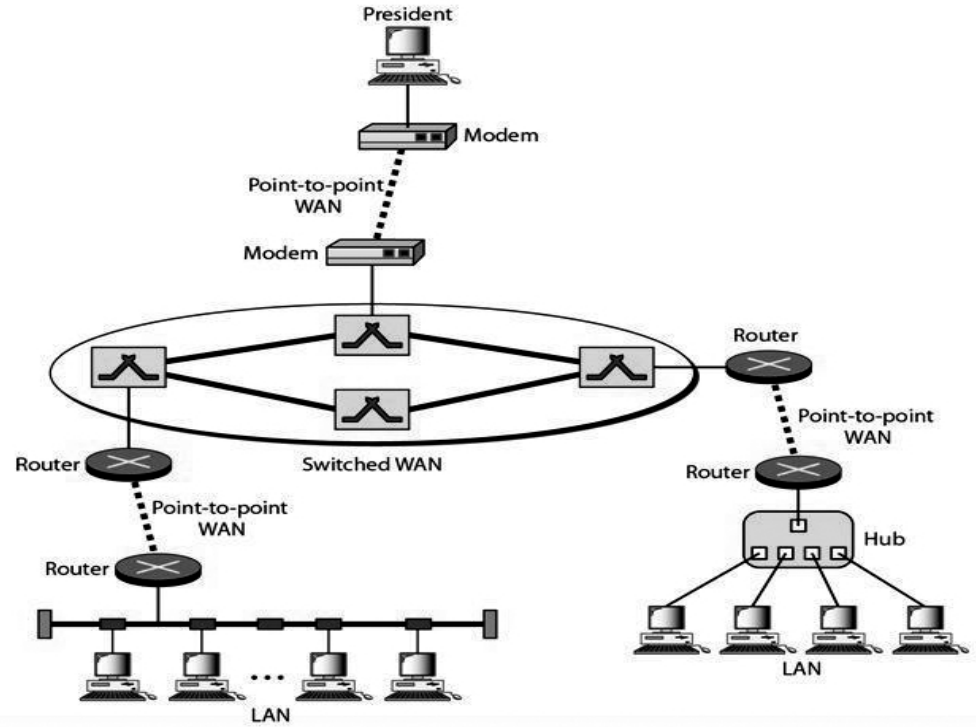


Figure 1.12: A heterogeneous network made of four WANs and two LANs [1]

Wireless Network

In wireless network, nodes are connected through radio (wireless channels).Wireless networking reduces jungle of wires as they are using wireless channel for communication. There is a standard for wireless LANs called **IEEE 802.11,** popularly known as **Wi-Fi**, which has becoming popular nowadays. Its speed is anywhere from 11 to hundreds of Mbps.802.11 networks consists of clients such as mobile phones and laptops, each of which has a radio modem and an antenna that it uses to

communicate with other nodes. The messages that originate from one node are passed to others through a networking device, basically known as an Access Point (AP). This device is usually placed at a high altitude, like the ceiling of a room. It passes the data packets between the wireless computers and also between the computers and the Internet. Figure 1.13 shows a wireless network with an access point.

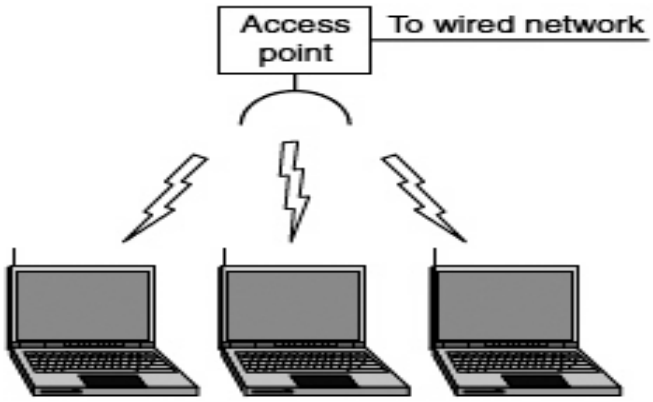


Figure 1.13: Wireless network with access point[1]

1.4 NETWORK SOFTWARE [6]

Networking software is available to analyze and govern networks of all dimensions, from the smallest home networks to the prevalent enterprise networks. Network software is now highly structured. In this section the software structuring technique has been discussed in detail.

Protocol Hierarchies

Networks are designed in the form of pile of **layers** or **levels**, each one assembled upon the one under it to reduce the design complexity. The properties differ from network to network such as number of layers, the name of each layer, the contents of each layer, and the functions of each layer. The aim of each layer is to deliver certain services to its immediate upper layer while hiding the fact of how the presented services are actually implemented. Every layer has some services to offer to its above layer. The fundamental idea is that a particular piece of software (or hardware) only shows the necessary information to its users hides its internal elements and algorithms from them. When layer *n* of a machine carries out a conversation with layer *n* of any other machine, the guidelines and resolutions used in this conversation are altogether known as the layer *n* protocol. A protocol is an agreement between the communicating parties of how the communication is to continue. Breaching the protocol will make communication more difficult.

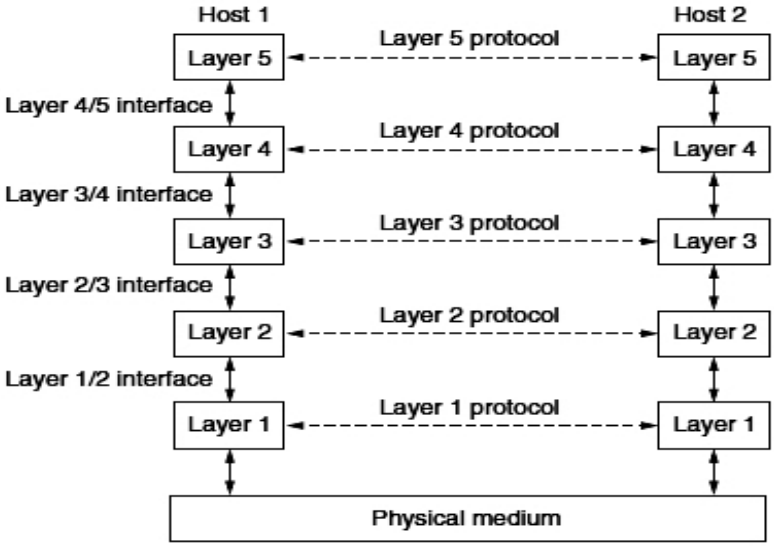


Figure 1.14: Layers, protocols and interfaces in a five layer network [6]

Figure 1.14aboveshows a five-layer network. The entities comprising the corresponding layers on different machines are called **peers**. The peer can be anything, a software process, hardware device, or even human beings. In other words, it is the peers that use the protocol to communicate to each other. The data is not directly transmitted from layer *n* of one machine to layer *n* on the other machine. Each layer passes data and control information to the layer underneath it, until it reaches to the lowest layer. The **physical medium**, through which the actual communication takes place, lies below layer 1.Dotted lines show virtual communication and solid lines show physical communication.

There is an **interface** between each pair of adjacent layers. The interface describes which primitive services and operations a lower layer makes available to its immediate upper layer. Most important consideration is defining clean interfaces between the layers. This requires each layer to perform a specific collection of well-understood functions. Network **architecture** is defined as a set of layers and protocols. The specification of network architecture must comprehend enough information. This knowledge allows an implementer to draft the program or build the hardware for each layer so that it will accurately obey the right protocol.

CHECK YOUR PROGRESS

1. Write short notes on LAN, MAN.
2. Describe network hardware.
3. Distinguish between MAN and WAN.
4. You have two computers connected by an Ethernet hub at home. Is this a LAN, a MAN, or a WAN? Explain your reason.

1.5 SUMMARY

This chapter covers the basic terminology related to computer networks and its uses for both, company and individuals. It describes the essential components of a communication model. At last, in section 1.4 and 1.5 computer networks hardware design and network software are explained.

1.6 TERMINAL QUESTIONS

1. What is network software?
2. What are the two transmission technologies used to transmit the data? Explain them.
3. Why protocol hierarchy is required?
4. List the various application area of computer networks.
5. Assume ten devices are arranged in a mesh topology. How many cables are needed? How many ports are needed for each device?
6. For each of the following four networks, discuss the consequences if a connection fails.
   a. Five devices arranged in a mesh topology
   b. Five devices arranged in a star topology (not counting the hub)
   c. Five devices arranged in a bus topology
   d. Five devices arranged in a ring topology
7. An alternative to a LAN is simply a big timesharing system with terminals for all users. Give two advantages of a client-server system using a LAN.

REFERENCES

[1] Behrouz A. Forouzan, Chapter 1, Data Communications and Networking (4th Edition).

[2] http://maulik245.blogspot.in/2011/02/components-of-data-communication.html

[3] http://what-when-how.com/data-communications-and-networking/circuits-data-communications-and-networking/

[4] http://dancingvideos.blogspot.in/2015/07/types-of-network-connections.html

[5] http://www.technologyuk.net/telecommunications/networks/local-area-networks.shtml

[6] Tanenbaum and Wetherall, Chapter 1, Computer Networks (5th Edition).

[7] http://www.slideshare.net/asad_ashu/dc-lec04-categories-of-network

UNIT-2 OSI and TCP/IP MODEL

Structure

2.0 INTRODUCTION

In this chapter, the journey begins by addressing some design issues related to layers. Then how each layer interfaces between them and what type of services they provide each other during communication process. The most essential concept is: briefing of the OSI model and how data moves through a network. Once the concept of OSI model is understood, it will be easier to design and use it in computer network. After OSI model, discussion will on TCP/IP Model, its layer services and functionalities.

The rest of the unit is organized as follows. Section 2.1 lists the objectives of the unit. Section 2.2 describes the design issues of various layers. Section 2.3 tells about the interfaces and services provided to layers. Sections 2.4 and 2.5 explain the OSI and TCP/IP models respectively. Section 2.6 gives an overview of the unit and section 2.7 ends the unit with an exercise for students.

2.1 OBJECTIVES

At the end of this unit, you should be able to:

- Address different design issues of layers.
- Define interfaces and services of each layer.
- Understand the basics of OSI Reference Model and TCP/IP Model.
- Summarize the different services and functionalities provided by layers of OSI and TCP/IP.

2.2 DESIGN ISSUES OF LAYERS [1]

There are several design issues in computer networks that come up one layer after another. Some of these design issues have been discussed below.

Addressing

Each layer requires a mechanism to identify the sender and the receiver in a network, where there are several computers with various processes running on them. Each process should be able to determine with whom it wants to communicate. An addressing technique is therefore required to identify the destination machine.

Error Control

An Error may occur in a data due to problem in physical medium, communication circuits, thermal noise or interference. Both the communicating parties must agree on a common error detecting and error correcting mechanism out of the many available. There should be a mechanism through which the receiver can inform the sender whether the data has been received successfully or not.

Flow Control

Suppose there is a slow receiver which is not able to process the data as fast as the sender is transmitting them. Due to this the receiver may eventually become overwhelmed, which will in turn lead to loss of packets at the receiver side. There are several mechanisms to prevent such situations such as increasing the buffer size at the receiver or telling the sender to slow down etc.

Routing

There may be multiple paths between the sender and the receiver. But selecting an optimal path can reduce the time and cost of communication. This judgment is made by a routing algorithm which chooses the optimized path to the destination.

Data transfer rule

A protocol must be selected that can determine the number of channels and priorities to be used. It is based on the mode of communication (simplex, half-duplex or full-duplex).

Multiplexing/ de-multiplexing

When data needs to be transmitted through the transmission medium separately for each pair of communicating devices, then it becomes very costly to setup a separate connection for each pair. Therefore physical layer employs a multiplexer (a device that combines multiple streams coming from multiple sources into a single stream to be transmitted over a single channel) at the sender site and a de-multiplexer (a device that separates the signals and routes them to their corresponding receivers) at the receiver site.

2.3 INTERFACES AND SERVICES [2], [3], [4], [5]

In computer network architecture, the primary function of each layer is to deliver services to its immediate upper layer. Active components of each layer are known as entities. An entity can be a hardware component or a software component. Entities use protocols to implement their service definitions. They are free to change their protocols at will, provided they do not change the service visible to their users. In this way, the service and the protocol are completely decoupled

2.3.1. Interfaces

A layer *n+1* uses the services provided by layer *n.* Hence layer *n+1* is known as the service user and layer *n* is known as the service provider. To give service to layer *n+1,* layer *n* can use service of layer *n-1*. Services are available at **SAPs (Service Access Points)**. Layer *n* SAP is an area which is used by layer *n+1* to access the offered services [2]. For example, if a layer offers email services, the service access point is the interface which provides software facilities to process emails. Every SAP identifies itself by a unique address. Figure 2.1 shows the use of service access point by two users.

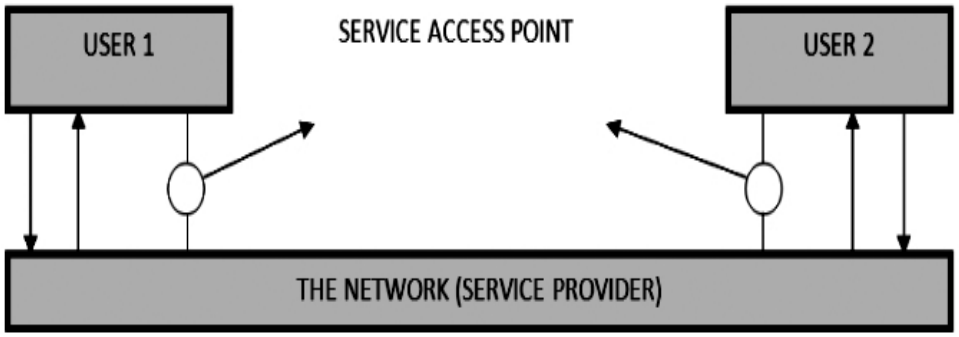


Figure 2.1: Use of Service Access Point [4]

For data transfer services, OSI defines the interface across the layers and between peer entities. The steps have been listed below [3].

1. The layer- *n* entity passes an **Interface Data Unit** (**IDU**) to the layer-(*n–1*) entity.
2. The IDU consists of a **Protocol Data Unit** (**PDU**) and **Interface Control Information** (**ICI**). PDU comprises of data and header information. The ICI contains length of the **Service Data Unit** (**SDU**), and the addressing information that the layer below needs to perform its function.

3. The layer-*n* PDU becomes the layer-(*n – 1*) service data unit (SDU), because it is the data unit that will be serviced by layer *n*.

4. When layer-(*n – 1*) receives IDU from the layer-*n*, it removes the ICI of layer-*n* and adds the header information for its peer entity across the network, adds ICI for the layer below, and passes the resulting IDU to the layer-(*n – 2*) entity as shown in Figure 2.2 below.

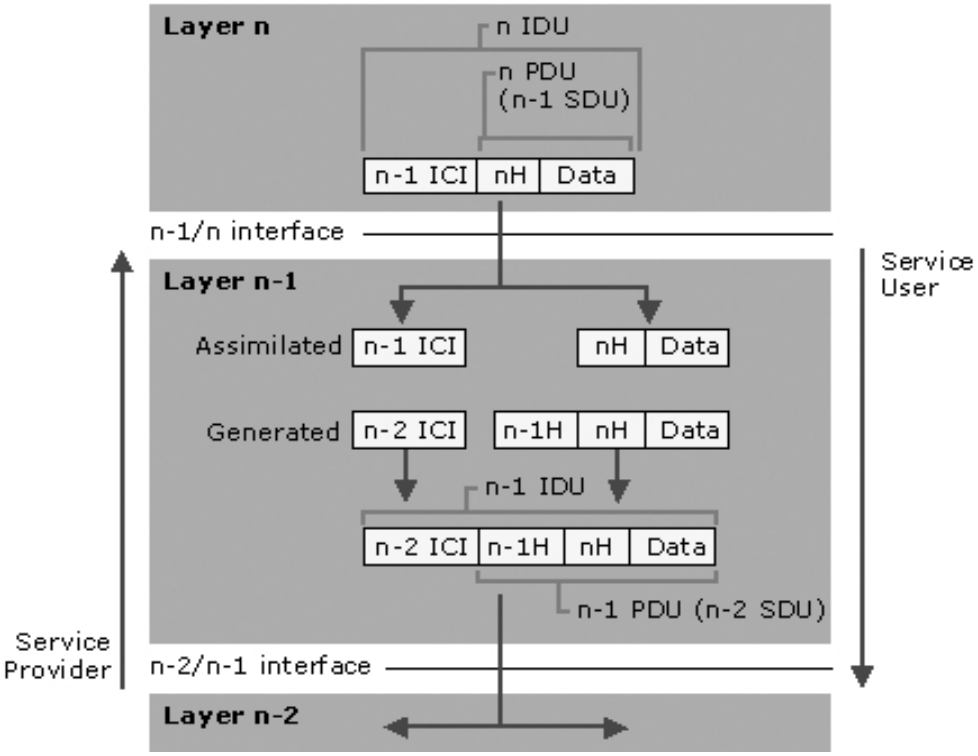


Figure 2.2: Vertical interface entities [3]

2.3.2. Services

A *service* comprises of basic operations that a layer*n-1* provides to the layer-*n*, which is executed on behalf of users. Services does not talk about implementation detail. There are two types of services: Connection Oriented Services and Connectionless Services.

Connection Oriented Services

In connection oriented services first a connection is established. Then the connection is used for data transfer and finally the connection is released [5]. Once a connection is set-up between the source and destination, the route for communication becomes static and transmission of messages follow this path only. Messages arrive at the receiver in the same order they are sent. In connection-oriented communication information is resend in case of error or packet drop at receiver's side. These type of services are very reliable. Only drawback is overhead of acknowledgement that adds to

the delay in communication. An example is **TCP** (**Transmission Control Protocol**).

Connectionless Services

In connectionless services, no connection is established between the sender and the receiver. Hence there is no static path for communication [5]. Messages are sent independent of each other with the full destination address. Messages may arrive out of order at the receiver site. Therefore ordering and regrouping of messages is required at the receiver site. These type of services are usually not reliable.

Unreliable connectionless services (without acknowledgement) are known as **datagram service**. We can analogy with telegram service, which also does not return an acknowledgement to the sender. An example of this type of service is **User Datagram Protocol** (**UDP**).

In some situations however, connection establishment may not be desired, but reliability is essential. Here no prior logical connection is set up, but datagrams (basic transfer units) are acknowledged by the receiver. This type of connectionless service is also known as **acknowledged datagram service**.

2.3.3. Service Primitives

The kind of primitive services depends on connection oriented and connectionless services. For example, following are the six service primitives to provide a connection-oriented [5].

LISTEN: In this service, server is waiting for connection request which is known as LISTEN.

CONNECT: In next step, the client establish a connection with the server through CONNECT as shown by (1) in Figure 2.3. The client process is suspended until there is a response.

ACCEPT: In next step, the server establishes the connection with the ACCEPT call. This sends a response (2) back to the client process to accept the connection. After this the client and server have established a connection.

RECEIVE: Now server is ready to accept data request by executing RECEIVE.

SEND: The client then implements SEND as in (3) followed by RECEIVE to get the reply. Server receives the packet request and runs SEND to reply (4). The client receives the answer.

DISCONNECT: After this client uses DISCONNECT to end the connection (5). Then upon receiving disconnection packet from client server also issues a DISCONNECT, acknowledging the client and releasing the connection (6).

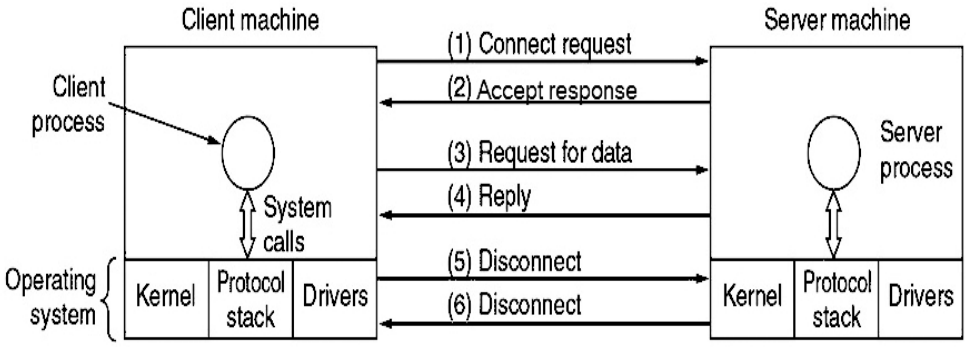


Figure 2.3: A simple client-server interaction [5]

CHECK YOUR PROGRESS

1. What are the design issues that layers have?
2. Define interfaces and services.
3. Write difference between Connection-oriented services and Connectionless services.

2.4 OSI REFERENCE MODEL [5], [6], [7], [8], [9], [10]

Open Systems Interconnection (OSI) model is based on the proposal developed by the International Organization for Standardization (ISO) in 1983 by Day and Zimmermann. This model is used for connecting open systems—that is, systems that are open for communication with other systems. There are seven layers in this model as shown in Figure 2.4 below.

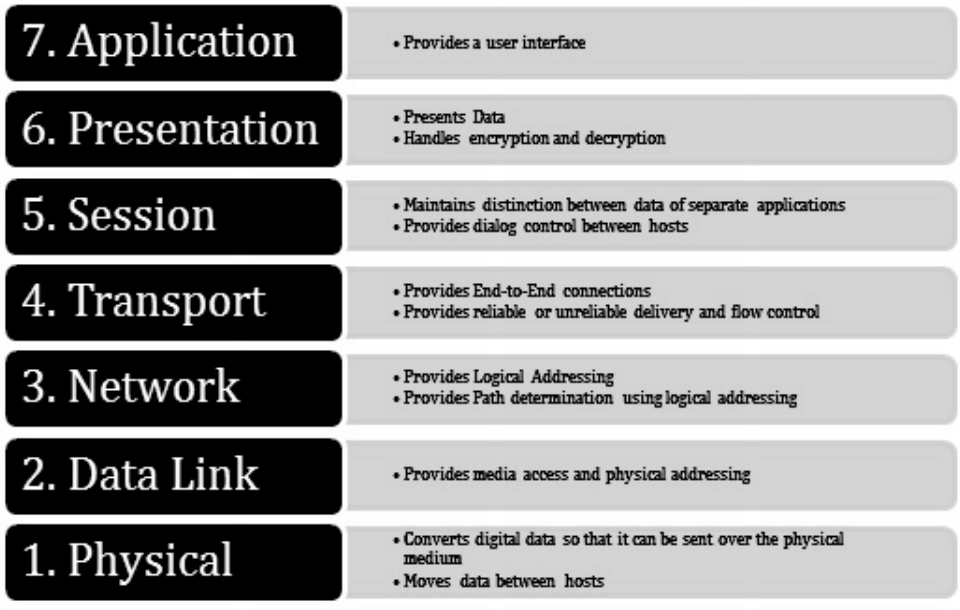


Figure 2.4: OSI Reference Model with their functions [6]

2.4.1 Functions of layers [5]

The OSI model consists of seven layers – Physical layer, Data Link layer, Network layer, Transport layer, Session layer, Presentation layer and Application layer as shown in Figure 2.4 above. Each layer performs some specific functions which have been listed below.

Physical Layer

1. It is the bottommost layer of the OSI model.
2. It transmits the raw bits over a communication channel. It explains the encoding style i.e. how 0's and 1's are transformed to signal. It converts the bits into the electrical signals.
3. This layer also specifies the voltages and data rates needed for transmission.
4. Physical Layer defines the mode of transmission between two devices: Simplex, Half Duplex, or Full Duplex.
5. It deals with the synchronization of the transmitter and receiver at the bit level.

The Data Link Layer

1. The main task of this layer is to provide a transmission facility which is free from undetected transmission errors. Duplication of frames are also prevented in Data Link Layer. Both these provisions fall under **error control** mechanism.
2. This layer manages the transmitting and receiving of sequential data frames.
3. The layer sends and receives the acknowledgement frames if the service is reliable. It also handles the resending of frames that have been sent but not acknowledged.
4. If the frames are to be distributed to different systems on the network, a header is added to the frame in order to define **physical address** (48-bit unique hardware address) of the sender and receiver of the frame.
5. There is a special sublayer, the **Media Access Control** (**MAC)** which controls accesses to the shared channel when the channel is being used by several devices for communication.
6. This layer provides the provision to slow down fast transmitters and thus prevents overwhelming of slow receivers. This provision falls under **flow control** mechanism.

The Network Layer

1. The network layer adds a header to the packet coming from the upper layer that includes, among other things, the **logical addresses** (a 32-bit address that uniquely identifies a device in a network) of the sender and the receiver.
2. The network layer controls the operation of the subnet.
3. The route of the packets from source to destination is determined by this layer.
4. Handling congestion is a responsibility of the network layer.
5. Quality of Service provided is also a network layer issue.
6. Network layer allows interconnection of heterogeneous networks.

The Transport Layer

1. Transport Layer header includes service point address which is port address. The layer above it sends message to it. Transport layer converts the message into smaller units and passes it on to the Network layer i.e. **Service Point Addressing**.
2. The transport layer provides error-free point-to-point channel to guarantee that the whole message arrives at the receiving transport layer without any fault i.e. **error control**.
3. This layer includes two types of **Connection control**:

a. Connectionless: Each segment is considered as an individual packet and sent to the transport layer at the destination machine.

b. Connection Oriented: A connection is made with the transport layer of the destination machine before delivering packets to them.

4. This layer is responsible for dividing the message into transmittable segments before transmission and then reassembling the segments to form the message at the receiving site.
5. The transport layer is also responsible for **flow control** that is performed end to end rather than across a single link.

The Session Layer

1. It helps users on different machines to create sessions between them i.e. **Dialog control.**
2. It prevents two parties from attempting the same critical operation simultaneously i.e. **token management.**
3. At this layer the process may add checkpoints to a stream of data which are considered as synchronization points i.e. **synchronization.**

The Presentation Layer

1. The **syntax and semantics** of the information to be transmitted is taken care by this layer.
2. Presentation layer allows higher-level data structures to be defined and exchanged.
3. It also manages the abstract data structures definition.
4. This layer performs **Data compression** (to reduce the bandwidth of the data to be transmitted), **Data encryption** (perform encryption and decryption at transmitter and receiver respectively), **Data conversion** (information in the form of numbers and characters should be transformed to bit streams) etc.

The Application Layer

1. Application layer contains a variety of protocols that are commonly needed by users like **HTTP** (**Hypertext Transfer Protocol -** underlying protocol used by the World Wide Web to define how messages are formatted and transmitted). Users can access and manage files in a remote computer i.e. **File Transfer Access and Management (FTAM).**
2. Other application protocols are also used for file transferring, network news and electronic mail i.e. **Mail Services**.
3. Accessing global information about various services is also provided by this layer i.e. **Directory Services**.
4. The application generates software simulation of a terminal at a remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on. Thus a **Network Virtual Terminal** is created to allow user to log on to a remote host.

2.4.2 Data formats at different OSI layers

The data format used at each layer is different and has been shown in Table 2.1 below. In the application, presentation and session layers data used is called **message**. The transport layer breaks the message into small units called **segments**. Data in the network layer is in the form of **packets**. In the data link layer it is in the form of sequential **frames**. Finally before transmission data is in the form of **bits** in the physical layer.

Table 2.1: Data formats at different OSI layers

OSI Layers	Data formats used
Application	Message
Presentation	Message (may be encrypted and/or compressed)
Session	Message
Transport	Segments
Network	Packets
Data Link	Frames
Physical	Bits

2.4.3 Protocols at different OSI layers [7], [8]

There are some basic protocols that operate at each layer of the OSI. The protocols that operate at each layer have been listed below. Table 2.2 shows the protocols used by each layer of OSI.

Physical layer

The major protocols used by the physical layer are:

1. **Bluetooth**: Bluetooth is a short-range wireless connection used to connect computers, mobile phones, computers, and PDAs (personal digital assistants).
2. **Ethernet (IEEE802.3**): It is a computer networking technology LANs and MANs.
3. **DSL**: **Digital Subscriber Line** (DSL) is a technology that uses ordinary copper telephone lines for providing high-bandwidth information.

4. **ISDN**: **Integrated Services Digital Network** (ISDN) is a telecommunications technology that uses standard phone lines to transmit digital data over it.

5. **WiFi** (**IEEE 802.11**): It is the wireless networking technology using radio waves that provide wireless high-speed Internet connections.

Data Link layer

The major protocols used by the data link layer are:

1. **ARP**: **Address Resolution Protocol** (ARP) is a protocol that translates Internet Protocol address (IP address) to a physical machine address.

2. **ATM**: **Asynchronous Transfer Mode (**ATM) is a dedicated-connection switching technology that transmits digital data over physical medium by using digital signal technology.

3. **HDLC**: **High-level Data Link Control (**HDLC) is a group of rules or protocols used to transmit data (organized into units called *frames*) between network points.

4. **PPP: Point-to-point protocol** (PPP) is a computer network protocol used to transfer a datagram between two directly connected (point-to-point) computers.

   FDDI: FDDI (**Fiber Distributed Data Interface**) is a set of ISO and ANSI standards used for data transmission over token ring protocol on fiber optic lines.

Network layer

The major protocols used by the network layer are:

1. **ICMP**: **Internet Control Message Protocol (**ICMP) is an error-reporting protocol. Error messages are generated by network devices for source IP address when delivery of IP packets are prevented due to network problems.

2. **IGMP**: **Internet Group Management Protocol (**IGMP**)** is an Internet protocol through which Internet computer informs its adjacent routers about its multicast group membership.

3. **IPsec**: **Internet Protocol Security (**IPsec) is a protocol suite that authenticates and encrypts each IP packet in a communication session.

4. **RIP**: RIP (**Routing Information Protocol**) is a dynamic protocol that finds the best path or route from source to destination (end-to-end) over a network by using a hop count algorithm/ routing metric.

5. **IPv4**: **Internet Protocol Version 4 (**IPv4) is the fourth revision of the IP protocol and used for data communication in networks.

6. **IPv6**: IPv6 (**Internet Protocol Version 6**) is the descendant to Internet Protocol Version 4 (IPv4) in which the IP addresses have been lengthened from 32 bits to 128 bits to prevent the shortage of network addresses in future.

Transport layer

The major protocols used by the transport layer are:

1. **TCP**: **Transmission Control Protocol** (TCP) is a network communication protocol that sends data packets over the Internet and create a connection between remote computers. It transports and ensures the delivery of messages over networks and the Internet.

2. **UDP**: **User Datagram Protocol** (UDP) is an unreliable, connectionless protocol that sends short messages called datagrams. It is a part of Internet Protocol suite.

Session layer

The major protocols used by the session layer are:

1. **NetBIOS**: NetBIOS (**Network Basic Input/Output System**) allows applications on different computers to communicate within a LAN.

2. **NFS:** NFS (**Network File System**) allows a remote computer file access on user's computer. In this it allows user to view, optionally store and update files.

3. **PAP**: PAP (**Password Authentication Protocol**) is used to provide authentication. The user's details (name and password) are sent over a network and compared to name-password pairs in a table.

4. **SCP**: SCP (**Session Control Protocol**) is a protocol that creates multiple light-duty connections from a single TCP connection.

Presentation layer

The major protocols used by the presentation layer are:

1. **JPEG**: JPEG (**Joint Photographic Experts Group**) is a lossy compression protocol used for digital images.
2. **MPEG**: MPEG stands for **M***oving* **P***icture* **E***xperts* **G***roup*. It is the family of digital compression standards and file formats developed by the group.
3. **TIFF**: **Tag Image File Format** (TIFF) is used for switching bitmap (raster graphics) images between applications.
4. **MIDI**: **Musical Instrument Digital Interface** (MIDI) is a protocol intended for recording and playing back music on digital synthesizers.

Application Layer

The major protocols used by the application layer are:

1. **DNS**: DNS (**Domain Name system**) maps internet domain names to the internet protocol (IP) network addresses they represent and enables websites to use names, rather than difficult-to-remember IP addresses.
2. **DHCP**: **Dynamic Host Configuration Protocol (**DHCP) is a communications protocol that network administrators requires to centrally automate and manage the network configuration of devices attaching to an IP network.
3. **FTP**: **File Transfer Protocol (**FTP) is a network protocol used to file transfer between a server and client on a network.
4. **SMTP**: **Simple Mail Transfer Protocol (**SMTP) is the standard protocol that send and receive email messages on a TCP/IP network.
5. **Telnet**: It is a TCP/IP network protocol that allows connection to remote computers (called hosts).
6. **LDAP**: **Lightweight Directory Access Protocol (**LDAP) is a software protocol that enables locating of individuals, organizations, and other resources (files and devices) in a network.
7. **SNMP**: **Simple Network Management Protocol (**SNMP) is the protocol that governs network management and the monitor's devices of network and their functions.

8. **HTTPS**: **Hyper Text Transfer Protocol Secure (**HTTPS) is the secure version of HTTP protocol over which data is sent between browser and the website that are connected.

Table 2.2: Basic protocols used at different OSI layers

OSI Layers	Basic protocols used
Application	HTTPS, SMTP, DHCP, FTP, Telnet, SNMP, LDAP, DNS
Presentation	JPEG, MPEG, TIFF, MIDI
Session	NetBIOS, NFS, PAP, SCP
Transport	TCP, UDP
Network	IPv4, IPv6, ICMP, IPsec, IGMP, RIP
Data Link	ARP, HDLC, PPP, ATM, FDDI
Physical	Bluetooth, DSL, ISDN, Ethernet, WiFi

2.4.4 Network devices at different layers of OSI [9]

The components that are used to connect computers or other electronic devices together is known as network devices. They can share files or resources like printers or fax machines. Network devices vary from layer to layer in the OSI Model. Network devices operating at various layers have been listed below. Table 2.3 shows at which layer each network device operates.

Physical layer

The network devices that operate at the physical layer are:

1. **Hub**: A hub is a networking device that has multiple nodes connected to it through multiple ports. The message received from a node is simple relayed to all the other nodes.
2. **Repeater**: A repeater is a device similar to the hub, but has additional features. It can amplify the input signal if necessary.

Data Link layer

The network devices that operate at the data link layer are:

1. **Layer 2 switch**: A layer 2 switch mainly helps in exchanging packets among devices within a LAN. It maintains a table of MAC addresses of devices for this.
2. **Bridge**: A bridge is a networking device that connects two networks that are using the same protocol. A bridge can also be used to divide a large network into small subnetworks.

Network layer

The network devices that operate at the network layer are:

1. **Layer 3 switch**: A Layer 3 switch is a specialized hardware device used in network routing. Layer 3 switches technically share much in common with traditional routers.
2. **Router**: The main function of a router is to connect networks to each other. It allows data from one network to move to another network.

Transport, Session, Presentation and Application layers

The network device that operates at all these layers is:

1. **Gateway**: It basically connects two networks that are using different protocols. They are placed at the edges of networks, often integrated with firewalls.

Table 2.3: Network devices operating at different OSI layers

OSI Layers	Network devices used
Application	Gateway
Presentation	
Session	
Transport	
Network	L3 switch, Router
Data Link	L2 switch, Bridge
Physical	Repeater, Hub

2.5 TCP/IP MODEL [5]

Transmission Control Protocol and Internet Protocol (TCP/IP) was developed by Department of Defense's Project Research Agency (ARPA, later DARPA). One of the major design goals was the ability to connect multiple networks in a seamless way. Some of the protocols used in the

TCP/IP model is shown in Figure 2.5. The points that stood out during the research, that leads to designing of the TCP/IP model were:

- It supports the flexible architecture which means that adding of more nodes to a network was easy.
- The network was robust, and connections remained unbroken until the destination and source machines were functioning.

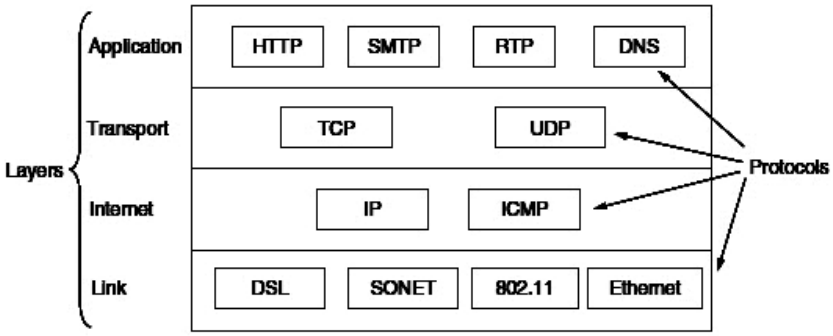


Figure 2.5. Protocols of TCP/IP [5]

2.5.1 Function of Different Layers of TCP/IP Model

Functionality of different layers in TCP/IP model is discussed below:

The Link Layer

1. The **lowest layer** of the model is Link Layer.
2. The link layer defines what links such as classic **Ethernet and** serial lines must do to meet the needs of this connectionless internet layer.
3. This layer works like an **interface** between hosts and transmission links.

The Internet Layer

1. This layer holds the whole architecture together.
2. The job of this layer is to permit hosts to inject packets into any network and help them travel independently to the destination.
3. **IP** (**Internet Protocol**), an official packet format and protocol is defined in this layer, plus a companion protocol called **ICMP** (**Internet Control Message Protocol**) that helps it function.
4. Order in which packets are received can be different from the way they are sent, in which case it is the job of higher layers to rearrange them.

The Transport Layer

1. The path for data transmission may be on parallel path or single path is decided by this layer.

2. This layer breaks the data (message) into small parts so that they are handled more efficiently by the network layer.
3. Two transport protocols (end-to-end) have been defined in this layer:
    a. **TCP** (**Transmission Control Protocol**) is a connection-oriented and reliable protocol that allows a byte stream delivered from one machine to another machine in the internet without any error.
    b. **UDP** (**User Datagram Protocol**), is an unreliable connectionless protocol used for client-server-type request-reply queries, one-shot and applications in which swift delivery is more important than accurate delivery (speech or video).

The Application Layer

All the higher- level protocols are described in this layer. Some of the protocols are:

a. **TELNET**: It is a virtual terminal that allows connecting to a remote machine and run applications on it.
b. **FTP**: **File Transfer Protocol** is used for file transfer among the users connected over a network.
c. **SMTP**: **Simple Mail Transfer Protocol** is used to transport electronic mail from source to destination.
d. **DNS**: **Domain Name System** is used for mapping host names onto their network addresses.
e. **HTTP**: **Hyper Text Transfer Protocol** is used for fetching pages on the World Wide Web.
f. **RTP**: It is used for delivering real-time media (voice or movies).

CHECK YOUR PROGRESS

1. Differentiate between OSI and TCP/IP Model.
2. What are the different data formats used by each layer in OSI Model?
3. Briefly describe functions of each layer of TCP/IP.
4. What are the main functions of the data link layer of the OSI model?

2.6 SUMMARY

In this the importance of layered structure is discussed. This chapter talks about the several design issues that a layer face at time of communication between them. Layers provide services to its upper layer by using service of the layer next to it in Internet model. For communication the layers establish either connection-oriented services or

connectionless services. Section 2.4 elaborates the OSI Model in detail followed by the discussion on each layer services. At the end of this chapter TCP/IP model is discussed.

2.7 TERMINAL QUESTIONS

1. Describe the OSI Model in detail.
2. List the protocols of each layer in TCP/IP.
3. Describe different service primitives used by a layer to provide service to its upper layer.
4. Write short notes on SAP, IDU and PDU.
5. Suppose a computer sends a packet at the transport layer to another computer somewhere in the Internet. There is no process with the destination port address running at the destination computer. What will happen?
6. Suppose a computer sends a packet at the network layer to another computer somewhere in the Internet. The logical destination address of the packet is corrupted. What happens to the packet? How can the source computer be informed of the situation?
7. If the data link layer can detect errors between hops, why do you think we need another checking mechanism at the transport layer?
8. What is the difference between a port address, a logical address and a physical address?

REFERENCES

[1] www.smusolutions.com/2011/12/q1-explain-all-design-issues-for.html

[2] http://punarvasi.com/what-is-interface-and-its-services-in-layered-architecture-of-computer-network/

[3] https://technet.microsoft.com/en-us/library/cc977589.aspx

[4] http://www.studytonight.com/computer-networks/connection-oriented-and-connectionless service

[5] Tanenbaum and Wetherall, Chapter 1, "Computer Networks (5th Edition)".

[6] http://www.freeccnastudyguide.com/study-guides/ccna/ch1/1-3-osi-reference-model/

[7] http://www.computernetworkingnotes.com/ccna-study-guide/osi-seven-layers-model-explained-with-examples.html

[8] http://www.webopedia.com/quick_ref/OSI_Layers.asp

[9] http://www.certiology.com/computing/computer-networking/network-devices.html

UNIT 3 : PHYSICAL LAYER

Structure

3.0 INTRODUCTION

The discussion starts with the lowermost layer of the Interne Model, the physical layer. Its working involves direct interaction with transmission media and connecting of network components physically altogether. It also carries the information physically, from one node to other in the network.

One of the major task of this layer is to offer services to the layer above it; the data link layer. The data link layer's consists of frames that holds data in 0s and 1s format. This data stream of 0's and 1's need to be first be changed into other entity called signals. The physical layer creates a signal that denotes the actual stream of bits (0s and 1s).

The physical layer also take care of the transmission medium and physical network, as there is no internal logic or program for control of transmission medium like other layers have. The physical layer decides the data flow directions and the number of logical channels for transporting the data coming from diverse sources.

The rest of the unit is organized as follows. Section 3.1 lists the objectives of the unit. Section 3.2 discusses the physical layer. Section 3.3 tells about different signal types and their representation. Sections 3.4 and 3.5 explain transmission modes and transmission impairments respectively. Section 3.6 discusses channel capacity and section 3.7 describes the types of transmission media. Section 3.8 gives the summary of the unit and section 3.9 closes the unit with a few terminal questions.

3.1 OBJECTIVES

By the end of this unit, you should be able to:

- Define physical layer and its services.
- How signal are converted by using data encoding techniques.
- Transmission modes of communication between two nodes.
- Different transmission impairments that can affect a signal.
- Transmission media used for physical transmission of signal between computers.

3.2 PHYSICAL LAYER

In OSI Layer, the lowest layer of all layers is Physical layer. It provides service to layer above it (data link layer). It sends bits (in form of signals) from one node to another. The meaning of bits is not the concern of this layer. It deals with the transmission and reception of signals and physical connection to the network.

This layer defines physical and electrical details represented as '0' or '1'. Physical layer consists of the hardware that provide the communication ability:

- Interface cards
- Wires
- Transmitters

It provides the communication link between the nodes.

3.2.1. Services of Physical Layer [1]

The physical layer transmits bits in the form of signals between sender and receiver. The physical layers of two adjacent nodes provide a logical pipeline through which bits can travel. Figure 3.1 shows the general services that a physical layer provides.

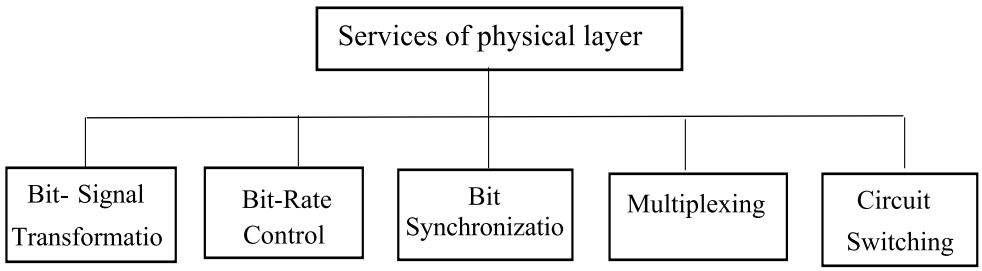


Figure 3.1: Physical Layer Services [1]

Bit – Signal Transformation: Transmission medium acts like the logical pipe between two physical layers *i.e.* either cable or air. As the transmission medium cannot carry the data in the form of bits, it is converted into an electromagnetic energy that can move through a medium i.e. signal.

Bit – Rate Control: The physical layer acts as the data rate controller even though the transmission medium determines the upper limit for it. The hardware and software of physical layer determine the data rate.

Bit Synchronization: In data communications the timing of the bit transfer is very important. The physical layer manages bit synchronization by employing clocking mechanisms that control the sender and the receiver.

Multiplexing: It is the mechanism to divide physical medium into logical channels to achieve better efficiency. Physical layer performs this by different techniques.

Circuit Switching: It is a switching method where a dedicated link is provided between two nodes for communication. This function is mostly provided in the physical layer.

3.3 SIGNALS [2]

A signal is something that carries a measurable amount of energy that varies with time. Before data is sent over the network it is first converted into electromagnetic signals. Signal representation is of two types:

1) ***Analog Signals***: Continuous wave forms that are denoted by continuous electromagnetic waves is known as ANALOG SIGNAL. A modem, for example, transmits a high pitch for a 1 and a low-pitched sound for a 0; the sounds themselves appears like sine waves when represented against time in graph as shown in figure 3.2a.

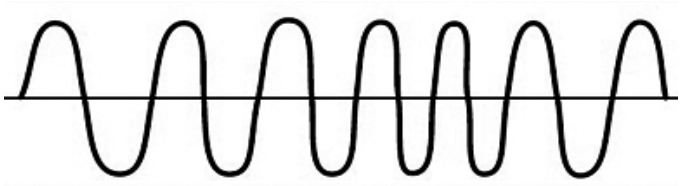


Figure 3.2 (a) Analog Signals [3]

2) ***Digital Signals***: A Digital Signal consists of 1s and 0s where a 0 means a low voltage and 1 represents a high voltage. It represents sequence of voltage pulses that are discrete in nature. They are used inside the computer system's circuitry. Digital signal when

represented over time in a graph shows a “square wave” shape as shown in Figure 3.2b.

Figure 3.2(b) Digital Signals [3]

A **periodic signal** completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a **cycle**. Period refers to the amount of time in seconds, a signal needs to complete 1 cycle. Frequency is the number of periods in 1 second. It is measured in Hertz. Frequency and period are inverse of each other. Therefore the following formulas hold:

$$f=1/T \text{ and } T=1/f$$

A nonperiodic signal on the other hand, changes without exhibiting a cycle or pattern that repeats over time. Both digital and analog signals can be periodic or a periodic in nature. But mostly periodic analog signals and nonperiodic digital signals are used.

3.3.1 Data Encoding

The input data can be in any form either digital or analog and can be converted into analog or digital signals.

Digital Data to Analog Signals*:* A modem (modulator-demodulator) changes digital data into analog signal. A digital data can be modulated into analog signal in 3 ways:

a) ***Amplitude Shift Keying (ASK)***: This represents digital data in form of amplitude carrier wave. Figure 3.3 shows digital data 10010110 converted into amplitude signal. Bit 1 is denoted by high amplitude and bit 0 is denoted by low amplitude.

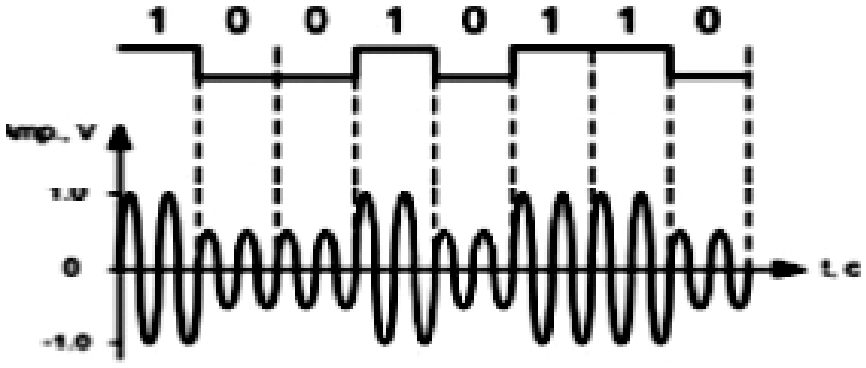


Figure 3.3. Amplitude Shift Keying[4]

b) ***Frequency Shift Keying (FSK)***:It is the modulation technique where alteration in frequency denotes different bits. Bit 1 is denoted by low frequency and bit 0 is denoted by high frequency. Figure 3.4 shows how digital data 10010110 is represented through frequency shift keying.

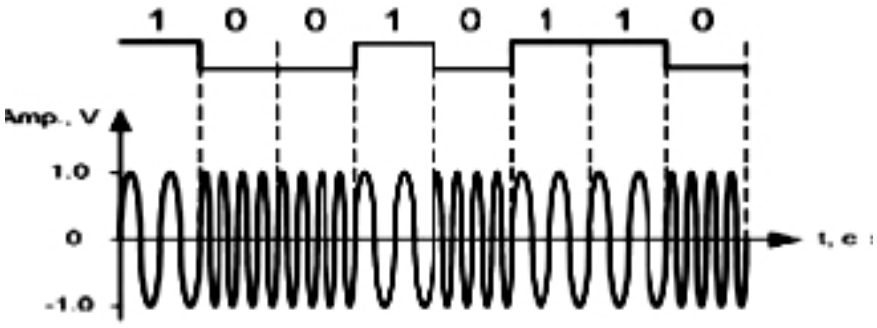


Figure 3.4. Frequency Shift Keying [5]

c) ***Phase Shift Keying (PSK)***: It is a digital modulation method that encodes data by shifting (modulating) the **phase** of the carrier wave (reference signal). The modulation is done by varying the cosine and sine inputs at a specific time. It is generally used for wireless LANs and Bluetooth communication. Figure 3.5 shows an example of phase shift keying for data 10010110.

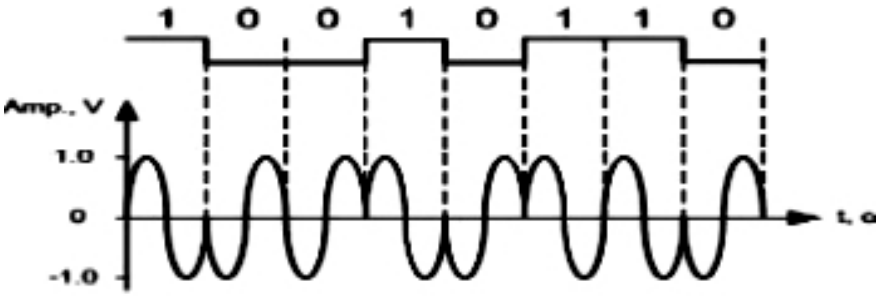


Figure 3.5. Phase Shift Keying [6]

Digital Data to Digital Signals: A digital signal is arrangement of discontinuous, discrete voltage pulses. Each pulse is a signal element. Encoding scheme is a significant aspect that how effectively the receiver understands the received signal. Following are some of the methods to map data bits to signal elements.

a) ***Non return to zero (NRZ)***

This code has the property that level of voltage remains constant through a bit interval. Bit 1 = High level voltage and bit 0= Low level voltage. An issue arises when there is a long arrangement of

1s or 0s i.e. the voltage level is kept at the same level for a longer time. This produces a difficulty on the receiving end because now, the clock synchronization is vanished due to absence of any shifts and hence, it becomes difficult to identify the exact number of 1s or 0s in the given sequence.

There are two variations of NRZ, described as following:

1. ***NRZ-Level (NRZ-L)***: In NRZ-L the level of the voltage determines the value of the bit. In Figure 3.6 below, for NRZ-L, bit 1 is represented by a high voltage and bit 0 is represented by a low voltage.
2. ***NRZ-Inverted (NRZ-I)***: In NRZ-I the inversion or the lack of inversion determines the value of the bit. If there is no change, the bit is 0; if there is a change, the bit is 1. This is shown in Figure 3.6 below, for NRZ-I encoding scheme.

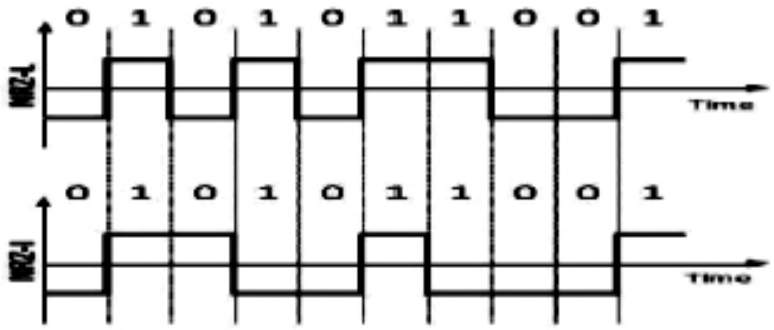


Figure 3.6. NRZ encoding schemes [7]

b) ***Biphase encoding***

Biphase encoding has the following characteristics:

- Biphase encoding has twice the modulation rate (modulation rate is defined as the rate at which level of the signal changes) of NRZ and correspondingly greater bandwidth.
- Clock can be extracted from signal itself because there is expected transition during each bit time. The receiver can synchronize its clock based on that transition.
- Clock operates at twice the data transfer rate because the transition can take place at the beginning as well as in the middle of the bit interval.

The following are the two encoding schemes that fall under Biphase encoding:

1. ***Biphase-manchester***: Transition from low to high in middle of interval = 0 and transition from high to low in middle of interval = 1 as shown in Figure 3.7.

2. ***Differential-manchester***: Transition always takes place in middle of interval. Transition at beginning of interval = 0 and no transition at beginning of interval= 1 as shown in Figure 3.7.

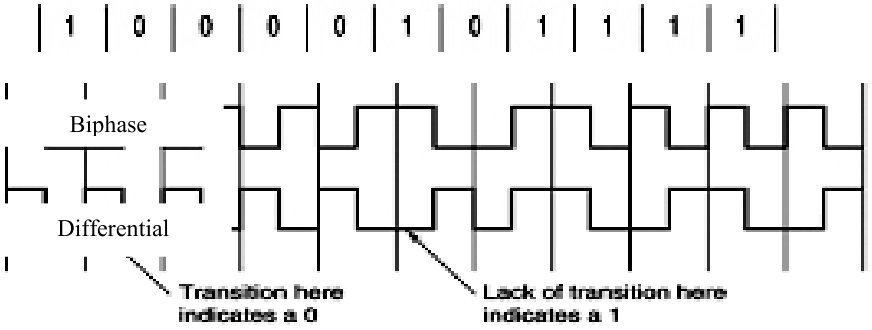


Figure 3.7: Biphase encoding schemes [8]

c) ***Bipolar encoding***

Bipolar encoding scheme uses 3 voltage levels- middle, upper and lower. There are two methods that fall under Bipolar encoding scheme – AMI and pseudoternary.

1. ***AMI (Alternate Mark Inversion)***: Middle level =0 and Lower, Upper level =1 such that consecutive 1s will be denoted interchangeably on lower and upper levels. An example is shown in Figure 3.8.

2. ***Pseudoternary***: Middle level =1 and Lower, Upper level=0. Consecutive 0s will be denoted interchangeably on lower and upper levels.

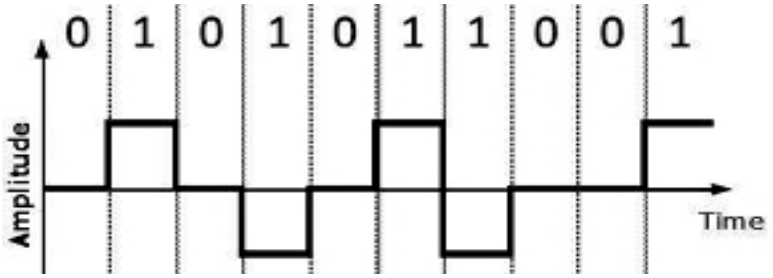


Figure 3.8. Bipolar encoding scheme [7]

Analog data to digital signal: This conversion is known as digitization. For regeneration of signal, sampling frequency must be at least two times that of maximum frequency value present in the signal. There are two techniques to convert analog data to digital signal – **PCM** (**Pulse Code Modulation**) and **DM** (**Delta Modulation**).

a) ***PCM***

PCM is a technique for converting analog data into digital signal. It consists of the following steps.

a) ***Sampling****:* In every *T* interval the analog signal is sampled. The rate at which analog signal is sampled is the most significant aspect in sampling. According to Nyquist Theorem, sampling frequency must be at least two times that of maximum frequency value existing in the signal. Figure 3.9 below shows the sampling mechanism.

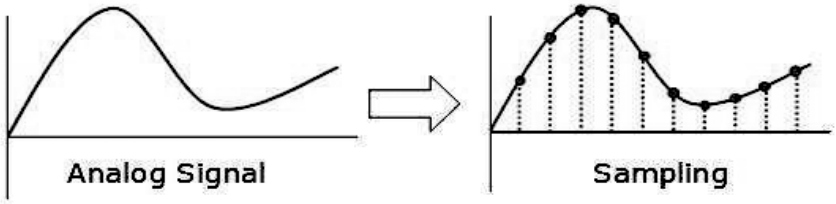


Figure 3.9: Sampling [7]

b) ***Quantization****:* Sampling converts the analog signal to a series of pulses of different amplitudes. Quantization is a method of assigning integral values in a specific range to the sampled instances. The result of Quantization is shown in Figure 3.10 below.

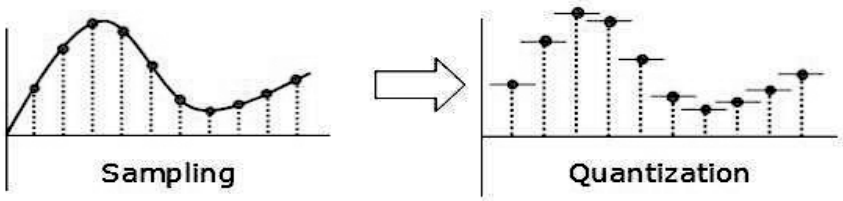


Figure 3.10: Quantization [7]

c) ***Encoding***: In encoding, each value is translated into its 7 bit binary equivalent. The eighth bit indicates the sign. Figure 3.11 below shows the encoding method.

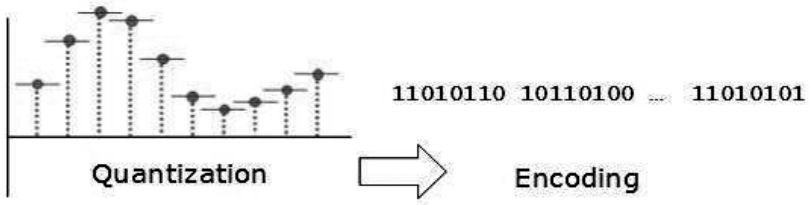


Figure 3.11: Encoding [7]

b) DM

Delta Modulation is a simple technique as compared to PCM. The modulator at the sender site creates a stream of bits from an analog signal. The detailed process is as follows. Figure 3.12 shows a graph of how the binary data is generated from the analog signal.

1. The modulator builds a second signal based on the original analog signal. This second signal resembles a staircase.
2. The modulator, at each sampling interval, compares the value of the analog signal with the last value of the staircase signal.
3. If the amplitude of the analog signal is larger, the next bit in the digital data is 1; if the amplitude of the analog signal is smaller, the next bit in the digital data is 0.

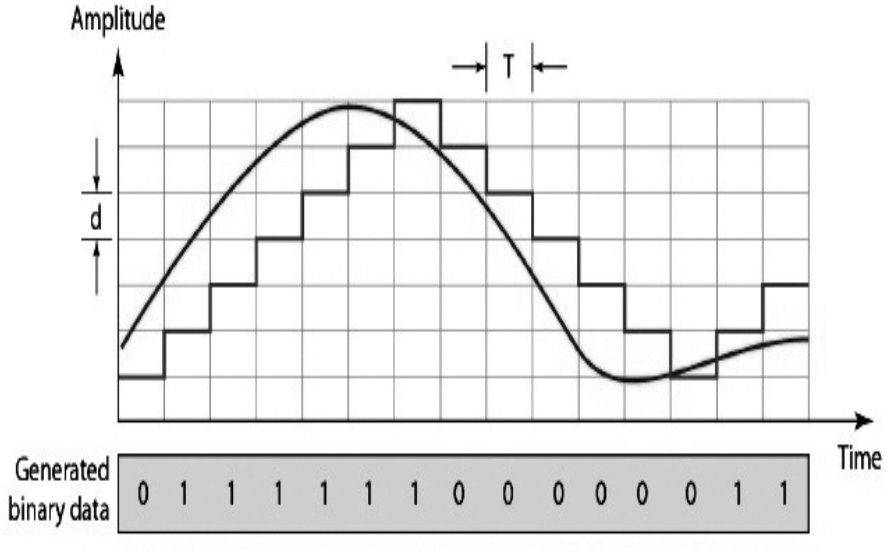


Figure 3.12: The process of delta modulation [9]

Analog data to analog signals: Analog modulation is the process of transferring an analog baseband (low frequency) signal over a higher frequency signal. In analog modulation, the amplitude of the carrier signal

is made to follow that of the modulating signal. Analog to analog conversion can be done in three ways: Amplitude, frequency and phase.

a) Amplitude Modulation

In AM transmission, the carrier signal is modulated as per the changing amplitudes of the modulating signal. The frequency and phase of the carrier remain the same; only the amplitude changes to follow variations in the information. This has been shown in Figure 3.13 below.

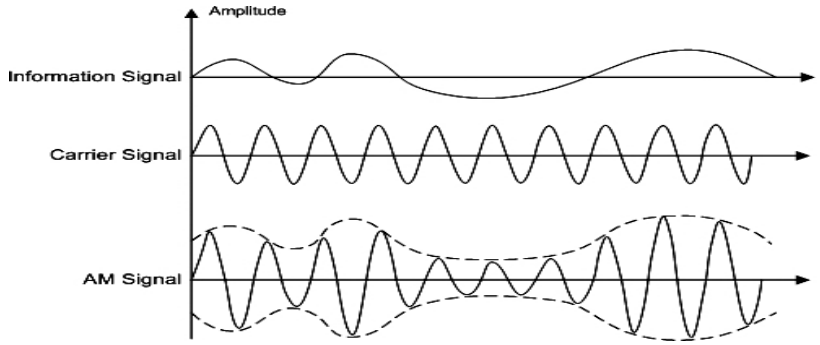


Figure 3.13: Amplitude Modulation [10]

b) Frequency Modulation

In FM transmission, the frequency of the carrier signal is modulated as per the changing in voltage level (amplitude) of the modulating signal. The peak amplitude and phase of the carrier signal remain constant that means information signal changes as per changes in frequency of the carrier. Figure 3.14 below shows the process of frequency modulation.

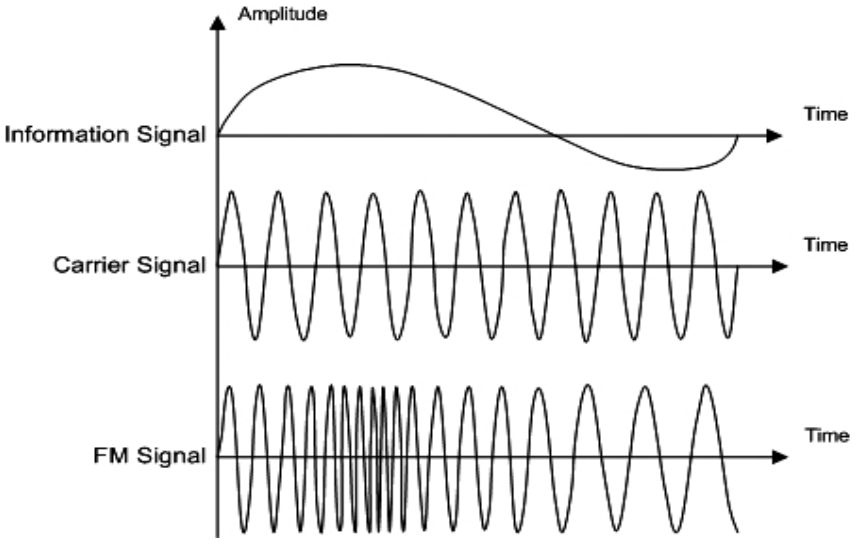


Figure 3.14: Frequency Modulation[10]

c) Phase Modulation

In PM transmission, the phase of the carrier signal is modulated to follow the changing voltage level (amplitude) of the modulating signal. The peak amplitude and frequency of the carrier signal remain constant, but as the amplitude of the information signal changes, the phase of the carrier changes correspondingly. Figure 3.15 shows the phase modulation technique.

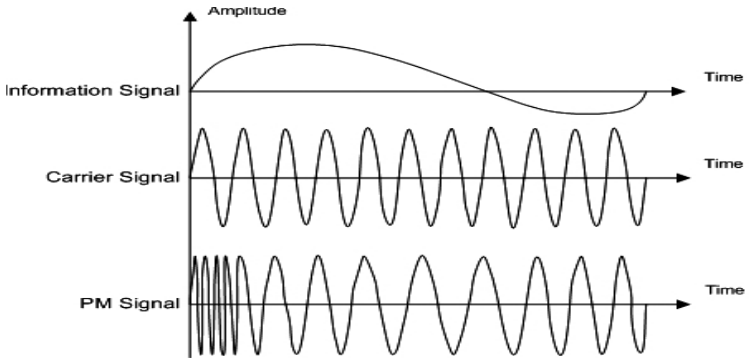


Figure 3.15: Phase modulation [10]

3.4 TRANSMISSION MODES [11]

How data is to be transmitted between two computers is decided by the transmission mode. For two devices connected by a transmission medium to interchange data, a high degree of co-operation is needed. Usually one bit of data is transmitted at a time. The bit transferring rate (timing, duration, and spacing) must be same for transmitter and receiver. The binary data in the form of 0s and 1s can be sent in two different modes: Serial and Parallel.

1. **Serial:** Bits are transported serially one after another. Only one communication channel is required for serial transmission as shown in Figure 3.16. It provides less bandwidth but is cheaper. It is suitable for long distance data transmission.

RECEIVER 0 1 1 1 0 1 0 1 SENDER

Figure 3.16: Serial Transmission

Serial transmission can be either asynchronous or synchronous as shown below.

a) Asynchronous Serial Transmission

In this transmission the importance of timing does not matter. Data-bits have definite arrangement and this assists receiver to recognize start and end data bits. For example, a 0 (start

bit) is attached at the beginning of every data byte and at the end one or more 1s (stop bits) are attached. There may be a gap between each byte. This gap can be represented either by an idle channel or by a stream of additional stop bits. The start and stop bits and the gap alert the receiver to the beginning and end of each byte and allow it to synchronize with the data stream.

b) Synchronous Serial Transmission

In this transmission there is no start and stop bits for the data recognition. Hence timing has a vital importance in synchronous transmission. In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits. The benefit of synchronous transmission is high speed, and there is no overhead of extra bits unlike asynchronous transmission.

For a receiver to determine the beginning or end of a data block, another level of synchronization is required. Here every block starts with a start code and ends with a stop code. These codes are also known as a flag bytes. Figure 3.17 shows how start code and stop code is introduced in a data block.

Start Code	Control Characters	DATA	Control Characters	Stop Code

Figure 3.17: Data block with start code and stop code

Data + control information is called a frame. Since any random bit pattern can be communicated, there is no guarantee that bit pattern for flag would not appear inside the frame. Hence it destroys synchronization of frame level. So to avoid this bit stuffing can be used.

In bit stuffing each frame begins and ends with a special bit pattern, 01111110. This pattern is a flag byte. Whenever the sender encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream. When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit.

2. ***Parallel:*** Separate parallel wires are used to transfer all bits of a byte simultaneously as shown in Figure 3.18. Over a large distance synchronization between multiple bits becomes difficult. Because the number of data lines is same as the number of bits in a frame, a complete data frame (group of bits) is sent at a time. The benefit of parallel transmission is high speed. It gives large bandwidth but is expensive. This type of transmission is preferred when devices are close to each other.

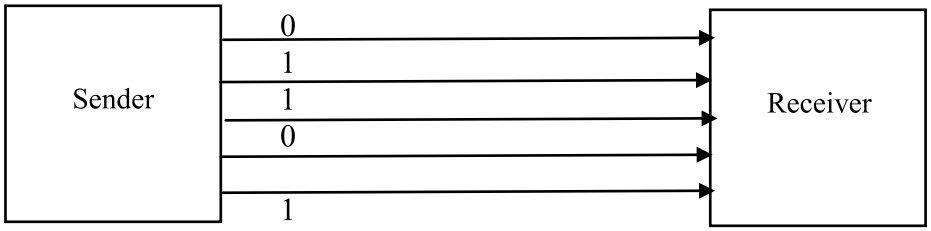


Figure 3.18: Parallel Transmission

CHECK YOUR PROGRESS

1. Suppose there is a channel with 10-MHz bandwidth. This channel has SNR of 63. What are the appropriate signal level and bit rate?
2. Transmission modes decide how data travels between two computers. Explain any one in detail.
3. Write short notes on NRZ, NRZ-L and NRZ-I, Pulse-code-Modulation and Frequency Modulation.
4. Write steps involved in Pulse Code Modulation.

3.5 TRANSMISSION IMPAIRMENTS [12]

In communications system, transmission media used by signals for travelling is not perfect. Signal distortion is caused due to this imperfection. This means that the signal in the medium is not same at the beginning when compared to signal at the end. The signal that is transmitted may differ from signal that is received due to various transmission impairments. For digital signals change in bit i.e. bit error may be introduced such that either a 0 is changed to a 1 or a 1 is changed to a 0. For analog signals, signal strength is degraded by these impairments. The major transmission impairments are:

Attenuation: It means loss of energy i.e. signal becomes weaker when it travels certain distance in a medium. Signal loses its energy overcoming the resistance of the medium. This loss of energy is compensated by using amplifiers that amplifies the signal. To show that a signal has lost or gained strength, the unit of the decibel is used. The decibel (dB) measures the relative strengths of two signals or one signal at two different points. The decibel is negative if a signal is attenuated and positive if a signal is amplified.

$$dB = 10\log_{10}(P_2/P_1) \text{ where } P_1 \text{ is input signal and } P_2 \text{ is output signal}$$

Distortion: When a composite signal travels through a medium, each signal component may arrive at the destination with a different delay

depending on its propagation speed. In other words, signal components at the receiver will have phases different from what they had at the sender. Therefore, the shape of the composite signal that is received is not same as that was sent.

Noise: For any data transmission event, the received signal will consist of the transmitted signal, modified by the various distortions. These distortions are enforced by the transmission system, plus supplementary undesired signals that are introduced somewhere between transmission and reception. Such unwanted signals constitute noise**.** Different types of noises are described below –

- Induced –Nearby devices behave as transmitter antenna and medium as receiving antenna. Example: from motors and appliances.
- Thermal –An extra signal created by random motion of electrons in the wire.
- Crosstalk –Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.
- Impulse - Spikes that are outcome of power lines, lightning, etc.

3.6 CHANNEL CAPACITY [13]

Channel capacity is defined as the maximum rate at which data can be communicated over a given communication channel or path, under given circumstances. It is affected by:

– The attenuation of a channel which varies with frequency as well as channel length.

– The noise added to the communication path that increases with distance.

– Because of clipping on the signal; a non-linear effect.

3.6.1. Nyquist Bandwidth

In an environment that is free of noise, the restriction on data rate is because of signal bandwidth. Nyquist formulates it as: if 2B is the rate of signal transmission then carrier signal frequency required to carry this data rate should not be greater than B. Vice versa is also true i.e. if bandwidth is B then the highest signal rate that can be transmitted is 2B.

Nyquist formulation becomes

$$C = 2B \log_2 M$$

where M = the number of voltage levels or discrete signal.

3.6.2. Shannon Capacity Formula

Nyquist formulation works in condition when there is no error in the communication system. But occurrence of noise can corrupt number of bits. On increasing the data rate, bits become "shorter" so more bits get affected by a given pattern of noise. Mathematician Claude Shannon formulated this based on concept of signal-to-noise ratio. Signal to Noise Ratio (SNR) represents the signal strength w.r.t the power of noise in the system. It is the ratio between two powers. It is usually specified in dB and referred as SNR_{dB}.

$$SNR = Signal\ Power/\ Noise\ Power$$

$$SNR_{dB} = 10\ log_{10}SNR$$

Shannon's uses this and result is that the maximum channel capacity, in bits per second, obeys the equation:

$$C = B\ log_2(1 + SNR)$$

where C is the channel capacity in bits per second and B is the channel bandwidth in Hertz.

3.7 TRANSMISSION MEDIA [14]

The function of physical layer is to transmit bits over the communication channel. Various types of physical media can be used and each one has its own role in terms of cost, delay, ease of installation and maintenance and bandwidth. They are roughly categorized into guided media, such as twisted-pair cable, coaxial cable and fiber-optic cable and unguided media, such as satellite, terrestrial wireless and lasers through the air.

3.7.1 Guided Media

a) Twisted Pair Cable

It is made up of two plastic insulated twisted (helical form) copper wires (thickness 1mm) that creates a single media as shown in Figure 3.19. One of these wires is used for ground reference and another wire carries actual signal. The turns between wires aids in minimizing noise (electro-magnetic interference) and crosstalk. Telephone system is the most common application of the twisted pair. They are used either to transmit digital or analog data. The bandwidth depends on the wire thickness and the distance traveled. Because of their low cost and adequate performance, twisted pairs are generally used.

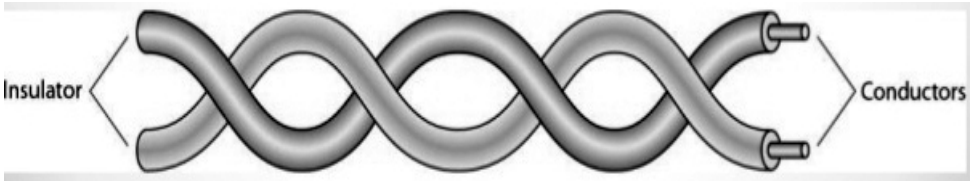


Figure 3.19: Twisted Pair Cables [14]

There are two kinds of twisted pair cables:

- Shielded Twisted Pair (STP) Cable: They are covered in metal foil that makes it more indifferent to crosstalk and noise.
- Unshielded Twisted Pair (UTP) Cable: UTP has seven classifications, each appropriate for specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. RJ45 connectors are used to connect UTP cables.

b) Coaxial Cable

Two copper wires are present in coaxial cables. The center is made up of solid conductor; the core wire. An insulating sheath is surrounded over the core. The second wire is wrapped around over the sheath and that too in turn enclosed by insulator sheath. Finally all this is covered by plastic cover as shown in Figure 3.20.

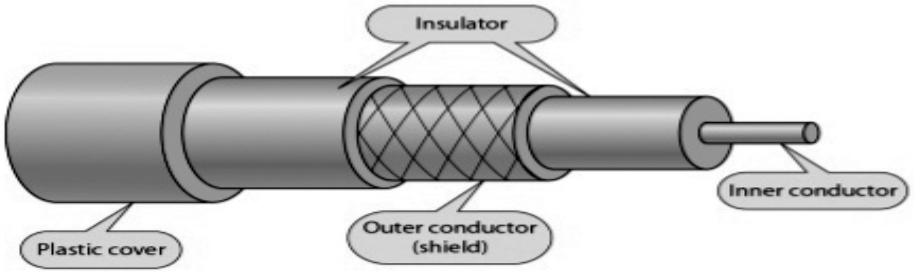


Figure 3.20: Coaxial Cables [14]

The shielding and construction of the coaxial cable gives it a good combination of excellent noise immunity and high bandwidth. The bandwidth possibly depends on the cable length and quality.

c) Fiber Optics

Reflection of light is the basic property used by fiber optics i.e. if the angle of incidence is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance. High quality plastic or glass is used to construct the core of fiber optic. Light is released from one side, which then travels through the fiber optics cable and reaches the other end. At the other side light detector is used that converts the detected light stream into electric data. Highest speed is achieved by fiber optics cable as compared to other guided media. It comes in two modes- **multimode** fiber and **single mode** fiber.

Multimode is capable of transporting multiple beams of light as shown in Figure 3.21a whereas single mode fiber can carry a single ray of light as shown in Figure 3.21b.

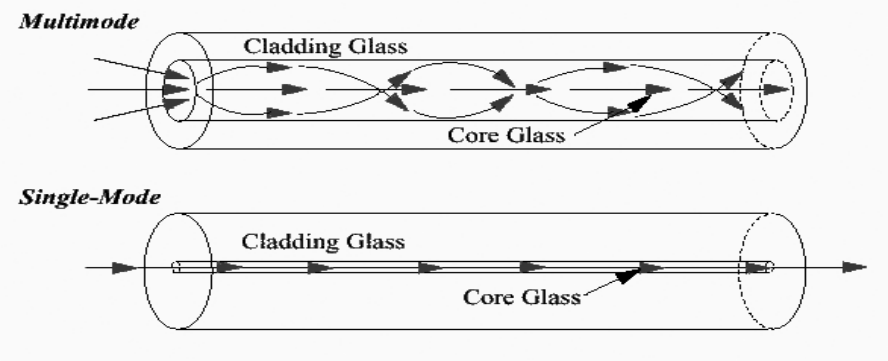
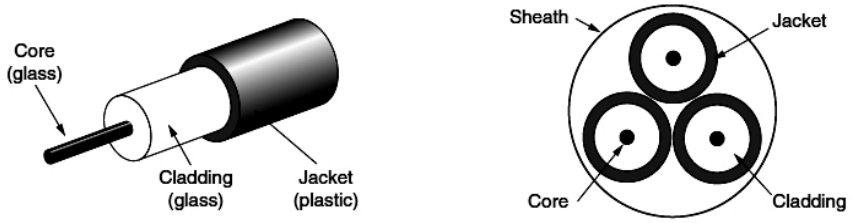


Figure 3.21: Fiber optics modes: a) Multimode b) single-mode [15]

Fiber optics is made up of a core enclosed by a glass cladding that has a lower refraction index in comparison of core that keeps all the light in the core. Next it has a thin plastic jacket to guard the cladding as shown in Figure 3.22 (a) and Figure 3.22 (b).Long-haul transmission uses the fiber optics in high-speed LANs (although so far, copper has always managed to catch up eventually), network backbones and high-speed Internet access. An optical transmission system has three main constituents: the light source, the detector and the transmission medium.



(a) (b)

Figure 3.22: Fiber optics (single mode) [16]

3.7.2. Unguided Media

Wireless Transmission is a form of unguided media. No physical link is involved for transmission between two devices. In this, antenna is used for transmission and reception. At sender's site electromagnetic energy are emitted into the medium (usually air)by antenna and receiver's site electromagnetic radiation waves are picked by antenna from the surrounding medium. For wireless transmission, there are fundamentally two types of configurations: directional and omnidirectional. For the directional configuration, a focused electromagnetic beam is transmitted by the transmitting antenna; hence the transmitting and receiving antennas must be cautiously aligned. In the omnidirectional case, many antennas can receive the transmitted signal spread out in all directions.

A small part of the electromagnetic spectrum (light, infrared, microwave and radio wave) is used for wireless transmission as shown in Figure 3.23.

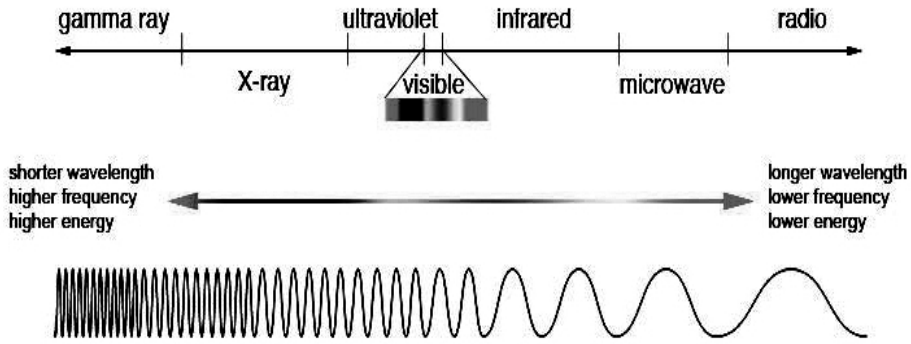


Figure 3.23: Electromagnetic Spectrum [17]

a) Radio Wave Transmission

Radio waves are widely used for indoor as well as outdoor communication because they can be generated easily and due to its larger wavelength can penetrate buildings. Radio waves are also omnidirectional, means from source they move in all directions. Hence, the transmitter and receiver do not have to be physically aligned. Radio waves can have wavelength from 1 mm – 100kms and frequency ranging from Extremely Low Frequency (3 Hz) to Extremely High Frequency (300 GHz).

Radio frequencies are further divided into 6 bands. Lower frequencies such as LF, MF, VLF bands can travel at an altitude of hundreds of kilometers over the earth's surface and can penetrate walls. Figure 3.24 (a) shows LF radio waves curvature. Whereas high frequency (HF) waves are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as VHF and HF bands are spread upwards. They are refracted back to the earth, when they reach Ionosphere as shown in Figure 3.24 (b).

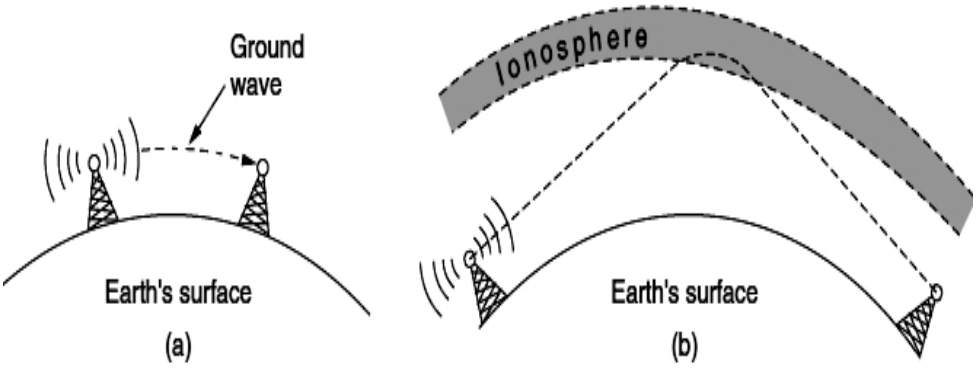


Figure 3.24: (a) LF radio waves follow curvature of earth, (b) HF bands bounce off the ionosphere [18]

b) Microwave Transmission

The waves above 100 MHz, travel in almost straight lines and can thus be narrowly focused. By means of parabolic antenna (like the familiar satellite TV dish) all the energy concentrated into a small beam which gives a much higher SNR (signal-to-noise ratio), but the transmitting and receiving antennas must be precisely aligned with each other as shown in Figure 3.25.

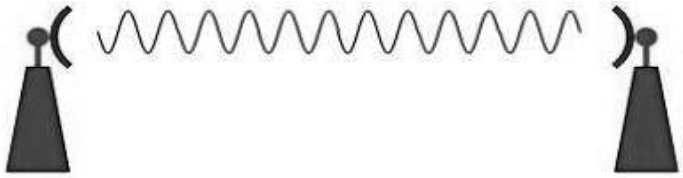


Figure 3.25. Microwave transmission [19]

The wavelength of microwaves ranges from 1 mm – 1 meter and frequency ranges from 300 MHz to 300 GHz. Microwave transmission highly depends on the climatic conditions and the frequency it is using.

c) Infrared Transmission

Mostly used for short range transmission and travels in straight line. The remote controls used on televisions, VCRs, and stereos all use infrared communication. Infrared wave ranges in between visible light spectrum and microwaves and has wavelength of 700 nm to 1 mm and frequency lies in the range from 300 GHz to 430 THz.

d) Light Transmission

Light transmission is achieved by using LASER. It tends to travel in straight line because it uses light frequency. Hence transmitter and receiver must be in line-of-sight as shown in Figure 3.26. Since laser transmission is unidirectional, for communication photo-detector and laser needs to be mounted at both ends. Laser beam is generally 1mm wide hence an accuracy is required to align two distant receptors each pointing to lasers source. Laser cannot penetrate obstacles and get distorted by atmosphere temperature, wind, or variation in temperature in the pathway.

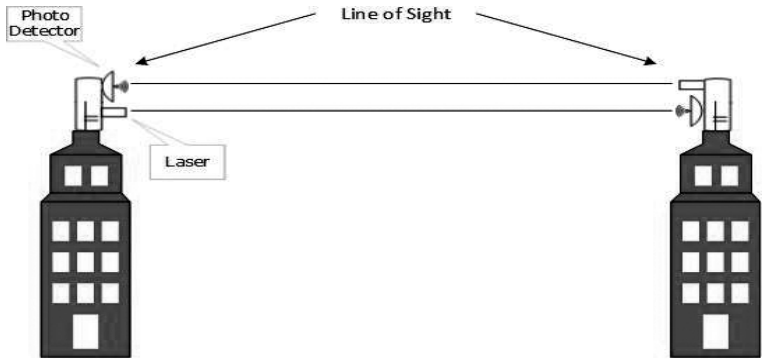


Figure 3.26: Light transmission [19]

CHECK YOUR PROGRESS

1. Differentiate between guided and unguided media.
2. Discuss about the channel capacity of communication path
3. If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700, and 900 Hz, what is its bandwidth? Draw the spectrum, assuming all components have a maximum amplitude of 10 V.

3.8 SUMMARY

This chapter summarizes the working of bottom most layer of the model- Physical Layer. For communication purpose the layer converts the received signal from analog to digital or vice-versa by using different data encoding techniques. Since physical layer takes care of data transmission physically therefore it uses different transmission media: guided media, such as fiber optics and copper wire, and unguided media, such as terrestrial satellite, wireless and lasers through the air for the transmission of data from machine to machine. While transmission there may be some impairment present in channel which can cause signal distortion. Thus the signal that is received by the receiver is not the same as what was transmitted by the sender.

3.9 TERMINAL QUESTIONS

1. Describe different services provided by physical layer.
2. What are the different transmission impairments that can affect the signals?
3. Distinguish between single-mode and multimode fiber optics.
4. Write short notes on different types of noise.
5. What are the propagation time and the transmission time for a 2.5 KB message if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 3×10^8 m/s.
6. If the peak voltage value of a signal is 20 times the peak voltage value of the noise, what is the SNR? What is the SNR_{dB}?
7. What is the Nyquist sampling rate for each of the following signals?

a. A low-pass signal with bandwidth of 200 KHz?

b. A band-pass signal with bandwidth of 200 KHz if the lowest frequency is 100 KHz?

8. A signal travels from point A to point B. At point A, the signal power is 100 W. At point B, the power is 90 W. What is the attenuation in decibels?

REFERENCES

[1] Behrouz A. Forouzan, Chapter 3, Data Communications and Networking (3rd Edition).

[2] Behrouz A. Forouzan, Chapter 4, Data Communications and Networking (4th Edition).

[3] http://autosystempro.com/analog-and-digital-principles/

[4]http://www.tmatlantic.com/encyclopedia/index.php?ELEMENT_ID=10420

[5]http://www.tmatlantic.com/encyclopedia/index.php?ELEMENT_ID=10422

[6] http://www.kprblog.in/cse/sem3/phase-shift-keying/

[7]https://www.tutorialspoint.com/data_communication_computer_network/digital_transmission.htm

[8] http://image.slidesharecdn.com/macsublayer-120315041525-phpapp01/95/mac-sub-layer-31-728.jpg?cb=1331785314

[9] https://sipdtdevelopers.wordpress.com/tag/quantization-process/

[10] http://pediaa.com/difference-between-analog-and-digital-modulation/

[11] http://becomeavictor.blogspot.in/2014/03/data-transmission.html

[12]http://ggnindia.dronacharya.info/ITDept/Downloads/QuestionBank%5COdd%5CIII%20sem/Lecture-7.pdf

[13] Behrouz A. Forouzan, Chapter 3, Data Communications and Networking (4th Edition).

[14] Behrouz A. Forouzan, Chapter 7, Data Communications and Networking (4th Edition).

[15] http://www.fiber-optic-equipment.com/what-is-singlemode-fiber.html

[16] Tanenbaum and Wetherall, Chapter 2, Computer Networks (5th Edition).

[17] http://imagine.gsfc.nasa.gov/science/toolbox/emspectrum1.html

[18] http://www.slideshare.net/ashvinisoni50/physical-communication-media-16109260

[19]https://www.tutorialspoint.com/data_communication_computer_network/wireless_transmission.htm

UNIT-4 ISDN AND SWITCHING TECHNIQUES

Structure

4.0 INTRODUCTION

This chapter describes different terminologies used in computer networks. The very first term explained in this chapter is MODEM i.e. made up from terms **mo**dulator and **de-m**odulator. Then because of slow working of MODEM another service is introduced known as ISDN services. It works on existing lines but at greater speed. Different switching techniques are used to transmit the information from source to destination. These techniques are circuit switching, message switching and packet switching. After coming across the data switching techniques, this chapter talks about the method how different data can be forwarded at same channel through time division multiplexing and frequency division multiplexing. At the end of this chapter, ATM method and X.25 packet switching protocol are explained.

The rest of the unit is organized as follows. Section 4.1 enlists the objectives of the unit. Section 4.2 describes the functioning of the MODEM. Section 4.3 talks about the services provided by ISDN. Section 4.4 explains the various switching techniques. Sections 4.5 and 4.6 discuss TDM and FDM methods respectively. Section 4.7 discusses the ATM and section 4.8 discusses X.25 packet switching. Section 4.9 summarizes the unit and section 4.10 closes the unit with an exercise for students.

4.1 OBJECTIVES

At the end of this unit, you should be able to understand:

- MODEM and its working procedure.
- ISDN and the services provided by it.
- Different switching techniques
- TDM and FDM methods
- ATM working
- X.25 packet switching technology

4.2 MODEM [1]

Modem is a terminology made from the terms modulator and demodulator. It is a device whose function is to translate the digital data stored in a computer into an analog signal so that it can be transmitted along a telecommunications channel. At the receiver site modem converts the analog signal back into machine readable form as shown in Figure 4.1. It basically modulates the signal at sender site and demodulates it at receiver site. The 'modulator-demodulator' or modem can be used to connect to an ISP or as a dial up for LAN.

The communication time taken by modem is relatively more as compared to other technologies like ISDN (Integrated Services Digital Network), cable and DSL (Digital Subscriber Line). For example the fastest modem available in market has a speed of 56 Kbps which is much slower than these technologies. Therefore modem is generally used while browsing through web pages or downloading small files. It is not suitable for downloading large files.

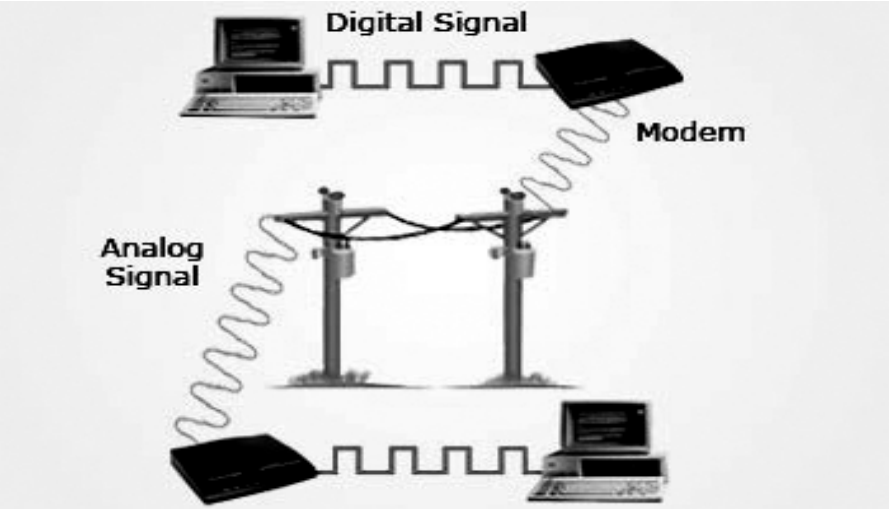


Figure 4.1: Modem translating the signals [2]

Modem can work as both an external device and an internal device. As an external device it connects to the serial port or the USB (Universal Serial Bus) port of a computer, or proprietary devices for handheld gadgets and other devices. As an internal device it works in the form of PC cards for laptops and Expansion cards for desktops (PC cards and Expansion cards are circuit boards that are placed inside laptops and desktops respectively to give extra facilities or memory).The configuration of an internal modem is different from an external modem.

Internal modem: Internal modems are usually cheaper then external modems. User is unaware of status of the modem directly.

External modem: The user is able to check the status of external modem with the help of status light or other sensor. Through this Internet connection status will be checked. In addition, because of the external power for the modem, less heat is created inside the computer. It also tends to be more expensive then internal modems.

4.3 ISDN SERVICES [3]

The set of digital transmission protocols defined by the ITU-T, an international standards body for telecommunications, is known as Integrated Services Digital Network (ISDN). Virtually every telecommunications carrier all over the world accepts these protocols as a standard for communication. It is a digital communication method that supports the conventional telephone system such that single line telephone wires becomes capable of carrying voice and data simultaneously that too at greater speed. But the difference between ISDN and telephone system is that ISDN is a fully digital network and not an analog network like the latter. The devices and applications in this network represent themselves in digital form. The information travels in the network in form of bits rather than waves. Figure 4.2 shows an example of an ISDN network.

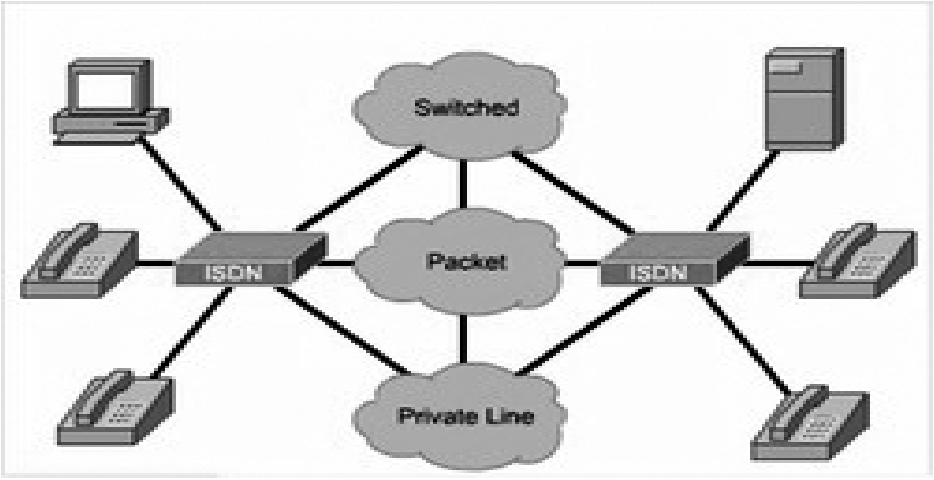


Figure 4.2 Example of ISDN network [4]

It basically handles data, voice, video, and images; everything that could ever be needed. It provides a single interface (in terms of both hardware and communication protocols) for fastening up computer, phone, videophone, fax machine, video-on-demand system, and our microwave. It is just a vision of how the future telephone network will look like. Applications include simultaneous voice, fax, data and e-mail, telecommuting, remote broadcasting, inexpensive videoconferencing and high quality audio transmission.

4.3.1 ISDN service levels

ISDN is supplied in two forms: Basic Rate and Primary Rate.

i) Basic Rate

- It is provided through **Basic Rate Interface (BRI)** also known as $\mathbf{S_0}$ Interface.
- Access to this type of network is called **Basic Rate Access (BRA)**.
- A BRI connection consists of two 64 Kbps **B-channels** and one 16 Kbps **D-channel**. Thus, a BRI delivers up to 128 Kbps of data.
- B-channels carry payloads (e.g., data or voice streams) and D-channels carry control and signaling information.
- Bit rate is chosen because existing telephone company wirings can carry baseband (digital) transmission at this speed.
- It is basically used for domestic purpose, small remote offices or telecommuters.

ii) Primary Rate

- **Primary Rate Interface** (PRI) is the interface through which Primary Rate is provided and is also known as $\mathbf{S_2}$ Interface.
- Access to this type of network is called **Primary Rate Access (PRA)**.
- In the United States, a PRI connection consists of 23 B-channels (1,472 Kbps total) and one 64 Kbps D-channel.
- In Europe a PRI connection consists of 30 B-channels (1,920 Kbps total) and 1 D-channel.
- To access this rate a high speed line installation is required at customer premises.
- It is typically used for fax servers, large remote access servers or PBXs (Private Branch Exchange) in medium sized or large offices.

4.3.2 ISDN Service types

ISDN provides two kind of services: Network Services and Bearer Services.

i) Network Services

- Interaction between the network and users is carried by network service. Example- setting up of calls and terminating them.
- It gives the definition of how the network and user interact with each other for call management.
- Users can use this service to make a request to network to perform the tasks like transferring calls to another user, making and clearing calls and so on.
- This activity is known as signaling.

ii) Bearer Services

- To carry data between two users, bearer services are used. For example- Encoding of fax or voice information in bit stream.
- It carries out all the user calling activity performed at a particular instant of time.
- There are two forms of this service: Structured data and unstructured data.

  a. ***Structured Data*****:** It is format in which information passing over bearer service can be understood by network at any point of time. Example: voice data

  b. ***Unstructured Data:*** It is the format that is only understood by the users at the either end and network is unable to understand it.

ISDN has two channel types – **Bchannel** and **Dchannel**. B channels carries the ISDN Bearer Services whereas D channel carries the ISDN Network Services.

4.4 SWITCHING

Switching is a process in which packets or frames are transferred across the network from source port to destination port. Switching approach resolves how switch will receive, process and forward the packets. There may be a number of nodes and switches in a communication network. Switching on basis of path can be divided into two classes: connection oriented and connectionless.

Connection Oriented: It is the technique in which before forwarding the packets towards destination, there should a pre-defined path or circuit between source and destination. This predefined path is then used to send frames. After data transmission the path can be immediately disconnected or may be kept for future use.

Connectionless: Forwarding tables are used to forward the data. No previous circuit is defined for communication and acknowledgements are optional in this.

4.4.1 Switching Methods [5]

Switching can be done in three ways: circuit switching, message switching and packet switching.

i) Circuit Switching

When the dedicated communication circuit is decided beforehand between two network nodes then it is known as circuit switching as shown in Figure 4.3. In this switching method, once a route is defined for communication, all the packets from the sender follow that route to reach to destination. Example: ordinary voice calling service. Before a user can make a call, a virtual circuit is established between the callee and the caller over the network. The circuit established may be temporary or permanent in nature. Applications that use circuit switching have to go through three phases:

1. Create a circuit for communication
2. Forward the data.
3. Disconnect/Terminate the circuit.

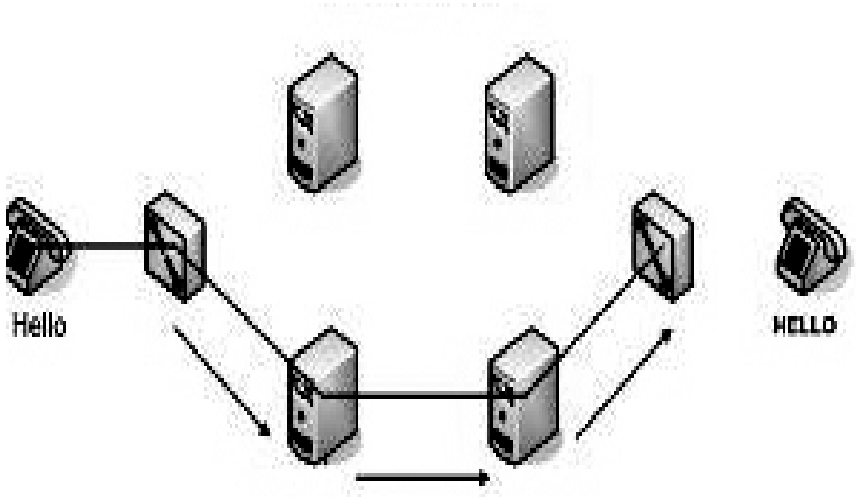


Figure 4.3 Circuit Switching for Voice Service [6]

ii) Message Switching

It is a method in which the message as a whole is treated as a single packet and sent to destination via number of intermediate nodes. For this communication there is no need to establish a path before communication. Message can follow any path to reach the destination as shown in Figure 4.4.

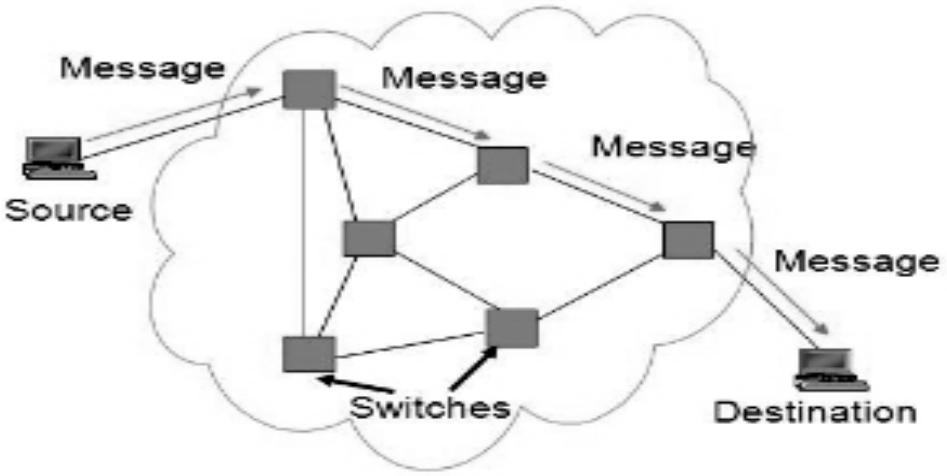


Figure 4.4 Message Switching [7]

Message switching uses the concept of store and forward to transfer the message. In this the switch receives the message and keeps it in buffer until it finds the next intermediate node to transfer the massage to. If there is not enough space in the next node to store the data as single unit, message is stored in the switch and switch waits. So, in this method the concept of time delay is introduced. It also requires a sufficient secondary storage capacity to store the incoming message, as it can be long.

This method can be treated as replacement of circuit switching. As in circuit switching the path established for communication between two nodes is kept blocked for any other communication. Still message switching also has drawbacks:

- Every intermediate switch should have enough memory to store the message as a whole.
- Message switching becomes slow because of store-and-forward technique and waits for the next node to become available.
- It is not the solution for the real time applications and streaming media.

iii) Packet Switching

Drawbacks of message switching gave birth to packet switching. The whole message is broken into small units called packets. Figure 4.5 shows the packet switching techniques. The information of switching is added to each packet in its header and forwarded as an independent unit.

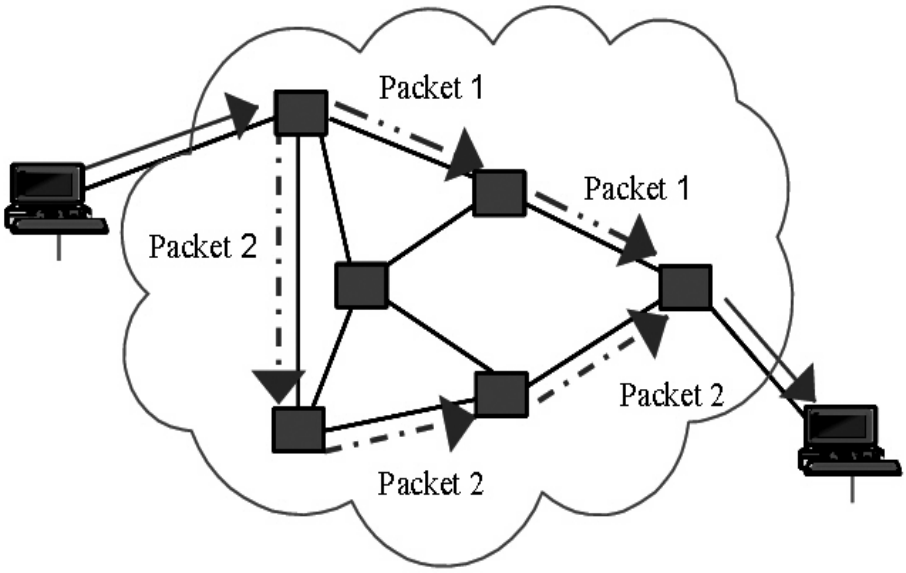


Figure 4.5 Packet Switching [8]

Now it becomes easier for intermediate nodes to store small size data in form of packets. Hence it doesn't require much resource either in form of internal node memory or on communication path. Internet uses packet switching technique. Packets of different applications can be multiplexed over carrier to enhance the efficiency of line. To provide quality of service, packets are stored and forwarded on basis of priorities allotted to them.

CHECK YOUR PROGRESS

1. What is MODEM and its drawback?
2. Differentiate between Circuit Switching and Message Switching.
3. You want to download files from a website. Which is more suitable for this – circuit switching or packet switching?

4.5 TDM (TIME DIVISION MULTIPLEXING)

Multiplexing is defined as a technique in which different signals or streams of information are processed together over the common transmission link. On the other hand de-multiplexing technique is used to retrieve the signals separately at receiver's site.

TDM is a type of multiplexing technique, generally applicable to digital signals but analog can also be used. The shared channel is divided on basis of time slots for the users. Every user can transmit the data in specified time slot only. Signals (digital) are divided into frames whose size is equivalent to time slots. Sender and receiver work in synchronized mode i.e. multiplexing and de-multiplexing are synchronized according to time. Multiplexer and de-multiplexer shift to next channel simultaneously.

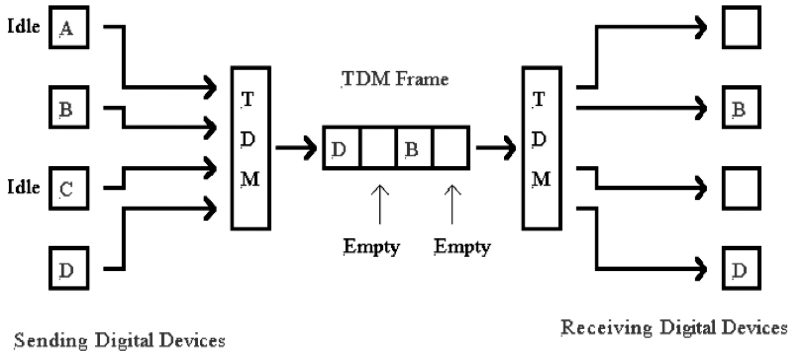


Figure 4.6 Time Division Multiplexing [9]

When a frame from channel B is transmitted at one end, then de-multiplexer at the other hand makes the media available to channel B. The moment time slot for channel B expires, multiplexer shifts to channel C. When the time slot for channel C expires, multiplexer shifts to channel D. On the other end, the de-multiplexer works in a synchronized manner and provides media to channel D as shown in Figure 4.6.

4.6 FDM (FREQUENCY DIVISION MULTIPLEXING)

FDM (Frequency Division Multiplexing) is also a type of multiplexing technique. FDM divides the spectrum bandwidth into logical channels of different frequency bands and assigns one channel to each user. Each user has an exclusive access to that channel and can use its frequency independently for transmitting the data. Channel division is done in such a manner that they do not overlap with each other. Small guard bands are used to separate the channels from each other. These guard bands are not used by any channel. Figure 4.7 shows how the spectrum is divided into separate frequency bands.

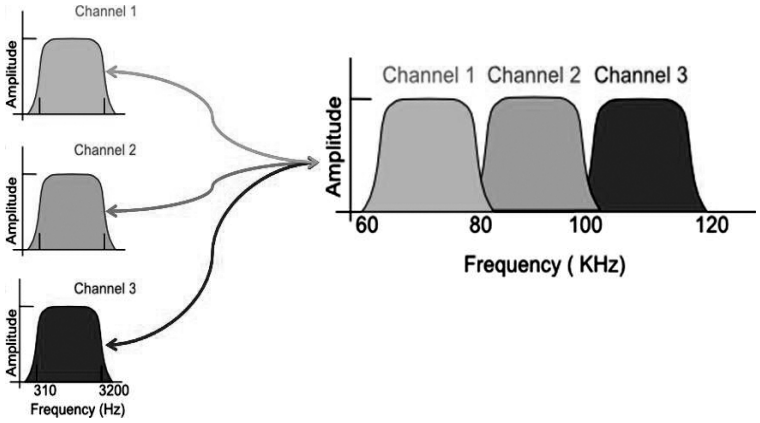


Figure 4.7: Frequency Division multiplexing [10]

4.7 ATM (ASYNCHRONOUS TRANSFER MODE) [11]

The ATM (Asynchronous Transfer Mode) enables a single data networking standard to be used for both packet-based networking and asynchronous channel networking. Multiple levels of quality of service for packet traffic are supported by asynchronous transfer mode**.** **A**synchronous transfer mode supports both packet-switched networks and circuit-switched networks by mapping both packet-streams and bit-streams. It not only includes standards for Layer 1, but also for Layer 2 and Layer 3. ATM handles all kind of information i.e. data, voice, text, image, and video and that too in an integrated manner. ATM gives a good bandwidth and can be used efficiently in LAN and WAN networks.

4.7.1 ATM Devices

There are two basic devices in an ATM system - ATM switch and ATM end point.

- ***ATM switch***: This receives the incoming packets (information) from other ATM entity (either ATM end point or ATM switch). It reads and updates the packet header information and forwards the information packet towards its destination.
- ***ATM end point****:* It is the device that contains the ATM network interface adaptor. This adaptor enables data entering or leaving from the ATM network to interface to the external world. Examples of these end points include LAN switches, workstations, video codecs etc.

4.7.2 ATM Virtual Connections

An ATM system has two types of connection as shown below:

- ***Virtual Channel Connection:*** In ATM, both endpoints are connected a virtual channel (VC), also called virtual circuit. It then sends a series of data frames which is known as cells.
- ***Virtual Path Connection:*** It is the combination of virtual channel connections. It is the end to end connection that routes all cells across the network through the same virtual path irrespective of the individual virtual channel connections. This makes the transfer fast.

4.7.3 ATM Cell format

ATM transfers information in fixed-size units called cells. Each cell consists of 53 bytes. The first 5 bytes contain cell-header information,

and the remaining 48 contain the payload (user information). Small, fixed-length cells are well suited to transferring voice and video traffic because such traffic is intolerant of delays that result from having to wait for a large data packet to download, among other things.

An ATM cell header can be one of two formats: UNI (User-Network Interface) or NNI (Network-Network Interface). The UNI header is used for communication between ATM endpoints and ATM switches in private ATM networks. The NNI header is used for communication between ATM switches. Figure 4.8 below shows an ATM cell, ATM UNI cell and ATM NNI cell.

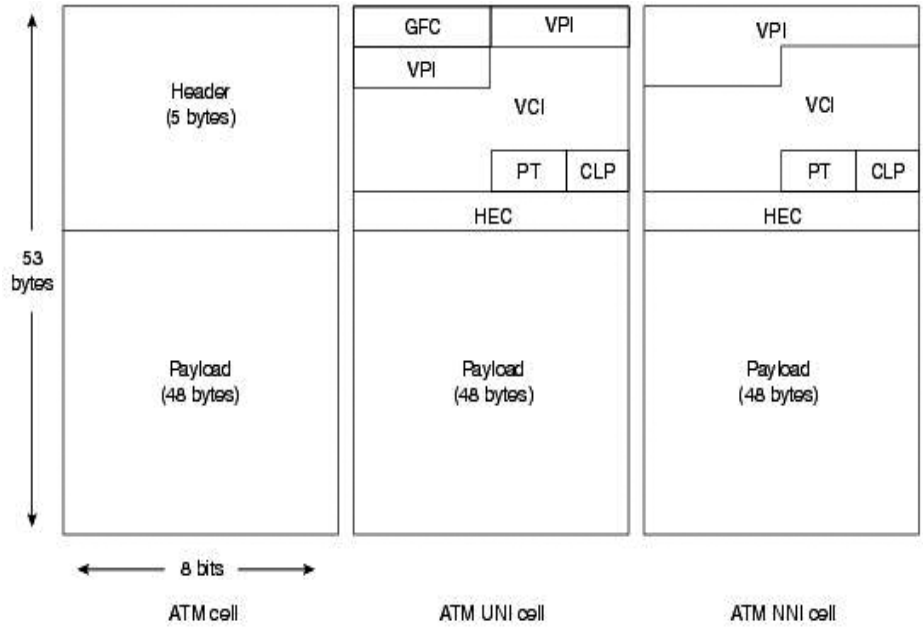


Figure 4.8: ATM cell, ATM UNI cell and ATM NNI cell [11]

Unlike the UNI, the NNI header does not include the Generic Flow Control (GFC) field. Additionally, the NNI header has a Virtual Path Identifier (VPI) field that occupies the first 12 bits, allowing for larger trunks between public ATM switches.

ATM Cell Header Fields

In addition to GFC and VPI header fields, several others are used in ATM cell header fields. The following descriptions summarize the ATM cell header fields illustrated in the above figure:

- ***Generic Flow Control*** (GFC) –GFC identifies multiple stations connected to a single ATM interface. This field is typically not used and is set to its default value of 0 (binary 0000).

- ***Virtual Path Identifier*** (VPI) - It identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.
- ***Virtual Channel Identifier*** (VCI) - In conjunction with the VPI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.
- ***Payload Type*** (PT) – It helps to identify user data or control data with help of first bit of PT. If the cell contains user data, the bit is set to 0. If it contains control data, it is set to 1. The second bit indicates congestion (0 = no congestion, 1 = congestion), and the third bit indicates whether the cell is the last in a series of cells that represent a single AAL5 frame (1 = last cell for the frame).
- ***Cell Loss Priority*** (CLP) –During congestion cells are being discarded. However, cell with CLP bit equals 1, will be discarded in preference to cells with the CLP bit equal to 0.
- ***Header Error Control*** (HEC) - Calculates checksum only on the first 4 bytes of the header. HEC can correct a single bit error in these bytes, thereby preserving the cell rather than discarding it

4.7.4 ATM Reference Model

The ATM architecture uses a logical model to describe the functionality that it supports. ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model as shown in Figure 4.9.

The ATM reference model is composed of the following planes, which span all layers:

- **Control -** This plane is responsible for generating and managing signaling requests.
- **User -** This plane is responsible for managing the transfer of data.
- **Management** - This plane contains two components:
  - **a.** Layer management manages layer-specific functions, such as the detection of failures and protocol problems.
  - **b.** Plane management manages and coordinates functions related to the complete system.

The ATM reference model is composed of the following ATM layers:

- ***Physical layer*** –It is similar to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission.
- ***ATM layer*** –ATM layer works like data link layer of the OSI reference model. The ATM layer is responsible for the simultaneous sharing of virtual circuits over a physical link (cell multiplexing) and passing cells through the ATM network (cell

relay). To do this, it uses the VPI and VCI information in the header of each ATM cell.

- ***ATM adaptation layer (AAL)*** - Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model. The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes. The adaptation layer prepares user data for conversion into cells and segments the data into 48-byte cell payloads.

Finally, the higher layers residing above the AAL accept user data, arrange it into packets, and hand it to the AAL.

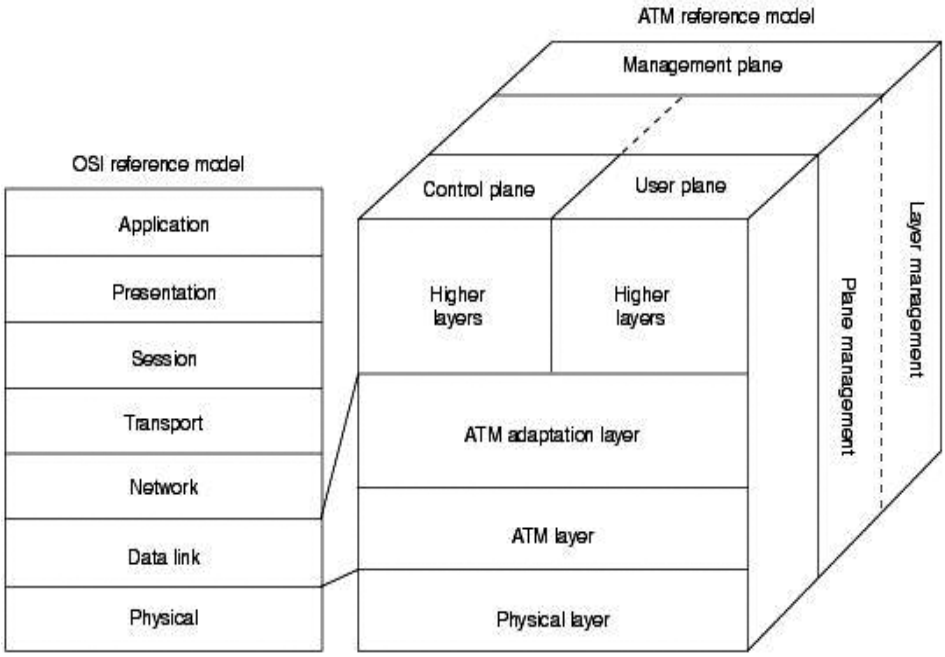


Figure 4.9: ATM Reference model [11]

4.8 X.25 PACKET SWITCHING

Remote devices communicate with each other on high speed digital links without the cost of individual leased lines through **X.25 Packet Switched networks.** Packet Switching routes individual packets based on addressing present in each packet to distinct destinations. The protocol X.25 is for first three layers of OSI Model: Physical Layer (Layer 1), Data Link Layer (Layer 2) and Network Layer (Layer 3). The devices of X.25 network is categorized into three types: **DTE (Data Terminal Equipment), DCE (Data Circuit-terminating Equipment), and PSE (Packet Switching Exchange)** as shown in Figure 4.10.

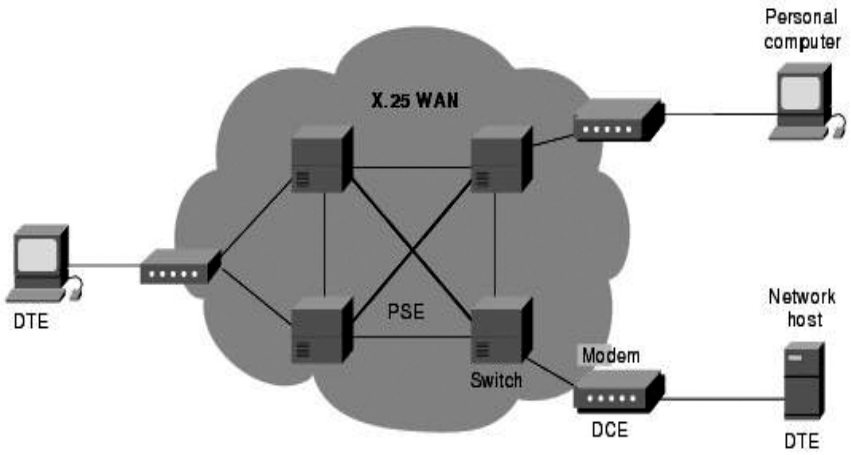


Figure 4.10: X.25 components and connection [12]

DTEs are basically the end systems (terminals, network hosts, personal computers) that communicate across the X.25 network. DCEs are devices that provides interface and communicates between DTE devices and a PSE, such as a switch or a modem. PSEs are switches that comprise the majority of the carrier's network. To establish the connection two logical channels are used: Permanent Virtual Circuits and Switched Virtual Circuits.

- ***Permanent virtual circuits (PVCs)***: Packet Switched Network administration establishes a permanent logical connection known as PVC. Hence, without any call setup mechanism, data may always be sent over this connection.
- ***Switched virtual circuits (SVCs)***: For SVCs first establishes a connection, then transmits the data and after that terminates the connection. A unique address is assigned to each DTE on the network. Example is telephone calls where each user is assigned a different telephone number.

4.8.1 X.25 Protocol Suite

ITU (International Telecommunications Union) organization develops the X.25 and maps it to bottommost three layers of the OSI reference model as shown in Figure 4.11 below. The layers description is as follows:

a. **Physical layer:** It deals with signaling or electrical waves. The main concern is on physical interface that attaches computer terminal with links that binds the computers to packet switching node. The standard called X.21that provides physical-level specification is used by X.25.

b. **Frame layer:** It enables a reliable transfer of data in form of sequence of frames across the physical link. It uses a standard

called LAPB (Link Access Protocol Balanced) which is a bit oriented protocol and subset of HDLC for link level transfer.

c. **Packet layer:** It facilitates two DTEs to have an end-to-end connection between them. It gives a virtual circuit service. PLP (Packet Layer Protocol) is the protocol used at this layer. Following functions are performed by this service:

- ❖ Establishes a connection between DTEs.
- ❖ Allows transmission of data in form of packet on external virtual circuits.
- ❖ Terminates the connection
- ❖ Controls the flow and checks the error in data.

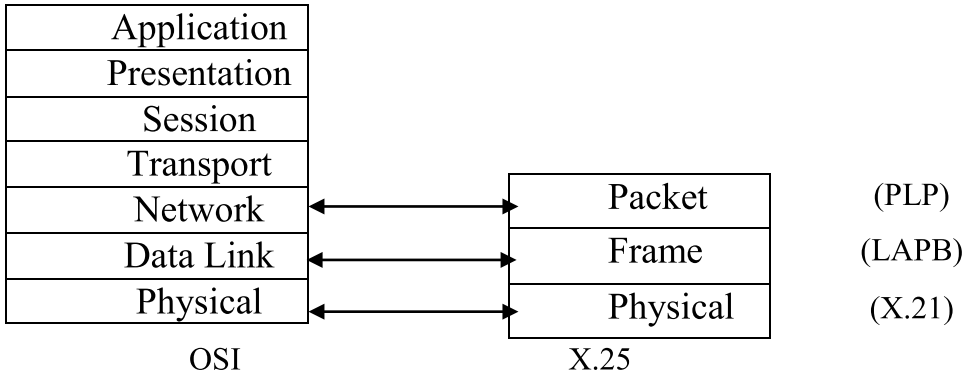


Figure 4.11: X.25 layer mapping with OSI model

4.8.2 X.25 PLP modes

There are five phases in PLP (Packet Layer Protocol): call setup, data transfer, idle, call clearing, and restarting. Figure 4.12 shows the call setup, data transfer and call release phases in X.25.

Call setup phase

It forms SVCs between DTE devices. To set up the virtual circuit, PLP usesX.121 addressing mechanism. To connect to remote DTE on SVC, calling DTE sends a **Call Request** packet. This packet includes the address of the remote DTE, address of sender DTE, and some other information. The remote DTE can accept or reject the call based on packet information. **Call Accepted** packet is issued if call is to be accepted, otherwise a **Clear Request** packet is issued. The virtual circuit is formed and transfer of data starts as soon as sender DTE gets the Call Accepted packet.

Data transfer

In this mode, data is transferred between two DTE devices over virtual circuit. Here, PLP manages error and flow control, bit padding, segmentation and reassembly. This mode works with both PVCs and SVCs and on per-virtual-circuit.

Idle mode

This mode is utilized when there is absence of data transfer over established virtual circuit. It works only with SVCs and on per-virtual-circuit.

Call clearing mode

This mode terminates the session of communication between two DTE devices and closes the SVCs. This mode works only with SVCs and on a per-virtual circuit. If one of the DTE requests for call termination, a packet called **Clear Request** is sent to other DTE, which then replies with a packet called **Clear Confirmation**.

Restarting mode

The transmission between locally connected DCE device and a DTE device is synchronized using this mode. This mode does not work on a per-virtual-circuit basis. The virtual circuits established by DTE device's gets affected by this mode.

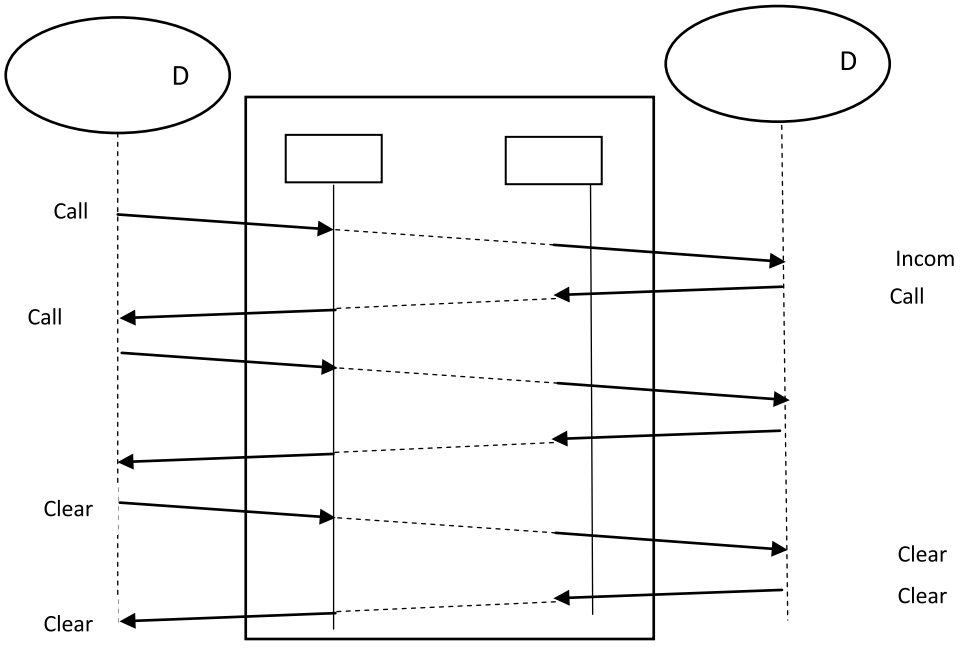


Figure 4.12: Call setup, data transfer and call release phases in X.25

CHECK YOUR PROGRESS

1. What is de-multiplexing? Distinguish between TDM and FDM.
2. Draw the cell format of ATM for UNI and NNI.
3. Differentiate between Structured and Unstructured data in ISDN Services.

4.9 SUMMARY

This chapter gives an overview of different technologies like MODEM and ISDN Services. It describes the basic working of these technologies and what protocols can be used to implement them. Switching is another method through which packets are delivered from source to destination. It can be of three types' circuit, message and packet switching. Message switching is designed to overcome flaws of circuit switching. And packet switching is the advanced version of message switching with the difference that message is divided into packets before forwarding to destination. X.25 packet switching technology makes transmission of data faster. TDM and FDM are the types of multiplexing techniques used to transmit different data on same channel. And ATM is a technology that supports both packet based networking and synchronous channel networking.

4.10 TERMINAL QUESTIONS

1. What are the different types of services that ISDN provides?
2. What are the benefits of Packet Switching over Message Switching?
3. Explain ATM.
4. Name the different devices of X.25. Also explain the types of connection used in X.25.
5. Briefly describe the packet switching with a diagram.
6. Classify the switching method on basis of path establishment. Also explain them.
7. Is message switching suitable for real time applications? Justify your statement.
8. How many virtual connections can be defined in a UNI? How many virtual connections can be defined in an NNI?
9. Are MODEMs suitable for downloading large files? Justify your statement.

REFERENCES

1. http://gonda.nic.in/swangonda/pdf/0789732556.pdf
2. http://www.wonderwhizkids.com/modems
3. http://mars.merhot.dk/mediawiki/images/6/69/ISDN_Overview.pdf
4. http://www.kariyerdersleri.com/bilgisayar%20ana%20klasor/network%20sayfalari/isdn-nedir-ozellikleri-nelerdir.aspx
5.]https://www.tutorialspoint.com/data_communication_computer_network/ physical_layer_switching.htm
6. http://www.gridgit.com/post_voip-network-diagram-wan_290758/
7. http://www.allsyllabus.com/aj/note/Computer_Science/Computer%20Networks%20-%20II/Unit1/Datagram%20and%20Virtual%20Circuits.php
8. http://www.allsyllabus.com/aj/note/Computer_Science/Computer%20Networks%20-%20II/Unit1/Datagram%20or%20 Connectionless%20Packet%20Switching.php
9. http://www.gordostuff.com/2011/11/digital-multiplexing-time-division.html
10. http://computernetworkingsimplified.com/physical-layer/overview-channel-multiplexing-techniques/
11. http://docwiki.cisco.com/wiki/Asynchronous_Transfer_Mode_Switching
12. http://docwiki.cisco.com/wiki/Frame_Relay

Uttar Pradesh Rajarshi Tandon
Open University

Bachelor of Computer Application

BCA-1.13
Computer Network

Block

2

Link Layer Issues and Access Protocols

Course Design Committee

Dr. Ashutosh Gupta — **Chairman**
Director (In-charge)
School of Computer & Information Sciences
UPRTOU, Prayagraj

Prof. R. S. Yadav — **Member**
Department of Computer Science and Engineering
MNNIT-Allahabad, Prayagraj

Ms Marisha — **Member**
Assistant Professor (Computer Science)
School of Science, UPRTOU, Prayagraj

Mr. Manoj Kumar Balwant — **Member**
Assistant Professor (Computer Science),
School of Sciences, UPRTOU, Prayagraj

Course Preparation Committee

Dr. Maheshwari Prasad Singh — **Author**
Assistant Professor, Department of CSE
NIT Patna

Dr. Rajiv Mishra — **Editor**
Associate Professor, Department of CSE
IIT Patna

Dr. Ashutosh Gupta (Director in Charge)
School of Computer & Information Sciences
UPRTOU, Prayagraj

Mr. Manoj Kumar Balwant — **Coordinator**
Assistant Professor (Computer Science),
School of Sciences, UPRTOU, Prayagraj

ISBN : 978-93-83328-18-5

Printed and Published by Dr. Arun Kumar Gupta Registrar, Uttar Pradesh Rajarshi Tandon Open University, 2019.

Printed By: Chandrakala Universal Pvt. Ltd. 42/7 Jawahar Lal Neharu Road, Prayagraj.

BCA-1.13/80

BLOCK INTRODUCTION

This is the second block on Link Layer Issues and Access Protocols. As name of this block indicate that this block will introduce the concept of how media access is being controlled. This block has four units namely, Data Link Layer, Multiple Access Protocol, The Medium Access Sub Layer and network devices. We will begin the first unit on data link layer. This unit presents functions of data link layer like error detection and correction. Different protocols namely, Simplex Stop and wait protocols, One bit sliding window protocol, Using Go-Back N have been discussed in details. You will also understand Flow control, Channel Allocation Problem. The second unit mainly discuss different kind of protocols like ALOHA, CSMA protocol, Collision Free protocol. It also discusses Polling technique along with FDM, TDM. In the third unit, Static and Dynamic Channel Allocation in LANs and MANs are being discussed. This unit discussed IEEE Standard 802.3, and Ethernet IEEE standard 802.4 and token Ring, IEEE Standard 802.5, Token Bus in details. In the last, the fourth unit introduces different types of network devices Hub, Bridges, Switch, Gateways, and Routers. This unit tells about working of these networking devices in details. It also presents disadvantages and advantages of these devices. As you study the material, you will understand the concept with the help of figures, tables, wherever required. Each unit has been describes using many sections. Every unit has summary and review questions in the end. These questions will help you to review yourself.

UNIT – 5 DATA LINK LAYER

Structure

5.0 INTRODUCTION

Data Link Layer (DLL) lies above the Physical layer in the OSI model. The basic work of Data Link Layer is framing, flow control, error control, addressing and media access control. It divides the stream of bits received from upper layer (Network Layer) into small units called frames. Next a header is added to each frame that contains the sender as well as the receiver address of the frame. If the rate at which receiver absorbs data is less than the rate at which sender produces data then DLL uses a flow control method to control the dataflow. DLL also adds mechanisms to detect and resend duplicate, damaged or lost frames. If two or more devices are using the same medium for communication then DLL decides which device should access the medium at a given time.

The rest of the unit is organized as follows. Section 5.1 enlists the objectives of the unit. Section 5.2 discusses various methods to detect and correct errors. Section 5.3 shows the classification of DLL protocols. Sections 5.4 and 5.5 analyze the DLL protocols that operate in noiseless and noisy channels respectively. Section 5.6 explains the features of static and dynamic channel allocation. Section 5.7 captures the summary of the unit and section 5.8 concludes it with an exercise for the students.

5.1 OBJECTIVES

After the end of this unit, you should be able to understand:

- Error detection and correction mechanisms

- DLL protocols that operate in Noiseless channels
- DLL protocols that operate in Noisy channels
- Static and dynamic channel allocation

5.2 ERROR DETECTION AND CORRECTION [1]

Whenever a bit flows from one location to another, it is subject to unforeseeable changes due to interference. Interference can cause a change in the shape of the signal. In a single bit error, just one bit is altered during transmission of a data unit (either a 0 is changed to a 1 or a 1 is changed to a 0). On the contrary, in a burst error, multiple bits are changed at a time.

Single-Bit Error

The term single-bit error means that only one bit of a data unit is changed from 0 to 1 or from 1 to 0. Figure 5.1 shows how a single-bit error affects a data unit. The bit in position 3 which was 0 originally, has changed to 1 during transmission, as can be seen below.

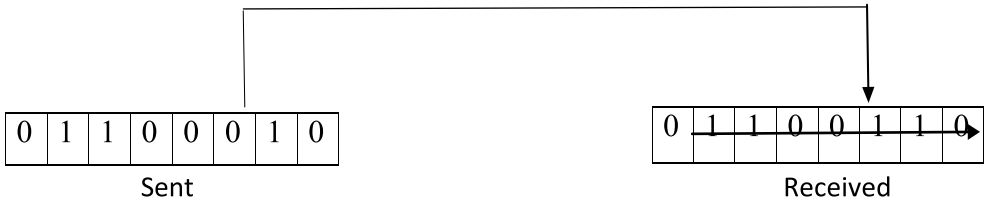


Figure 5.1: Single-Bit Error [1]

Burst Error

In burst error, 2 or more bits in the data unit change from 0 to 1 or from 1 to 0. The length of the burst is calculated from the initial corrupted bit to the final corrupted bit. Figure 5.2 shows such a scenario where a burst error has affected a data unit. All the bits in a burst error may not necessarily be corrupted as has been shown below.

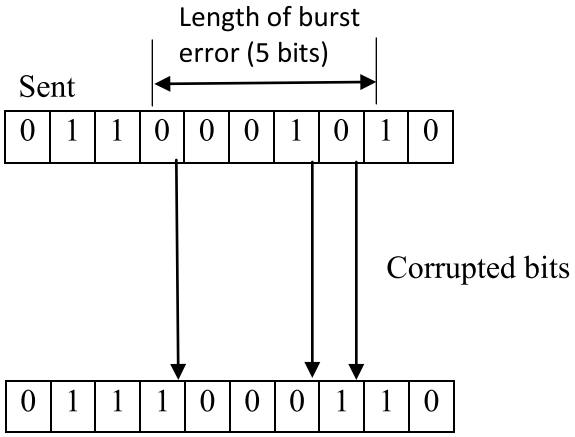


Figure 5.2: Burst error of length 5[1]

Error Detection

As explained above, data units are prone to unpredictable changes during transit. Error detection mechanisms are employed to look for such changes in data units that arrive at the receiver side. There are basically three error detecting mechanisms as shown in Figure 5.3 below.

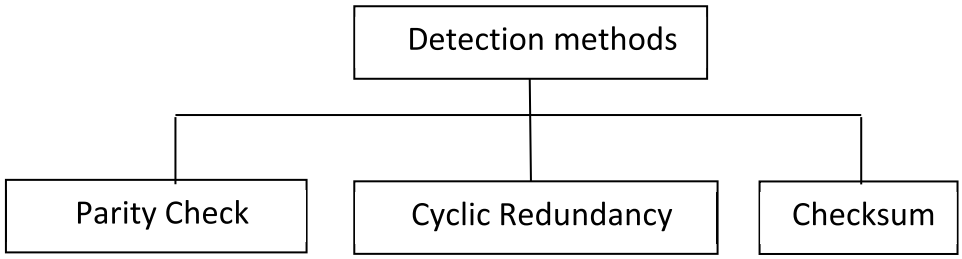


Figure 5.3: Error Detection methods [1]

Parity Check

Parity Check is the most common and the least expensive method for error detection. Parity checking can be either simple or two-dimensional as explained below.

Simple Parity Check

In this method, an extra bit, called a parity bit, is added to the end of each data unit so that the total number of 1s in the data unit (along with the parity bit) becomes even (or odd).

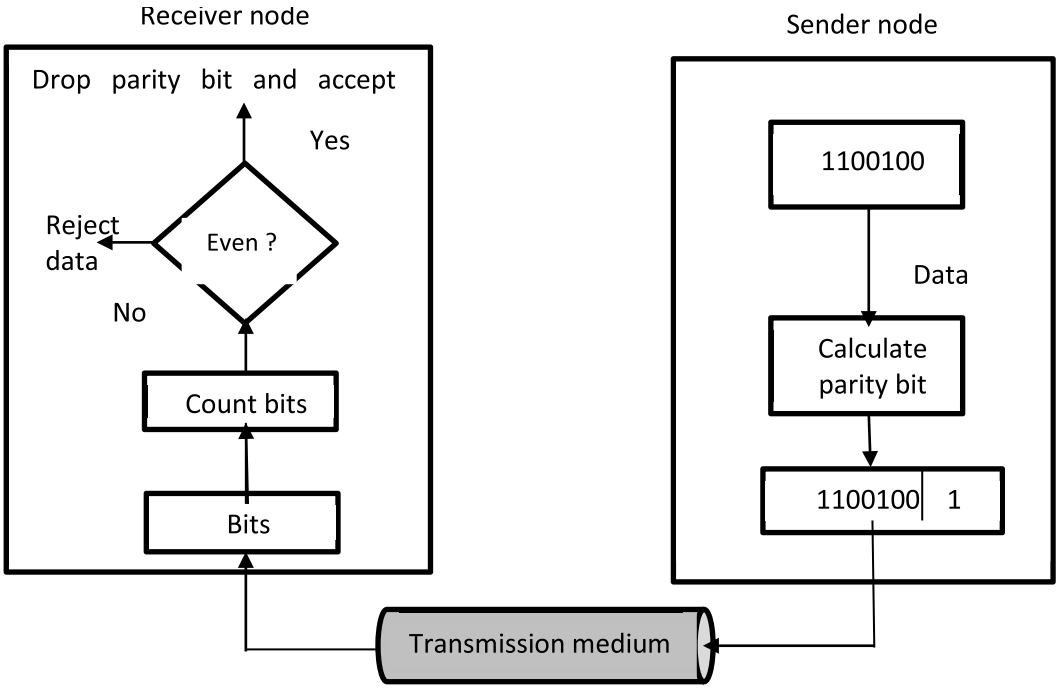


Figure 5.4: Even-parity concept [1]

As shown in the Figure 5.4 above sender node passes the 7 bit data to the parity generator. It counts three 1s and appends the parity bit (1 in this case) to the end. The total number of 1s now becomes 4. The whole data (8 bits now after adding the parity bit) is sent to the receiver. Parity checker on the other side counts four 1s, an even number, and the data unit passes. If the data is modified during transit and the receiver counts odd number of 1s then received data unit is rejected. In some cases odd-parity checking may also be used, where the number of 1s (including the parity bit) should be odd.

Two-Dimensional Parity Check

In this method data units are arranged in a two-dimensional array. The original data in Figure 5.5 below consists of four data units. First the parity bit is calculated for each data unit. Then all the data units along with their parity bits are organized into a table. Next parity bit is calculated for each column. This gives us a new row (column parities) as shown below.

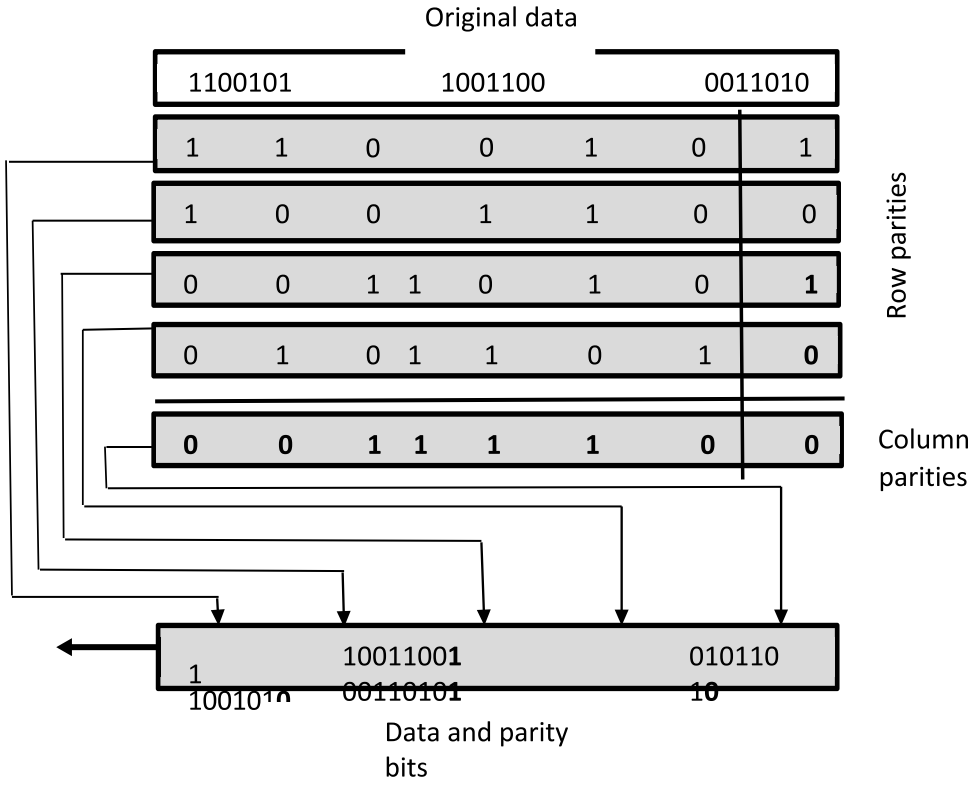


Figure 5.5: Two-dimensional parity [1]

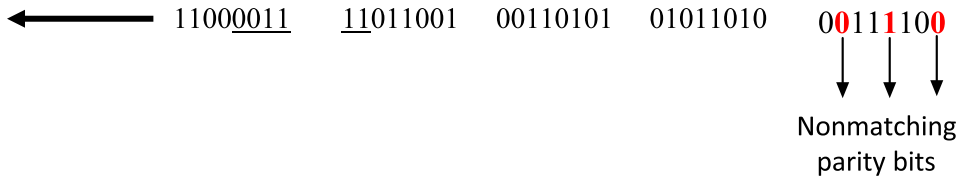
Suppose the last block generated above is sent to the receiver.

← 11001010 10011001 00110101 01011010 00111100

However a burst noise of length 6 hits the block and some bits become corrupted.

← 11000011 11011001 00110101 01011010 00111100

When the receiver examines the parity bits, some of them do not obey the even parity rule. Therefore the complete block is rejected. The nonmatching parity bits have been shown below.



Cyclic Redundancy Check

Cyclic Redundancy Check (CRC) works on the basis of binary division. First a string of n 0s is appended to the end of the original data unit. The resulting data unit is now divided by a predetermined binary number which is n+1 bits long. The remainder, called CRC is n bits long. It is appended to the end of the original data unit (replacing n 0s added previously) and sent to the receiver as shown in Figure 5.6 below.

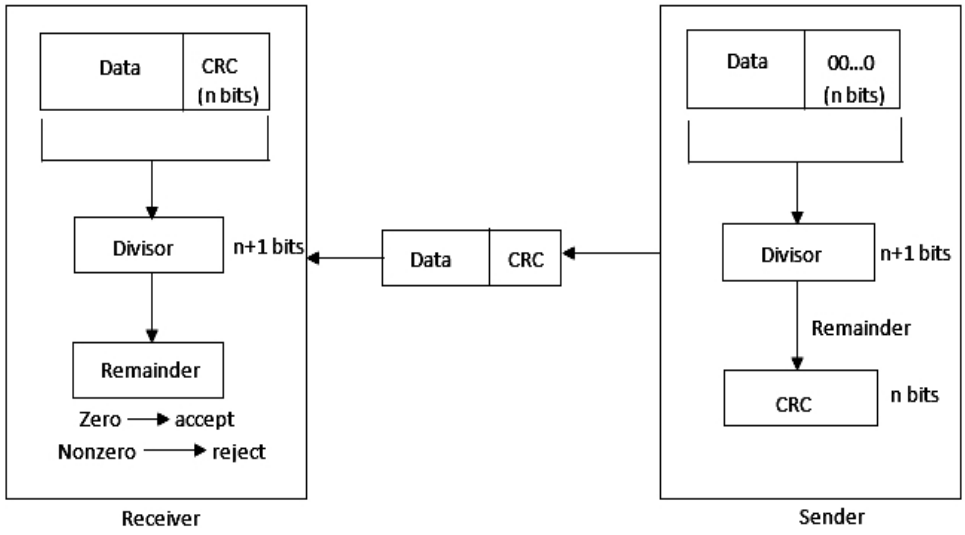


Figure 5.6: CRC generator and checker [1]

On the receiver side the whole string is treated as a single unit and divided by the same divisor. If the string has arrived without any changes then the remainder generated is zero. In such a case the data unit is accepted. If the string has arrived with one or more changes, the division produces a nonzero remainder and the data unit is rejected.

Suppose 100100 is the original data unit and 1101 is the predetermined 4 bit divisor. Next three 0s are appended to the end of data unit and the resulting string is divided by the divisor. The remainder called CRC (001 in this case) is appended to the end of data unit replacing the three 0s and the resulting string (100100001) is sent to the receiver. Figure 5.7 shows the binary division in the CRC generator.

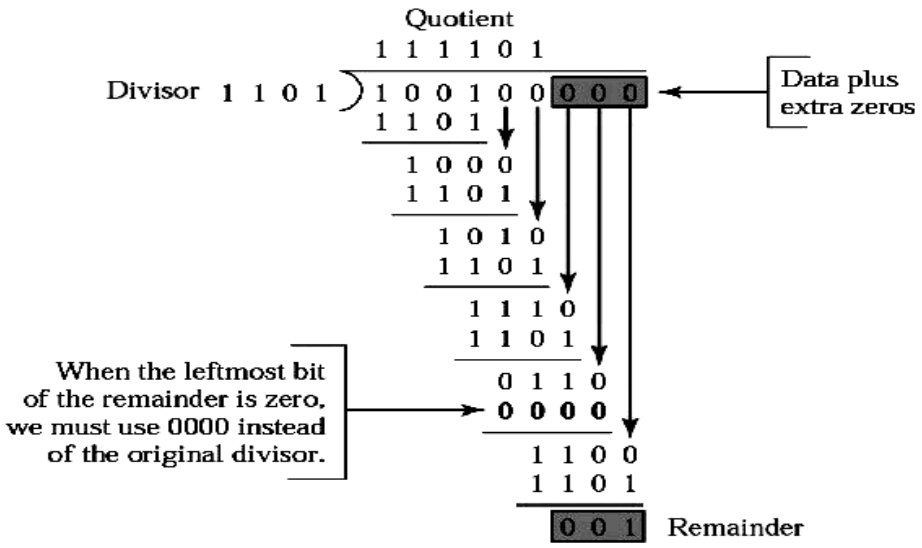


Figure 5.7: Binary division in CRC generator [1]

On the receiver side the string 100100001 is divided by the same divisor (1101). The remainder in this case is zero as shown in Figure 5.8 below. The receiver thus assumes that the data is not corrupt and accepts it.

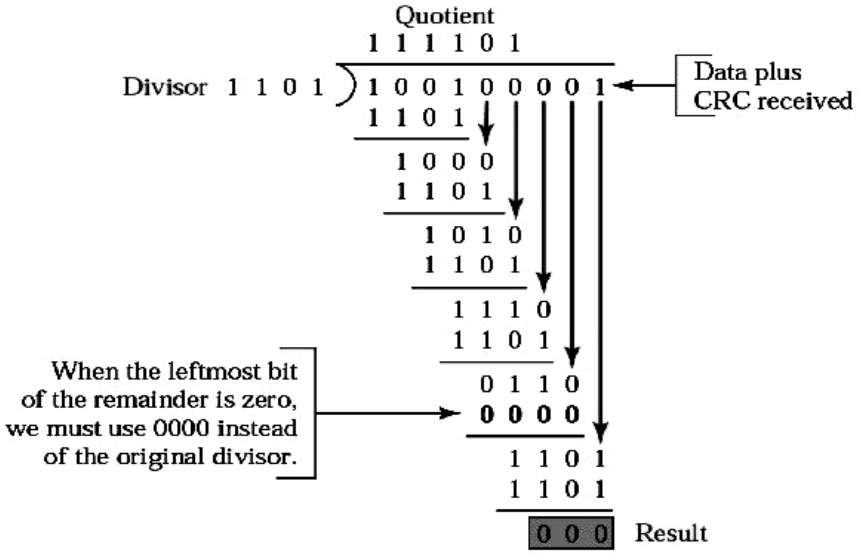


Figure 5.8: Binary division in CRC checker [1]

Checksum

On the sender side, data unit is partitioned into equal segments of n bits by the checksum generator. Next, ones complement arithmetic is used to add these segments in such a way that the total is also n bits long. The complement of this total is then appended to the end of the data unit. These extra bits added to the trail, form the checksum of the data. The

expanded data unit is then transmitted to the receiver. The Figure 5.9 below explains the entire procedure.

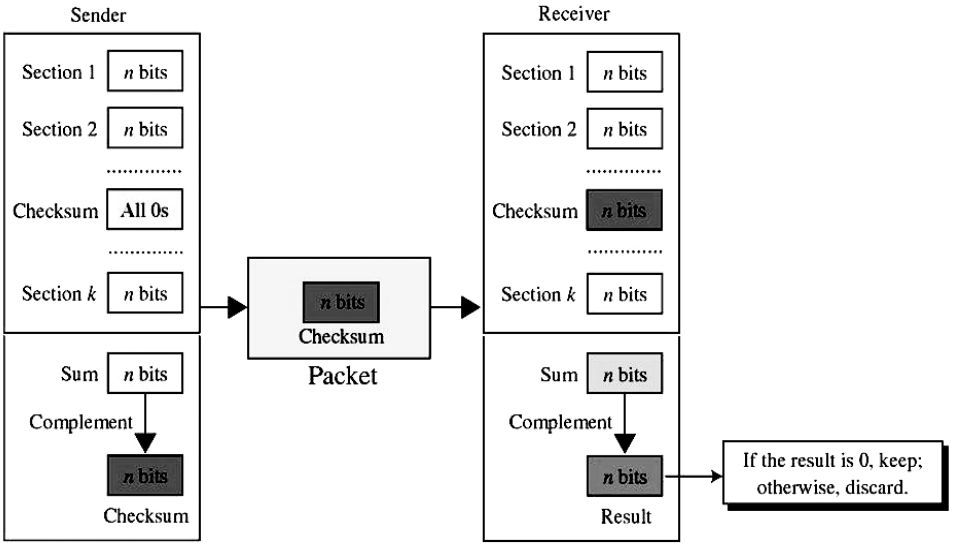


Figure 5.9: Checksum [1]

When the expanded data unit arrives at the receiver side, it is again divided into equal segments of n bits. Then the receiver adds all the segments and computes the complement of the result (addition). If the expanded data unit arrives without any changes then the complement yields a zero. If the complement yields a non-zero number, then the data unit is rejected by the receiver.

Let us suppose that the following block of 16 bits is to be transmitted with a checksum of 8 bits appended to its trail.

10101000 00111011

Now ones complement arithmetic is used to add these numbers. Then the complement is computed.

```
  10101000
  00111011
  --------
  11100011    (sum)
complement
  00011100    (checksum)
```

The following block is sent to the receiver.

10101000 00111011 00011100

Checksum

The receiver receives the above block and then adds all the three segments. The addition of the three segments gives all 1s and the complement of the same gives all 0s. The receiver then accepts the data.

	10101000
	00111011
	00011100
Sum	11111111
Complement	00000000 ← means that data is OK.

Error Correction

The two most common methods employed for error correction are forward error correction and error correction by retransmission.

Error correction by retransmission

Error correction by retransmission is usually implemented through Automatic Repeat reQuest (ARQ) which is a protocol for error control in data transmission. When the receiver receives a packet, it checks the packet for errors. If any error is detected then the receiver requests the sender to retransmit the packet. This procedure is repeated until the correct packet arrives or the upper limit for the number of retransmissions is reached. Section 5.5 describes these error control protocols in detail.

Forward Error Correction

In forward error correction (FEC), a receiver can use an error-correcting code, which automatically corrects certain errors. If *m* bits of data is to be sent, *r* redundant bits are appended to the trail of the data unit. The length of the expanded data unit thus becomes *m+r*. Here r should be able to denote a minimum of m+r+1 different states. Of these, one state indicates no error, and the rest *m+r* states indicate the occurrence of an error in each of the *m+r* locations. Therefore 2^r (all the states that r can indicate) must be greater than or equal to*m+r+1*.

Hamming code provides a solution to this problem. To send a 7 bit ASCII code, 4 redundant bits can be used ($2^4 >= 7+4+1$) as has been proved in the above paragraph. These bits are placed in 1st, 2nd, 4th and 8th bit positions (the positions are powers of 2). We call these bits r1, r2, r4 and r8 respectively. Figure 5.10 shows the positions of redundancy bits in Hamming code.

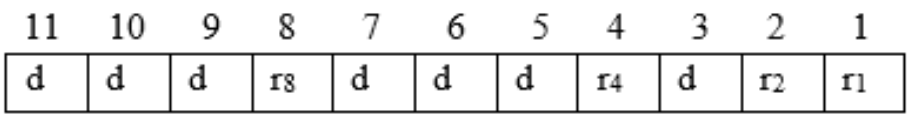


Figure 5.10: Positions of redundancy bits in Hamming code [1]

In the Hamming code, each r bit is the parity bit for the combination of data bits, as shown below:

r1 → 1, 3, 5, 7, 9, 11 (bit positions)
r2 → 2, 3, 6, 7, 10, 11 (bit positions)
r4 → 4, 5, 6, 7 (bit positions)
r8 → 8, 9, 10, 11 (bit positions)

To calculate the *r* values each bit of the original character is placed in its appropriate position in the 11 bit unit. For each combination of bits the even parity is calculated and placed in the corresponding position. The following Figure 5.11 shows the generation of parity bits and their placement in their corresponding positions.

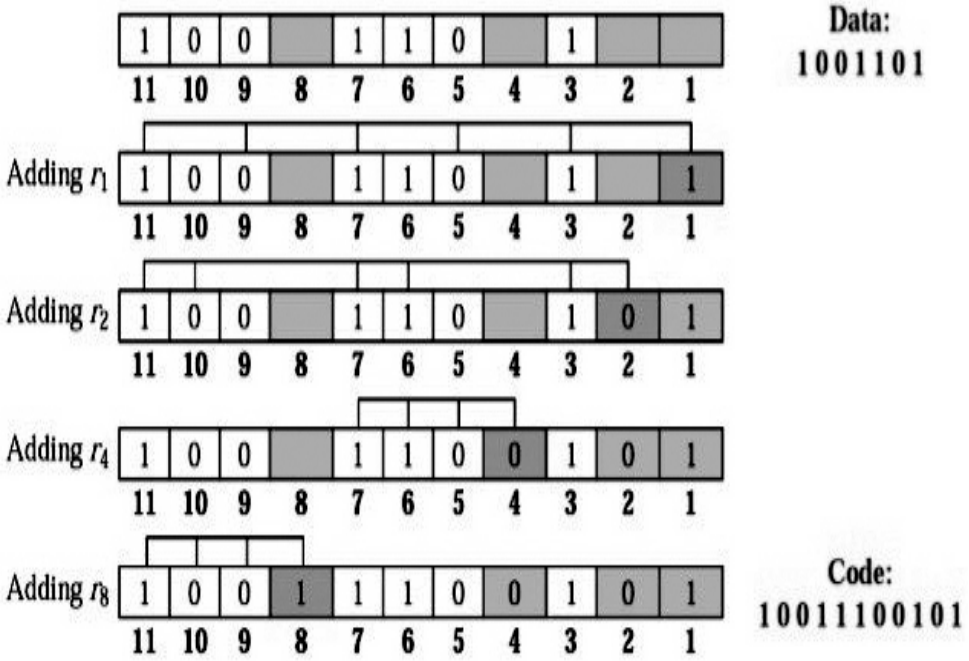


Figure 5.11: Redundancy bit calculation [1]

The generated string (10011100101) is sent through the network. But during transit the bit in 7th position changes from 1 to 0. Thus the string that arrives at the receiver is 10010100101. Receiver again calculates the parity bits as shown in Figure 5.12 below. The new parity values are then assembled in the form of a binary number in the order of r's position (r8, r4, r2, r1). This step gives the binary number 0111 (decimal representation is 7). Thus the bit in position 7 is in error. After the identification of the bit, receiver can reverse its value and correct the error.

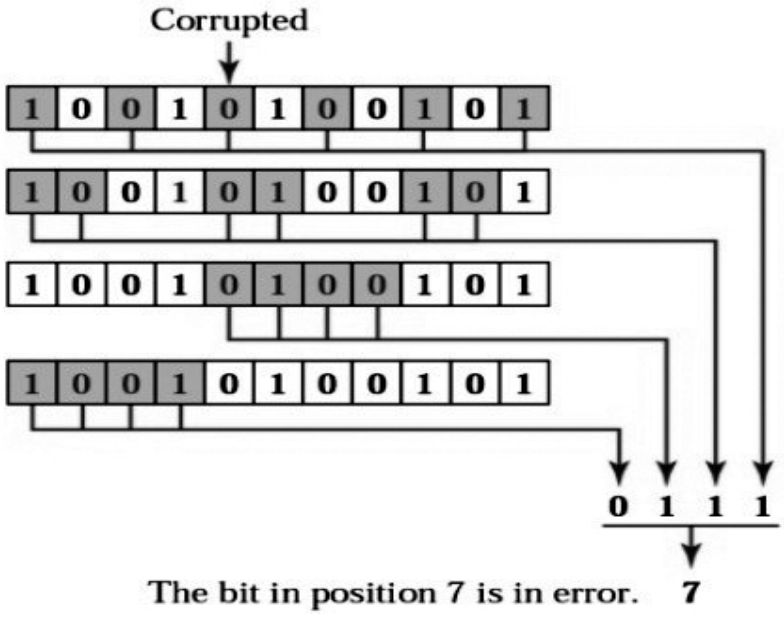


Figure 5.12: Error detection using Hamming code [1]

CHECK YOUR PROGRESS

1. A data block '1001010 1011001' is to be sent. Show how the Two-dimensional parity introduces parity bits in the block before it is sent.
2. Given a 10-bit sequence 1010011110 and a divisor of 1011, find the CRC. Check your answer.

5.3 DATA LINK LAYER PROTOCOLS [2]

The primary responsibilities of DLL are flow control and error control. Before incoming data can be used, it should be checked and processed. But the rate of processing is slower as compared to the rate of transmission. Flow control tells the sender how much data it can transmit before it has to wait for an acknowledgement packet from the receiver. The flow of data should not overwhelm the receiver.

Error control is a combination of error detection and error correction techniques. It allows the receiver to inform the sender if any frames are lost or damaged during transmission. It also allows the receiver to cooperate with the sender for the retransmission of such frames. In Data Link Layer, error control mainly refers to error detection and retransmission. If any frame is lost or damaged, receiver requests the sender to resend it. This procedure is called Automatic Repeat reQuest (ARQ)

DLL protocols can be basically divided into two types: protocols that can be used for noiseless channels and protocols that can be used for noisy

channels. Protocols for noiseless channels cannot be used in the real life but they serve as a basis for understanding the protocols for noisy channels. The Figure 5.13 shows the classification of protocols based on the type of channel they operate in.

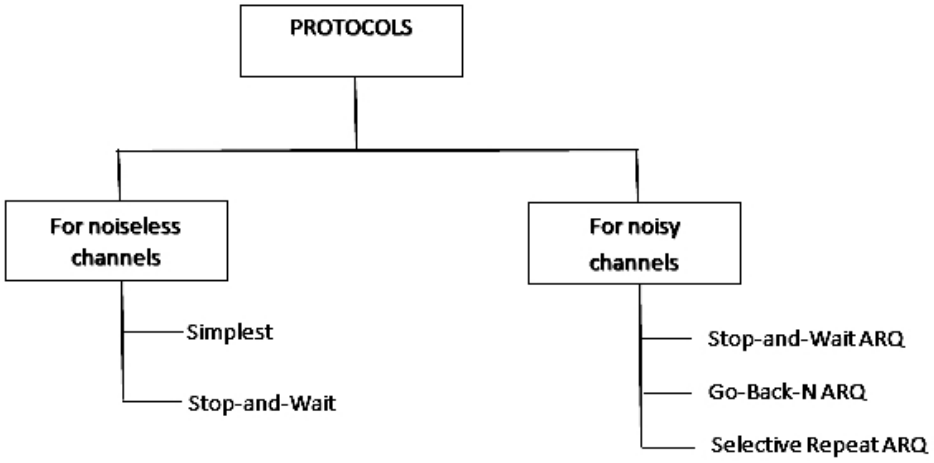


Figure 5.13: Taxonomy of protocols [2]

5.4 NOISELESS CHANNEL [2]

This is an ideal channel in which no frames are lost, duplicated, or corrupted. There are basically two protocols for noiseless channels: Simplest protocol and Stop-and-Wait protocol. Neither of the protocols employ error control mechanisms as it has been assumed that they operate in noiseless channels. On the contrary, flow control mechanism is implemented in the second protocol but not in the first protocol.

Simplest protocol

Simplest protocol does not employ either any flow control mechanisms or any error control mechanisms. Here data frames are transmitted in one direction only- from the sender to receiver. It is presumed that the receiver can instantly handle any frame it receives from the sender with a very low processing time that can be neglected. The header of the frame is instantly removed by the data link layer of the receiver and then the data packet is handed over to the network layer. So, the receiver is never overwhelmed by the inbound frames.

The data link layer of the sender acquires data from its network layer, builds a frame out of the data, and transmits it. The data link layer of the receiver accepts a frame from its physical layer, extracts data from the frame and then sends the data to its network layer. A data link layers provides transmission services to its network layer and uses the services provided by its physical layer (such as multiplexing, signaling etc.) to

physically transmit bits. Figure 5.14 shows the design of the simplest protocol.

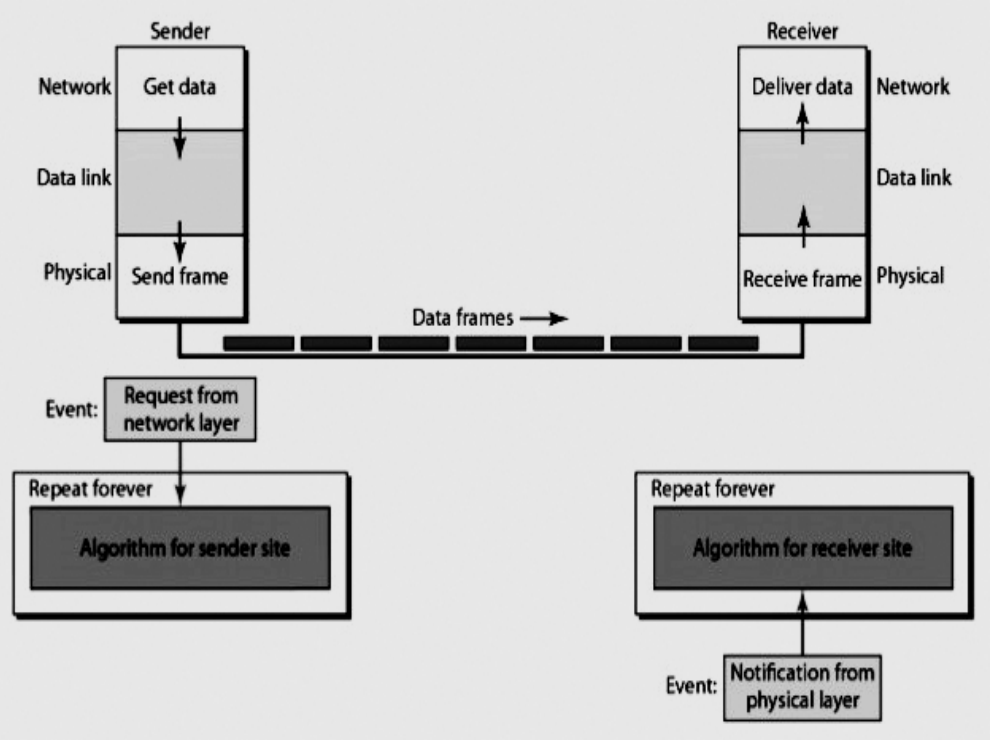


Figure 5.14: Design of Simplest protocol [2]

Stop-and-wait protocol

If the rate of arrival of data frames is more than the rate at which the receiver can process them, it could easily become overwhelmed. To avoid such a situation the frames need to be stored in a temporary location before they can be retrieved for processing. However the receiver does not have a memory space big enough to store numerous data frames, specifically when it is receiving frames from multiple senders. As a result of this the receiver may either reject the incoming frames when its memory is full, or it may deny service to senders waiting to transmit frames. This situation can be avoided by allowing the receiver to send some kind of feedback message to the sender asking it to slow down.

Stop-and-Wait protocol is named so because the sender waits for an acknowledgement frame from the receiver after sending a frame. The acknowledgement frame confirms that the receiver has successfully received the previous frame and is ready to receive the next frame. The data frames move from the sender towards the receiver and the acknowledgement frames move from the receiver towards the sender. Figure 5.15 illustrates the mechanism. At a particular moment, either there is a data frame on the forward channel or there is an acknowledgement frame on the reverse channel. Thus, this protocol needs a half-duplex link to function.

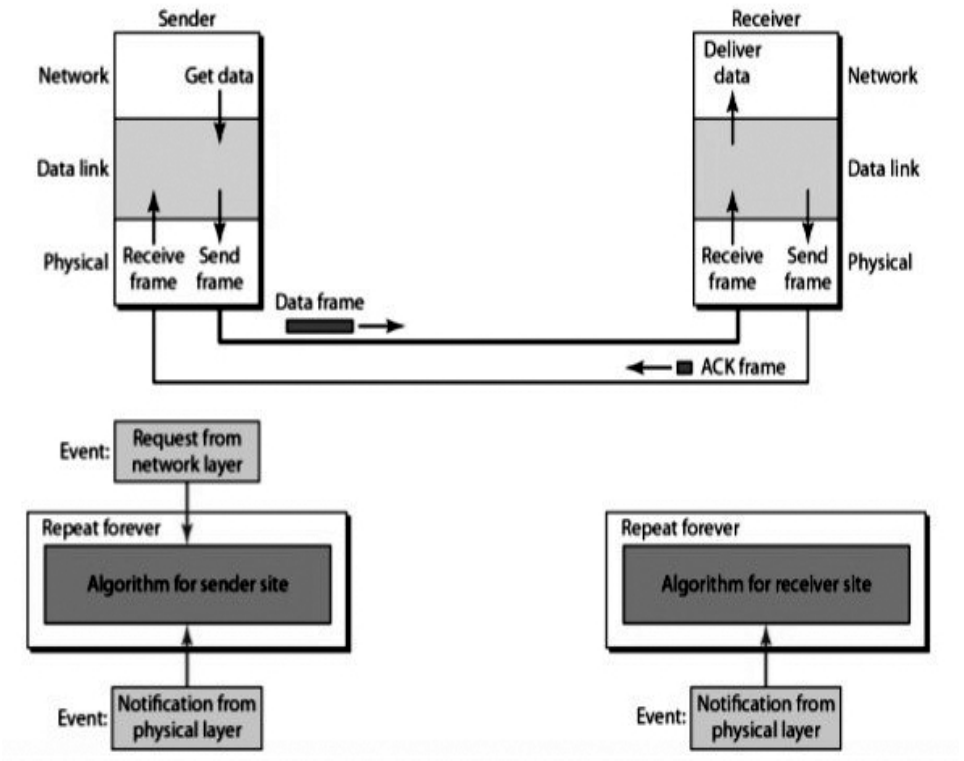


Figure 5.15: Design of Stop-and-wait protocol [2]

5.5 NOISY CHANNEL [2]

In noisy channels frames may be lost, duplicated or corrupted during transmission. So error control mechanisms are needed for error detection and retransmission. The three basic mechanisms for flow and error control are: Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective-Repeat ARQ.

Stop-and-wait ARQ

Stop-and-wait ARQ is the simplest mechanism for flow and error control. It has the subsequent characteristics.

The sending device retains a replica of the last transmitted frame until it receives an acknowledgement from the receiver. For identification purposes data frames and acknowledgement frames are numbered 0 and 1 alternatively.

To acknowledge a data frame 0 sent by the sender, the receiver transmits an acknowledgement frame ACK 1. When ACK 1 reaches the sender, it is assured that the receiver has successfully received data frame 0 and is now expecting data frame 1. In the same way receiver acknowledges a data frame 1 with an acknowledgement frame ACK 0. If any error is detected in the received frame then the receiver rejects the frame and does not send any acknowledgement. In the same way if the arrived data frame is out of

sequence (1 instead of 0 or 0 instead of 1), the receiver rejects the frame and does not send any acknowledgement.

The sender has a control variable S, which contains the number of the frame that was recently sent (either 0 or 1). Similarly the receiver has a control variable R, which contains the number of the frame which the receiver is expecting next (either 0 or 1).

As soon as the sender sends a frame it starts a timer. If the sender does not receive any acknowledgement packet from the receiver within a stipulated time, it is assumed that the frame is either lost or damaged. In such a case sender resends the frame.

While sending a frame four cases may arise: operation is normal, frame is lost, acknowledgement is delayed, or acknowledgement is lost.

Normal operation

In a normal working condition, sender sends a frame 0 and waits for acknowledgement frame ACK 1. When ACK 1 arrives, sender sends frame 1 and then waits for ACK 0. The same process is repeated over and over again, unless there is any error. For the operation to work normally the acknowledgement frame should be received before the timer set for the frame expires. Figure 5.16 shows a normal working scenario.

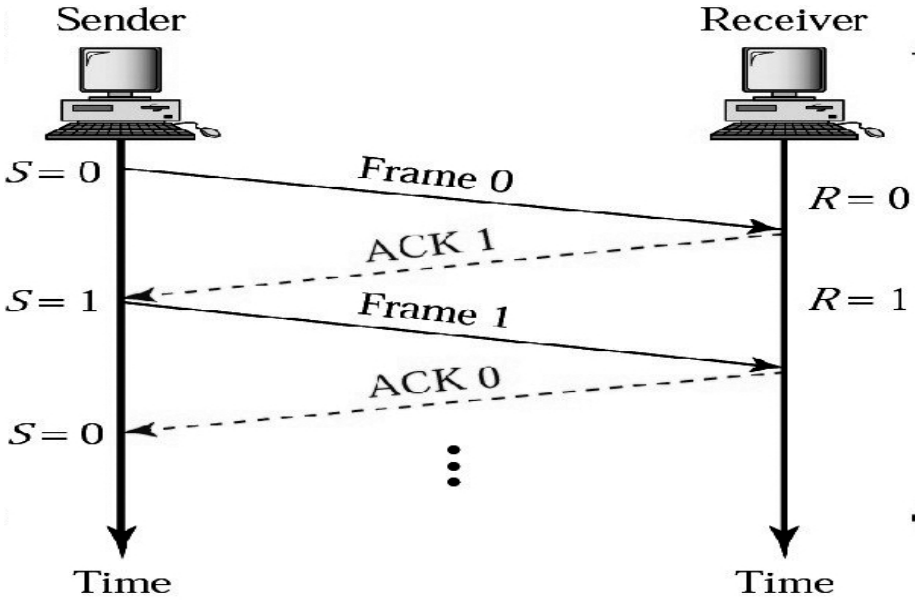


Figure 5.16: Stop-and-Wait ARQ, normal operation [2]

Loss or Damaged Frame

The receiver treats a lost or damaged frame in the same way. It stays silent and retains its value of R in both the situations. In Figure 5.17 below, sender waits for ACK 0 after transmitting frame 1. When the sender does

not receive any acknowledgement even after the expiry of the timer it sends another copy of frame 1. The receiver responds with ACK 0.

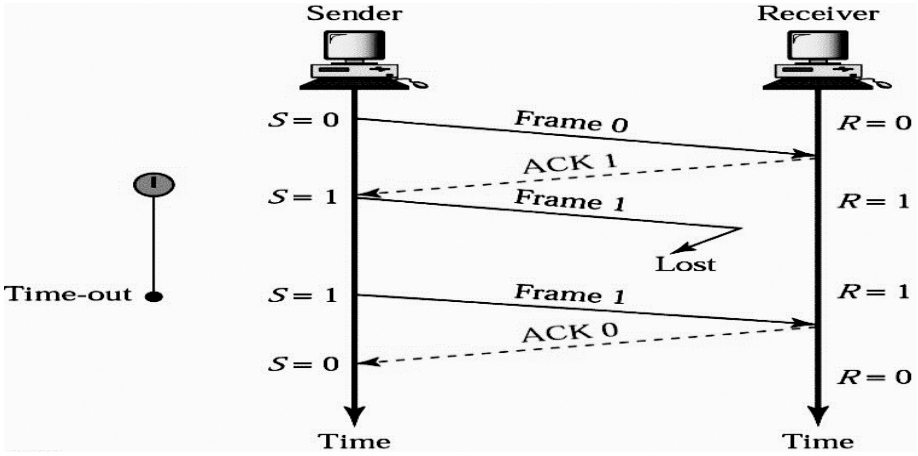


Figure 5.17: Stop-and-Wait ARQ, lost frame [2]

Lost acknowledgement

The sender handles a lost acknowledgement and a damaged acknowledgement in the same way. When the sender receives a damaged acknowledgement, it rejects the same. Figure 5.18 shows a scenario where ACK 0 sent by the receiver is lost in transit. The sender does not know whether frame 1 has reached the receiver or not. When the timer for frame 1 expires, sender resends the frame. The receiver however, is waiting for frame 0. It rejects the duplicate frame (copy of frame 1) and replies with ACK 0.

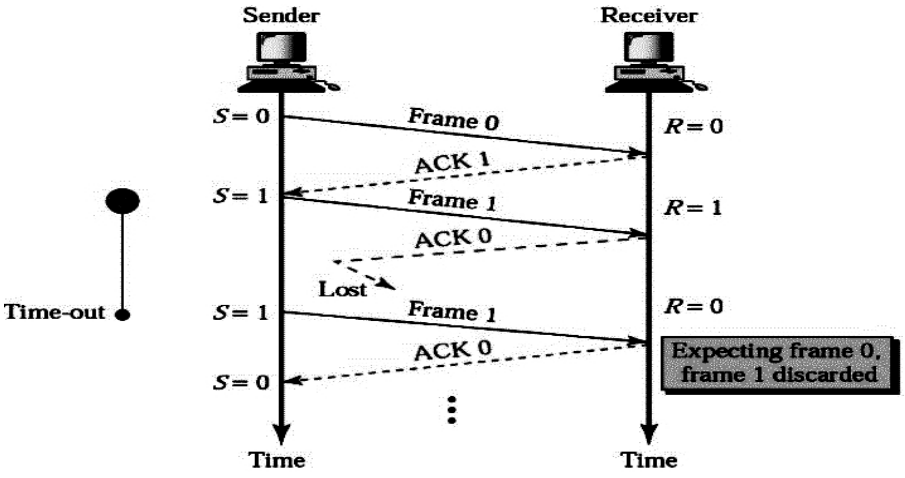


Figure 5.18: Stop-and-Wait ARQ, lost ACK frame [2]

Delayed acknowledgement

An acknowledgement can be delayed due to some problem in the link. In Figure 5.19 the first ACK 1 is delayed. It is received by the sender after

the timer for frame 0 has expired. By this time the sender has retransmitted a copy of frame 0. However, the control variable R at the receiver site holds the value 1. So the receiver rejects the copy of frame 0 and sends ACK 1 again.

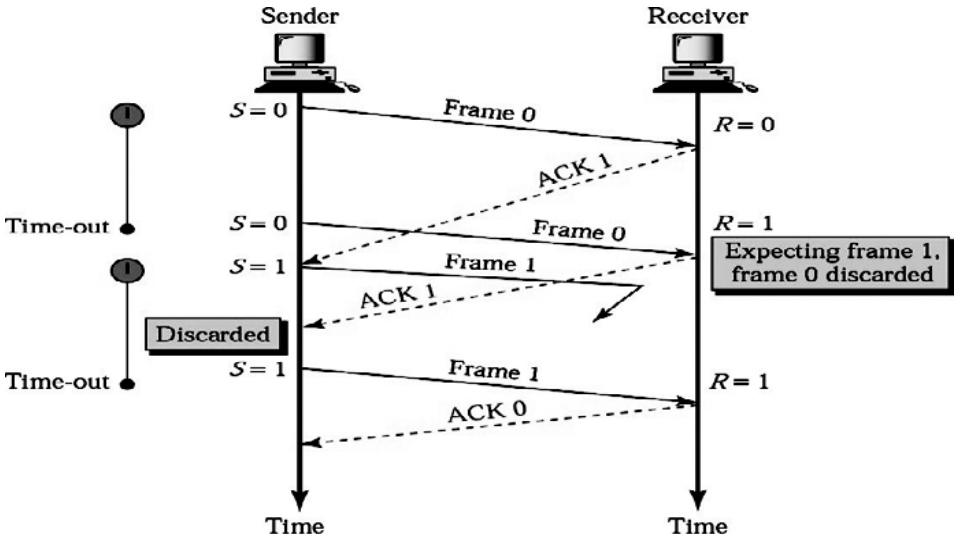


Figure 5.19: Stop-and-Wait ARQ, delayed ACK [2]

As shown above, two ACKs are received by the sender. The first acknowledgement arrives late and the second acknowledgement is sent after receiver receives the copy of frame 0. After the arrival of the delayed ACK 1 (first ACK 1), sender transmits frame 1. It is however lost and is not received by the receiver. Then the sender receives a second ACK 1 which is sent in response to the copy of frame 0 received by the receiver. The second ACK 1is discarded straightaway by the sender. After the timer for frame 1 expires, sender retransmits frame 1. Receiver acknowledges frame 1 with ACK 0.

Go-Back-N ARQ

Go-Back-N ARQ allows the sender to send multiple frames before receiving an acknowledgement from the receiver. Some additional features have been added to this mechanism to make it possible.

Sequence numbers

Sender sends out frames that are numbered sequentially. If m bits are allotted for the sequence number then the range of sequence numbers is from 0 to 2^m -1. Let us take an example. If m = 3, then the sequence numbers range from 0 to 7. Sequence numbers can be repetitive. Therefore the sequence numbers are:

0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1,……..

Sender Sliding Window

Sender uses the concept of a window to hold outstanding frames till they have been acknowledged. Frames that have already been acknowledged lie to the left of the window. Such frames can now be dismissed. Frames that cannot be sent now lie to the right of the window. Such frames cannot be sent until the window slides over them. The size of the window is 2^m-1 at the most. Figure 5.20a shows that frames 0 through 6 have been transmitted. In Figure 5.20b, the window slides over two frames to the right. This is so because sender has received an acknowledgement for frames 0 and 1.

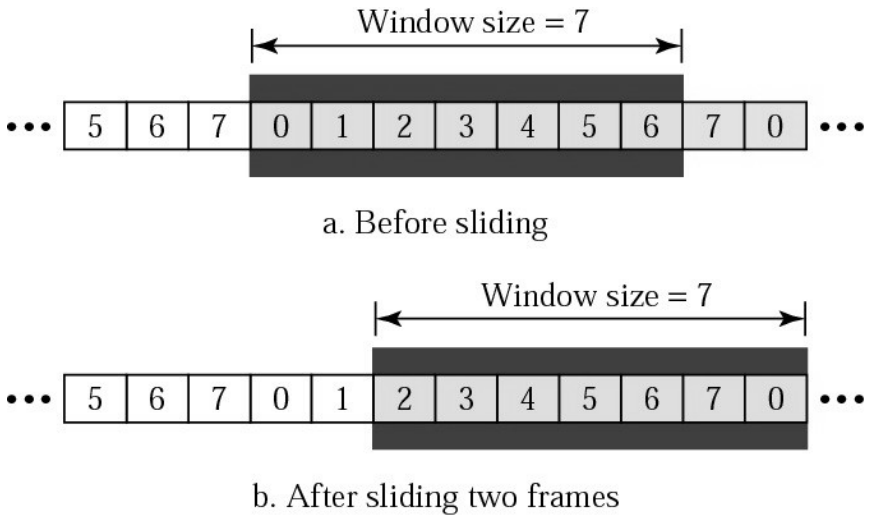


Figure 5.20: Sender sliding window [2]

Receiver Sliding Window

The receiver has a sliding window of size 1. At any moment the receiver is expecting the arrival of a particular frame. If any out of order frame arrives at the receiver site it is discarded. In Figure 5.21a the receiver is expecting frame 0. After the arrival of frame 0 the window slides over one frame to the right. Figure 5.21b denotes that the receiver is now expecting frame 1.

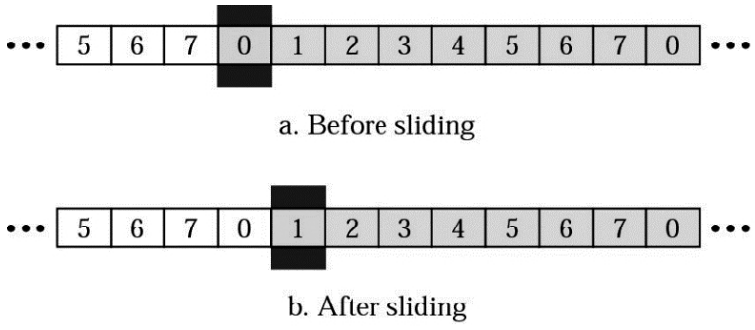


Figure 5.21: Receiver sliding window [2]

Control variables

There are three variables at the sender site: S, S_F and S_L. The variable S holds the sequence number of the frame which has recently been sent. S_F holds the sequence number of the first frame in the window. Similarly S_L holds the sequence number of the last frame in the window. The receiver has only one variable R, which holds the sequence number of the frame that the receiver is expecting now. Figure 5.22 shows the control variables used in sender and receiver window.

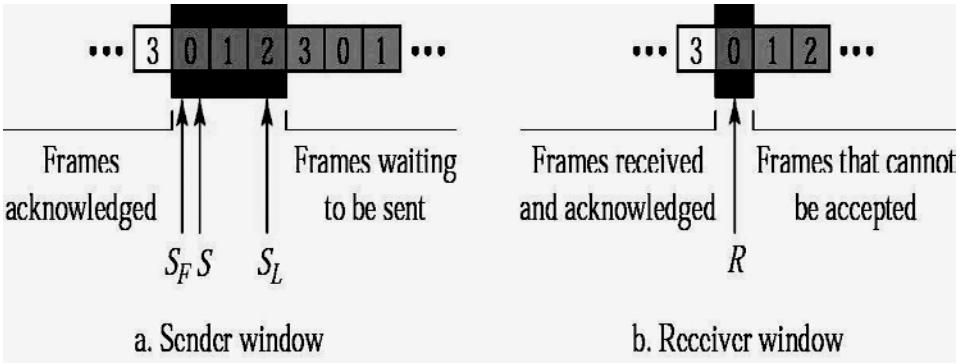


Figure 5.22: Control variables [2]

Acknowledgement

The receiver does not have to acknowledge each and every frame that it receives. Instead it sends one cumulative acknowledgement for several frames. If any damaged or out of order frame is received, the receiver stays silent and does not send any acknowledgement. It also discards all the subsequent frames until it receives the frame it has been expecting. If the sender does not receive any acknowledgement for a frame till the expiry of its timer, it goes back and resends all the frames starting from the one whose timer expired.

Let us suppose the sender has already sent frame 7, but the timer for frame 4 expires. This means that frame 4 has not been acknowledged. So the sender goes back and sends frames 4, 5, 6 and 7 again.

Various situations which may arise in the Go-Back-N ARQ mechanism have been discussed here:

Normal operation

Figure 5.23 shows how the Go-Back-N ARQ protocol functions under normal conditions. As shown below sender sends frame 0 and frame 1. Receiver sends a cumulative acknowledgement ACK 2 for both the frames. After receiving ACK 2 the sender window slides over two frames to the right. Similarly, after sending ACK 2 receiver window slides over the frame with sequence number 2, denoting that it now expects frame 2.

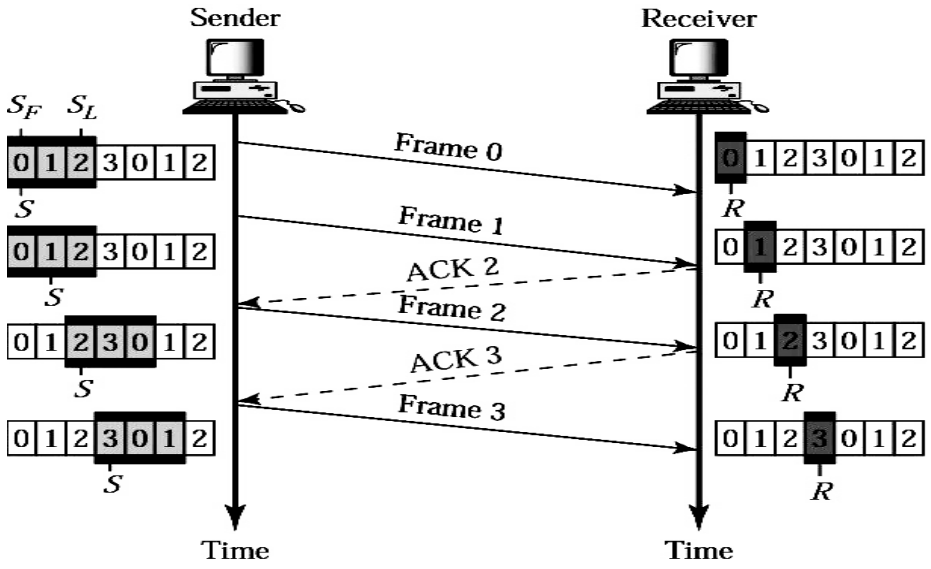


Figure 5.23: Normal operation of Go-Back-N ARQ [2]

Damaged or Lost frame

Figure 5.24 shows that frame 2 is lost and does not reach the receiver. Frame 3 arrives at the receiver site but it is discarded. The variable R at the receiver site holds the sequence number 2. This indicates that the receiver is expecting frame 2. It will keep discarding all subsequent frames till it receives frame 2. When the timer for frame 2 expires, the sender goes back and sends frame 2 and 3 again.

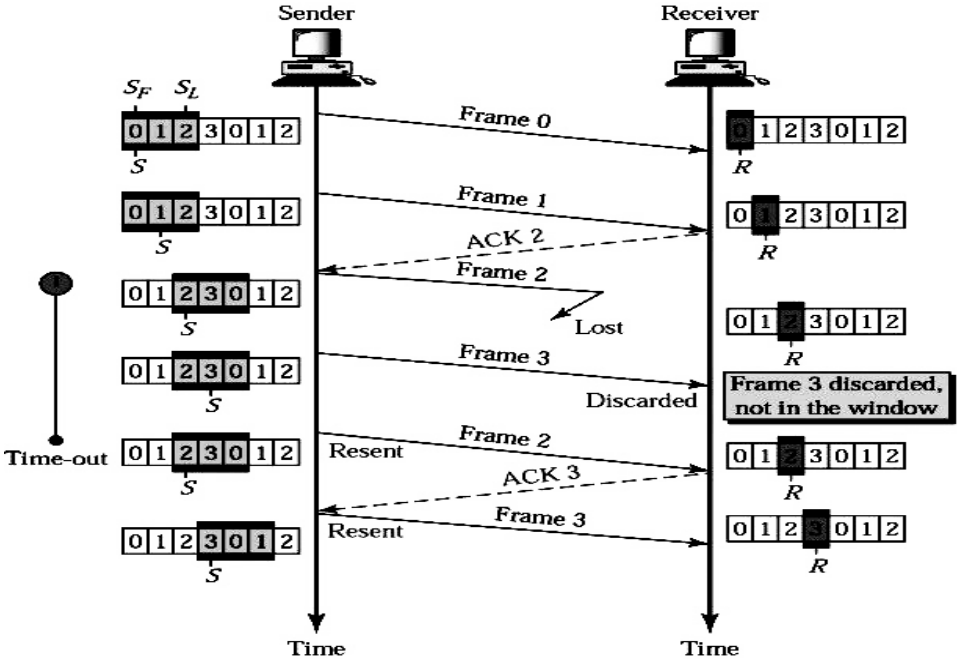


Figure 5.24: Go-Back-N ARQ, lost frame [2]

Damaged or Lost or Delayed Acknowledgement

A damaged or lost acknowledgement may give rise to two situations. Let us suppose that sender sends frame 0 and frame 1 subsequently. For frame 0 the receiver responds with ACK 1, but it is lost in transit. For frame 1 the receiver responds with ACK 2. ACK 2 may arrive at the sender site either before the expiry of timer for frame 0 or after the expiry of timer for frame 0. If the sender receives ACK 2 before the timer has expired then it does not have to go back to resend frames 0 and 1. The fact that ACK 1 was lost during transmission will have no effect at all. But if ACK 2 arrives at the sender site after the timer has expired then the sender will go back and retransmit both frames 0 and 1. In the same way a delayed acknowledgement also leads to retransmission of frames. Receiver never resends an acknowledgement.

Selective Repeat ARQ

In this mechanism N frames do not need to be resent when only one frame is damaged. The sender resends only the damaged frame. It is more efficient for noisy links when compared to the previous mechanism but the processing at the receiver site is more complex.

Sender and Receiver Windows

The size of the sending window is at most half of the value 2^m. The receiving window must be the same size as the sending window. Unlike Go-Back-N, in Selective repeat, the receiver expects a range of sequence numbers. The receiver has two control variables R_F and R_L. R_F holds the sequence number of the first frame in the window. R_L holds the sequence number of the last frame in the window. Selective Repeat ARQ allows the receiver to send a negative acknowledgement (NAK) that informs the sender about the damaged or lost frame before the timer has expired. Figure 5.25 shows the sender and receiver windows.

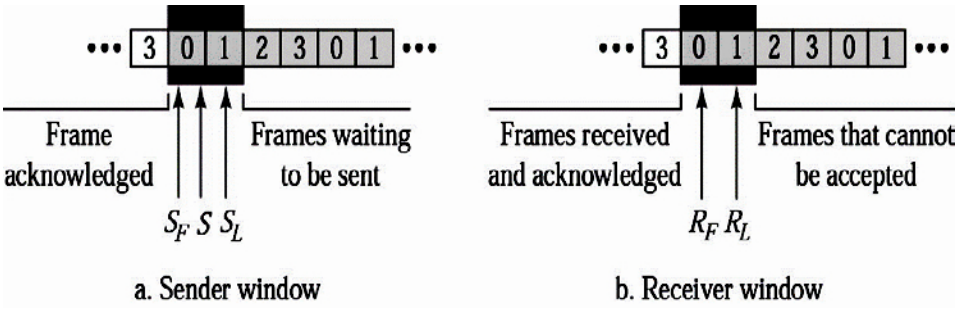


Figure 5.25: Selective Repeat ARQ, sender and receiver windows [2]

Selective Repeat ARQ, lost frame

In Figure 5.26 sender sends frames 0 and 1. The receiver sends a cumulative acknowledgement ACK 2. When sender receives ACK 2 the sending window slides over two frames to the right as can be seen below. Sender then sends frame 2, which, due to some reason is lost during

transmission. Next the sender sends frame 3. This frame is accepted by the receiver as it is now expecting frames 2 and 3 as specified by the range of its window. But frame 3 is acknowledged by NAK 2 which informs the sender that the receiver has not yet received frame 2. When the sender receives NAK 2, it retransmits frame 2.

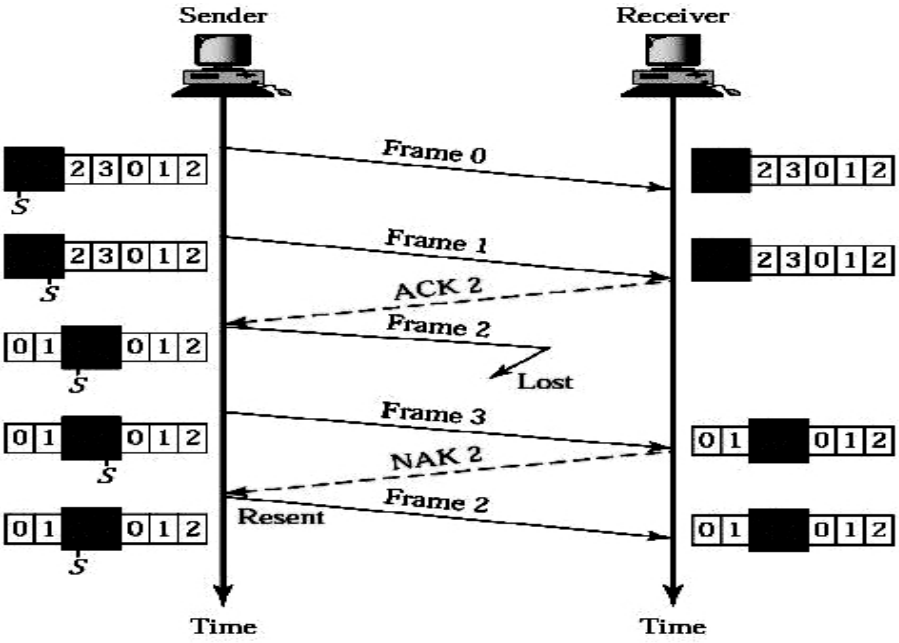


Figure 5.26: Selective Repeat ARQ, lost frame[2]

5.6 Channel Allocation Problem [3]

When multiple users try to access the same channel at the same time then it may lead to collision of signals. The solution to this problem is to divide the channel into time slots or separate frequency bandwidths and then allocate a portion of the channel to each user. Channel allocation can be static or dynamic. This section explains the properties of Static Channel Allocation and Dynamic Channel Allocation.

Static Channel Allocation

In Frequency Division Multiplexing (FDM) the available bandwidth is divided into N portions of equal size if the number of users is N. Each user is then assigned a portion of the bandwidth which is not accessible to any other user. This eliminates the problem of interference among users. But the method works proficiently only when the number of users is small and fixed with a stable stream or a heavy traffic load in each partition. The division of available bandwidth among FM radio stations is a good example of FDM. Each radio station broadcasts its signal using its own frequency band.

However, when the number of users is very high and changing or the traffic is bursty, the division does not work efficiently. Let us suppose that the available bandwidth is divided into N partitions as there are N users. But presently much less than N users are interested in communicating. This leads to the wastage of a large portion of the spectrum. If more than N users are interested in communicating at the same time, then some of them cannot be given permission due to lack of bandwidth. Although some existing users may be rarely using their allocated frequency bands for communication, new users cannot be accommodated due to the lack of available bands.

In Time Division Multiplexing (TDM) the channel is divided into N time slots if there are N users. Each user is then allocated a time slot for communication. TDM presents the same problem as FDM when the number of users vary or when allocated slots are underutilized. If more than N users want to communicate, some of them cannot be assigned any slots as all available slots have already been distributed. Some users may be hardly utilizing their slots for communication purposes. Such slots are basically being wasted as they cannot be allotted to new users.

Dynamic Channel Allocation

The following are five key assumptions that underline all the work done in this area:

1. **Independent Traffic**. The model consists of N independent stations. Each station generates its own frame for transmission. After generating a frame, the station stays put and does not take any action until the frame has been sent.

2. **Single Channel**. Only one channel is available for all communications. Each station can utilize the channel to transmit and receive data. It is assumed that all stations are equal in capacity. However, some stations can be assigned high priorities by implementing specific protocols.

3. **Observable Collisions**. If two or more stations transmit simultaneously, their signals may collide and the resulting signal is distorted. Such an event is termed collision. A collision can be detected by all the stations. A collided frame needs to be resent later by its sender. Other than those generated by collisions no other errors occur.

4. **Continuous or Slotted Time**. Time may be continuous or slotted. If the time is continuous then frame transmission can begin at any moment. But if time is slotted then frame transmission should begin at the start of a slot. There can be 0, 1 or more frames in a slot depending on the fact whether the slot is idle, the transmission is successful or there is a collision.

5. **Carrier Sense or No Carrier Sense**. A station can tell if the channel is busy or idle if it senses the channel before trying to use it. If the channel is busy then the sensing station does not attempt to use it. On the contrary in the absence of carrier sense, stations do not check the channel to see if it is idle or not before trying to use it. They just move forward and send their data. They can only determine later if the transmission was successful.

CHECK YOUR PROGRESS

1. How does the Stop-and-Wait ARQ handle a lost acknowledgement? Explain the procedure with the help of a diagram.
2. Explain how the sender and receiver sliding windows work in Go-back-N ARQ.

5.7 Summary

The basic duties of the Data Link Layer are framing, addressing, flow control, error control and media access control. The three common error detection methods are Parity Check, Cyclic Redundancy Check and Checksum. Similarly the two common methods for error correction are Error Correction by Retransmission and Forward Error Correction. DLL protocols can be divided into those that can be used for noiseless (error-free) channels and those that can be used for noisy (error-creating) channels. The two protocols implemented in noiseless channels are simplest protocol and Stop-and-Wait protocol. Simplest protocol has no flow control or error control. Stop-and-wait protocol has flow control but no error control. The three common flow and error control mechanisms for noiseless channels are Stop-and-wait ARQ, Go-Back-N ARQ and Selective-Repeat ARQ. In Stop-and-wait ARQ, each data frame sent by sender is acknowledged by the receiver. In Go-Back-N ARQ, N frames are resent starting from the one for which the acknowledgement has not been received even after the expiry of the timer. In Selective-Repeat ARQ, N frames do not need to be resent, only the damaged frame is resent. Static channel allocation permanently divides the channel among N users. Dynamic channel allocation on the contrary, allocates a segment of the channel only to a user requesting access to it.

5.8 Terminal Questions

1. Differentiate between single-bit error and burst-error with the help of examples of your own.
2. A 7 bit ASCII code ‘1011101’ is to be sent. Show how Hamming code inserts redundancy bits into the data.

3. A frame transmitted by the sender does not reach the receiver. How does Selective Repeat protocol deal with the situation when:
   (i) NAK is received before timeout (ii) NAK is received after timeout
4. In Selective Repeat ARQ the size of the receiving window is same as that of the sending window. Does this feature provide Selective Repeat ARQ any advantages over Go-back-N ARQ?
5. A receiver receives the bit pattern 01101011. If the system is using even parity, is the pattern in error?
6. A data block '10110010 00101011' is received with a checksum '00100010' appended to its end. How does the receiver check if the block is corrupted or not.

REFERENCES

[1] Behrouz A. Forouzan,Chapter 10, "Data Communications and Networking (3rd Edition)".

[2] Behrouz A. Forouzan,Chapter 11, "Data Communications and Networking (3rd Edition)".

[3] Tanenbaum and Wetherall, Chapter 4, "Computer Networks (5th Edition)".

UNIT-6 MULTIPLE ACCESS PROTOCOL

Structure

6.0 INTRODUCTION

When numerous stations are using a common channel to communicate then a multiple-access protocol is needed to manage the access to the channel. This situation can be compared to a discussion in which many people participate to share their views and ideas. Certain rules should be followed for the discussion to be productive. Only one person should be allowed to speak at a time. Each and every person must get a chance to talk. Nobody should be allowed to speak more than the time allotted to him. The same conditions are applicable for a channel which is used by multiple stations for communication purposes. Many protocols have been formulated to coordinate access to shared channels. Multiple Access Protocols are basically classified into Random-access protocols, Controlled-access protocols and Channelization protocols.

The rest of the unit is organized as follows. Section 6.1 enlists the objectives of the unit. Sections 6.2, 6.3 and 6.4 discuss various random-access protocols, controlled-access protocols and channelization protocols respectively. Section 6.5 captures the summary of the unit and section 6.6 concludes it with an exercise for the students.

6.1 OBJECTIVES

After the end of this unit, you should be able to understand:

- Random-access protocols like ALOHA, Carrier Sense Multiple Access/Collision Detection (CSMA/CD) and Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

- Controlled-access protocols like Reservation, Polling and Token Passing mechanisms

- Channelization protocols like Frequency Division Multiple Access (FDMA) , Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA)

6.2 RANDOM ACCESS PROTOCOL [1], [2]

This mechanism allows each node to access the medium without being controlled by any other node. The problem arises when two or more nodes try to access the medium at the same time. This leads to frames from multiple nodes, to travel in the same channel at the same time. The result is collision among the frames in which they are either modified or damaged. To prevent such access conflicts or resolve them as they happen, the first method that was devised was ALOHA. It used a very simple method called multiple access (MA). An additional feature was later added to upgrade the method that made it compulsory for stations to sense the channel (to find out if the channel is busy or idle) before trying to use it. This was called Carrier Sense Multiple Access (CSMA). CSMA further evolved into two methods: CSMA with collision detection (CSMA/CD) and CSMA with collision avoidance (CSMA/CA).

ALOHA

ALOHA protocol uses the concept of a central controller. Every frame that originates from a source station is first sent to the base station (BS). BS then for forwards the frame to the receiver station. Thus the BS acts as the central controller here. For uploading transmission (from a station to the BS) 407 MHz frequency is used. Similarly for downloading transmission (from the BS to a station) 413 MHz frequency is used. The medium (air) is shared between the stations. Suppose a station is transmitting frames to the BS at 407 MHz frequency. At the same time another station tries to communicate with the BS on the same frequency. This can lead to a collision among the frames of both the stations. The basic structure of an ALOHA network is shown in Figure 6.1.

The ALOHA protocol follows two simple rules which have been shown below:

Multiple Access–If a station has a frame to transmit, it transmits the frame.

Acknowledgement – Once the frame has been sent, the sender waits for an acknowledgement. If it does not receive any acknowledgement within a stipulated time, it assumes that the frame is lost. After a random amount of time, the sender tries to retransmit the frame.

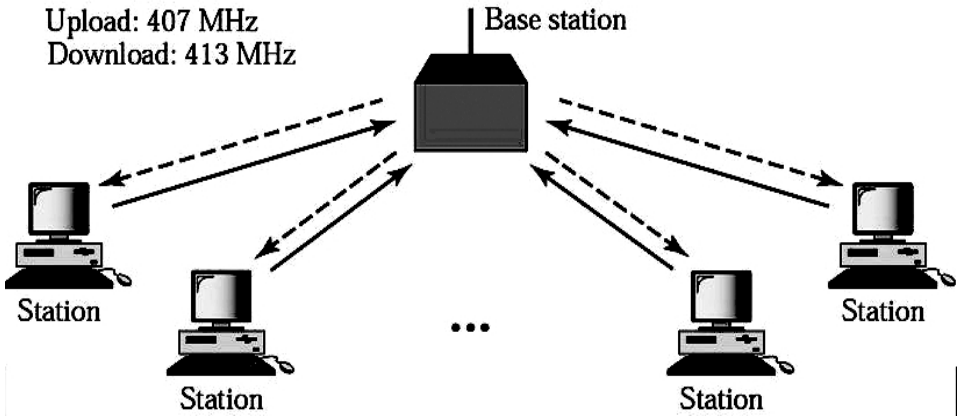


Figure 6.1: ALOHA network [1]

Two variants of ALOHA have been discussed in this section: Pure ALOHA and Slotted ALOHA.

Pure ALOHA

When a station has a frame to transmit, it transmits the frame. After the transmission, the station waits for the acknowledgement to arrive. The waiting period is 2 times the maximum propagation delay. Maximum propagation delay is the amount of time needed to transmit a frame between two most widely separated stations. If the acknowledgement arrives at the sender site within the stipulated time, the transmission is successful. If the sender does not receive any acknowledgement during this period, it uses a backoff strategy (waits a random amount of time before sending again) and transmits the frame again. If the acknowledgement does not arrive even after several attempts, the station gives up. Figure 6.2 explains the working procedure of pure ALOHA in detail.

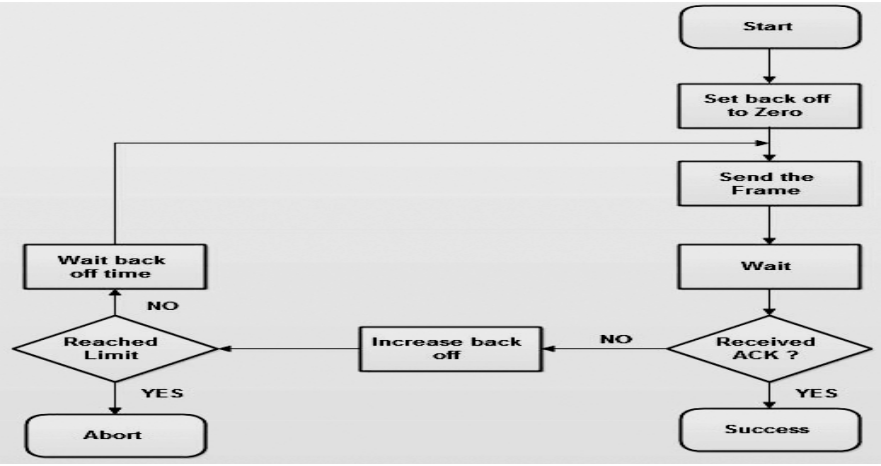


Figure 6.2: Procedure for pure ALOHA protocol [1]

Frame transmission

There is no concept of synchronization between the stations. Any station can transmit whenever it has data. As shown in the Figure 6.3 below each station is transmitting two frames. Frame 1.1 of station 1 and frame 3.2 of station 3 do not collide with any frame from any other station. But frame 1.2 of station 1, frame 2.1 of station 2, frame 3.1 of station 3 and frame 4.1 of station 4 fall in the first collision duration. Similarly frame 2.2 of station 2 and frame 4.2 of station 4 fall in the second collision duration.

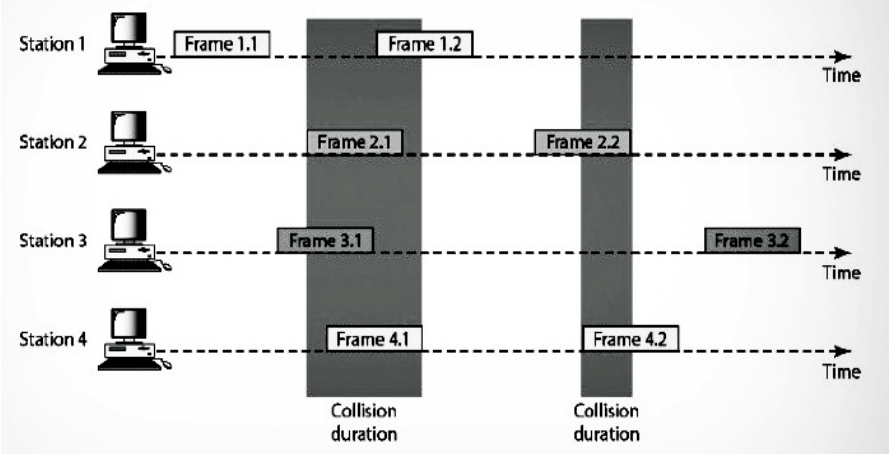


Figure 6.3: Frames in a pure ALOHA network [2]

Vulnerable time

Vulnerable time is the time in which there is a possibility of collision. It is assumed that frames of all the stations are equal in size. It takes T_{fr} seconds for the transmission of each frame. Figure 6.4 below shows the vulnerable time for station A. Here, station A sends a frame at time t. Station B has already transmitted a frame between t -T_{fr} and t.

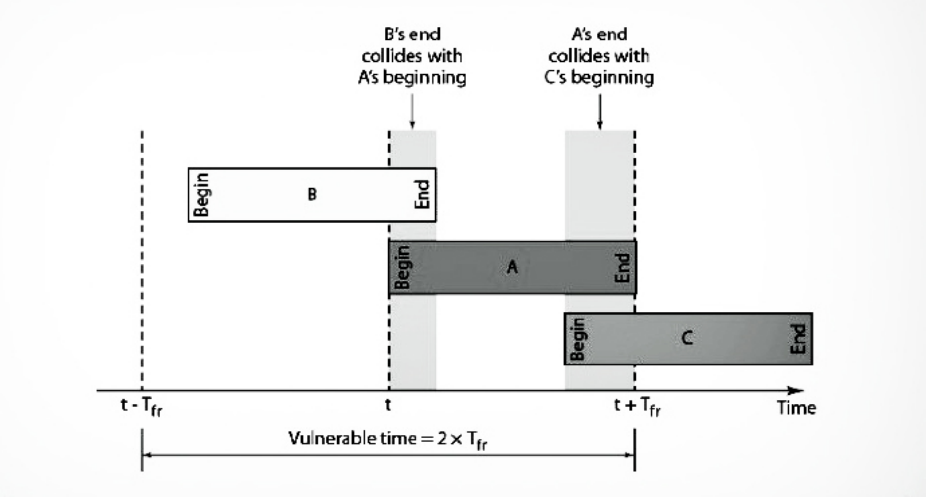


Figure 6.4: Vulnerable time for pure ALOHA protocol [2]

Thus the end of frame B collides with the beginning of frame A. Station C also sends a frame between t and t + T_{fr}. So the end of frame A collides

with the beginning of station C. Figure 6.4 above shows that the vulnerable time for pure ALOHA is twice the transmission time of the frame.

Throughput

Suppose that the average number of frames produced by the system during one frame transmission time is G. So the average number of successful transmissions for pure ALOHA is $S=G\times e^{-2G}$(throughput for pure ALOHA). The maximum throughput s_{max} is 0.184 for G=1/2. So if one-half a frame is produced during one frame transmission time, then 18.4 percent of these frames reach their destination successfully.

Slotted ALOHA

Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA, time is divided into slots of T_{fr} seconds. Each station is allowed to transmit only at the beginning of a time slot. If a station misses a chance, it has to wait until the beginning of the next time slot.

Frame transmission

Figure 6.5 shows the frame transmission in a slotted ALOHA network. The time has been divided into different slots. Frame 1.1 of station 1, frame 2.2 of station 2, frame 4.2 of station 4 and frame 3.2 of station 3 are in slots where they do not collide with any frame from any other station. But frames 2.1 and 3.1 from stations 2 and 3 respectively are transmitted in slot 2 which leads to a collision among them. Similarly frames 1.2 and 4.1 from stations 1 and 4 respectively are transmitted in slot 3 which leads to a collision among them.

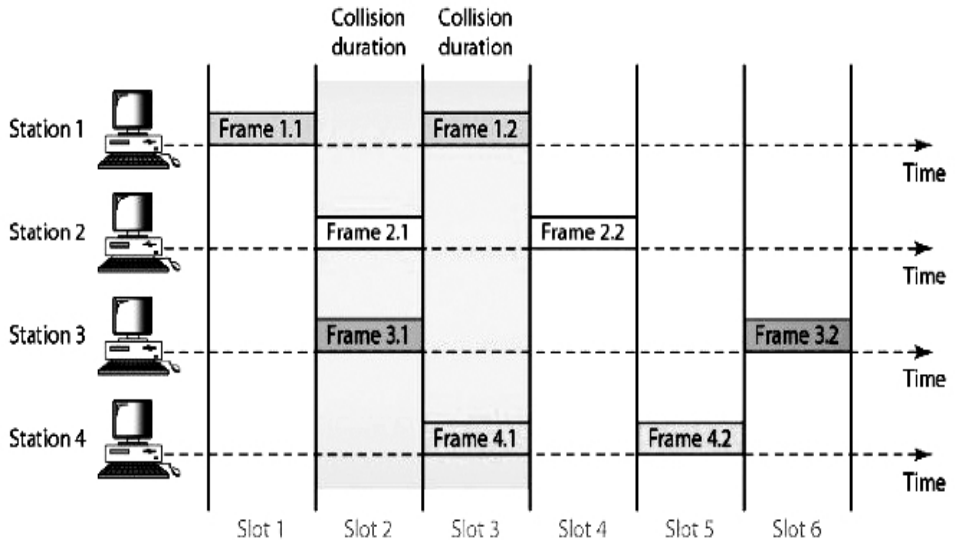


Figure 6.5: Frames in slotted ALOHA network [2]

Vulnerable time

Vulnerable time is the time in which there is a possibility of collision. It is assumed that frames of all the stations are equal in size. It takes T_{fr} seconds for the transmission of each frame. In Figure 6.6 below station B sends a frame at time t-T_{fr}. It does not collide with any other frame. On the contrary, stations A and C send frames at time t. Both the frames collide in time slot 2. The vulnerable time for slotted ALOHA protocol is equal to the transmission time of the frame as shown below.

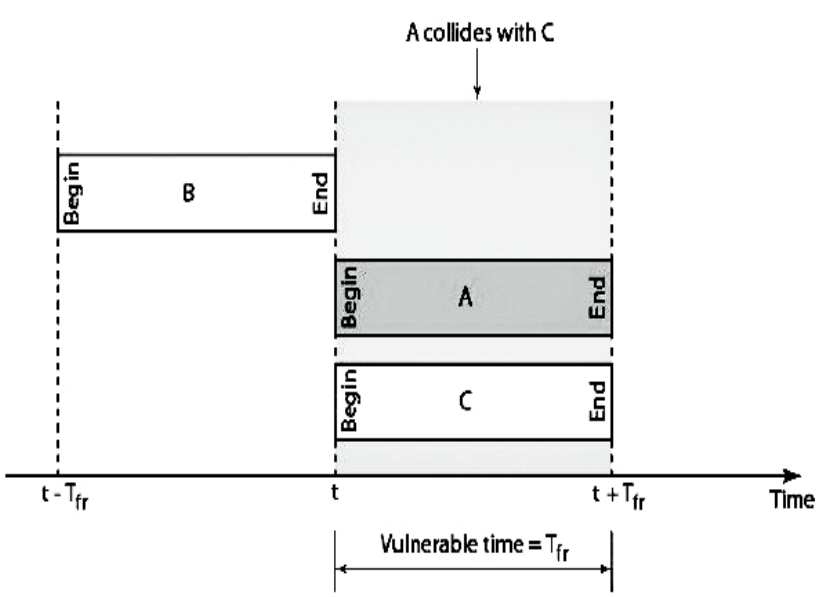


Figure 6.6: Vulnerable time for slotted ALOHA protocol [2]

Throughput

Suppose that the average number of frames produced by the system during one frame transmission time is G. The average number of successful transmissions for slotted ALOHA is $S=G\times e^{-G}$ (throughput for slotted ALOHA). The maximum throughput s_{max} is 0.368 for G=1. So if one frame is produced during one frame transmission time, then 36.8 percent of these frames reach their destination successfully.

CSMA

CSMA makes it mandatory for every station to sense the channel before trying to use it. Sensing the channel will clarify whether it is busy or idle. Though CSMA can diminish the chances of a collision, it cannot be totally eradicated. When a station transmits a frame, it takes some time for the first bit to arrive at every station. A station can sense the bit only after it is received by the station. If a station senses the channel when the bit has not yet arrived, it assumes that the channel is idle and transmits its own frame. This leads to a collision between the two frames. Figure 6.7 shows the collision.

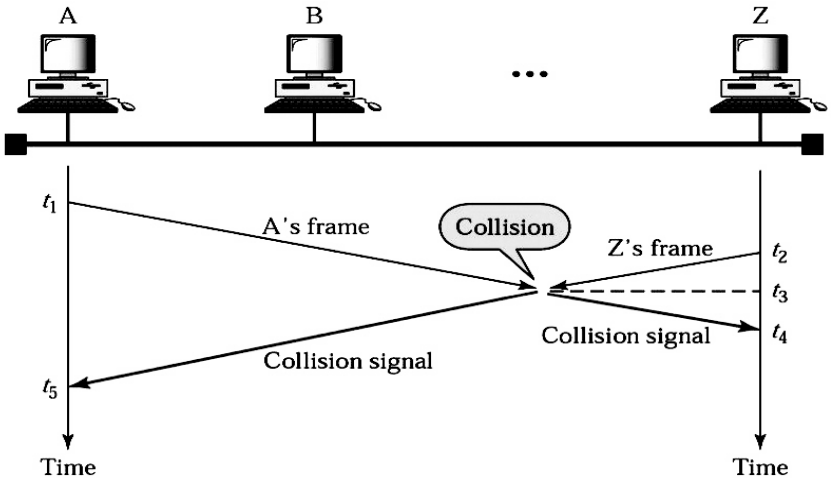


Figure 6.7: Collision in CSMA [1]

Here station A senses the channel at time t_1. It finds the channel idle and sends its frame. Station Z senses the channel at time t_2 ($t_2 > t_1$). The propagation from station A has not reached station Z by this time. Therefore station Z also assumes that the channel is idle. It then transmits its own frame. The two frames collide at time t_3 ($t_3 > t_2 > t_1$). The collision results in a garbled signal that travels in both directions. Station Z receives the garbled signal at time t_4 ($t_4 > t_3 > t_2 > t_1$) and station A receives it at time t_5 ($t_5 > t_4 > t_3 > t_2 > t_1$).

Persistence Strategy

The persistence strategy defines the procedures for a station that senses a busy medium. Two sub strategies have been devised: Nonpersistent and Persistent. The two methods have been shown in Figure 6.8 below.

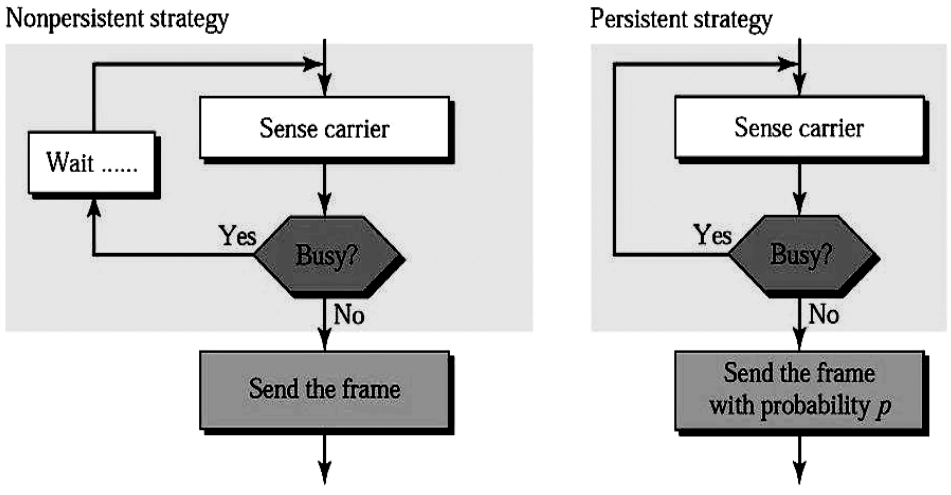


Figure 6.8: Persistence strategies [1]

Nonpersistent

In a nonpersistent strategy, a station that wants to transmit a frame senses the channel first. If the channel is idle, the station transmits its frame immediately. If the channel is busy, the station waits for a random amount of time and then checks the channel again. This approach decreases the chance of a collision as it is unlikely that two or more stations will wait for the same amount of time and then sense the channel again at the same time.

Persistent

In a persistent strategy, a station senses the medium. If the medium is idle, the station sends a frame. This method has two variations: **1-persistent** and **p-persistent**.

In the 1-persistent method, if a station finds the medium idle, it transmits its frame immediately (with a probability of 1). This method increases the chance of collision because two or more stations may send their frames after finding the medium idle.

In the p-persistent method, if the station finds the medium idle, the station may or may not send. It sends with probability p and refrains from sending with probability 1-p. For example, if p is 0.2, it means that each station, after sensing an idle channel, sends with a probability of 0.2 (20 percent of the time) and refrains from sending with a probability of 0.8 (80 percent of the time). The station generates a random number between 1 and 100. If the random number is less than 20, the station will transmit; otherwise the station does not send.

CSMA/CD

CSMA/CD adds a procedure to handle a collision. When a station wants to send a frame it sets the backoff parameter to zero. Then the station uses one of the persistent strategies to sense the channel. When the station finds the channel idle, it transmits the frame. If the station does not hear a collision until the entire frame has been sent, it assumes that the transmission was successful. But if the station hears a collision, it transmits a jam signal. This signal notifies other stations that a collision has occurred. So all stations reject the part of the frame they have received.

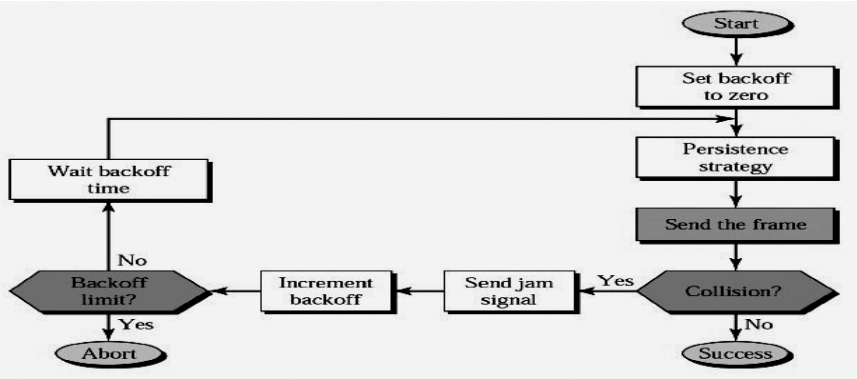


Figure 6.9: CSMA/CD procedure [1]

The backoff parameter's value is now incremented by 1. The station then checks if the value has exceeded its limit (15 usually). If the value has crossed the limit, the station aborts the process and does not attempt again. If the value has not crossed its limit, the station waits for a random backoff period on the basis of the present backoff parameter value and senses the channel again. Figure 6.9 above shows the CSMA/CD working procedure. The station waits between 0 and 2 × (maximum propagation time) for the first time, between 0 and 2^2 × (maximum propagation time) for the second time, and so on.

CSMA/CA

CSMA/CA avoids collision. The first step is to set the backoff parameter to zero. Then the station sense the channel using one of the persistent strategies. If the station finds the channel idle, it waits for an IFG (interframe gap) amount of time. Then it waits for a random amount of time. After that, the sender transmits the frame and sets a timer. It now waits to receive the acknowledgement from the receiver. If the acknowledgement arrives before the expiry of the timer, the sender assumes that the transmission was successful. If no acknowledgement arrives, the sender assumes that either the frame or the acknowledgement is lost. In that case sender increases the backoff parameter value, waits for a backoff period and senses the channel again. Figure 6.10 below shows how the CSMA/CA works.

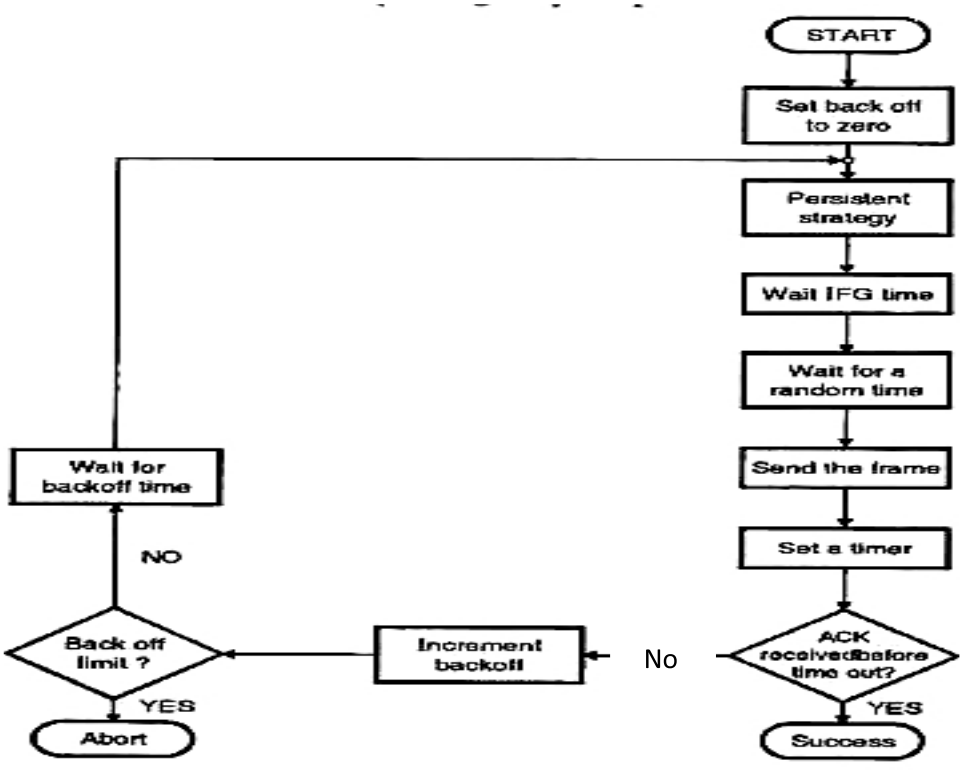


Figure 6.10: CSMA/CA procedure [1]

CHECK YOUR PROGRESS

1. What is the purpose of a jam signal in CSMA/CD?
2. Differentiate between the vulnerable time and throughput of pure ALOHA and slotted ALOHA.

6.3 CONTROLLED ACCESS PROTOCOL [1]

Controlled access protocol makes it compulsory for stations to negotiate with each other to find which station should be allowed to transmit. A station cannot transmit if it has not been approved by other stations. The three standard controlled-access protocols are Reservation, Polling and Token Passing.

Reservation

In this access type, any station that wants to send data has to make a reservation. Time is divided into intervals. A reservation frame leads the data frames in each interval. The number of reservation minislots in a reservation frame is equal to the number of stations in the system. So each station owns a minislot in the reservation frame. A station has to make a reservation in its minislot if it wishes to transmit a frame. Stations that do not make reservations in their minislots cannot send data frames after the reservation frame.

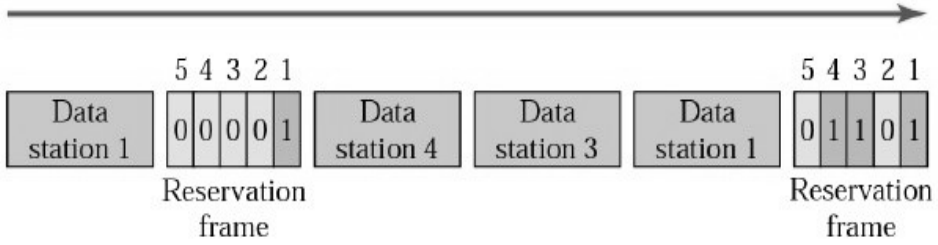


Figure 6.11: Reservation access method [1]

Figure 6.11shows five stations and a reservation frame with five minislots. Three stations i.e. station 1, station 3 and station 4 make reservation in the first interval. Whereas only station 1 makes reservation in the second interval.

Polling

In this access method a single station is nominated as the primary station and the rest are nominated as secondary stations. The primary station manages the channel that is used for communication. All the secondary stations obey the commands of the primary station. The primary station decides which secondary station can access the channel at a given time. If the primary station wishes to receive data, it questions the secondary stations if they have to send something; this is called polling. Similarly if the primary station wants to send data, it instructs the concerned station to be prepared for the reception; this is called selecting.

Select

When the primary station wants to send data, it first alerts the concerned secondary station. In Figure 6.12 below, primary station sends a select (SEL) frame to station B instructing it to get ready to receive a frame. If station B is ready, it responds with an acknowledgement message ACK. On receiving the ACK, the primary station sends the data frame to station B. Station B responds again with an ACK message which shows that the frame has been successfully received by it.

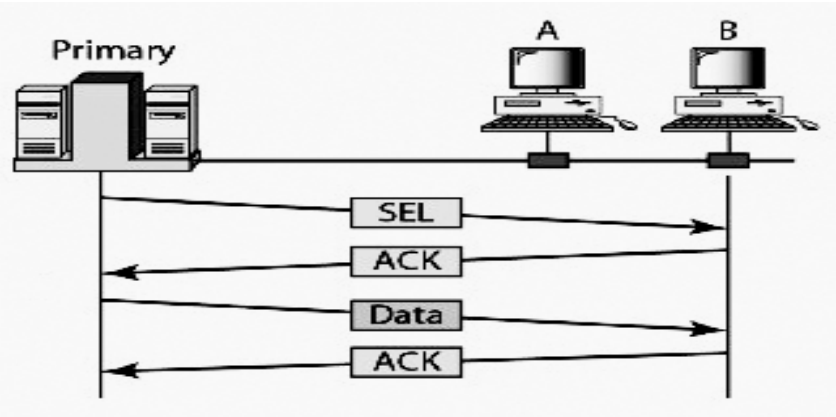


Figure 6.12: Select method [1]

Poll

When the primary station wishes to receive data it questions (polls) each secondary station to know if the secondary station has anything to send. In Figure 6.13 below primary station first asks station A by sending a Poll frame to it. Station A has no data for the primary station. It therefore responds with a NAK frame. Next the primary station asks station B if it has anything to send. Station B has a data frame that it wants to send to the primary station. So station B sends the data frame. Primary station then responds with an ACK message informing station B that the data frame has been successfully received.

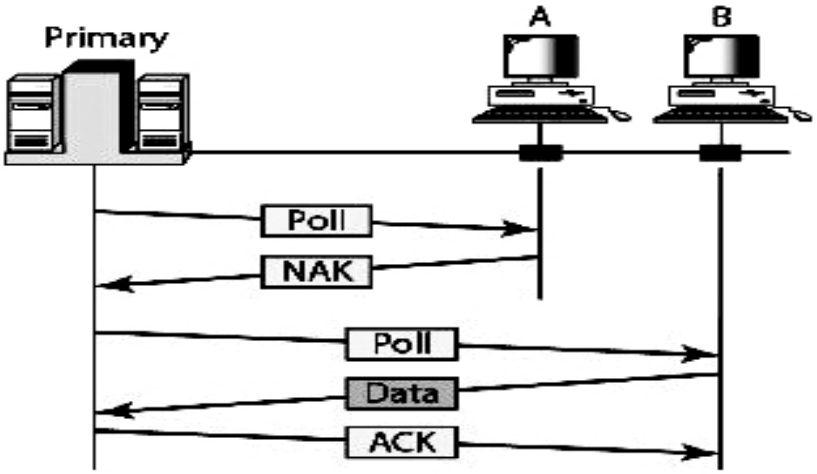


Figure 6.13: Poll method [1]

Token Passing

In the token-passing method, stations are organized in a ring. Every station has a successor and a predecessor. Only the station that gets the token (a special frame) has the right to transmit data. Figure 6.14 explains the situation.

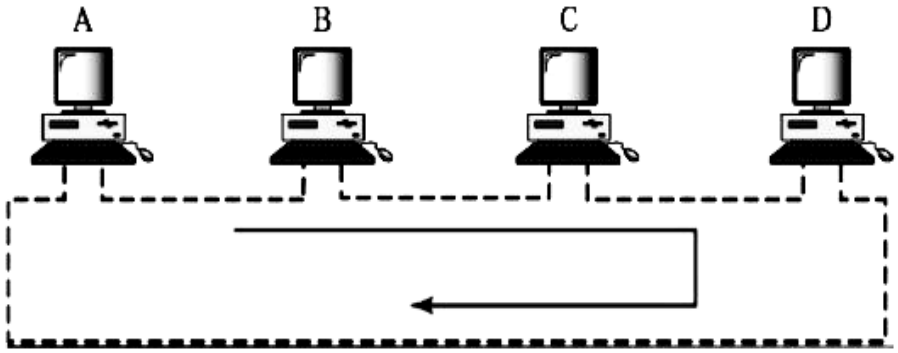


Figure 6.14: Token-passing network [1]

The token keeps moving about the ring. The station which wants to send data waits for the token. As soon as the token arrives it is captured. The station then starts sending data frames. This process continues until the station has sent all its data frames or the allocated time has not expired. Finally the token is released to continue circulating about the ring, till it is captured again by another station. Figure 6.15 shows the procedure in detail.

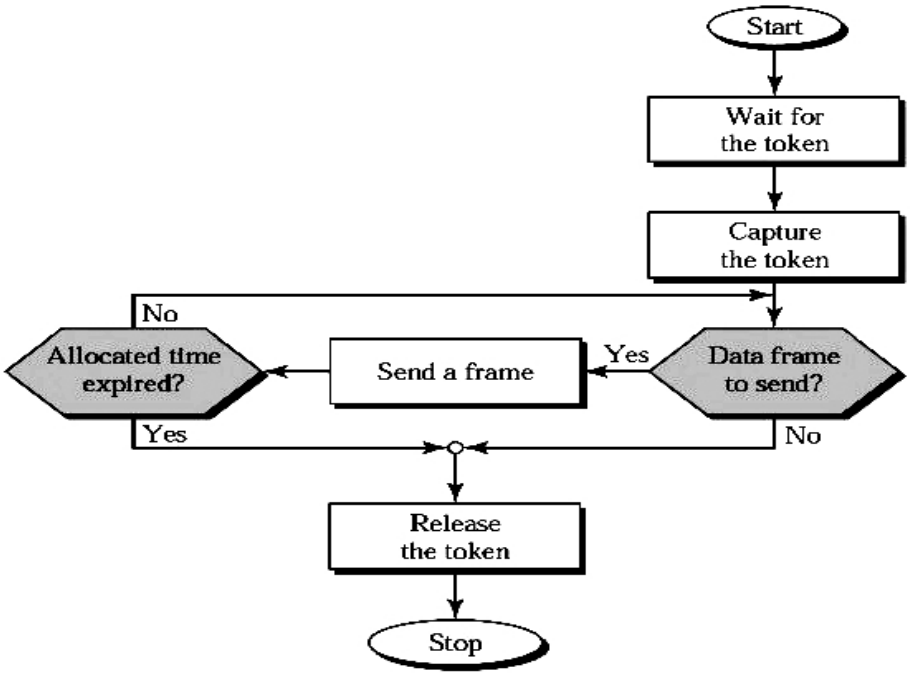


Figure 6.15: Token-passing procedure [1]

6.4 CHANNELIZATION PROTOCOL [1]

Channelization protocols allows the available bandwidth of the channel to be divided into different time slots, frequency bands or through code and to be distributed among all stations present. The channelization protocols that have been discussed in this section are: Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA) and Code-Division Multiple Access (CDMA).

Frequency Division Multiple Access (FDMA)

In frequency-division multiple access (FDMA), the available bandwidth of the channel is partitioned into different frequency bands. Each station is assigned a frequency band to transmit its data. Thus each band is reserved for a particular station. The station uses it whenever it needs to send any data. Each frequency band is separated from the other by a narrow unused band called a guard band. It prevents stations from interfering with each other. Figure 6.16 explains the scenario in detail.

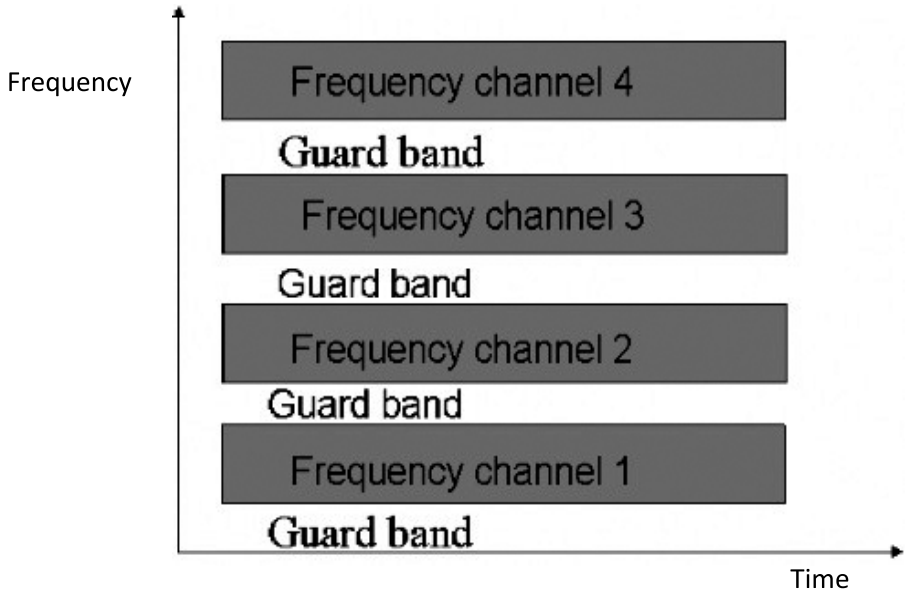


Figure 6.16: Frequency-Division Multiple Access [3]

Multiplexing

FDM is an analog process. In Figure 6.17 below, a signal of the same frequency range is produced by each telephone. These signals enter the multiplexer where each signal is modulated onto a different carrier frequency (f_1, f_2 or f_3) as shown below. Then a single composite signal is produced by joining these three modulated signals. The composite signal is sent over a channel that has sufficient bandwidth to support it.

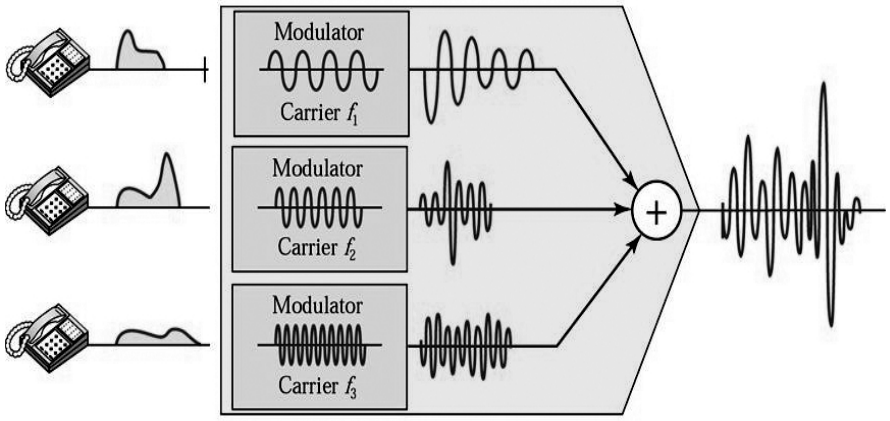


Figure 6.17: FDM multiplexing process [1]

Demultiplexing

The multiplexed signal enters the demultiplexer which has a series of filters. These filters separate the multiplexed signal into its constituent modulated signals. Each modulated signal passes through a demodulator that separates the carrier frequency from it. Finally the individual signals are sent to their respective receivers. Figure 6.18 below explains the demultiplexing process of the multiplexed signal generated above.

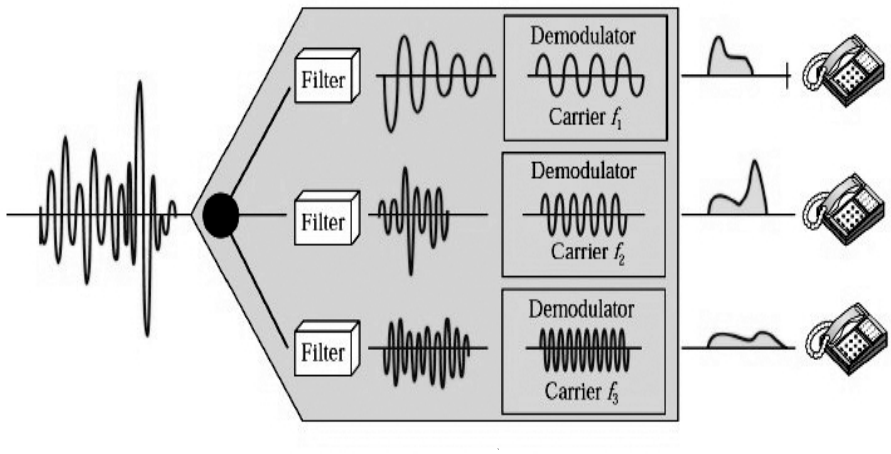


Figure 6.18: FDM demultiplexing process [1]

Time Division Multiple Access (TDMA)

TDMA allows the bandwidth of the channel to be shared by different stations by allocating each station a specific time slot. Only the designated station can send data in that time slot. It cannot be used by any other station for transmission. The problem with this access method is synchronization between different stations. Each station must be aware of the beginning and end of its time slot. A station should also know the location of its time slot. This is challenging due to the propagation delays introduced into the system when stations are scattered over a huge area.

To minimize the effect of these delays, guard times are inserted in between the allotted time slots. Synchronization is achieved by placing some synchronization bits at the beginning of each time slot. Figure 6.19 shows how time slots are maintained in TDMA.

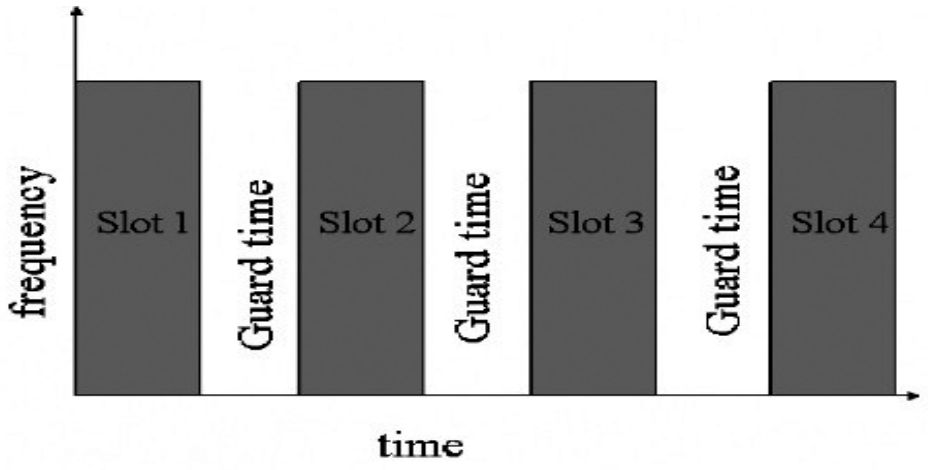


Figure 6.19: Time-Division Multiple Access [3]

Time Slots and Frames

In each connection the data flow is divided into units. To build a frame the link combines one unit from each connection. The size of a unit can be one or more bits. If the number of input connections to the multiplexer is *n* then the minimum number of time slots in each frame is also *n*. Each slot contains a single unit from each connection. To guarantee dataflow, the data rate of the link that carries data from *n* connections should be *n* times the data rate of a connection. So the duration of a unit in a connection is n times more than the duration of a time slot in a frame.

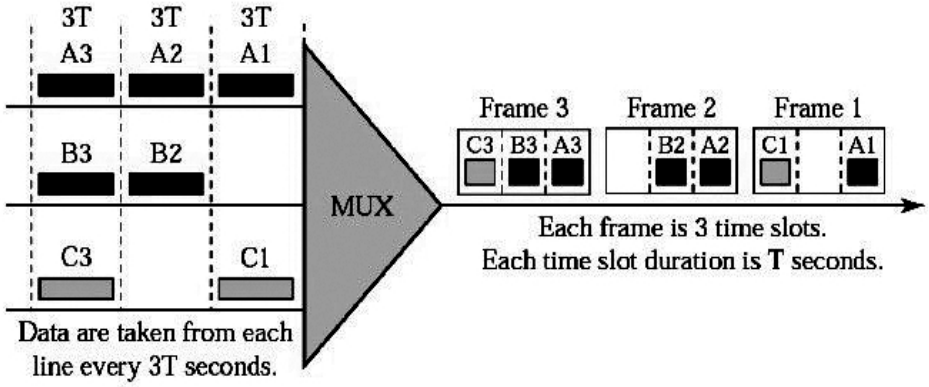


Figure 6.20 TDM time slots and frames [1]

In Figure 6.20the link data rate is 3 times more than the data rate of the connection. Similarly the duration of a unit on the connection is 3 times

more than duration of the unit on the link. Each unit is 3 times longer in duration before multiplexing than after.

Interleaving

TDM can be imagined as two rapidly rotating switches as shown in Figure 6.21. One switch is located on the multiplexing side and the other is located on the demultiplexing side. The switches rotate with the same speed but in reverse directions. When the switch opens in front of a connection at the multiplexing side, that connection gets the chance to pass a unit to the link. This procedure is called interleaving. Similarly when the switch opens in front of a connection at the demultiplexing side, that connection gets the chance to collect a unit from the link.

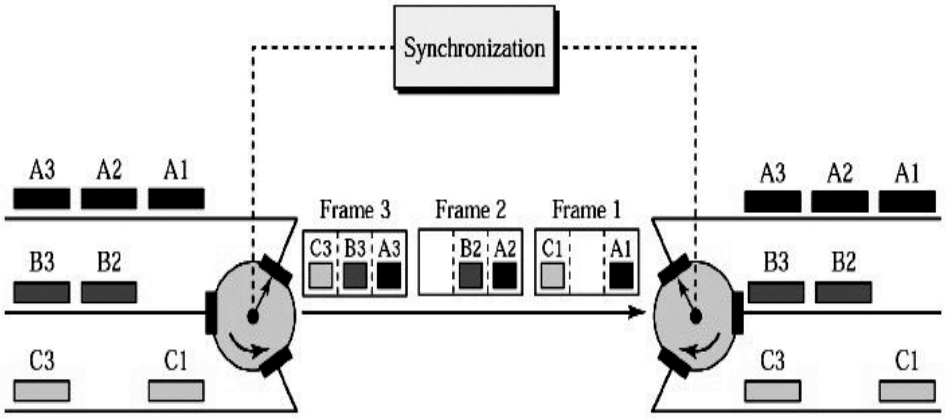


Figure 6.21: Interleaving [1]

Synchronization

In TDMA, synchronization between the multiplexer and the demultiplexer is a major problem. If they are not synchronized then a bit intended for a specific channel may be accepted by a wrong channel.

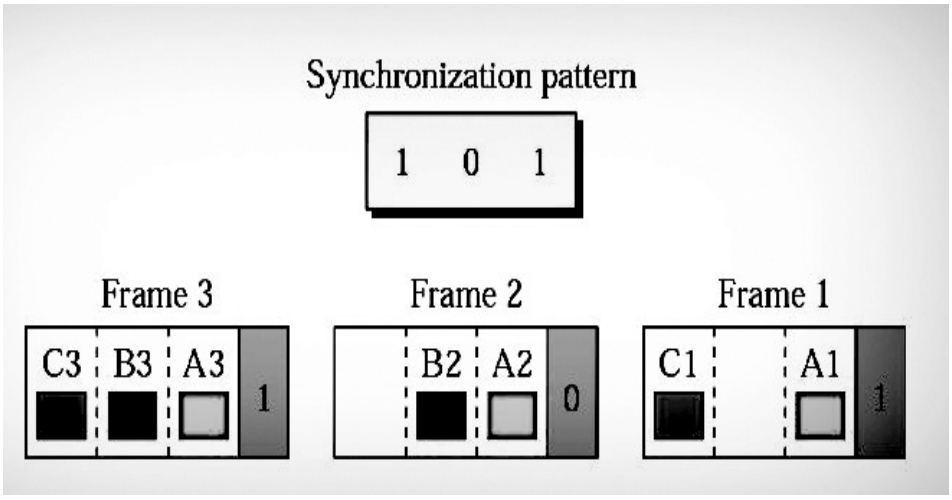


Figure 6.22: Synchronization [1]

Therefore one or more synchronization bits are added at the start of every frame. These bits are called framing bits. They are arranged in a specific way which helps the demultiplexer to synchronize with the inbound stream and separate the time slots precisely. The synchronization pattern consists of 1 bit per frame alternating between 0 and 1. Figure 6.22 above shows the synchronization pattern.

Code-Division Multiple Access (CDMA)

In CDMA a single channel occupies the complete bandwidth of the link, whereas in FDMA the available bandwidth is divided into different frequency bands. CDMA also differs from TDMA, as in CDMA, all stations can transmit at the same time and there is no need of sharing the bandwidth in time. CDMA is based on coding theory. A unique code is allotted to each station. Each code is a sequence of numbers called chips.

Let us take four stations for instance. Each station has a sequence of chips which we label A, B, C and D. If a station has to transmit a 0 bit, it transmits a -1. If the station has to transmit a 1 bit, it transmits a +1. An idle station sends no signal, which is denoted by a 0. Figure 6.23 shows the chip sequences.

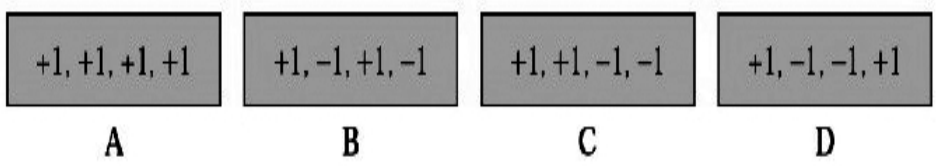


Figure 6.23: Chip sequences [1]

In this example the 1-bit interval of a link is shared by four stations. Stations 1 and 2 send a 0 bit, station 4 sends a 1 bit and station 3 remains silent. The procedure can be repeated for additional intervals.

Multiplexer

1) The multiplexer receives one encoded number from each station (-1, -1, 0 and +1).
2) The encoded number sent by station 1 is multiplied by each chip in sequence A. A new sequence is the result (-1, -1, -1, -1). Similarly, the encoded number sent by station 2 is multiplied by each chip in sequence B. The same is true for the remaining two encoded numbers. The result is four new sequences.
3) All first chips are added, as are all second, third, and fourth chips. The result is one new sequence.
4) The sequence is transmitted through the link. Figure 6.24 shows the working of the multiplexer.

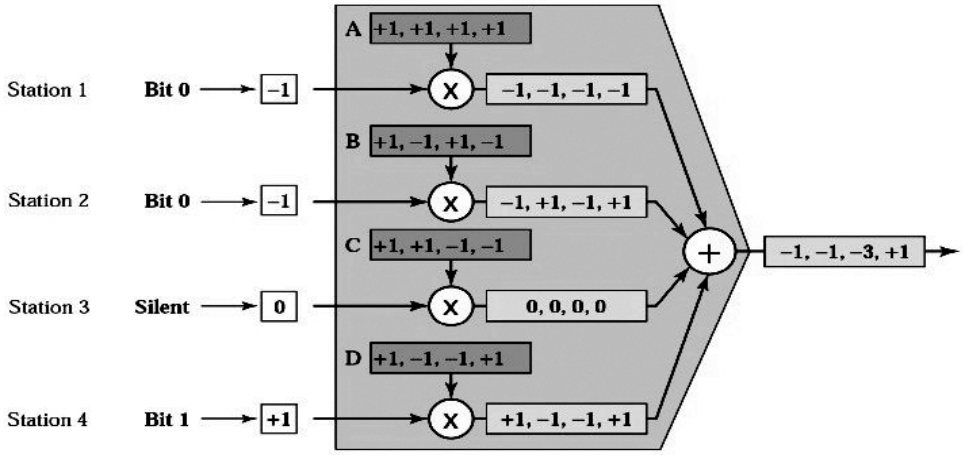


Figure 6.24: CDMA multiplexer [1]

Demultiplexer

1) The demultiplexer receives the sequence sent across the link.
2) It multiplies the sequence by the code for each receiver. The multiplication is done chip by chip.
3) The chips in each sequence are added. The result is always +4, -4, or 0.
4) The result of step 3 is divided by 4 to get -1, +1, or 0.
5) The number in step 4 is decoded to 0, 1, or silence by the receiver. Figure 6.25 shows the working of the demultiplexer.

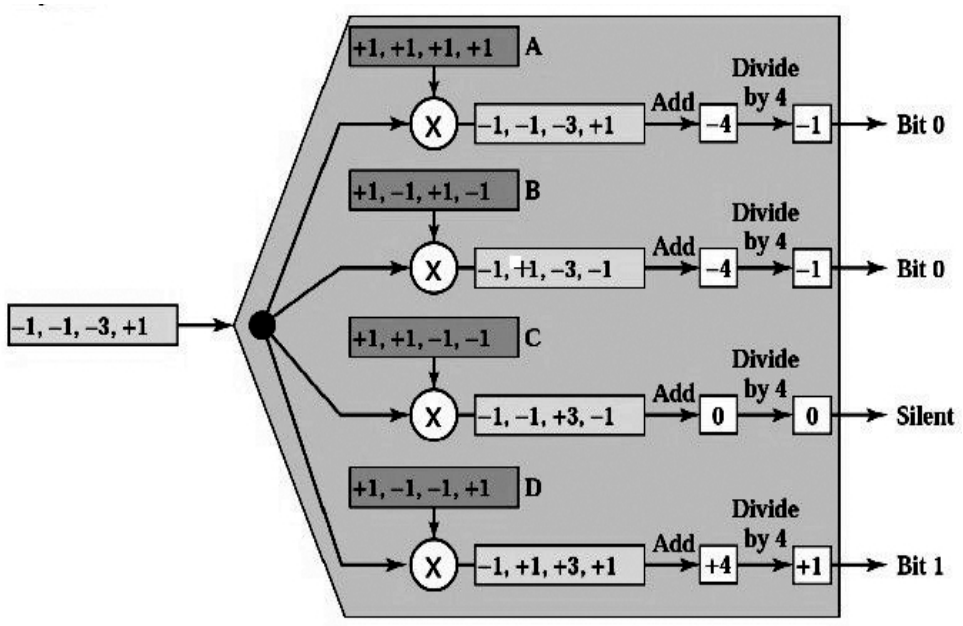


Figure 6.25: CDMA demultiplexer[1]

CHECK YOUR PROGRESS

1. Discuss the difference between Polling and Selecting with the help of suitable diagrams.
2. How does TDMA deal with the synchronization problem between the multiplexer and the demultiplexer?
3. What is the importance of guard bands in FDMA?

6.5 SUMMARY

Multiple Access protocols are used to coordinate access to the link when multiple nodes or stations are using the same link for transmission. They are basically classified into Random-access protocols, Controlled-access protocols and Channelization protocols. In case of Random-access protocols, ALOHA was the first method to be used. Every station that needs to send a frame to another station first sends it to the base station. The base station receives the frames and relays it to the intended destination. The next method CSMA requires, that each station first listen to the medium (or check the state of the medium) before sending. CSMA has two variants: CSMA/CD (for collision detection) and CSMA/CA (for collision avoidance). Similarly three popular Controlled access protocols are Reservation, Polling and Token Passing. In the Reservation access method, a station needs to make a reservation before sending data. In Polling method, it is up to the primary device to determine which secondary device is allowed to use the channel at any given time. In Token Passing method, a station is authorized to send data when it receives a special frame called a token. Channelization protocols can be divided into FDMA, TDMA and CDMA. In FDMA, the available bandwidth is divided into frequency bands and each station is allocated a band to send its data. In TDMA each station is allocated a time slot during which it can send data. In CDMA, different users use same frequency at the same time, but with different spreading code.

6.6 TERMINAL QUESTIONS

1. Write down the steps involved in Token Passing method.

2. A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces:

a. 1000 frames per second

b. 500 frames per second

c. 250 frames per second

Find the throughput in case of slotted ALOHA for the same three conditions as shown above.

3. Station 1 has to send a 1 bit and station 2 has to send a 0 bit. What is the sequence generated by the multiplexer if CDMA is used? Draw a suitable diagram to support your answer.
4. Is the reservation access method suitable for a very large network in which many stations are idle? Why or why not?
5. With the help of a neat and labelled diagram show the working of CSMA/CA.

REFERENCES

[1] Behrouz A. Forouzan,Chapter 13, "Data Communications and Networking (3rd Edition)".

[2] Behrouz A. Forouzan,Chapter 12, "Data Communications and Networking (4th Edition)".

[3] http://www.memoireonline.com/08/08/1453/m_study-of-smart-antennas-on-mobile-communications17.html

UNIT-7 THE MEDIUM ACCESS CONTROL SUBLAYER

Structure

7.0 INTRODUCTION

The Medium Access Control Sublayer allows effective sharing of the media among multiple nodes trying to transmit signal at the same time. It is not certain if the bit stream accepted by the data link layer is free from errors. Some bits may have been altered and the number of bits received may be more or less than what was transmitted. Data Link Layer usually partitions the bit stream into frames. It then appends a checksum to each frame and sends the frames to the Physical layer.

This unit discusses three IEE Standards: 802.3 (Ethernet), 802.4 (Token Bus), 802.5 (Token Ring). Ethernet is the most widely installed local area network (LAN) technology. Three generations of Ethernet have been discussed here: Traditional Ethernet, Fast Ethernet and Gigabit Ethernet. Token Bus is a Local Area Network (LAN) in which the stations connected to a bus or a tree constitute a *logical ring. The token is passed from one node to other and only the node holding the token can transmit.* A token ring network is a local area network (LAN) in which all the stations are linked in the form of a ring or a star topology and pass tokens from one host to another.

The rest of the unit is organized as follows. Section 7.1 points out the objectives of the unit. Section 7.2 discusses the framing techniques of Data Link Layer. Sections 7.3, 7.4 and 7.5 explain the IEEE Standards 802.3 (Ethernet), 802.4 (Token Bus) and 802.5 (Token Ring) respectively. Section 7.6 gives an overview of the unit and section 7.7 marks the end of the unit with an exercise for students.

7.1 OBJECTIVES

After the end of this unit, you should be able to understand:

- Basic framing methods of the Data Link Layer
- IEEE Standard 802.3: Ethernet
- IEEE Standard 802.4: Token Bus
- IEEE Standard 802.5: Token Ring

7.2 FRAMING [1]

Data Link Layer partitions the bit stream into distinct frames. It then appends a checksum to each frame and sends the frames to the Physical layer. When a frame arrives at the receiver site, the checksum is calculated again. If the newly calculated checksum is same to the one appended to the arrived frame then the frame has not been corrupted in transit. Data link layer can then accept the frame. But if the calculated checksum is different from the one appended to the arrived frame then the frame has been corrupted. In such a case data link layer discards the frame and may also send back an error report. The following four framing methods have been discussed in this section:

1. Byte count.
2. Flag bytes with byte stuffing.
3. Flag bits with bit stuffing.
4. Physical layer coding violations.

Byte Count

This is the first framing method where a new field is added to the header which indicates the count of bytes in the frame. When the data link layer of the receiver reads the field, it learns the length of the frame and hence where it ends. Figure 7.1a shows a bit stream consisting of four frame. Frames 1 and 2 are 5 bytes long each. Similarly frames 3 and 4 are 8 bytes long each.

But the method fails if the value in the field is altered. For example, in Figure 7.1b a single bit flip changes the byte count of frame 2 from 5 to 7. This will desynchronize the receiver which now misreads frame 2 and subsequently all the frames that follow. Therefore this framing method is seldom used. Figure 7.1 shows the Byte framing method with and without error.

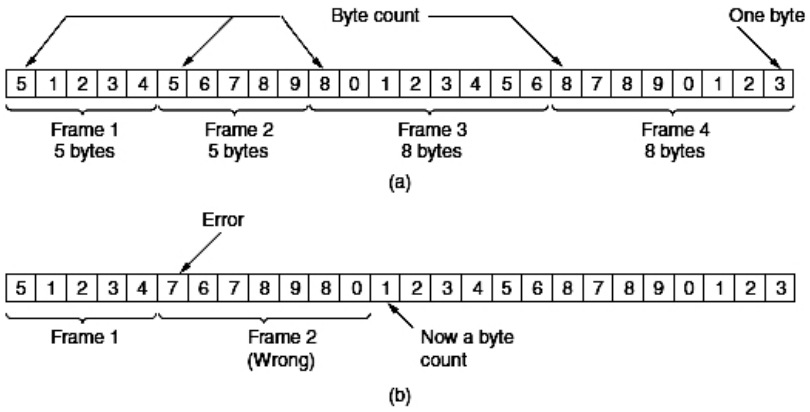


Figure 7.1 A byte stream (a) Without errors (b) With one error [1]

Flag bytes with byte stuffing

In this method a special byte is added to the beginning and end of each frame. This byte is called a *flag byte*. Two successive flag bytes denote the end of one frame and the beginning of the subsequent frame. So if the receiver is out of synchronization it searches for two adjacent flag bytes and infers that this is the end of the existing frame and the beginning of the subsequent frame.

Figure 7.2a shows how the flag bytes can mark the start and end of a frame.

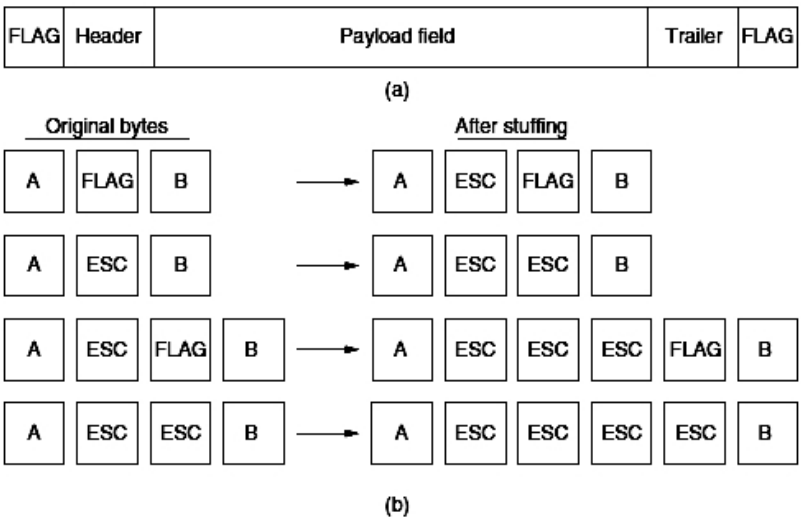


Figure 7.2: (a) A frame delimited by flag bytes (b) Four examples of byte sequences before and after byte stuffing [1]

A flag byte may also occur in the course of the data, specifically when the binary data consists of songs or photographs. The receiver may thus loose synchronization and misreads the frames. This problem can be solved by having the data link layer of the sender introduce a special escape byte (ESC) just prior to a flag byte in the data. Thus, the presence or absence of an escape byte before a flag byte will tell the receiver if it the flag byte is just a part of the data or it is a framing byte. The data link layer of the receiver will remove the escape byte before handing the data to the network layer. *This method is called byte stuffing*. Figure 7.2b shows four examples of byte sequences before and after byte stuffing.

Data may also contain an escape byte sometimes. In this case too an additional escape byte is inserted right before it. When data reaches the receiver, it removes the first escape byte and leaves the data byte that follows. The data byte may be an escape byte or a flag byte. The byte sequence after destuffing is exactly similar to the original byte sequence.

Flag bits with bit stuffing

In this framing method a special bit pattern, 01111110 (0×7E in hexadecimal) is inserted at the beginning and end of each frame. This pattern is a flag byte. Each time the data link layer of the sender comes across five successive 1s in the data, it inserts a 0 bit after it. This **bit stuffing** is equivalent to byte stuffing, in which an escape byte is inserted before each flag byte that happens to be a part of the data.

When the receiver finds five successive1s, followed by a 0, it removes the 0. Bit stuffing is also transparent to the network layer in both computers just like byte stuffing. If flag pattern 01111110 is contained in user data, it is transmitted as 011111010. When the receiver sees the data, it removes the 0 following the five successive 1s. The data is thus stored as 01111110 in the memory of the receiver. Figure 7.3 below explains the scenario.

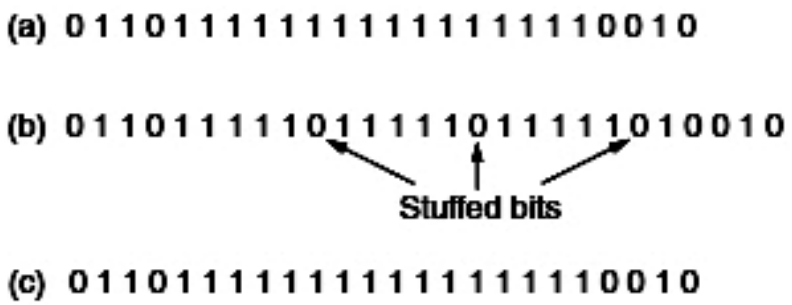


Figure 7.3: Bit stuffing (a) Original data. (b) Data as it appears during transmission. (c) Data as it is stored in the receiver's memory after destuffing [1]

Through bit stuffing the beginning and end of a frame can now be located without any ambiguity. This is so because the pattern 01111110 does not appear anywhere in the middle of the data. If the receiver is out of

synchronization it just has to look for these patterns in the received bit stream.

Physical layer coding violations

Bits can be encoded as signals, which leads to redundancy. It means that some signals won't appear within the data. For instance in the 4B/5B line code each 4 bit data is mapped into a 5 bit pattern to ensure sufficient bit transitions. In this case 16 patterns out of the 32 possible patterns are not utilized. Some reserved signals are utilized to mark the beginning and end of frames. The advantage of this method is that, now it is easy to identify the beginning and end of a frame without the need to insert special bytes in the data.

A combination of these methods are used by several data link layer protocols. The frames in Ethernet and 802.11 have a specific pattern called a *preamble* at their beginning. A preamble may be very long (72 bits for 802.11). It lets the receiver prepare for the inbound frame. It is again followed by a length field in the header that helps the receiver to identify where the frame ends.

CHECK YOUR PROGRESS

1. A bit string, 011111101111101111110, needs to be transmitted at the data link layer.
2. What is the string actually transmitted after bit stuffing?
3. The following data fragment occurs in the middle of a data stream for which the byte stuffing algorithm is used: A B ESC C ESC FLAG FLAG D. What is the output after stuffing?

7.3 IEEE 802.3 ETHERNET [2]

IEEE 802.3 is a working group and a collection of IEEE standards produced by the group that defines the physical layer and the data link layer's media access control (MAC) of the wired Ethernet. This is basically a local area network technology having some wide area network applications. Nodes and/or networking devices (routers, switches, hubs) are physically connected by various kinds of fiber or copper cables. This section describes three generations of Ethernet: Traditional Ethernet, Fast Ethernet and Gigabit Ethernet.

A. Traditional Ethernet

Traditional Ethernet was devised to function at 10 Mbps speed. The medium is shared by all the available devices. Each devices accesses the medium through a contention method (CSMA/CD).

Frame

The Ethernet frame consists of seven fields: preamble, start frame delimiter (SFD), destination address (DA), source address (SA), length or type of protocol data unit (PDU), upper layer data and the CRC. There is no provision for acknowledgement of received frames in Ethernet. This makes it an unreliable medium. Figure 7.4 shows the 802.3 MAC frame.

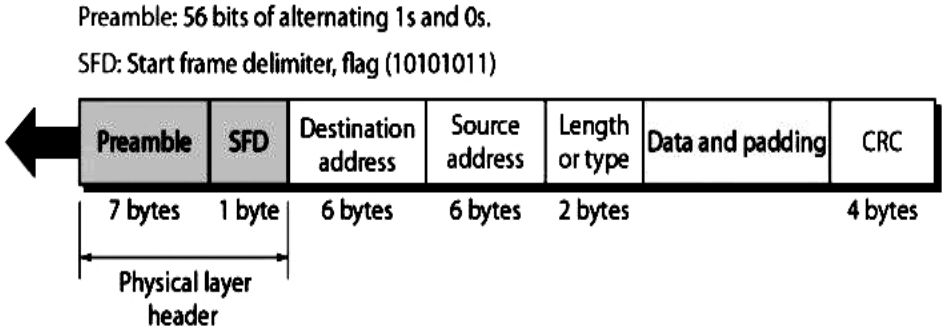


Figure 7.4: 802.3 MAC frame [3]

Preamble: The initial field in the 802.3 MAC frame is the preamble that is 7 bytes long. It consists of alternating 0s and 1s that inform the receiver of the inbound frame and allow it to synchronize. Preamble is formally not a part of the frame and is actually attached by the physical layer.

Start frame delimiter (SFD): The next field is 1 byte in length (10101011). It indicates the start of the frame. The last two bits of the byte are 11 and they inform the receiver that the succeeding field contains the address of the destination.

Destination address: This field is 6 bytes long. It holds the physical address of the station/stations to which the packet is destined.

Source address: This field is also 6 bytes in length. It holds the physical address of the station which is source of the frame.

Length/Type: This field contains the length or the type of the PDU packet. If the value in the field is smaller than 1518, it is a length field and denotes the length of the data field that follows. If the value is more than 1536, it is a type field and defines the type of the PDU packet that is contained in the frame.

Data: This field has a minimum length of 46 bytes and a maximum length of 1500 bytes. It holds data encapsulated from the upper-layer protocols.

CRC: The last field contains the error detecting code.

Physical Layer

Figure 7.5 shows the physical layer for 10-Mbps Ethernet which consists of four sublayers – Physical Layer Signaling (PLS), Attachment Unit Interface (AUI), Medium Attachment Unit (MAU) and Medium-Dependent Interface (MDI).

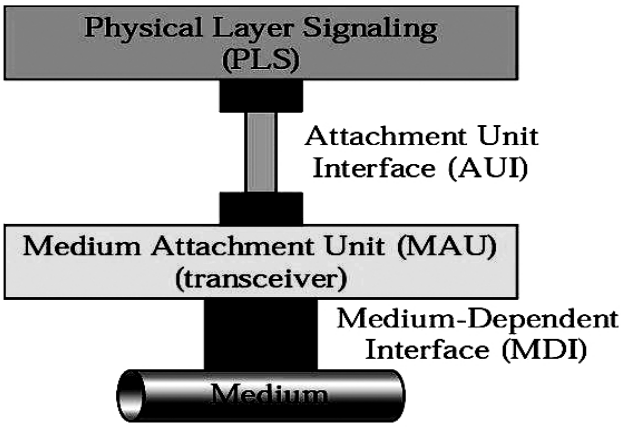
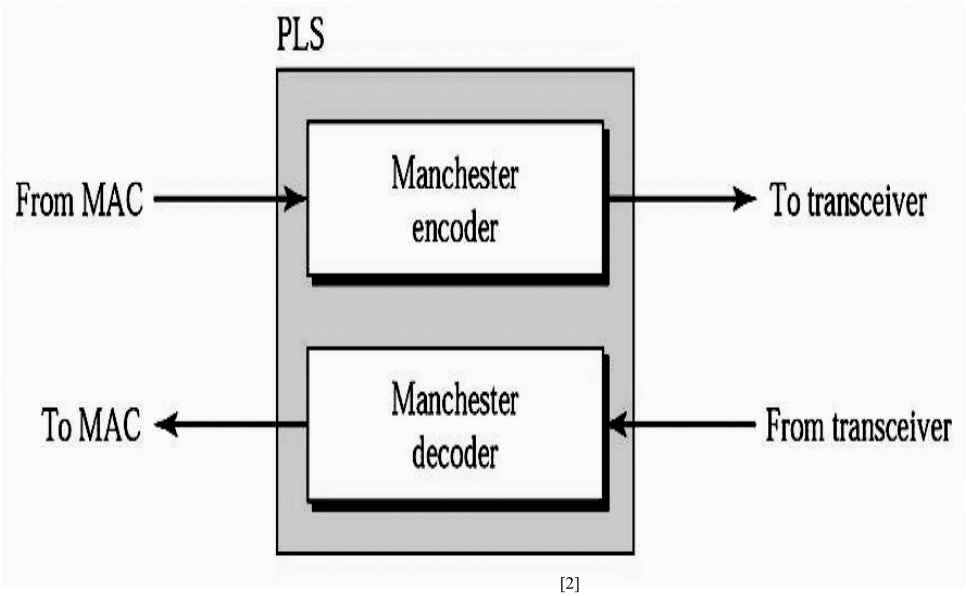


Figure 7.5: Physical Layer [2]

1. PLS

The Physical Layer Signaling (PLS) sublayer receives data from MAC, encodes it and then forwards the encoded data to the transceiver (Medium Attachment Unit). Similarly when it receives data from the transceiver it decodes the data and then forwards it to the MAC. PLS operates at a data rate of 10 Mbps. Figure 7.6 shows the working of PLS.



[2]

Figure 7.6: PLS

2. AUI

AUI describes the interface between the PLS and the MAU. This interface was used in the first implementation of Ethernet. It used 4 pairs of twisted-pair cable. Figure 7.7 shows how AUI connects PLS and MAU.

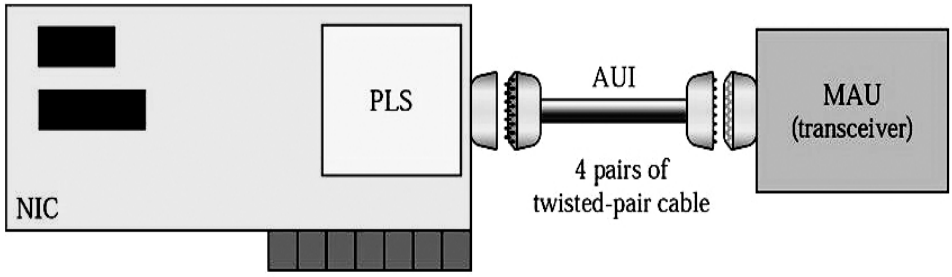


Figure 7.7: AUI [2]

3. MAU (Transceiver)

The MAU or transceiver is medium-dependent. Each type of medium (coaxial cable, twisted pair cable or fiber-optic cable) needs a MAU that supports it. MAU forwards signals to the medium and receives signals from the medium. It is also able to detect collisions. Figure 7.8 shows the functions of MAU.

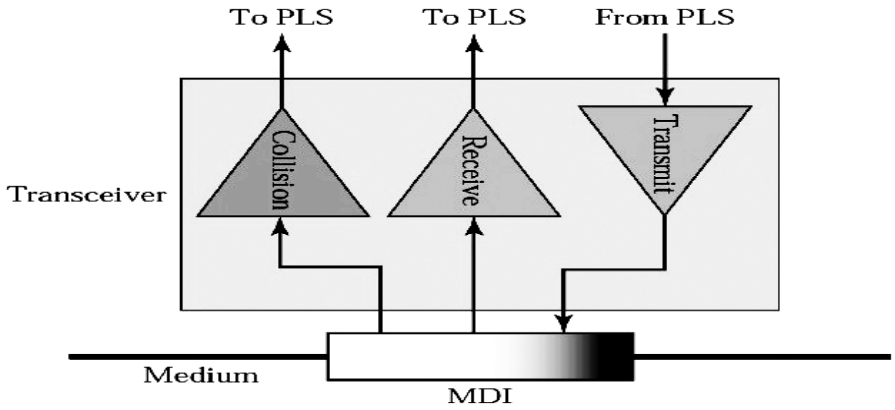


Figure 7.8: MAU (Transceiver) [2]

4. MDI

MDI is simply a hardware that is used to connect the transceiver to the medium.

Physical Layer Implementation

There are four common baseband implementations of the Traditional Ethernet as shown in the Figure 7.9 below.

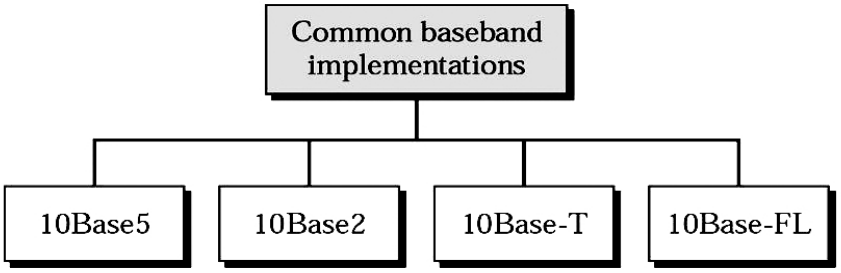


Figure 7.9: Categories of traditional Ethernet [2]

1. 10Base5: Thick Ethernet

The first implementation is named 10Base5, thick Ethernet, or Thicknet. The cable used in this implementation is almost as thick as a garden hose and rigid enough to be bent by one's bare hands. 10Base5 uses a bus topology. It has an external transceiver which is connected to a thick coaxial cable through a tap. Figure 7.10 shows the connections in the Thick Ethernet.

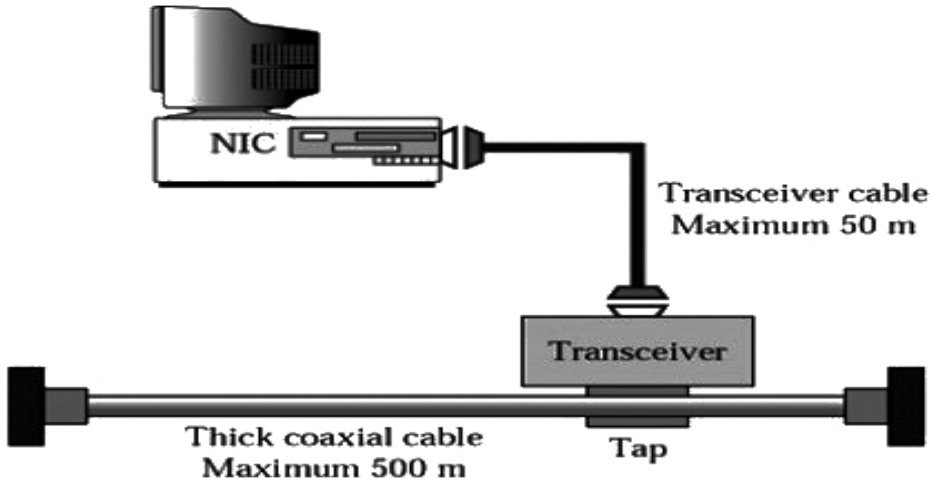


Figure 7.10: Connection of a station to the medium using 10Base5 [2]

2. 10Base2: Thin Ethernet

The second implementation is named 10Base2, thin Ethernet, or Cheapernet. AUI cable is not required if the station has an internal transceiver. On the other hand, if the station does not have an internal transceiver then an external transceiver should be connected to it through an AUI cable. 10Base2 uses a bus topology with an internal transceiver or a point-to-point connection via an external transceiver as shown in Figure 7.11.

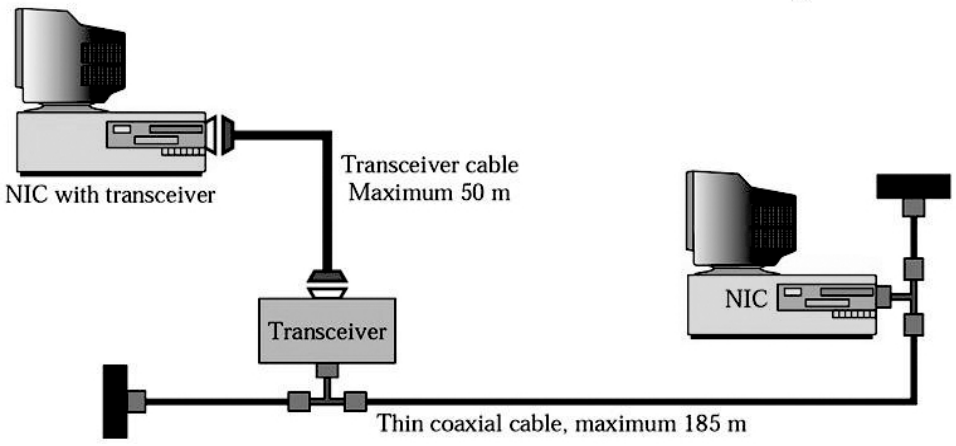


Figure 7.11: Connection of stations to the medium using 10Base2 [2]

3. 10Base-T: Twisted-Pair Ethernet

10Base-T is based on the star topology. AUI cable is not needed if the station has an internal transceiver. If the station does not have an internal transceiver then it is connected to an external transceiver through an AUI cable. The transceiver is then connected to the hub, as shown in the Figure 7.12 below.

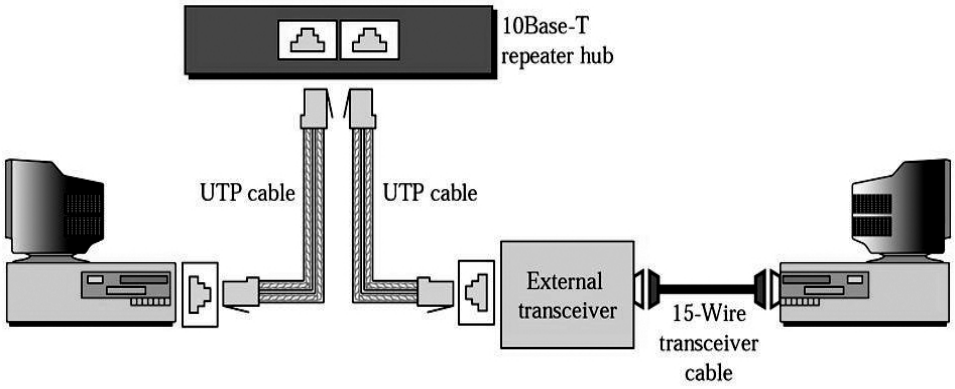


Figure 7.12: Connection of stations to the medium using 10Base-T [2]

4. 10Base-FL: Fiber Link Ethernet

10Base-FL is also based on the star topology. It is implemented through an external transceiver called fiber-optic MAU. AUI cable is used to connect the station and the transceiver. The transceiver is linked to the hub by means of two pairs of fiber-optic cables. Figure 7.13 shows the complete setup.

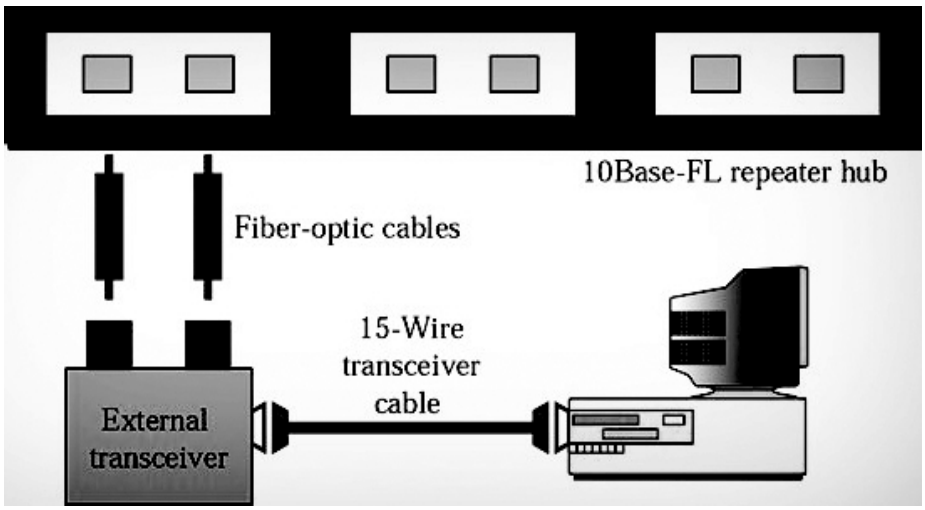


Figure 7.13: Connections of stations to the medium using 10Base-FL [2]

Bridged Ethernet

In Figure 7.14a, a network with 12 stations has been shown. The total capacity of the network is 10 Mbps which is shared between the 12 stations. The same network has been divided into two subnetworks with 6 stations each in Figure 7.14b. Each newly formed subnetwork, now has a

capacity of 10 Mbps which is shared between 6 stations (actually 7 because the bridge acts as a station in each segment). Thus if a network is divided into two or more segments then more bandwidth is gained for each segment.

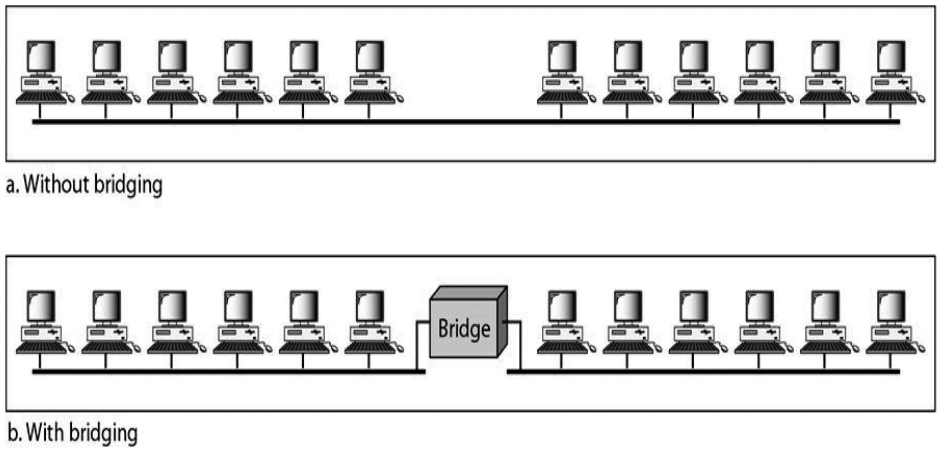


Figure 7.14: A network with and without a bridge [2]

Another advantage of a bridge is the separation of the collision domain. With bridging the collision domain becomes smaller and the probability of collision is also reduced. In Figure 7.14a, without bridging, 12 stations are contendingto access the medium. In Figure 7.14b, with bridging, only 6 stations are contending to access the medium.

Switched Ethernet

In Switched Ethernet a network is divided into N subnetworks. N is the number of stations on the local area network. Basically an N-port switch is implemented here. The bandwidth is thus shared only between the station and the switch (5 Mbps each). The collision domain is also divided into N domains. Figure 7.15 shows the network architecture in Switched Ethernet.

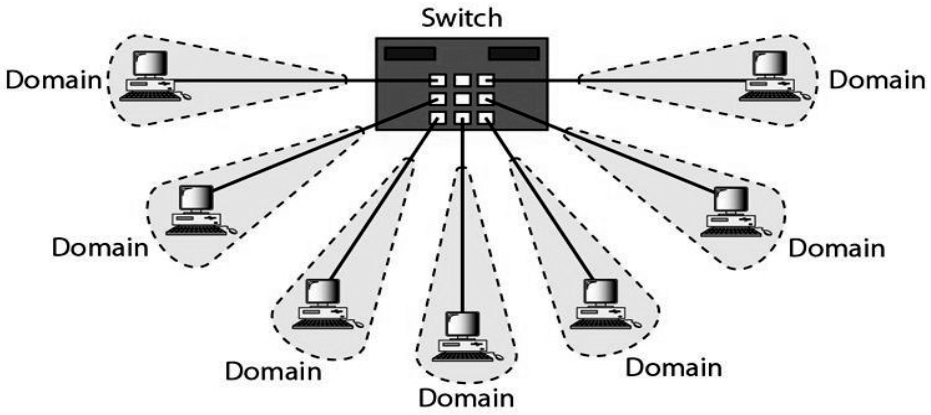


Figure 7.15: Switched Ethernet [2]

Full-Duplex Ethernet

The full-duplex mode increases the capacity of the network from 10 Mbps to 20 Mbps. Figure 7.16 below shows the full duplex mode of a switched Ethernet. The configuration uses two links instead of a single link. One link is for transmitting data from the station to the switch and the other link is for receiving data from the switch.

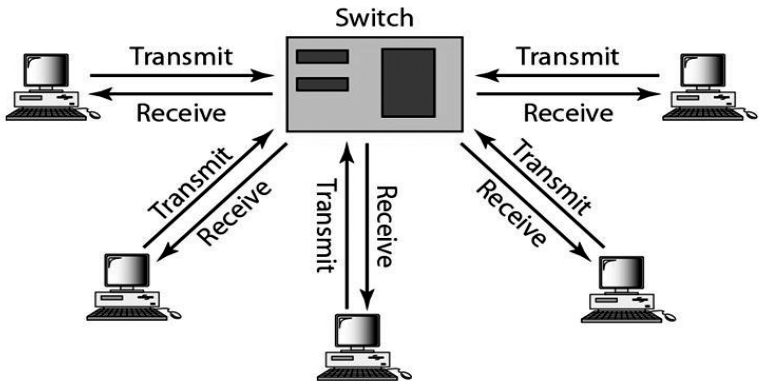


Figure 7.16: Full-duplex switched Ethernet [2]

B. Fast Ethernet

Fast Ethernet has a much higher data rate (100 Mbps) as compared to Traditional Ethernet. The access method is CSMA/CD. However for a full-duplex connection there is no need for CSMA/CD. Frame format, addressing, minimum and maximum frame lengths are all similar to the Traditional Ethernet. A new feature called *Autonegotiation* is added which allows two devices to discuss the data rate or mode of the operation. It allows two incompatible devices to connect to each another.

Physical Layer

The physical layer is made up of four sublayers: Reconciliation (RS), Medium-Independent Interface (MII), Physical Layer Entity (PHY), and, Medium-Dependent Interface (MDI). Figure 7.17 shows the physical structure for Fast Ethernet. RS is present in all the implementations. The PHY and MDI are medium-dependent.

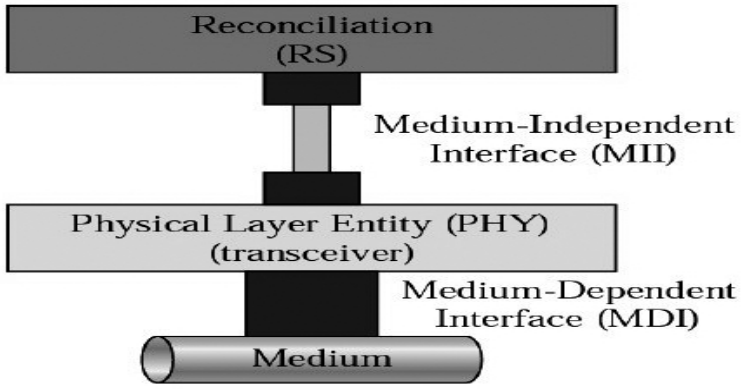


Figure 7.17: Fast Ethernet physical layer [2]

1. RS

The RSsublayer in Fast Ethernet substitutes the PLS sublayer in the Traditional Ethernet. PHY sublayer now performs the encoding and the decoding of data. The RS sublayer is accountable for everything else including the forwarding of data in 4-bit format to the MII.

2. MII

The MII sublayer in Fast Ethernet replaces the AUI sublayer in the Traditional Ethernet. MII operates at 10 and 100 Mbps. It uses a parallel data path which can transmit 4 bits at a time between the PHY sublayer and the reconciliation sublayer. Figure 7.18a shows a scenario where MII is used but Figure 7.18b shows a scenario where MII is not used.

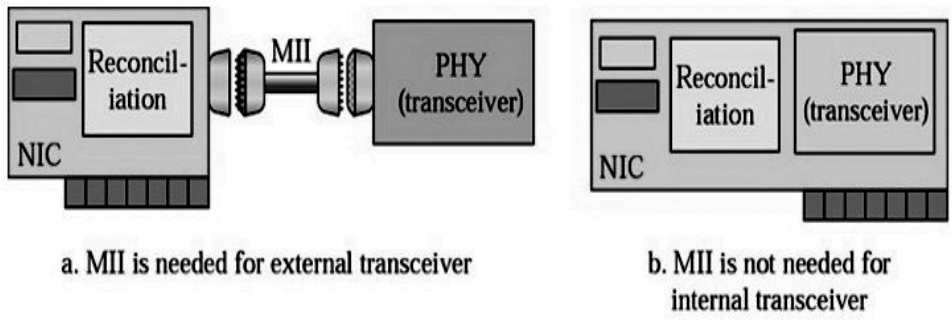


Figure 7.18: Connection between RS and PHY (a) With MII (b) Without MII[2]

3. PHY (Transceiver)

In Fast Ethernet, the transceiver is called the Physical Layer Entity (PHY). The PHY sublayer here performs encoding and decoding, besides the regular functions performed by transceiver of Traditional Ethernet. If the station does not have an internal transceiver then it is connected to an external transceiver through an MII cable. But if the station has an internal transceiver then an MII cable is not needed.

4. MDI

Medium-Dependent Interface (MDI) is simply a hardware that connects the transceiver (either internal or external) and the medium.

Physical Layer Implementation

Fast Ethernet can be classified either into a two-wire implementation or a four-wire implementation. The two wire implementation is called 100Base-X, which is again divided into two subcategories: 100Base-TX (twisted-pair cable) and 100 Base-FX (fiber-optic cable). The four-wire implementation is called 100Base-T4 which is devised only for the twisted-pair cable. Figure 7.19 shows the implementations of Fast Ethernet.

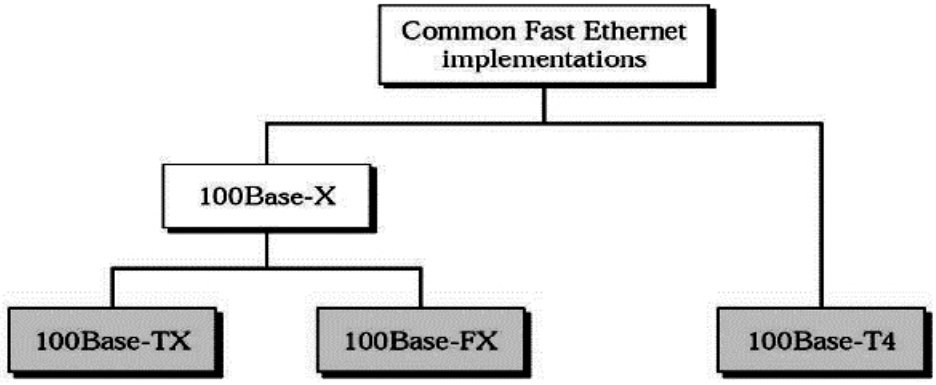


Figure 7.19: Fast Ethernet implementations [2]

1. 100Base-TX

It uses two pairs of twisted-pair cables in a star topology. Either category 5 UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair) is used. The station may have an internal transceiver or an external transceiver (with an MII cable) as shown in the Figure 7.20 below.

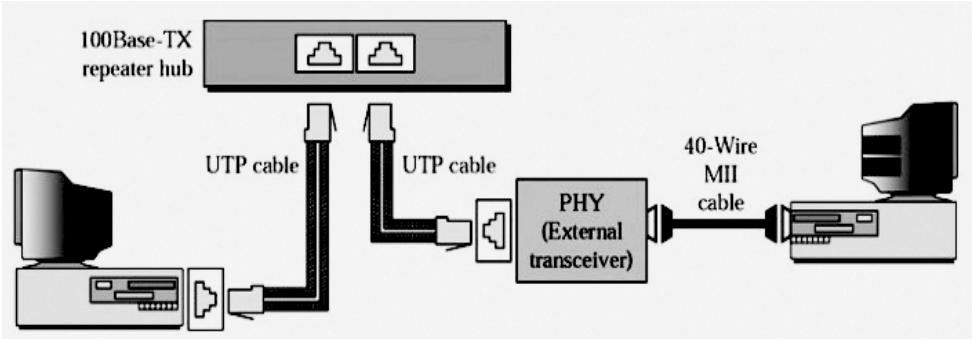


Figure 7.20: 100Base-TX implementation [2]

2. 100Base-FX

100Base-FX uses two fiber-optic cables in a star topology. The transceiver can be internal or external to the station. An MII cable is used in case of an external transceiver as can be seen in the Figure 7.21 below.

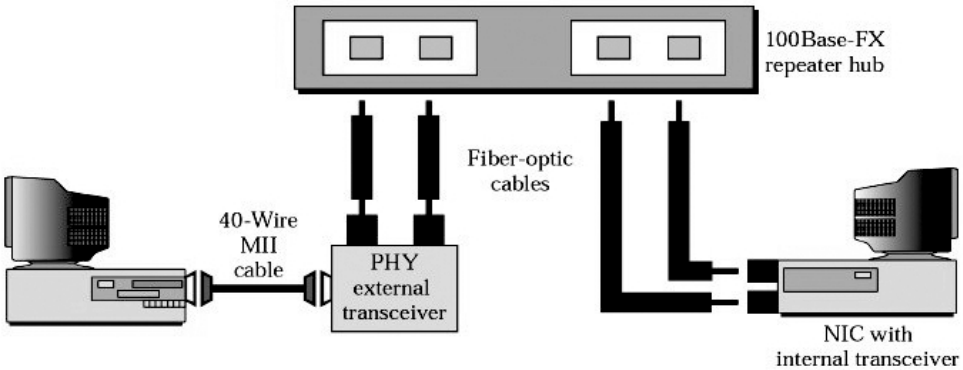


Figure 7.21: 100Base-FX implementation [2]

3. 100Base-T4

100Base-T4 was designed to use category 3 or higher UTP. The implementation uses four pairs of UTP for transmitting 100 Mbps. The transceiver function is similar to all other implementations but encoding and decoding is more complex. Figure 7.22 shows the implementation of 100Base-T4.

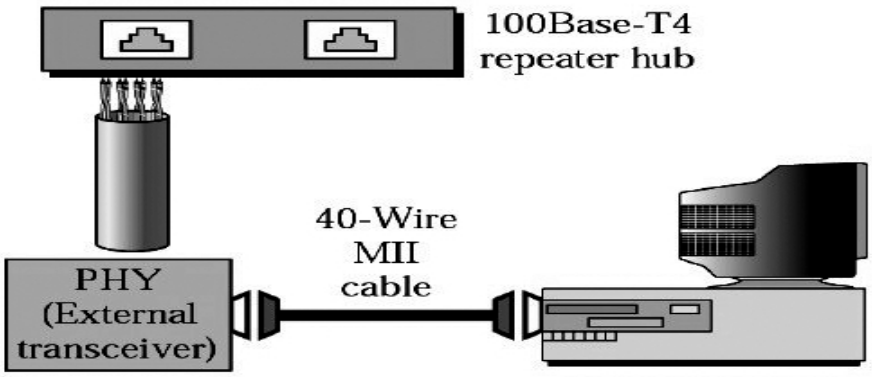


Figure 7.22: 100Base-T4 implementation [2]

C. Gigabit Ethernet

Gigabit Ethernet has two different methods for accessing the medium: full-duplex communication where CSMA/CD is not needed and half-duplex communication that uses CSMA/CD. More or less all implementations of Gigabit Ethernet use the full-duplex method.

Physical Layer

The physical layer is made up of four sublayers: reconciliation, GMII, PHY, and MDI. The reconciliation sublayer is present in all the implementations. Both PHY and MDI are medium-dependent sublayers. Figure 7.23 below shows the physical layer.

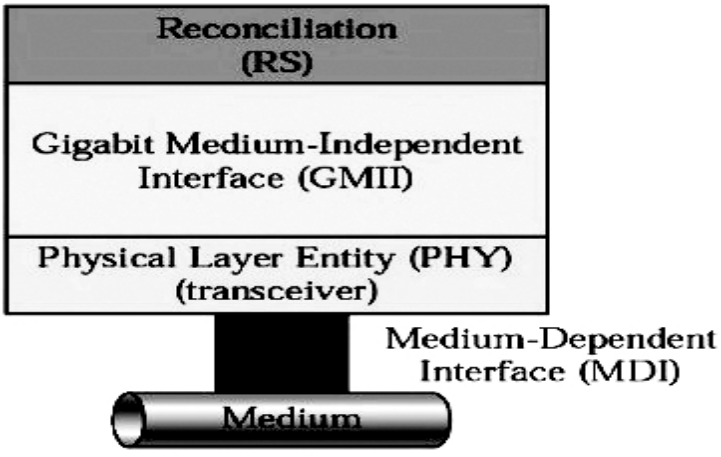


Figure 7.23: Physical Layer in Gigabit Ethernet [2]

1. RS

The RS sublayer forwards 8-bit parallel data to the PHY sublayer through the GMII interface.

2. GMII

GMII (Gigabit medium-independent interface) is a specification that defines how the reconciliation sublayer is to be connected to the PHY sublayer (transceiver). GMII is the counterpart of MII in Fast Ethernet. But it is not located outside the NIC. It operates only at 1000 Mbps and specifies a parallel data path (8 bits at a time) between the RS sublayer and the transceiver.

3. PHY (Transceiver)

The transceiver, similar to that in Fast Ethernet, is medium-dependent and also encodes and decodes. As there is no external GMII to provide connection, the transceiver can only be located inside the station.

4. MDI

MDI connects the transceiver to the medium just as in Fast Ethernet. Only RJ-45 and fiber-optic connectors are defined in Gigabit Ethernet.

Physical Layer Implementation

Gigabit Ethernet can be classified into either a two-wire implementation or a four-wire implementation as shown in Figure 7.24. The two-wire implementation is called 1000Base-X which can be further divided into 1000Base-SX (shortwave optical fiber), 1000Base-LX (long-wave optical fiber) and 1000Base-CX (short copper jumpers). The four wire implementation called 1000Base-T utilizes twisted-pair cable.

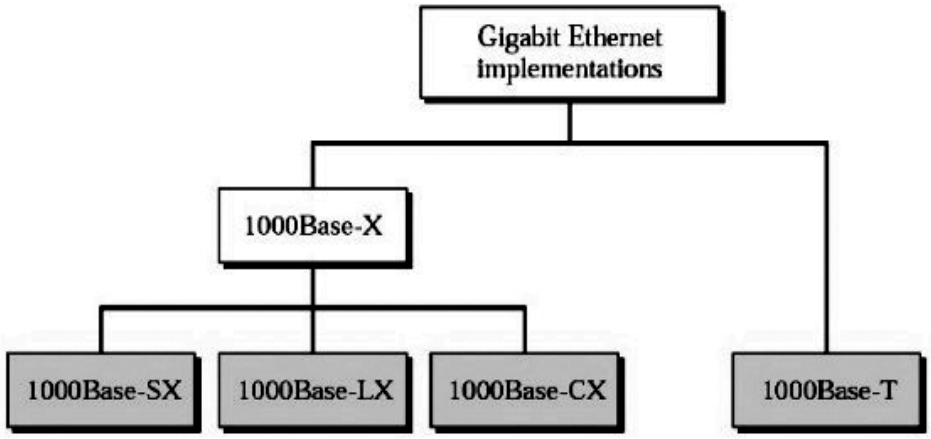


Figure 7.24: Gigabit Ethernet implementations [2]

1. 1000Base-X

Both 1000Base-SX and 1000Base-LX use two fiber-optic cables. 1000Base-SX uses shortwave laser and 1000Base-LX uses long-wave laser. In all the implementations internal transceiver is used. 1000Base-CX was designed to use STP cable, but it has not been implemented yet. Figure 7.25 below shows the implementation of 1000Base-X.

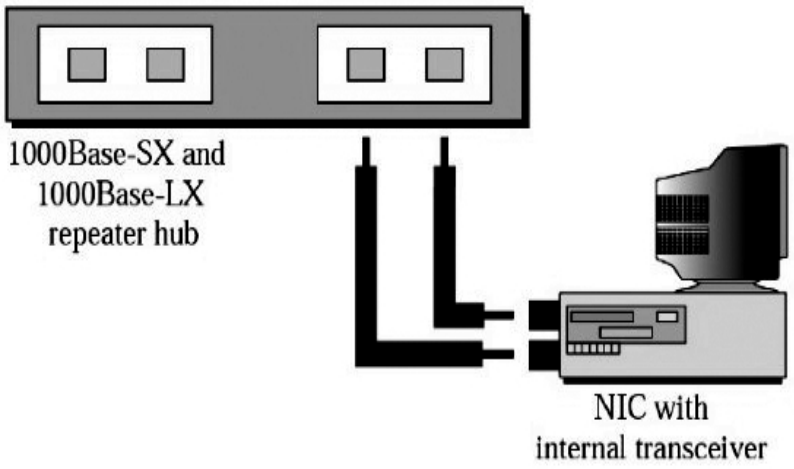


Figure 7.25: 1000Base-X implementation [2]

2. 1000Base-T

1000Base-T was designed to use category 5 UTP. Four twisted pairs achieve a transmission rate of 1 Gbps. Figure 7.26 shows the implementation of 1000Base-T.

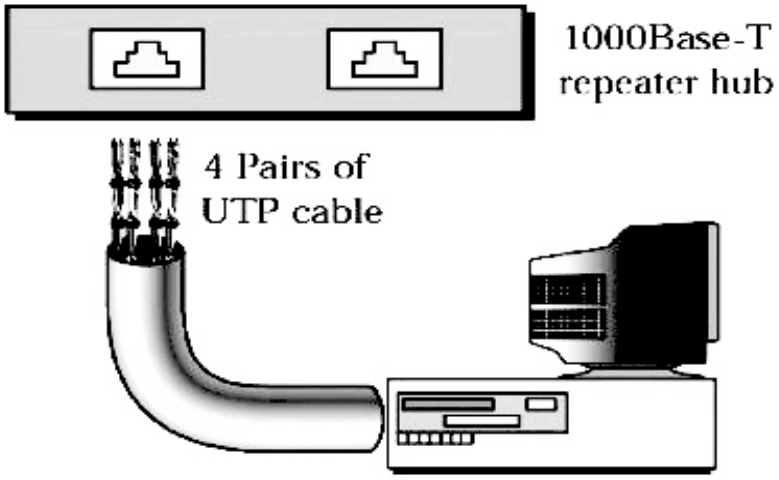


Figure 7.26: 1000Base-T implementation [2]

7.4 IEEE 802.4 TOKEN BUS [4]

In Token Bus, stations are connected to each other through a bus topology, but they follow the working procedure of a ring topology. The basic architecture of a Token Bus network is shown in the Figure 7.27 below.

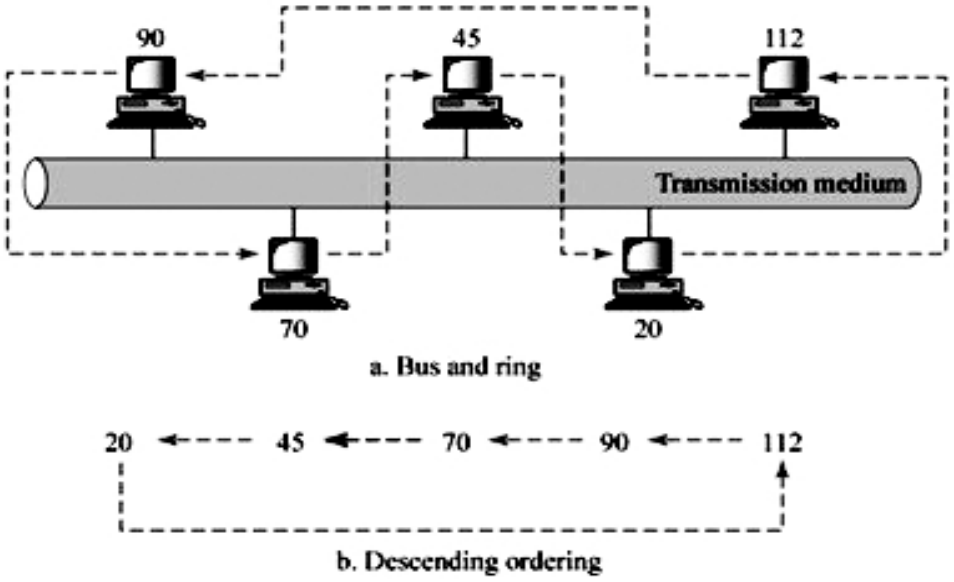


Figure 7.27: A Token Bus Network [5]

Basic procedure

In a Token Bus Network, each station is allotted a position in an ordered sequence. The last station in the sequence is followed by the first station as shown in the Figure 7.27 above. Each station knows the address of the station located to its left and right in the sequence. Tokens and data frames are passed from one station to another only according to this sequence. When a station needs to send frames, it grabs the circulating token and then starts sending frames. This process continues until the time limit has expired or the station has finished sending its frames.

Finally the token is released and is available to the next station in the sequence. Except the destination all the other stations discard the frame as soon as they receive it. Destination on the other hand, accepts the frame, marks it as read and sends it around the ring. When the sender receives the acknowledged data frame, it generates a new token. It then marks it as being available for use and sends it to the next station.

Classification of station

- Four priority classes, 0, 2, 4, and 6 have been defined in the Token Bus for traffic. Priority class 0 has the lowest priority and priority class 6 has the highest priority.
- As shown in the Figure 7.28 below each station is classified into four substations each having a different priority level (0, 2, 4 or 6)
- When data arrives from the upper layers, its priority is checked and then the data is forwarded to the appropriate substation (any one out of the four).
- In each substation a queue of frames is maintained waiting to be transmitted.

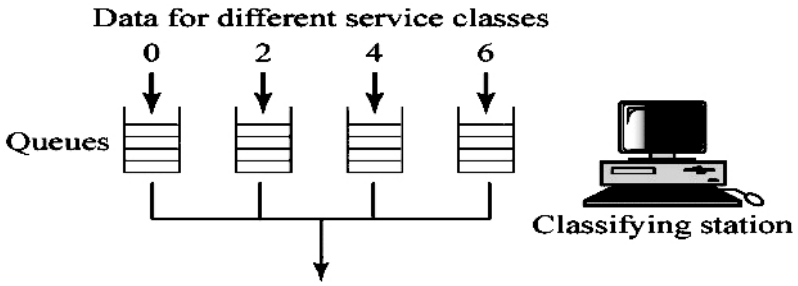


Figure 7.28: Classifying Station into substations [5]

- When a token arrives at a station, it is internally passed to priority 6 substation first. If the substation has any frames it can start transmitting them.
- When substation 6 finishes transmitting frames or when the time limit expires, the token is forwarded to substation 4.
- In this way the token reaches substation 0. Substation 0 releases the token after it has transmitted all the frames or the timer has expired.
- Finally the token is forwarded to the next station in the logical ring.

Frame format of Token Bus

The different fields present in the Token Bus frame format are:

Preamble: This field is minimum 1 byte in length. It serves the purpose of synchronization.

Start Delimiter: This field is 1 byte in length. It indicates the start of a frame.

Frame Control: This is a 1byte field. It differentiates a data frame from a control frame. In case of a data frame, this field holds the priority of the frame and a bit that can be set by the destination as an acknowledgement. In case of a control frame, this field specifies the type of the frame. The allowed types are ring maintenance frames and token passing frames.

Destination address: This field is 2- 6 bytes long. It holds the address of the destination.

Source address: This field is also 2- 6 bytes long. It holds the address of the source.

Data: This field may be 8182 bytes in length when 2 byte addresses are used and 8174 bytes in length when 6 byte addresses are used.

Checksum: This field is 4 bytes in length. It contains the error detecting code.

End Delimiter: This is a 1 byte field. It indicates the end of a frame.

The Figure 7.29 below shows the frame format of IEEE 802.4 (Token Bus) in detail.

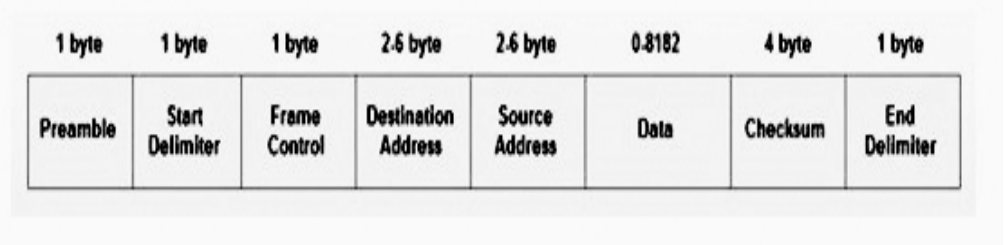


Figure 7.29: IEEE 802.4 frame format [4]

Control frames

The various control frames used in token bus are shown in Figure 7.30 below.

Frame Control field	Name	Meaning
00000000	Claim_token	Claim token during ring initialization
00000001	Solicit_successor_1	Allow station to enter the ring
00000010	Solicit_successor_2	Allow stations to enter the ring
00000011	Who_follows	Recover from lost token.
00000100	Resolve_contention	Used when multiple stations want to enter.
00001000	Token	Pass the token
00001100	Set_successor	Allow station to leave the ring.

Figure 7.30: Token Bus Frame Control [4]

7.5 IEEE 802.5 TOKEN RING [6]

A token ring network is a LAN where all the stations are linked to each other in a ring topology. A 3 byte frame called token keeps moving about the ring. The station that wants to send frames captures the token and then starts sending the frames. The process continues until the station has transmitted all its frames or the timer has expired. After that the token is released and it starts moving in the ring again. Collision is prevented as only the token holder has the authority to transmit and the number of available tokens is under control.

Basic procedure

The station that has a frame to transmit grabs the circulating token. It then marks the token as busy and attaches data and control information to it. The token is now converted into a data frame which is passed to the next station on the ring. The frame moves about the ring from one station to another until it reaches the destination. The destination station keeps a copy of the data, marks the frame as read and forwards it to the next station. In this way the acknowledged frame reaches the source station. The source station then generates a new token, marks it as being available for use and sends it around the ring. Figure 7.31 below shows the basic architecture of Token Ring Network.

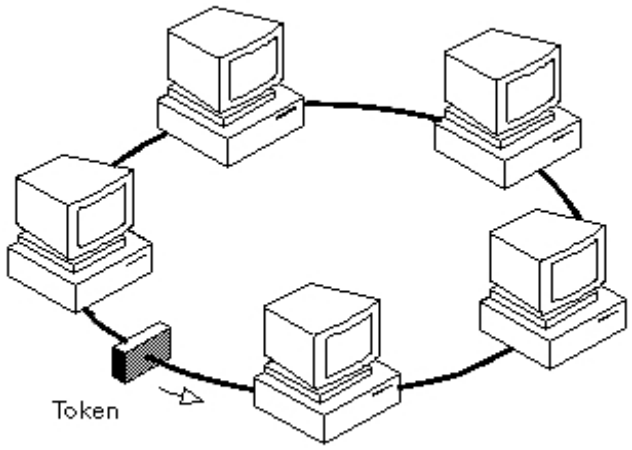


Figure 7.31: A Token Ring Network [7]

Priority System

Token Ring networks allow the use of priority systems. Some stations may be labelled as high priority stations to allow them to use the network more often. A token frame has two fields to control priority – the priority field and the reservation field. The token can be captured by a station only if its priority is equal to or higher than the value contained in the priority field of the token. When the token is being used, only a station with a higher priority than that of the transmitting station can reserve the token for the next pass. As soon as the next token is created, its priority is set to that of the reserving station. A station that increases the priority level of the token must also restore the priority to the previous level after using the token.

Fault Management

One station can be designated as the active monitor. It functions as the central source of timing information for the rest of the stations. It also carries out different maintenance operations, like ensuring that a token is available in the network at all times. If a station fails after sending a frame then the frame may circulate in the network infinitely, preventing any

other station from accessing the network. To avoid such a situation active monitor sets the monitor bit of any data or command frame that it encounters on the network. When the active monitor sees a frame with the monitor bit already set, it eliminates the frame from the network and creates a new token. Any station that identifies a problem in the network will generate a beacon frame. This beacon frame will warn other stations about the situation, following which, they will perform a diagnosis and try to reconfigure the network.

Token frame format

The two basic type of frames used in Token Ring network are - tokens, and data/command frames. A token is a frame that is 3 bytes in length. It consists of a start frame delimiter, an access control byte, and an end frame delimiter. The format of a token is shown in the Figure 7.32 below.

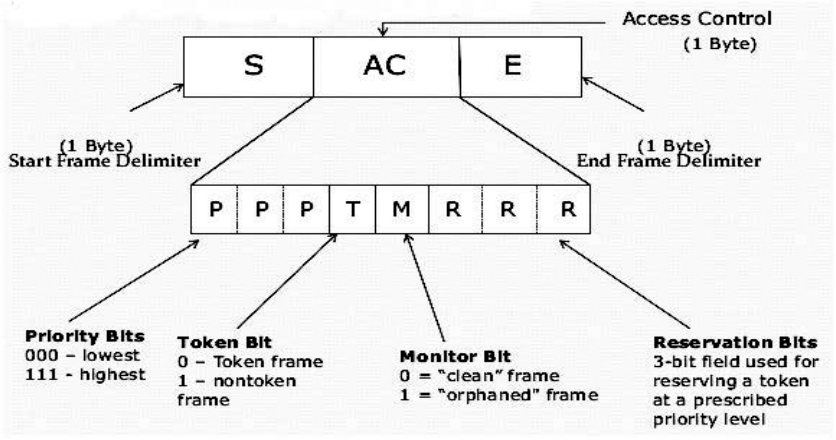


Figure 7.32: Token Frame Format [8]

Start Frame Delimiter: This is a 1 byte field. It indicates the beginning of the token frame.

Access Control: It is a 1 byte field. The first three bits hold the priority value of the token. The next bit if set indicates that the frame is a data/command frame, otherwise it is a token frame. The monitor bit if set indicates that the frame has been orphaned (source has failed after transmitting the frame), otherwise it is a clean frame. The last three bits are used for reservation purpose.

End Frame Delimiter: This is a 1 byte field. It indicates the end of the token frame.

Data/Command frame format

A data/command frame has a total of 9 fields. The format of the data/command frame is shown in the Figure 7.33 below.

Start delimiter	Access control	Frame control	Destination Address	Source Address	Data	FCS	End delimiter	Frame status

Figure 7.33: Data frame format [6]

Start delimiter: It is a 1 byte field. It indicates the start of the frame.

Access control byte: It is also a 1 byte field. It consists of priority field, token bit, monitor bit and reservation field.

Frame control byte: This field is 1 byte in length. It specifies whether the frame is a data frame or a control frame. In case of a control frame, this byte indicates the control information type.

Destination addresses: This field is 2-6 bytes long. It holds the MAC address of the destination.

Source address: This field is 2-6 bytes in length. It holds the MAC address of the source.

Data: This fields contains the data to be delivered. The maximum length of this field is bounded by the token holding time of the ring.

Frame check sequence (FCS): This field is 4 bytes long. The value of the field is calculated and filled by the sender based on the contents of the frame. The destination recalculates this value to check whether the frame has been corrupted during transmission. If so, the frame is rejected.

End delimiter: This is a 1 byte field. It marks the end of the frame. It also contains bits that may be used to identify a corrupted frame.

Frame status: It is a 1 byte field which closes the frame. It contains one bit address-recognized and frame-copied fields. These fields, if set, indicate that the frame has been received by the destination and the data has been read. Both the bits are duplicated within this field.

CHECK YOUR PROGRESS

1. A token, currently at priority level X, is in use. A station with priority level Y (Y>X) wants to reserve the token for the next use. Write down the steps involved in the procedure.
2. How does an active monitor help in fault management in a Token Ring network?

7.6 SUMMARY

Data Link Layer breaks the bit stream into discrete frames and appends a checksum to each frame. It then forwards the frames to the Physical Layer. Four framing methods discussed here are: Byte Count, Flag bytes with byte stuffing, Flag bits with bit stuffing and Physical layer coding violations. The first framing method uses a field in the header to specify the number of bytes in the frame. In the second framing method special bytes called Flag bytes mark the start and end of frames. The third framing method marks the start and end of each frame with a special bit pattern. In the fourth framing method reserved signals are used to indicate

the start and end of frames. The three generations of Ethernet discussed here, are, Traditional Ethernet, Fast Ethernet and Gigabit Ethernet. Traditional Ethernet was designed to operate at 10 Mbps. Fast Ethernet has a much higher data rate (100 Mbps) as compared to Traditional Ethernet. Gigabit Ethernet operates at 1 Gbps which is 100 times much faster than Traditional Ethernet. In Token Bus the nodes are physically connected as a bus, but logically form a ring with tokens passed around to determine the turns for sending. Token Ring unlike Token Bus, is a LAN in which all computers are connected in a ring topology, but tokens are passed here from node to node and the node that holds the token can send data.

7.7 TERMINAL QUESTIONS

1. Explain in detail the frame format of 802.3 MAC frame.
2. Why is there no need of CSMA/CD on a Full Duplex Ethernet LAN?
3. With the help of a diagram show how a station is classified into 4 different substations in a Token Bus network.
4. Explain in detail the common physical layer implementations of Fast Ethernet.
5. Is Switched Ethernet better than Bridged Ethernet in terms of bandwidth utilization? Give an example to justify your statement.
6. Compare the RS sublayer in Fast Ethernet with the PLS sublayer in Traditional Ethernet.

REFERENCES

[1] Tanenbaum and Wetherall, Chapter 3, “Computer Networks (5th Edition)”.

[2] Behrouz A. Forouzan,Chapter 14, “Data Communications and Networking (3rd Edition)”.

[3] http://slideplayer.com/slide/9378268/

[4] http://ecomputernotes.com/computernetworkingnotes/computer-network/what-is-ieee-8024-protocol

[5] http://www.slideshare.net/DhavalKaneria/token-bus-standard

[6] http://www.technologyuk.net/telecommunications/networks/token-ring.shtml

[7] http://www.webopedia.com/TERM/T/token_ring_network.html

[8] http://www.slideshare.net/Pnkj_Sharma/1742610-634994247305828750

UNIT-8 NETWORK DEVICES

Structure

8.0 INTRODUCTION

Networking devices are physical devices that are used to connect nodes on a computer network or to connect different networks to each other. Networking devices operate in different layers of a network. These devices operate in different layers of the network. The layer matters because different devices use different pieces of information to decide how to switch. Devices like repeaters and hubs work in the physical layer. Bridges and switches are found in the data link layer. Routers are implemented in the network layer. Gateways however, can operate at any network layer. The following sections describe the functionalities of all these network devices in detail.

The rest of the unit is organized as follows. Section 8.1 lists the objectives of the unit. Sections 8.2, 8.3, 8.4, 8.5 and 8.6 talk about various networking devices like hubs, bridges, switches, gateways and routers respectively. Section 8.7 summarizes the unit and section 8.8 finishes the unit with a few terminal questions for students.

8.1 OBJECTIVES

After the end of this unit; you should be able to understand:

- Basic functioning of Hub as a networking device
- Basic functioning of Bridge as a networking device
- Basic functioning of Switch as a networking device
- Basic functioning of Gateway as a networking device

- Basic functioning of Router as a networking device

8.2 HUB[1]

A hub is a networking device which operates at the physical layer of the network. Networks that use hubs basically use twisted pair cables for communication between devices. A hub has been devised to just forward the packets that it receives to all the connected devices. It sends the received packet to each connected device irrespective of the fact whether it is the intended receiver or not.

Hubs basically fall in the following two categories:

1. Active Hub -

Active hubs do not just forward the signals to all connected devices but also strengthen and regenerate the signals as they enter and exit the hub. Active hubs are also called repeaters.

2. Passive Hub -

Passive hubs are not capable of strengthening or regenerating the signals. They just receive the signal and forward it to all the devices connect to them.

Hubs are not generally used for sophisticated networking as they cannot do any complicated processing of data packets. They are low cost and therefore popular among households and small businesses. However, because of its working mechanism, a hub is not so secure and safe. Moreover, copying the data packets on all the interfaces or ports makes it slower and more congested. Figure 8.1 shows the basic architecture of a network in which a Hub is connected.

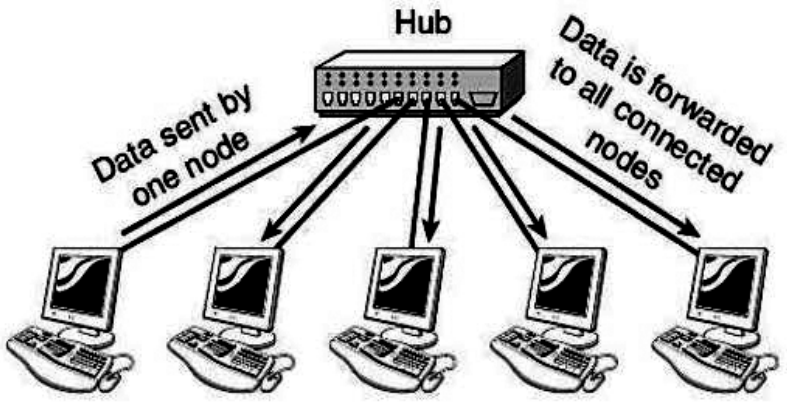


Figure 8.1: A Hub connecting multiple nodes [2]

8.3 BRIDGE [3]

A bridge is a networking device that connects two networks that are using the same protocol. A bridge operates at the data link layer of a network. A bridge can also be used to divide a large network into small subnetworks. The bridge performs this task by introducing itself between the two subnetworks and regulating the dataflow between them.

Figure 8.2 shows a bridge connecting two LANs: LAN 1 and LAN 2. Let us suppose that the bridge receives a packet from a device located on LAN 1. It first inspects the MAC address of the destination device on the received packet. It then checks if the destination device is located on LAN 2. If so, the packet is forwarded to LAN 2. Otherwise the packet is prevented from passing over the bridge. If the packet is forwarded to LAN 2, it is received by all the devices located on LAN 2. Only the destination device accepts the packet. All the other devices reject the packet.

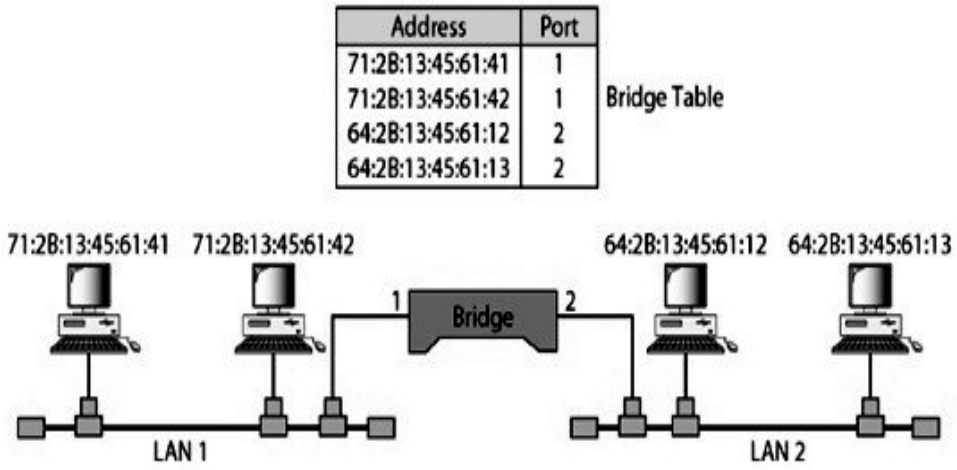


Figure 8.2: A bridge connecting multiple networks [4]

Bridges can be basically categorized into the following three types:

1. **Source Route Bridge -**
   - A source-routing bridge is basically found in Token Ring networks.
   - Source-routing bridges do not learn from observing tables.
   - When a node wants to send a frame, it needs to know the exact route to the network/bridge to which the frame has to be sent.
   - If the node does not know the exact route, it sends out a discovery frame.
   - The discovery frame makes its way to the final destination. It records the route on its way back to the source node.

- A source-routing bridge is named so because the packet records the route that it takes through the network.

2. Transparent Bridge -

- A transparent bridge observes all traffic and builds routing tables from this observation.
- This observation is called backward learning.
- Each bridge has two connections (ports) and there is a routing table associated with each port.
- A bridge observes each frame that arrives at a port, extracts the source address from the frame, and places that address in the port's routing table.
- Transparent bridges are primarily implemented in the Ethernet networks.
- They are named so because their presence and operation are transparent to network hosts.

3. Translational Bridge -

- Translational Bridges allow two different networks such as Ethernet networks and Token Ring that work on different protocols to be connected.
- A translational bridge can add or remove information and fields from a frame based on the direction in which the frame is moving.
- It basically changes the format of a frame, from what is supported by the network it comes from, to what is supported by the network it is going to.

8.4 SWITCH [5], [6], [7]

A switch is a networking device that operates in the data link layer of the network. It can be connected to multiple devices through multiple ports just like a hub. Twisted pair cables are used for connection purposes just as in the case of hubs. But unlike the hub, the switch forwards data only to the port through which it is connected to the destination device. This is possible as the switch has a built-in learning capability through which it learns the MAC addresses of all the devices connected to it. Figure 8.3 shows a switch connecting four devices.

Modes of network switches

There are three common switching modes which have been shown below [6]:

1. Cut-through switching –

A switch operating in cut-through mode forwards a packet as soon as it is received. Basically the switch forwards the frame as soon as it sees the destination MAC address and identifies the specific port. The problem with this mode is that the switch may also forward corrupted frames to the destination.

2. Store and forward switching –

A switch operating in store and forward mode copies the entire frame to its memory and recalculates the Cyclic Redundancy Check (CRC). If the frame is found to be corrupted, it is discarded, otherwise it is forwarded to the destination. This mode delays frame delivery due to the checking procedure involved.

3. Fragment-free switching –

Fragment-free switching was designed to retain the benefits of both the *cut-through* mode and the *store and forward* mode. A switch operating in fragment-free mode reads the first 64 bytes of the frame to determine if it has been damaged due to a collision. If so, it is not forwarded, otherwise it is forwarded.

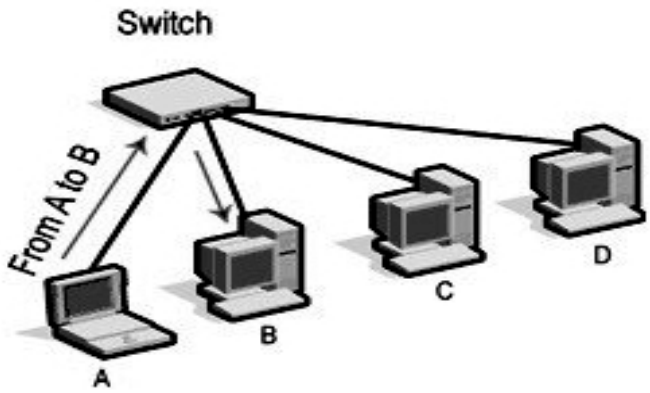


Figure 8.3: A Switch connecting multiple devices [8]

Network switch categories

On the basis of configuration network switches are divided into the following three types [5]:

1. **Managed Switches:** Managed switches have the ability to prioritize time-sensitive packets. They can control the access to a specific portion of the network. In addition, managed switches allow us to observe each device on the network and restrict the amount of bandwidth that can be used by a device.
2. **Unmanaged Switches:** Unmanaged network switches are basically implemented in home networks and small firms. They are cheap as compared to managed switches and do not support any of the above features. They are simple devices that are easy to set up and can be used only to connect devices in a network.

3. **Smart Switches:** Smart switches provide some of the features of the managed switches. But these features are limited when compared to the latter. Smart switches are cheaper and are mostly used in fast LANs.

Layer 2 Switching

A layer 2 switch mainly helps in exchanging packets among devices within a LAN. It maintains a table of the MAC addresses of the devices that it has learnt along with the ports that they are connected to [7]. For example, if a switch receives a packet from a device having MAC address Z on port 3, it knows that all packets intended for MAC address Z can directly be sent to port 3.

As Layer 2 information is easily recovered, packets can be dispatched very swiftly, usually, at the network wire speed. Layer 2 switching, hence, has little or no influence on the bandwidth and performance of the network. Layer 2 switches do not require any set up or management which makes their deployment cheap and easy.

Layer 3 Switching

A layer 3 switch has more capabilities as compared to a layer 2 switch. They work more or less like a router as they maintain tables for IP routing. They have the capability to logically partition a network into smaller subnetworks [7]. Layer 3 switches also provide improved security features to stop illegitimate setup changes. They can prioritize different packets to provide guaranteed Quality of Service (QoS).

Layer 3 switches require extra processing power to retrieve information as compared to layer 2 switches. They are also costlier because of the extra processing power and memory required. Such switches also require setup and management unlike layer 2 switches.

CHECK YOUR PROGRESS

1. Active hubs are also called repeaters. Justify this statement.
2. Differentiate between Cut-through and Store and forward switches.
3. A switch, unlike a hub, forwards a packet to a specific device. State the reason.

8.5 GATEWAY [9]

A gateway is a networking device that can operate at any layer of the OSI model. It basically connects two networks that are using different protocols. A network gateway can be implemented as a hardware, as a software, or as a combination of both. As network gateways are placed at the edge of networks, they are also integrated with firewalls. Usually a broadband router works as the network gateway on home networks. Ordinary computers can also be configured to perform the same functions.

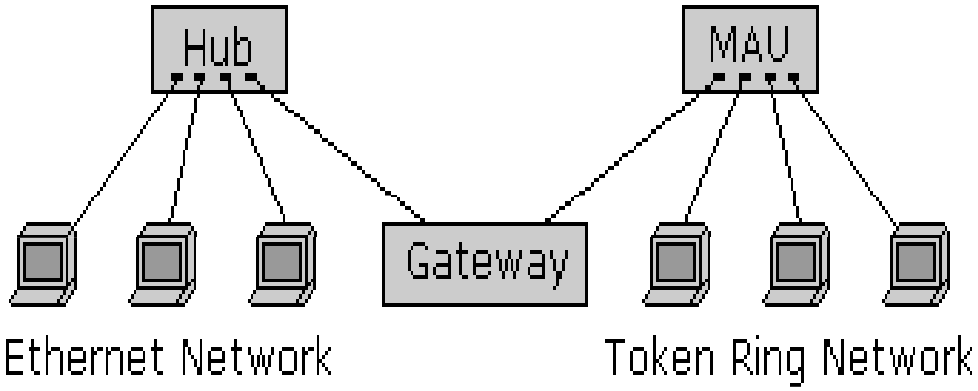


Figure 8.4: A Network Gateway connecting two networks [10]

Figure 8.4 shows an Ethernet network and a Token Ring network connected by a gateway. Here the gateway translates the data received from one network into a format or protocol recognized by the other network.

A router is common type of gateway which works in home networks. It permits devices in a local network to transmit and accept packets over the internet. A firewall on the other hand, is a more complicated gateway that can filter incoming or outgoing packets. This prevents unauthorized access to the devices on the local network. A proxy server is a gateway that uses a combination of hardware and software to filter packets that are moving from one network to another. For instance, a proxy server may allow only some specific computers to access a group of authorized websites.

Some basic network gateway types are as follows:

1. **Default gateways:** A default gateway functions as an access point or IP router that is used by a computer in one network to send data to a computer on another network. It may also be used by the computer to send or receive packets over the internet.

2. **Media gateways:** A media gateway is a translational device that is used to convert various types of digital media protocols for effective multimedia communication. Media gateways are widely used in connecting different networks (such as 2G, 3G, 4G and LTE), hence their main function is to convert different coding and transmission techniques to enable communication between the networks.

3. **Payment gateways:** Payment Gateway is the service that manages the payment transaction between the merchant and the shopper. It is typically a third-party service that is essentially a system of computer processes. They process, validate, and accept or decline credit card transactions on the merchant's behalf via a secure internet connection.

4. **VoIP gateways:** Voice over Internet Protocol (VoIP) gateway converts analog signals to digital signals. After digital signal has been generated, VoIP gateway arranges it into small data packets and

encrypts them for transmission. The basic tasks of a VoIP gateway is compressing/decompressing voice and fax, call routing, packetization and control signaling.

8.6 ROUTER [11]

A router is a device that operates at the network layer of the OSI model. The main function of a router is to connect networks to each other. It allows data from one network to move to another network [11]. It also acts as a firewall to protect our device from unwanted access by other devices.

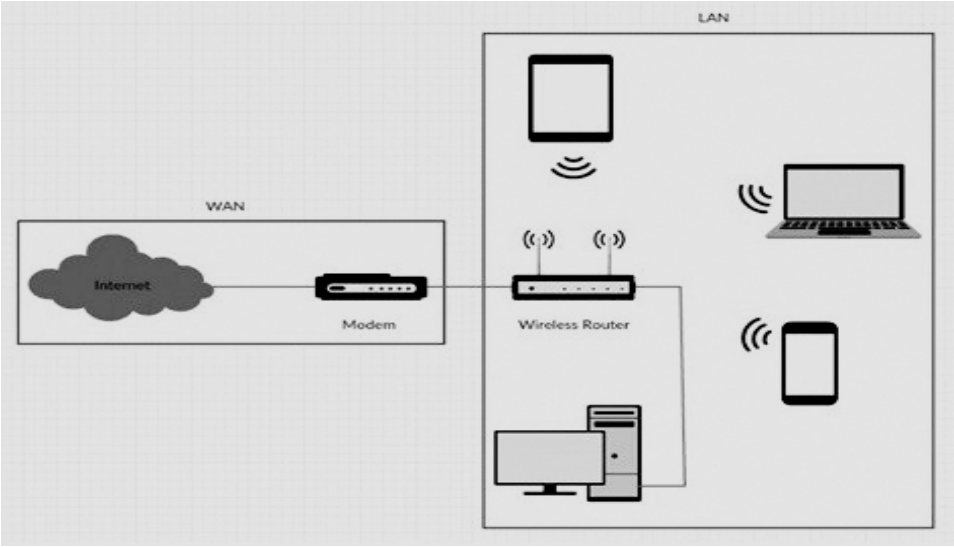


Figure 8.5: Router connecting WAN and LAN [12]

The router can take information from the devices connected to it (LAN – Local Area Network) and send it to the internet (WAN – Wide Area Network). When a response comes back from the internet (WAN), the router sends that response to the correct device (LAN). In this respect, the router is "routing" traffic from a device (LAN) to the internet (WAN) and then back to the device (LAN). Figure 8.5 shows a router connecting a WAN and a LAN.

When the router receives a packet, it looks for the destination address in the header of the packet. After finding the address, router checks its routing table to know the route to the destination. It then forwards the packet to the next hop on the route. The next hop could be just another router or the final destination.

Routing tables play a very essential role in the decision making of a router. Therefore it is necessary for a router to regularly update its routing table. A router can receive information through two ways as has been shown below:

1. Static Routing: In static routing, the routing information is manually entered into the routing tables. This makes the task time-taking as well as

susceptible to errors. Every time there is a topology change all the routing tables need to be manually updated with utmost care. Hence static routing is feasible for very small networks with a very few number of routers.

2. Dynamic Routing: In dynamic routing, all the routing tables are automatically updated. A router shares the routing messages and information with other routers in the network. When a router finds any change in the network topology, it advertises this topology change to other routers. In this way all the routers learn about the new network structure and update their routing tables. No human intervention is needed unlike the static routing. Dynamic routing is suitable for larger networks with many routers.

CHECK YOUR PROGRESS

1. What are the advantages of dynamic routing over static routing?
2. Describe a scenario where a router acts as a gateway.

8.7 SUMMARY

Network devices are components used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines. Hub is a networking device which works at physical layer. Hubs can be categorized into active hubs and passive hubs. Passive hub just relays the incoming signal through all the ports but an active hub can regenerate, concentrate and even strengthen the signal before sending them to their destination. A bridge is a networking device that is implemented at the data link layer. It connects two physical LANs into larger logical LAN or two segments of the same LAN that use the same protocol. A switch is a networking device that operates in the data link layer. They are categorized into Layer 2 switches and Layer 3 switches. Layer 2 switches use MAC addresses to transfer data between two devices located on the same network. Layer 3 switches on the other hand are capable of working like routers as they have their own IP address table that they use to forward data. A gateway is a device that can operate at all network layers and can even be used to join networks using different base protocols. A router is a device that forwards data packets along networks. Routers are located at gateways, the places where two or more networks connect.

8.8 TERMINAL QUESTIONS

1. How does a transparent bridge update its table? Why is it named so?

2. A Layer 3 switch has more functionalities than a Layer 2 switch. Explain the statement.
3. What do you mean by payment gateways? Give an example to show how they work.
4. What are the different types of network switches based on configuration?
5. How does a translational bridge connect two networks working on different protocols?

REFERENCES

[1] http://www.certiology.com/computing/computer-networking/network-devices.html

[2] http://www.vce-download.net/study-guide/comptia-networkplus-1.9-install-configure-common-network-devices.html

[3] http://www.slideshare.net/snowqueensscas/computer-networks-54765056

[4] http://slideplayer.com/slide/6445155/

[5] http://wifinotes.com/computer-networks/what-is-networking-switch.html

[6] http://www.omnisecu.com/cisco-certified-network-associate-ccna/methods-of-switching.php

[7] http://www.itpro.co.uk/88699/layer-2-and-layer-3-switches

[8] http://www.networking-basics.net/network-switch-vs-hub/

[9]http://www.globalspec.com/learnmore/communications_networking/networking_equipment/network_gateways

[10] http://bucarotechelp.com/networking/standards/97020910.asp

[11] http://www.certiology.com/computing/computer-networking/network-devices.html

[12] http://www.thewirie.com/what-is-a-router/

Uttar Pradesh Rajarshi Tandon
Open University

Bachelor of Computer Application

BCA-1.13

Computer Network

Block

3

IP Addressing and Routing Issues

Course Design Committee

Dr. Ashutosh Gupta — **Chairman**
Director (In-charge)
School of Computer & Information Sciences
UPRTOU, Prayagraj

Prof. R. S. Yadav — **Member**
Department of Computer Science and Engineering
MNNIT-Allahabad, Prayagraj

Ms Marisha — **Member**
Assistant Professor (Computer Science)
School of Science, UPRTOU, Prayagraj

Mr. Manoj Kumar Balwant — **Member**
Assistant Professor (Computer Science),
School of Sciences, UPRTOU, Prayagraj

Course Preparation Committee

Dr. Maheshwari Prasad Singh — **Author**
Assistant Professor, Department of CSE
NIT Patna

Dr. Rajiv Mishra — **Editor**
Associate Professor, Department of CSE
IIT Patna

Dr. Ashutosh Gupta (Director in Charge)
School of Computer & Information Sciences
UPRTOU, Prayagraj

Mr. Manoj Kumar Balwant — **Coordinator**
Assistant Professor (Computer Science),
School of Sciences, UPRTOU, Prayagraj

ISBN : 978-93-83328-18-5

Printed and Published by Dr. Arun Kumar Gupta Registrar, Uttar Pradesh Rajarshi Tandon Open University, 2019.

Printed By: Chandrakala Universal Pvt. Ltd. 42/7 Jawahar Lal Neharu Road, Prayagraj.

BCA-1.13/162

BLOCK INTRODUCTION

This is the third block on IP Addressing and Routing Issues. As name of this block indicate that this block will introduce the requirement of IP address and design aspect of it. This block has three units namely, IP Protocol and Addressing, Connection Management, and Routing in Network Layer. We will begin the first unit on Network layer design issue, IP Protocol, IP Addresses, subnets. This unit discussed different types of IP addresses classes. It also discussed the issues of network layers. It will make you understand the need of subletting from user and administrative perspective. The second unit mainly discusses basics of Internetworking. Further it presents connectionless and connection oriented services. Again it explains tunneling, and IP Fragmentation. You will understand that why IP fragmentation is important and how it is being used. It also discussed the use and need of Firewall. Finally this unit presents different types of Internet Controls Protocols. In the last unit, how packet is being transferred from source to destination PC. So, it discussed different types of routing algorithms. It also emphasizes the importance of shortest path routing. Different types of routing protocols namely Flooding, Flow-based routing, Broadcast routing are being discussed in details. In routing congestion is obvious. So, this unit discussed different types of Congestion Control Algorithm. It also presents congestion prevention policies. As you study the material, you will understand the concept with the help of figures, tables, wherever required. Each unit has been describes using many sections. Every unit has summary and review questions in the end. This questions will help you to review yourself.

UNIT-9 IP PROTOCOL AND ADDRESSING

Structure

9.0 INTRODUCTION

In the Internet protocol suite, IP (Internet Protocol) is the basic communications protocol for transmitting datagrams through boundaries of networks. Its routing function allows internetworking, and establishes the Internet. IP delivers packets from the sending host to the receiving host based only on the IP addresses contained in the packet headers. To facilitate this, IP outlines packet structures that encapsulate the data that is to be sent. It also defines addressing methods that are used to insert source and destination addresses into datagrams.

The rest of the unit has been organized as follows. Section 9.1 enlists the objectives of the unit. Section 9.2 explains the network layer design issues. Section 9.3 discusses IP protocols and section 9.4 discusses IP addresses. Section 9.5 contains a few problems on IP addresses. Section 9.6 summarizes the unit and section 9.7 closes it with some terminal questions for students.

9.1 OBJECTIVES

After the end of this unit, the reader should be able to:

- Understand network layer functionalities and features
- Learn message forwarding and implementation of connection-less and connection -oriented service
- Learn network layer protocols

- Learn addressing and subnetting

9.2 NETWORK LAYER DESIGN ISSUE

Layer 3 in the OSI model is known as Network layer. Network layer has responsibility to deliver the packets host-to-host, routing the packets through router, host and network addressing, and managing subnetwork and internetworking.

Functions of the network layer are to mapping different addressing schemes and protocols within or outside of a subnet, to route the packets from source to destination.

Network Layer Functionalities:

Devices which operate at the Network Layer focus primarily on routing. Routing may consist of different tasks to achieve a single goal.

These tasks can be:

- Routing table's population or static routes.
- Addressing networks and devices.
- Outgoing and incoming data queuing and then sending it according to QoS constraints fixed for those packets.
- Internetworking between two or more different subnets.
- Provides the connection oriented and connection less services.
- Packets delivering to destination with the best efforts.

Network Layer Features:

Network layer can provide various features with its standard functionalities such as:

- Quality of services management, link management and load balancing
- Inter-relation of various protocols and subnets with different schema or outline.
- Security
- Different logical network design over the physical network design.
- To provide end to end dedicated connection used by Network layer, Virtual private network (VPN) and tunnels.

Here, some of the issues have been faced by the network designers at the network layer being discussed. These issues shall comprise the services that have been provided to the internal design of network and transport layer.

9.2.1 STORE AND FORWARD PACKET SWITCHING

The main components of the system, the carrier's equipment (routers are joined through transmission lines), have been displayed inside the oval, and the customer's equipment have been displayed outside the oval.

In the Figure 9.1, Host H_1 is connected to router A (one of the carrier's routers) by a leased line. Host H_2 is connected to the same LAN to which router F is connected. It is owned and operated by the customer. Router F is connected to router E (one of the carrier's routers) through a leased line.

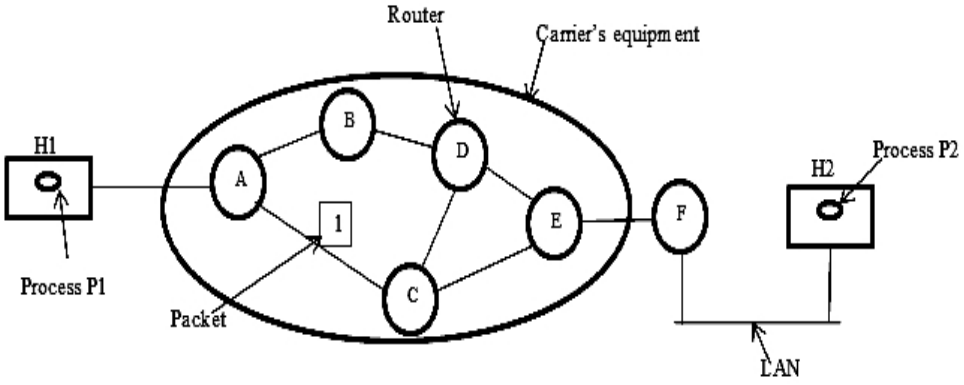


Figure 9.1: The environment of the network layer protocols [1]

The above mechanism has been used as follows:-A host that wishes to send a packet, forwards it to the nearest router, either on its own LAN or through a point to point dedicated link to the carrier's. The packet has been stored there till it has fully arrived and then ,it is checked for errors by recalculating the checksum and comparing it with the checksum already appended to the data. If the data is not corrupted then the packet is forwarded; otherwise it is discarded.

The packet, if not corrupted, is forwarded to the next router onthe path. This continues until the packet has reached the destination host. The complete mechanism is known as **store-and-forward packet switching**

9.2.2 SERVICES PROVIDED TO THE TRANSPORT LAYER

Network layer delivers the services to transport layer. These services have been designed with the following goals in mind:

- The transport layer should be shielded from the numbers, type, and topology of the routers present [1].
- The router technology should not affect the services provided to the transport layer.

- The network addresses are also accessible to the transport layer and it must be in a uniform numbering rule, even across or over LANs and WANs.

9.2.3 IMPLEMENTATION OF CONNECTIONLESS SERVICE

The packet forwarding decision in a connectionless packet switching is based on the destination address of the packet, i.e. the packets in a message are routed independently from path. No need of setup in advanced. Here, the packets are known as **datagrams** and this type of network is known as **datagrams network**.

How does a datagram subnet work: - let us suppose in Figure 9.2, Process P1 holds a long message and wants to transmit at process P2 that is running on host H2. First of all it hands over the message to the transport layer with some instruction to deliver it at the process P2 that is running on Host H2.

Host H1 runs the Transport layer program/code with in operating system then it attached a header in the front of message and then it will send the result to the network layer. Here attached is known as Transport header.

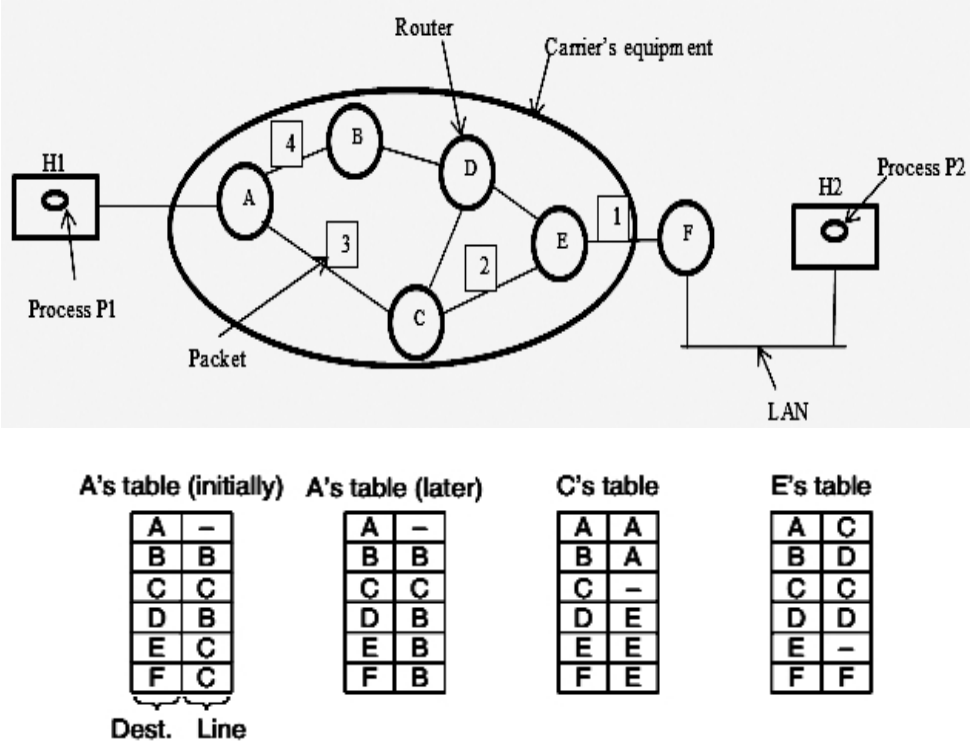


Figure 9.2: Routing within a datagram subnet [1].

Assume that the message is being transmitted is too large, approximately four times larger than the MTU packet size so it has to be divided in to four packets namely packet 1, 2, 3,and 4 and send each of these packets using some point-to-point protocol (PPP) in turn to router A.

Now at this moment the carrier's takes control for routing these packets, these packets routing is decided by routing table of router. The entries of the routing table being decide the possible destinations where the router should send the packets next. Here table entries of the router are consist of a pair of destination address and outgoing line which is use for the destinations.

In Figure 9.2, simply the direct-connected lines can be used. For example, router A has two outgoing lines - A to C and A to B. Each inbound packet can be sent to one of these routers, even if some other router is the actual destination. In the Figure 9.2, A's preliminary routing table is displayed with the label "**initially**".

At the router *A*, packets 1, 2, and 3 have been arrived and each of packets being forwarded according to the table entries of the router A's, onto the outgoing link to router C with in a new frame. Finally packet 1 is arrived at router E and then forwarded it to the router F. Once it arrived at router F, being sent within a frame over the LAN at the host H2and also Packets 1 and packet 2 will follow the same route.

Something different happens with packet 4 however. When it is received by router A, it is forwarded to router B, even though the destination of this packet is router F. Router A for some reason decides to send packet 4 through a different route and not through the route that was followed by packets 1, 2 and 3.

Actually router A learns that there is a traffic jam somewhere along the path A-C-E. Therefore it updates its routing table and forwards packet 4 through a new path and not through the old path. The updated routing table of A has been shown with the label "**later**". The algorithm that maintains tables and decides the routes is called a routing algorithm.

9.2.4 IMPLEMENTATION OF CONNECTION-ORIENTED SERVICE

In connection-oriented service, there are some relations among all packets to a message. It needs a virtual-circuit connection setup, before all datagrams in a message to be sent. The provision behind virtual circuits is to avoid choosing a new path for each of the packet to be sent, as Shown in Figure 9.2.

In this type of service, the packet holds information like the source and destination addresses, flow label (a virtual circuit identifier that is used to define the virtual path the packet should follow).

Whenever a connection is setup, a connected path from the sending networking device to the receiving networking device has been chosen as part of the connection setup procedure and this connected path is stored in routing table's entries that are maintained by routers. This route is used for

all the packets moving through the connection, for example, telephone system works on the principle of connection-oriented service.

When the connection is terminated, the virtual circuit setup should be terminated as well. In case of connection-oriented service, each of the packets contains an identifier that states which virtual circuit it belongs to. For example, consider the scenario of Figure 9.3, host H1 has been setup a connection namely 'connection identifier 1'with host H2 and first entries of each of the routing tables shows this connection.

The line first of routing table A's specifies that a packet is coming from host H1 and going to router C through connection identifier 1; Similarly, the first entry at router C and router E's specifies that a packet is coming from router A and router C and going to router E and router F through connection identifier 1 respectively.

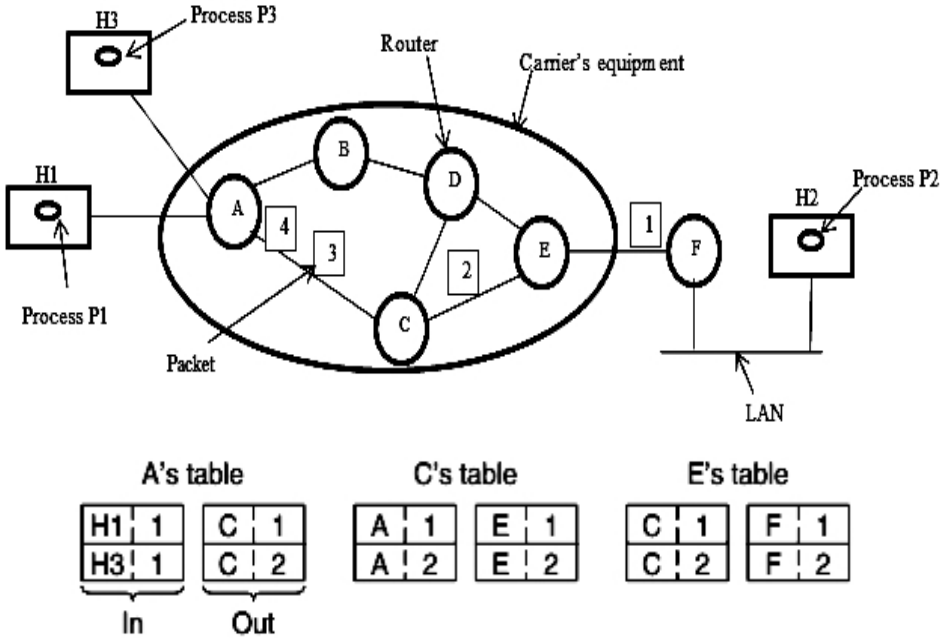


Figure9.3: Routing within a virtual-circuit subnet [1].

Now, let us suppose host H3 wants to send a packet to host H2. For this, connection identifier would be 1, as it is the first connection between host H3 and H2. Now, since the connection identifier of connection between H1 and H2 is also 1. This causes the confusion at router A but it can easily resolve this confusion as it is directly connected to H1 and H3. However, the router C and router B is not able to distinguish whether the packet is coming from H1 or H3. For this, router A replaces the connection identifier 1 as connection identifier 2for every outgoing packet.

9.2.5 COMPARISON OF VIRTUAL-CIRCUIT AND DATAGRAM SUBNETS

We have to make sure that the packets received are in correct order at the network layer. Many models exist to address this problem. The two models namely virtual circuit and datagram is significant.

Inside the subnet, between virtual circuit and datagrams, many trade-off exist. There is a trade-off between bandwidth and router memory space.

Instead of full destination address, virtual circuits allow packets to contain circuit numbers. In case of short packet, a full destination address in every packet wastes the bandwidth significantly. Virtual circuits, initially takes the table space within the routers.

The other trade-off is between setup time and address parsing time. Virtual circuits require a setup phase, which is time consuming. For making decision about the data packet in a virtual-circuit subnet, the circuit numbers is used by the routers to index into a table. Whereas, in a datagram subnet, a lookup method is more complicated to locate the entry for the destination.

10 The major issues of datagram and virtual-circuit are listed in Table9.1.

Table 9.1: Comparison of datagram and virtual-circuit subnets [1]

Issue	Datagram	Virtual circuit
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
QoS	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

9.3 IP PROTOCOLS

The responsibility of Internet Protocol (IP) is addressing hosts and routing datagrams (packets) from a source host to a destination host in the IP networks. For this, the Internet Protocol specifies the format of packets and provides an addressing system. This helps in Identifying hosts and providing a logical location service.

The first version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).Protocols implemented at the network layer are following:

- Internet Protocol version 4 i.e. **IPv4**
- Internet Protocol version 6 i.e. **IPv6**
- Novell Internetwork Packet Exchange i.e. IPX
- AppleTalk
- Connectionless Network Service i.e. CLNS/DEC Net

This Unit explains only IPv4 and IPv6.

9.3.1 INTERNET PROTOCOL VERSION 4 (IPV4)

The Internet Protocols IPv4 and IPv6are used to carry data. Some information about IPv4 is as follows:

- Version 4 of IP (IPv4) is presently the most widely used version of Internet Protocol.
- Network layer protocol is used to carry data over the Internet.
- Over an interconnected system of networks, it provides only the functions that are necessarily used to deliver a packet from a source to a destination.
- This protocol has not been designed to track and manage the flow of packets. This is managed by some other protocols in other layers.

The basic characteristics of IPv4 are: connectionless, best effort, media independent.

Connectionless -means no connection is setup before sending data packets.

Best Effort (unreliable) - means to guarantee packets delivery, no overhead is used.

- Unreliable means being incapable to manage and recover undelivered or corrupted packets.
- Other layers protocols can manage reliability, tracking packets and ensuring theirs delivery.
- IP has been allowed to work very efficiently at the Network layer.

Figure 9.4 shows Best Effort packet delivering in IPv4 protocol.

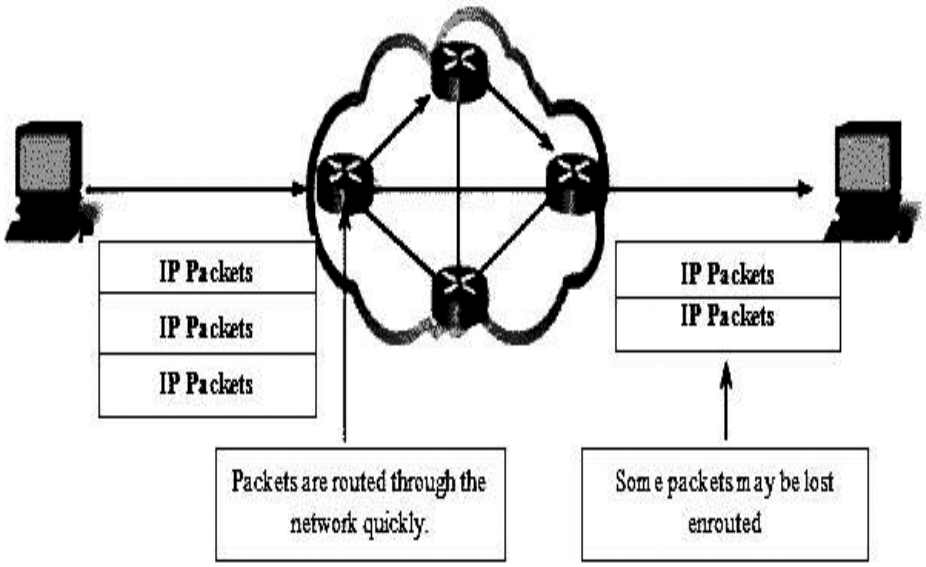


Figure 9.4: Best Effort Packet delivering [2]

Media Independent Media Independent - the medium carrying data operates independently.

- IPv4 and IPv6 both operate independently from the media that carry the data at lower layers of the protocol stack. Figure 9.5 below shows how IP packets operate independently of the media.
- Individually each of the IP packets may be communicated electrically over cable, as optical signals over fiber, or wireless as radio signals.
- OSI Data Link layer takes an IP packet and prepare it for transmission over the communications medium.

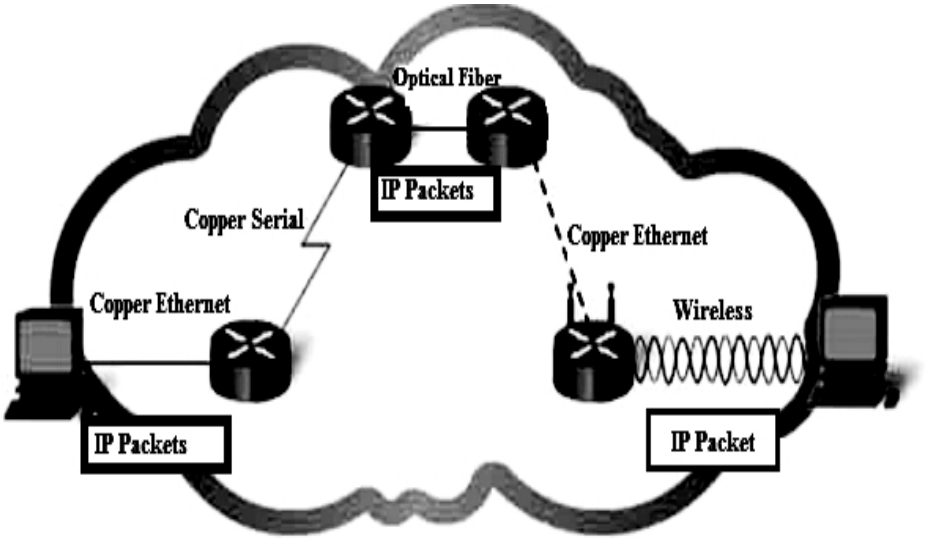


Figure 9.5: Media independence [2]

- The Network layer considers **the maximum size of a PDU** that each medium can transport. This is known as the Maximum Transfer Unit (MTU).
- MTU is the maximum number of bytes that a data link layer protocol can handle or encapsulate. It varies from protocol to protocol. MTU is passed to upper layer i.e. to the Network layer by Data Link layer. Then Network layer determines the size of the packets to create. In some cases, an intermediary networking device - like router - splits packet before it forwards from one media to a media with a smaller size of MTU, this process is known as fragmentation. **Fragmentation** is the process of dividing the datagram into smaller units so as to accommodate the MTU of a data link protocol [3].

9.3.2 IPV4 PACKET HEADER [3]

The different fields in the packet header in IPv4 protocol is shown in the Figure 9.6.

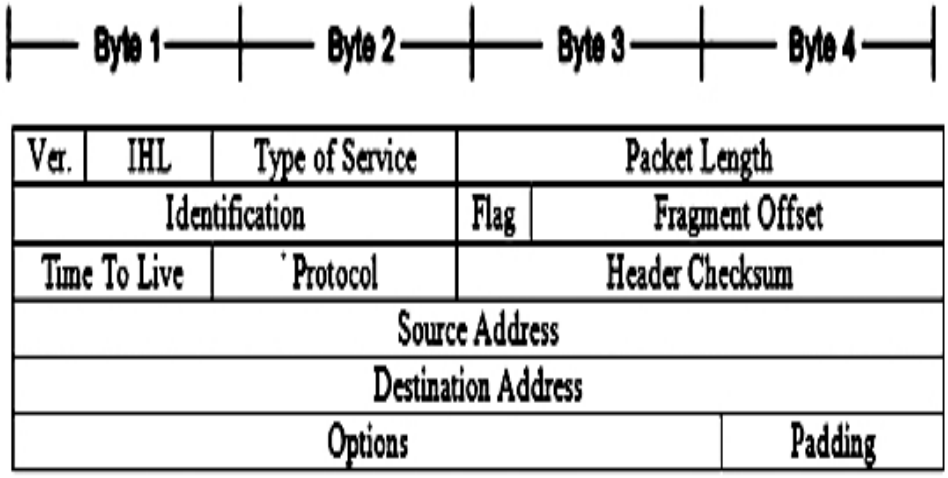


Figure 9.6: IPv4 Packet Header [2]

Version (4-bit): Specifies the Internetworking protocol version 4.

Internet Header Length (IHL): This specifies the size of packet header.

For example if IHL = 5; size of header in 32 bit words (4 bytes) i.e. here header would be 5*4 = 20 bytes, and this is the minimum valid size.

Type-of-Service: This field determines the priority of each packet and it holds 8-bits binary value. The Quality-of-Service (QoS) mechanism is also enabled by this field.

Packet Length: It specifies the complete packet size, including header and data in bytes.

Identification: IP packet fragments are uniquely identified by this field.

Flag: if Flag = 0 then it indicates that the packet can be fragmented when required.

Fragment Offset: If Fragment Offset = 0; It means that this packet is presently not fragmented.

Time-to-Live (TTL): It is of 8-bit and specifies the "life" of the packet. Each time the router encounters a packet the TTL value has been decreased by at least one and ones the value becomes zero, then the router drops or discard the packet.

To prevent packets from indefinite looping in the network, TTL is used. When the packet is approaching to the router, this value will be automatically decremented , i.e. ones values becomes zero, that packets is discarded and send a time exceeded message to source

Protocol: This field contains 8-bit binary value and it indicates the data payload type that the packet is carrying. This field is used to allow the Network layer to pass the data to the proper upper layer protocol.

For Example values are:

01 is used for ICMP

06 is used for TCP

17 is used for UDP

Header Checksum: This field contains (16-bits) and it is used for error checking in the packet header.

IP Source Address: This field represents (32-bits) the IPv4 address of the packet source. This field must be unchanged during the time IPv4 datagram travels from the source host to destination host.

IP Destination Address: This field represents the packet destination Network layer host address and contains a 32-bit binary values

Options: IPv4 header has some provision for additional fields to some other services but it is rarely in used.

CHECK YOUR PROGRESS

1. Explain IPv4 header format, and which fields of the IPv4 header change from router to router?
2. The size of the option field of an IPv4 datagram is 20 bytes. What is the value of HLEN? What is the value in binary?
3. Why is the need of IPv6 addressing and also explain the reason for the elimination of the checksum in the IPv6 header.

9.4 IP ADDRESSES

IP addresses can be represented by using Classful (A, B, C, D, E) or Classless (CIDR: Classless Inter Domain Routing) notation. IP address is logical address. These addresses are used for universal communications

which are independent from physical networks. Due to different address formats of different networks, physical addresses are not adequate for universal communication. So there is need of universal addressing system in which each of the hosts can be identifying uniquely. A logical address (IPv4 address) is currently a 32-bit address using in the Internet, which can uniquely identifying a host over the Internet. A logical address contains two components namely Network ID and Host ID, which is illustrated in later section.

9.4.1 IPV4 ADDRESSING

The main function of IP is to provide logical addressing for hosts. The hierarchical structure has been provided by IPv4 addressing to uniquely identifying host and a network in which host exists.

An IP address has four octets, separated by dot (.), each of the octets is composed of 8-bit number, that's result in a 32-bitaddress, and these addresses are unique and universal. The smallest and largest values of the octets are 0 in decimal (or 00000000 in binary) and 255 in decimal (or 11111111in binary) respectively.

For example, 146.16.7.6

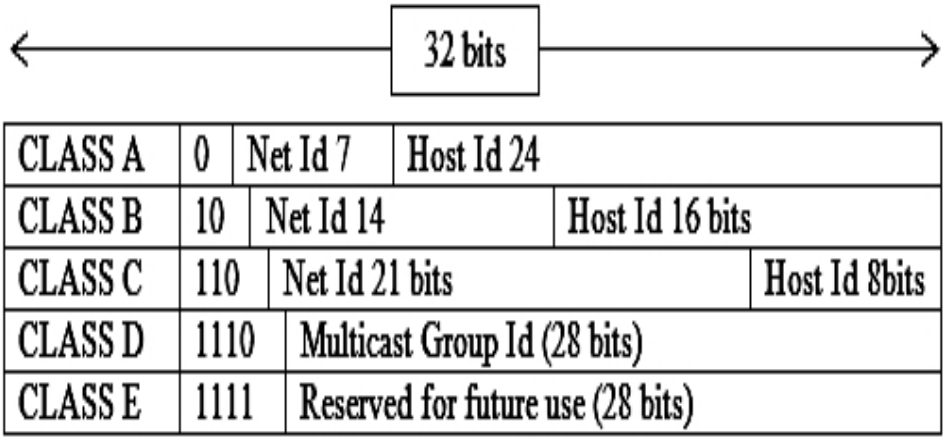
10010010.00010000.0000111.00000110

IPv4 has total 2^{32}addresses.IP version 4 has been divided in to five classes, namely class A, class B, class C, class D and class E and each of the classes holds some parts of the whole address spaces, and this architecture is known as **Classful address**.

Here, Class A addresses start with 0 so it has a prefix of 0, Class B address start with 10 so it has a prefix of 10, Class C address start with 110so it has a prefix of 110, Class D start with 1110 so it has a prefix of 1110and Class E start with 1111 so it has a prefix of 1111.

IPv4 address formats and its Class Range:

IPv4 address formats



Class Range (As "Dotted Quad")

Class Range of IPv4 Addresses			
CLASS A	0.0.0.0	to	127.255.255.255
CLASS B	128.0.0.0	to	191.255.255.255
CLASS C	192.255.255.255	to	223.255.255.255
CLASS D	224.255.255.255	to	239.255.255.255
CLASS E	240.255.255.255	to	255.255.255.255

CLASS OF IPv4 ADDRESS

CLASS A

Class A address have a first bit is 0 in the first octet.

In binary notation its look like

Octet 1	Octet 2	Octet 3	Octet 4
0xxxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Its range is from 0 to 126 and 127 is actually reserved for loopback address(127.x.x.x), where x is any integer value lies between 0 to 255.

255.0.0.0 is default subnet mask of Class A IP address, i.e. Class A has 126 networks address (2^7-2) and 16777214 hosts (2^{24}-2).

CLASS B

Class B addresses has been provided an equal number of networks and hosts.

First two octets are network address and remaining last two octets are host addresses.

Class B addresses have first two bit is 10 and in binary notation its look like

Octet 1	Octet 2	Octet 3	Octet 4
10xxxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

The range of Class B IP Addresses is from 128.0.0.0 to 191.255.255.255.

IP address 255.255.0.0 is known as the default subnet mask for Class B IP addresses. Class B has up to2^{14}i.e. 16384 Network addresses and up to 2^{16}-2 i.e. 65534host addresses.

CLASS C

Class C has greatest number of network addresses, but very few host addresses,

The first 3 bits are 110 and in binary natation its look like

Octet 1	Octet 2	Octet 3	Octet 4
110xxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

IP addresses of Class C range varies from 192.0.0.0 to 223.255.255.255.

IP address 255.255.255.0 is known as the default subnet mask address for Class C IP addresses.

Class C has up to 2^{21} i.e. 2097152 Network addresses and up to 2^{8}-2 i.e. 254 Host addresses.

CLASS D

Class D is designed for special multicast addresses. Each address of Class D is used to illustrate one group of host on the internet.

The first 4 bits of Class D is start with 1110 and in binary notation its look like

Octet 1	Octet 2	Octet 3	Octet 4
1110xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Class D has IP address ranges from 224.0.0.0 to 239.255.255.255.

It is reserved for multicasting and does not have any subnet mask.

CLASS E

This IP Class is reserved for experimental purposes for R&D or in future use.

The first 4 bits of Class E is start with 1111and in binary notation its look like

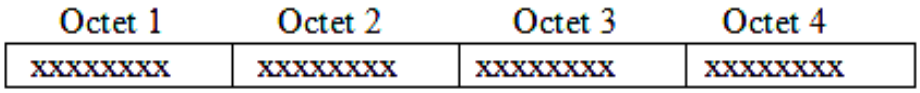
Octet 1	Octet 2	Octet 3	Octet 4
1111xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Class E has IP addresses ranges from 240.0.0.0 to 255.255.255.254.

Similar to Class D, this class does not have any subnet mask.

Net ID and Host ID

In Classful addressing, The Class A, B and C should be divided in to *netid* and *hostid*.



For class A 1 byte is reserved for netid and 3 byte reserved for the hostid. For class B netid and hostid both reserved 2 bytes and for class C, 3 byte reserved for netid and 1 byte reserved for hostid.

Netid and hostid do not apply to classes D and E.

9.4.3 SUBNET MASK

It is a part of an IP address which is used to identify the network, and other part of the IP address is used to identify the host, i.e. mask help us to recognized or find the netid and hostid. The subnet mask has been follows two rules:

- Bits on left side are set to be 1's (or high) in a subnet mask; the corresponding bits in the address recognize the network.
- Bits on right side are set to be 0's (or low) in a subnet mask; the corresponding bits in the address recognize the host.

  The given subnet mask for the network portion must be continuous bits of 1's. For example, a subnet mask of 255.255.0.0 is valid whereas 255.0.255.0 is invalid.

  In order to calculate the Netid, to make the bit wise AND with IP address of the host and the Net mask.

  The mask can also be denoted in the form of /27 (CIDR notation) means that 27 bits from LSB are set with 1's in the mask. Mask is may also denoted as prefix/length.

  Example- 193.167.5.32/27 denotes the network 193.167.5.32 with a mask of 255.255.255.224.

(a) Address Classes vs. Subnet Mask

First of all recall the following three rules to identify the class of IP address along with net Id and Host Id:

- The first octet of an IP address states the corresponding class of that address.
- With the help of subnet mask, to determine which portion of an address illustrates the network, and which portion illustrates the host.

- Each of the class has a default subnet mask.

The network using its default subnet mask is referred to as a **Classful network**.

For example, 15.5.5.5 belongs to Class A IP address, and its default subnet mask is 255.0.0.0 (/8 in CIDR).

Despite of using default mask, it might be possible to use some other subnet mask. For example, it might be possible to apply a Class B subnet mask to Class A IP address: 15.5.5.5/16, but class of IP address is remains Class A and has been subnetted with Class B mask.

(b) Subnet and Broadcast Addresses

There are two host addresses of each of the IP network should be reserved for special purpose use; the first one is Subnet (or network) address and second one is the broadcast address. None of these addresses should be assigned to a real host. For identification of the network, the subnet mask is to be used. In the host portion of the IP address, subnet addresses contain all 0's bits.

For example, subnet address: 193.169.3.0/24 can be determined by fixing the 24-bits 1's form left side at the IP address and remaining 8-bits set to be 0's so subnet mask in binary:

IP Address: 11000001.10101001.00000011.00000000

Subnet Mask: 11111111.11111111.11111111.00000000

Note: In this case all host address bits are set to 0.

The broadcast address is an IP address which is used to allow communication of a message to every connected node of a network. For finding the broadcast addresses, all bits are set to 1's in the host portion of the address.

For example, 193.169.3.255/24 is a broadcast address. Here all host bits are set to be 1's:

IP Address: 11000001.10101001.00000011.00000000

Subnet Mask: 11111111.11111111.11111111.00000000

Broadcast IP Address: 11000001.10101001.00000011.11111111

Broadcasts can be classified in to three types of IP packets:

- **Unicasts**: In unicasts packets have to be sent from single host to some other specific host i.e. in this case there is a singles sender and single receiver.
- **Multicasts** are packets or piece of information sent from one or more host to a set of hosts.
- **Broadcasts** are packets or piece of information sent from one host to all other hosts those are connected on the local network i.e. in this case there is a single sender but information is sent to all connected receiver.

9.4.4 SUBNETTING[4]

Subnetting is the process by which creating new subnetworks or subnets by stealing or withdrawing bits from the host portion of a subnet mask, i.e. dividing a network in to smaller units.

Consider the following Class C IP address of a network:

193.169.254.0

The default subnet mask for the above Class C network is 255.255.255.0. This single network has been divided, or to be subnetted into multiple subnetworks.

For example, let us suppose that a minimum of 12 new networks is required.

To determine this by using the following mathematical formula:

$$2^p$$

Where 'p' is the number of bits to withdrawn from the host part of the subnet mask. The default mask of Class C IP address is 255.255.255.0, and it is in binary:

11111111.1111111.1111111.00000000

Here, there are 24 bits set to be 1's, which has been used to identify the network, and remaining 8 bits set to be 0's, that is used to identify the host, and these host bits can be withdrawn.

Withdrawing bits have been involved changing host bits (set to 0 or off) in the subnet mask to network bits (set to 1 or on). Recall, the network bits in a subnet mask **must be contiguous**1's- skipping bits here is not allowed.

Consider the situation, if three bits are withdrawn.

Now, using the above stated mathematical formula 2^p:

i.e. $2^p = 2^3 = 8 = 8$ new networks created; where p=3,

But, these 8 new networks do not meet the requirement of10 networks. So, Consider the situation if four bits are withdrawn then:

$2^p = 2^4 = 16 = 16$ new networks created, where p=4;

These totals of 16 new networks meet the requirement of at least 12 networks. Withdrawing four host bits leads in the following new subnet mask:

11111111.11111111.11111111.11110000 i.e. 255.255.255.240

In the above example, a Class C network is subnetted to create 16 new networks, using a subnet mask of 255.255.255.240 (or /28 in CIDR). Four bits were withdrawn in the subnet mask and remaining four bits for hosts.

To find the number of usable hosts, for each of the new 16 networks, a slightly modification is required in the above formula:

$$2^p - 2$$

Consider the situation if four bits are available for hosts:

$$2^p - 2 = 2^4 - 2 = 16 - 2 = 14$$, **i.e. only 14 usable hosts per network**

Thus, subnetting of a Class C network with a /28 mask, creates 16 new networks with only 14 usable hosts per network.

- Mathematical formula for calculating **usable hosts** is $2^p - 2$, why not is 2^p**?**

  Because it is **not possible** to assign a host with all 1's or all 0's bits in the host portion of the address. These addresses have been

  network is subnetted, but useable host addresses are lost and it is considerable.

Check Your Progress 1 :-

What is broadcast address for IP network 172.16.0.0 with subnet mask 255.255.0.0?

9.4.5 PRIVATE VS. PUBLIC IPV4 ADDRESSES [3]

Due to the rapid growth of the Internet, leads to shortage of available IPv4 addresses. In response, a particular subset of the IPv4 address space was classified as private, to temporarily suffering this problem.

If **public address** may be routed on the Internet, then hosts that must be Internet-accessible and must be configured with or reachable by public addresses. The allocation of public addresses has been governed by the Internet Assigned Numbers Authority (IANA).

For internal use within a home or organization, to prefer **private address**, and can be freely used by anyone. Yet, private addresses cannot be routed on the Internet. In fact, routers have been configured to immediately drop traffic with private addresses.

For each IPv4 class**,** there are **three private address ranges** defined in **RFC 1918**:

- Class A **- 10.x.x.x /8(10.0.0.0 - 10.255.255.255)**
- Class B **- 172.16.x.x /12(172.16.0.0 - 172.31.255.255)**
- Class C **- 192.168.x.x /24(192.168.0.0 - 192.168.255.255)**

9.4.6 RESERVED IPV4 ADDRESSES

In the IP addressing architecture, in addition to the three private **IPv4 ranges** as mentioned above, the Internet Assign Number Authority

(IANA) and Internet Engineering Task Force (IETF) has reserved the several IPv4 addressing for the special purposes.

The address 0.0.0.0/0 is known as default route of IPv4 addressing, often it is also called **quad–zero route**. If no specific route can be determine for a given IP destination then it will be used.

The **0.0.0.0 /8** IP address ranges are used to identify hosts on the local network or used for broad cast message; these ranges addresses can only be used for source address. The 0.0.0.0/32IP address used when a host dynamically trying to learn IP address through Dynamic Host Configuration Protocol (DHCP).

The entire **127.x.x.x/8** IP address ranges are known as loopback address and it is reserved for diagnostic purposes.

The **169.254.x.x /16** ranges are used to link-local addresses between two hosts on a single link. By auto-configuration, hosts obtain these addresses such as when a DHCP server may not be found.

The **224.x.x.x to 239.x.x.x** IP address ranges have been reserved for **multicast,** and to be referred to as **Class D** addresses.

The **240.x.x.x to 255.x.x.x** IP address ranges have been reserved for **R&**D and future use. These IP addresses ranges are known as **Class E**IP addresses.

The **255.255.255.255** IP address has been used as a **broadcast address** of the zero address network 0.0.0.0.

9.4.7 IPv6 Addressing

IPv6 Design goals: IPv4 address is a 32-bit address, which has limited number of possible addresses up to 4,294,967,296. IPv4 will be replaced by IP Version 6 (IPv6), due to following reasons:

IPv4 is very successful but due to the limited addresses, it posed problems.

Second problem is, the routing information were not inherent geographically in addresses.

Thirdly, On the basis of experience it has been shown that some of the IPv4 header fields were used very rarely and this leads to basic issues, these fields are:-

Option headers

Fragments

Type of service [TOS]

Simplification for IPv6

IPv6 address simplification is that to move in to a 128-bit IP address. It will assign a fixed format to every header. There is no provision of the

header checksum so this field has to be deleted. It uses extension header instead of options. Hop-by-hop segmentation procedure has been removed, i.e. need not be segment or divided it somewhere in between a packet that is transmitting and then somewhere in between you try to fragment it, yet, due to this fragmentation, to keep the fragmentation number, identification of the packet etc. so all of these have been removed.

IPv6 Header

Most recently version of internet protocol is IPv6; it is simpler than the IPv4 Headers. In this header have few fields and then the source address. Let us assume that this is 32, as previously IPv4 address is only one line but now here four lines is there, i.e. 128-bits for source address as well as 128-bits for destination address. Figure 9.7 shows the IPv6 packet header.

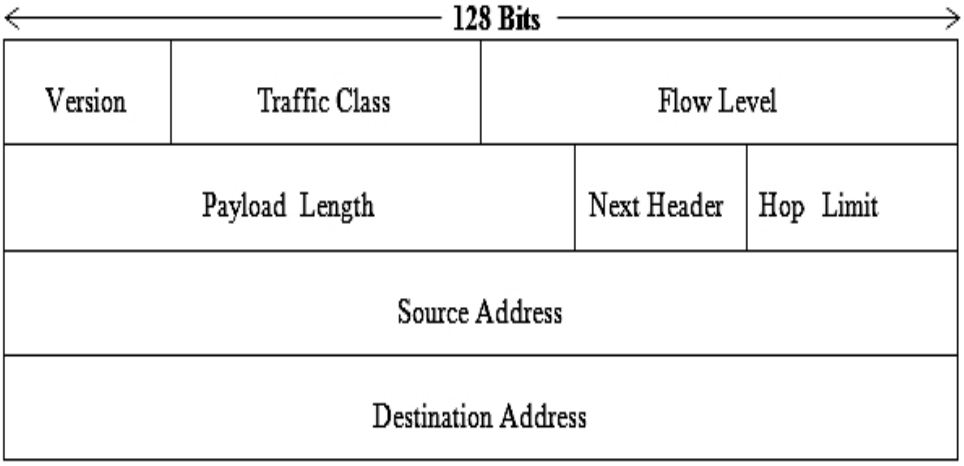


Figure 9.7: IPv6 Packet Header [5]

Let us look at each of the fields:-

Version (4 Bits): It contains version number 6, but as previously it was 4 in IPv4.

Traffic Class (8 Bits): This field holds 8 bits; it is divided into two parts. The first most significant 6 bits are used for Type of Service, which classify the packets, and the remaining 2 bits has been used for Explicit Congestion Notification (i.e. ECN).

Flow Level (20 bits): This field holds 20 bits. Flow label has been used to maintain the sequential flow of the packets transmission. This is designed for streaming/real-time media. This field also helps to avoid re-ordering of data packets and detecting spoofed packets.

Payload Length (16 Bits): It holds 16 bits and defines IP datagram length without excluding the base header. This is 16-bits for that so packets are once again less than or equal to 64 k.

Next Header (8 bits): This field length is 8 bits and defines the header that follows base header in the datagram i.e. it specifies the type of extension header or it indicates the upper layer PDU.

Hop Limit (8 Bits):- This field length is 8 bits and work as TTL field in IPv4, i.e. stop packets from infinitely looping in the network.

Source address (128 Bits):-This field length is 128 bits and indicates original source address of the datagram.

Destination address (128 Bits):- This field length is 128 bits and identifies the final destination address of the datagram.

9.5 EXAMPLES

Now, let us discuss some example problems.

Problem: If the IP address of a system is 66.67.68.70, then calculate the Network Id.

Solution:

Given IP Address ---------- 66.67.68.70----------→Class A

Default Mask address of Class A ----------255. 0. 0. 0

Now, perform the AND operation between system IP address and Mask address, so

66.67.68.70--------01000010.01000011.01000100.01000110

255. 0. 0. 0---------11111111.00000000.00000000.00000000 Perform **AND** Operation

66.0. 0. 0----------01000010.00000000.00000000.00000000-----→Network id

> ***Check Your Progress 2:***
>
> Find the **Class, networkid** and **hostid** of the given following IP addresses.
>
> (i) 15.35.15.35 (ii) 153.65.9.16 (iii) 229.3.49.59

Problem: If the IP address of an organization is 218.17.16.15, then calculate the default mask address, Network Id and address of the 1st host on that network.

Solution:

Given IP address ------218.17.16.15-------→Class C

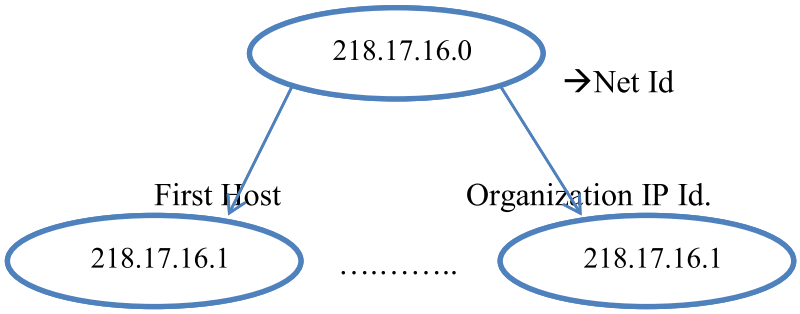
Given IP address comes under Class C IP range so default mask is **255.255.255.0**

Now,

218.17.16.15 -----11011010.00010001.00010000.00001111

255.255.255.0-----11111111.11111111.11111111.00000000 Perform **AND** Operation

218.17.16. 0 -----11011010.00010001.00010000.00001111 →Net Id.



i.e Address of 1st host is 218.17.16.1

Check Your Progress 3:

If the IP address of the system is 201.192.130.131, calculate the Net ID of the next network, 1st host, last host, broadcast address of the next network.

CHECK YOUR PROGRESS

1. Find the **Class, netid** and **hostid** of the following given IP addresses.
   (a) 115.35.2.8 (b) 135.56.8.6 (c) 209.33.54.12
2. In a block of addresses, if the IP address of one host is 25.34.12.56/16. What are the first address (network address) and the last address (limited broadcast address) in this block?

9.6 SUMMARY

A global identification system that uniquely finds every host on the internet and for delivering packets from host to host, router is required at the network layer. IPv4 address is 32 – bits long. It is uniquely and universally defines a host on the network. IPv4 address has been categories in to five classes namely, class A, B,C,D and E. Subnetting is a process in which a large network has been divided in some smaller subnetwork by adding an intermediate hierarchal level in IP addressing.IPv4 addressing is connectionless unreliable protocol and has been responsible for delivering the packet from source to destination host. These packets are known as datagrams. To overcome with the shortage of IPv4 addressing, IPv6 addressing has been used.

IPv6, the modern version of the Internet Protocol, is 128-bit long IP address and has been revised header format, new options, support for resource allocation, an allowance for extension, and increased some additional security measures.

9.7 TERMINAL QUESTIONS

1. If the value of HLEN in an IPv4 datagram is 7. How many option bytes are present?

2. An IP router with a Maximum Transmission Unit (MTU) of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. What is the values of the Most Fragment bit, datagram length and offset fields in the header of the third IP fragment generated by the router.

3. An IPv4 datagram has arrived with the following information in the header (in hexadecimal):

Ox45 00 00 54 00 03 58 50 20 06 00 00 7C 4E 03 02 B4 OE OF 02

(a) Is the packet corrupted?

(b) Are there any options?

(c) Is the packet fragmented?

(d) What is the size of the data?

(e) How many more routers can the packet travel to?

(f) What is the identification number of the packet?

(g) What is the type of service?

4. An organization is allotted the block 130.56.0.0/16. The organization administrator wants to create 1024 subnets.(a) Find the subnet mask. (b) Find the number of addresses in each subnet. (c) Find the first and last addresses in subnet 1. (d) Find the first and last addresses in subnet 1024.

5. Host A (on TCP/IPv4 network A) sends an IP datagram D to host B (also on TCP/IPv4 network B). Assume that no error occurred during the transmission of D. When D reaches B, which of the following IP header field(s) may be different from that of the original datagram D?

(i) TTL

(ii) Checksum

(iii) Fragment Offset

REFERENCE

[1] Tanenbaum& Wetherall, Chapter 5,"Computer networks (5th Edition)".

[2] http://www.highteck.net/EN/Network/OSI_Network_Layer.html

[3] Forouzan, Chapter 20, "Data communications and Networking (4th Edition)".

[4] IPv4 Addressing and Subnetting v1.41 – Aaron Balchunas(www.routeralley.com/guides/**ipv4**.pdf)

[5] https://en.wikipedia.org/wiki/IPv6_packet

UNIT-10 CONNECTION MANAGEMENT

Structure

10.0 INTRODUCTION

This unit discusses how the internetwork is created and the challenges of establishing efficient and effective network. After that we shall learn concepts of connectionless and connection oriented services, fragmentation, tunneling, firewall, and Internet control message protocols.

The rest of the unit is organized as follows. Section 10.1 lists the objectives of the unit. Section 10.2 explains internetworking. Section 10.3 discusses connection-oriented and connectionless services. Sections 10.4, 10.5 and 10.6 describe fragmentation, tunneling and firewalls respectively. Section 10.7 describes ICMP and its message types. Section 10.8 gives the summary of the unit and section 10.9 ends the unit with an exercise for students.

10.1 OBJECTIVE

After reading this unit, the reader should be able to:

- Understand Internetworking and its challenges.
- Learn connectionless and connection oriented services and its advantages/disadvantages.
- Understand tunneling, fragmentation, and firewall.
- Learn Internet control message protocol.

10.2 INTERNETWORKING

An internetwork is an assembly of different networks linked by networking devices, and operates as one big network. It is a packet network intercommunication protocol. When routers forward the packets from source to destination then the packet may cross various separate networks. Internetworking refers to the processes that meet the challenge of building and managing internetworks. Figure 10.1 portrays how different network technologies can be connected through various networking devices and routers to build an internetwork.

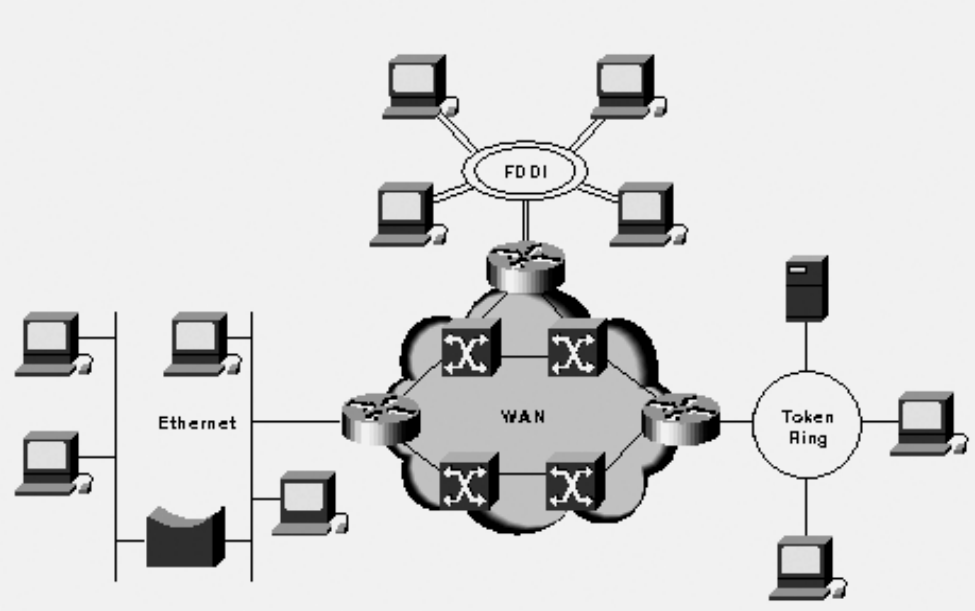


Figure 10.1: Different network technologies can be connected to create an internetwork [1]

Challenges: Connectivity, flexibility, network management and reliability are the key areas in establishing an effective and efficient internetwork.

- The challenge in connecting the various systems is to support communication between different technologies. For example, different sites may utilize different types of media, or they may function at different speeds.
- Reliable service must also be ensured in any internetwork. The entire organizations and individual users are dependent on reliable access to network resources.
- Centralized support and troubleshooting capabilities must be provided by network management in an internetwork. For the internetwork to function smoothly security, configuration, performance, and various other matters should be taken care of.
- Flexibility is required for network expansion and for new services and applications.

10.3 CONNECTION ORIENTED AND CONNECTIONLESS SERVICES

The following two techniques are used to transfer data over the internet.

Connection-Oriented service: Various operations are followed on connection oriented service. These are:

1. Establishing of the connection.
2. Sending information.
3. Releasing the connection.

In this service before starting the communication we have to establish a connection between sender and receiver. After connection establishment we transmit the information from sender to the receiver and then we release the connection. This service is more trusted than connectionless service. TCP is an example of a connection-oriented protocol.

Connectionless service: In connectionless service the data packets are transmitted in one direction from source to destination without checking that destination is ready to accept data or not. Each packet independently sent from source to destination. There is no numbering of data packets. They may be lost or delayed or may reach out of sequence. There is also no mechanism of acknowledging the received frames. The received order of the data at the receiver end can be different from the sent order. Authentication is not required here. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

10.4 FRAGMENTATION

When a large packet is travelling through a network and maximum packet size is too large to handle**,** the large packet is divided into small packets called fragments and the fragments are sent as individual Internet packets**.** It happens when a datagram in network layer is broken up into smaller datagrams to fit and encapsulated in the frame size of a network.

Maximum Transfer Unit (MTU): Each protocol of the data link layer possesses its own frame format. One of the fields specified in the frame format is the maximum size of the data field. That is, if a datagram is encapsulated in a frame, the total size of the datagram should be less than the maximum size of the frame format and it is specified by the restrictions forced by the hardware and software used in the network.

Suppose a datagram reaches at a router interface with 1500 data bytes, and the outgoing interface has 576 bytes MTU. Surely, the datagram requires dividing into smaller fragments as shown in Figure 10.2below.

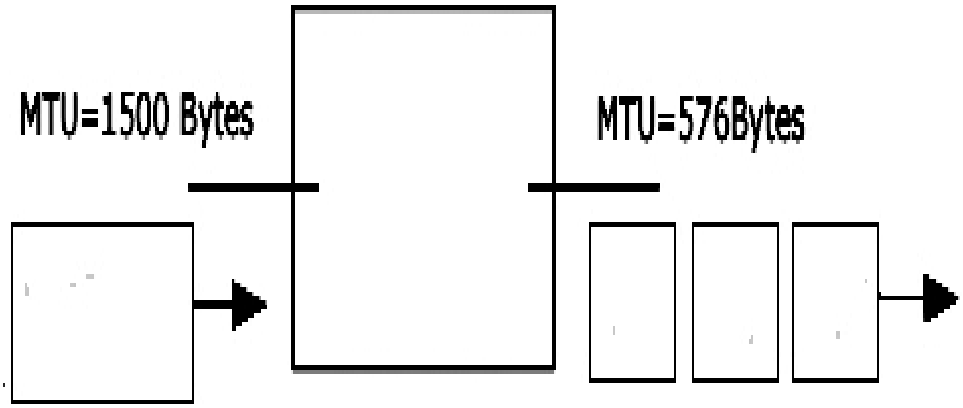


Figure 10.2: Fragmentation [2]

When a datagram is fragmented, it is reassembled only at the destination host's IP layer before delivering to the transport layer. Each and every fragment becomes an IP datagram by itself and moves independently in the network and these fragments can be fragmented further. The fragment must carry enough information for reassembling process at the destination host. IP datagram fragmentation and reassembly is provided by the Identification (ID), flags and fragment offset fields of IP header as shown in Figure 10.3 below.

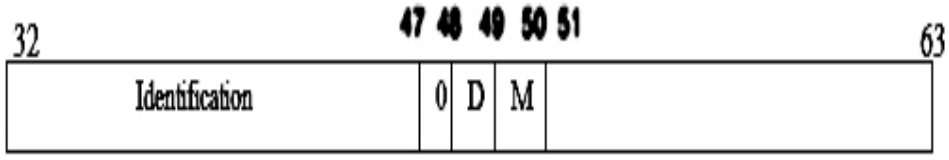


Figure 10.3: ID, flags and fragment offset fields [2]

Let the original incoming 1500-byte datagram consists a 20-byte IP header and 1480 bytsof data. Also assume that the ID field is 398210 (in decimal). Then the fragmentation process divides the data into three parts, where each with 556, 556, and 368 bytes (total = 1480 bytes) respectively, includes a 20-byte IP header to each of the fragments and transmits to the destination end. The flag bits and the offset values are set to the packets. The unique ID field of the datagram is copied to all fragments. This process is shown in the Figure10.4 below.

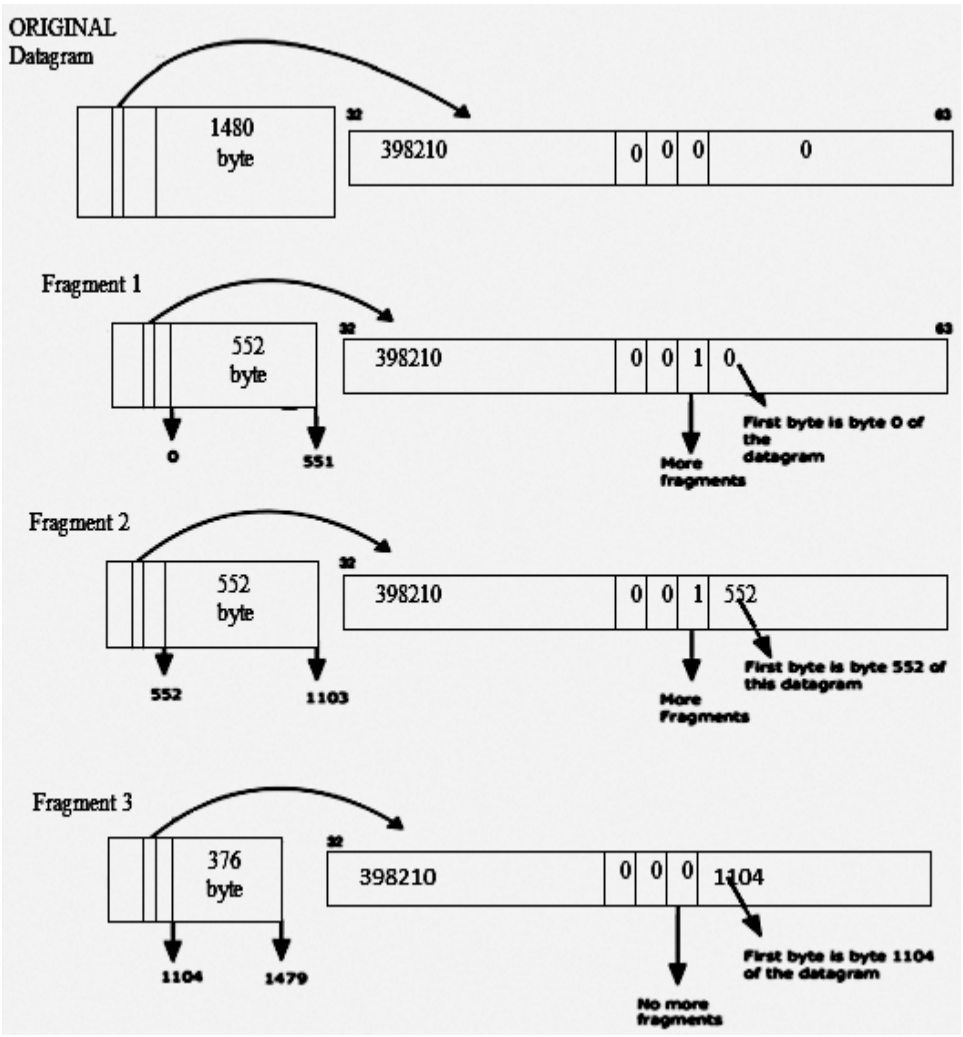


Figure 10.4: Packet fragmentation [2]

The third flag bit called M flag or more fragments flag of each fragment is set to 1, except the last one set to 0 indicating no more fragments. This field informs the destination IP that this datagram is a fragment of a whole datagram. The offset value indicates the destination IP that where the fragment belongs in the datagram and this is required for the reassembling process of the datagram. A necessary condition of fragmentation is that all the fragments must have multiples of 8 bytes of data within them. In the above example the first two fragments has 552 bytes and the last one is 376 bytes. The ID field is uniquely identifies the fragments are from same datagram.

Re-assembly of fragments: Each fragment is a datagram. They do not arrive at a destination in order and do not follow the same route. If an IP receives a datagram and the M flag is set, then it accepts tha t it has receive-d fragmented datagram. IP keeps the fragment in a re-assembly buffer and starts a timer. If it gets all the fragments within a

mentioned time, the datagram is re-assembled and pushed to the transport layer. If the timer expires before arriving of all the fragments, a "reassembly time exceeded "message is transmitted to the source (an Internet Control Message Protocol (ICMP) message).

If a datagram reaches with M flag bit not set, then the offset value is checked by IP. If offset value is 0, then IP assumes it is the entire datagram and if offset value is not zero, then it is the last fragment, and IP requires to wait for the other fragments.

Fragmentation is time taking process and complicated and also uses resources. Therefore it must be avoided. IPv6 has no provision for fragmentation.

10.5 TUNNELING

Tunneling strategy is used when two networks of same IP protocol want to communicate through a network that operates on a different IP protocol. For example, two IPv6 networks want to talk to each other but the packet has to move through an IPv4 network. The packet must possess an IPv4 address to move through the IPv4 network. To solve this issue, the IPv6 packet is encapsulated in an IPv4 packet when it enters the IPv4 region. As the IPv6 packet exits the region it leaves the capsule. So it appears as if the IPv6 packet goes through a tunnel at one end and emerges at the other end. Tunneling is shown below in Figure 10.5.

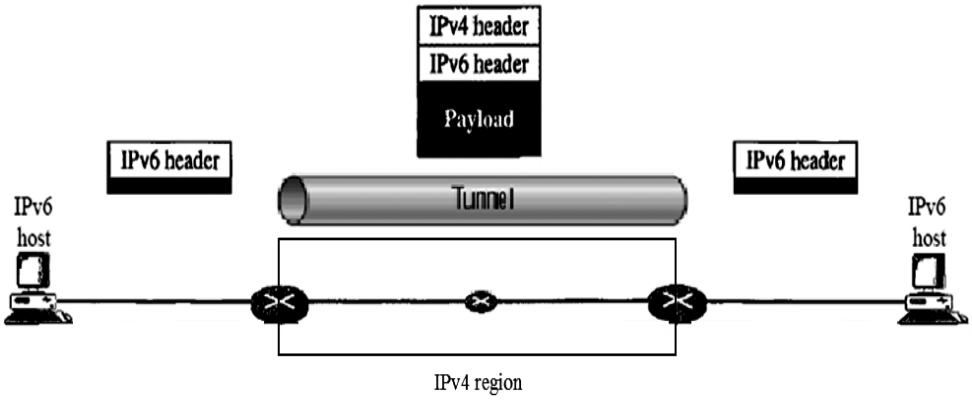


Figure 10.5: Tunneling strategy [3]

10.6 FIREWALL

The primary function of a firewall is to prevent a computer system connected to a network from being accessed by unauthorized personnel. A firewall is usually placed at the boundary of a network that separates it from the rest of the Internet. It basically filters incoming packets and allows only the authorized packets to enter the network. A firewall can also deny access to a particular service in an organization or even a particular host. Firewalls are classified into two types: Packet-filter firewalls and Proxy-based firewalls.

Packet-Filter Firewall: A packet-filter firewall filters (i.e. allows to pass or stops) the packet on the basis of the information contained in the network layer and transport layer header. The information in the transport layer and network layer headers are following.

(i) Type of protocol (TCP or UDP)

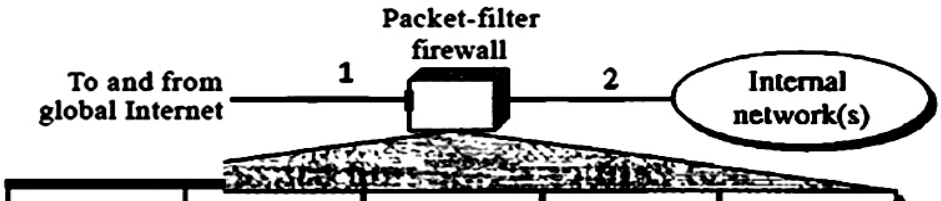
(ii) Source port address and destination port address

(iii) Source IP address and destination IP address

A packet-filter firewall operates more or less like a router. It employs a filtering table to select which packets can be forwarded and which packets cannot be forwarded. As shown in Figure 10.6, the following packets are filtered.

1. Outbound packets whose destination is an HTTP server (port 80) is blocked. This is so because the company does not want its employees to access Internet.

2. Inbound packets destined for any internal TELNET server (port 23) are stopped.
3. Inbound packets from network 131.34.0.0 are stopped (security measure).
4. Inbound packets destined for internal host 194.78.20.8 are stopped. This is so because the organization wants the host to be used for internal purposes only.
5. Note that here * (asterisk) means “any”



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Figure 10.6: Packet-filter firewall [4]

Proxy Firewall: Proxy firewall filters packets based on the information contained in them. Let us suppose that a company wishes to restrict the

access to its webpages. It wants to give access to only those Internet users who have established business relations with the company previously. Except for them all other users should be prevented from accessing the webpages. In such a situation packet-filter firewall cannot be used as it cannot distinguish between the packets from authorized users and unauthorized users. To solve the problem a proxy firewall can be employed. It is also known as an application gateway which is placed between the corporation computer and the customer computer. When the application gateway receives the client packet it starts a server process. The packet is opened by the server at the application level and it is checked whether the request is valid or not. If the request is valid then the server works as a client process and forwards the packet to the real server in the organization. If the request is not valid then the packet is discarded and an error message is sent back to the external user. Figure 10.7 shows how an application gateway filters HTTP packets.

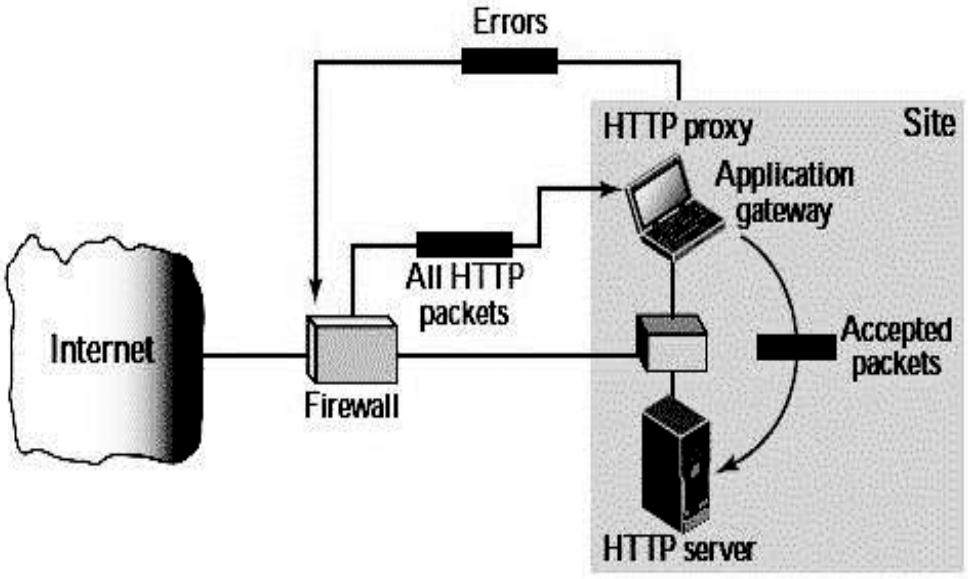


Figure 10.7: Proxy firewall [5]

10.7 INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

IP gives unreliable and connectionless datagram delivery. IP lacks in providing error control and assistance mechanism. ICMP was designed to take care of both the above issues. The routers and hosts use ICMP to send network control information to each other. ICMP is encapsulated in an IP packet, but is assumed to be the part of the IP or Internet layer.

ICMP Messages: ICMP messages are categorized into two basic types:

- Error-reporting message: When devices like routers encounter problems in the network or with the datagrams then they generate error messages which is sent back to the source.

- Query message: When a network manager or router needs some specific information about a host or a router then query messages are exchanged between them.

Figure 10.8 shows the types of ICMP Error-reporting and Query messages.

Category	Type	Message
Error-reporting message	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request to reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router solicitation or advertisement

Figure 10.8: ICMP messages [6]

Message Format: An ICMP message contains a header which is 8 bytes long and a data section which is of variable size. The general header format for each message type is different, but the first 4 bytes of all the messages are same. As shown in Figure 10.9, the first field in the ICMP message format is the ICMP Type. It is 8 bits long and denotes the message type. The next field is the Code that is 8 bits long. It gives the reason for the particular message type. The checksum which is 16 bits long is the last field. The rest of the header is different for each type of message.

The data section in an error message holds the information that helps in finding the original packet that contained the error. The data section in a query message contains additional information based on the query type. Format of ICMP messages is shown below in Figure 10.9.

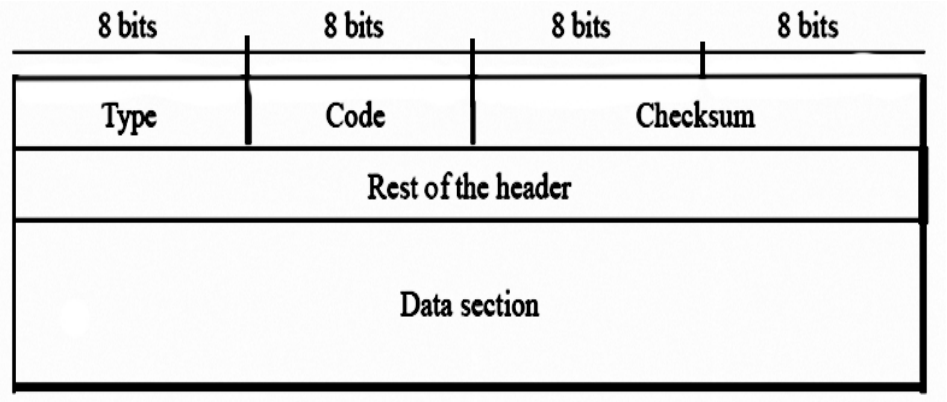


Figure 10.9: ICMP message format [7]

ICMP Error Messages: ICMP sends error messages to the source which generated the datagram. Five different error types are handled here: Source quench, parameter problems, destination unreachable, time exceeded and redirection.

Following are the key facts about ICMP Error Messages:

- No ICMP error message will be created if a datagram carries an ICMP error message.
- No ICMP error message will be created if a datagram has a special address like 127.0.0.0 or 0.0.0.0.
- No ICMP error message will be created if a datagram has a multicast address.
- No ICMP error message will be created if a fragmented datagram is not the first fragment.

Figure 10.10 shows the types of Error-reporting messages in ICMP.

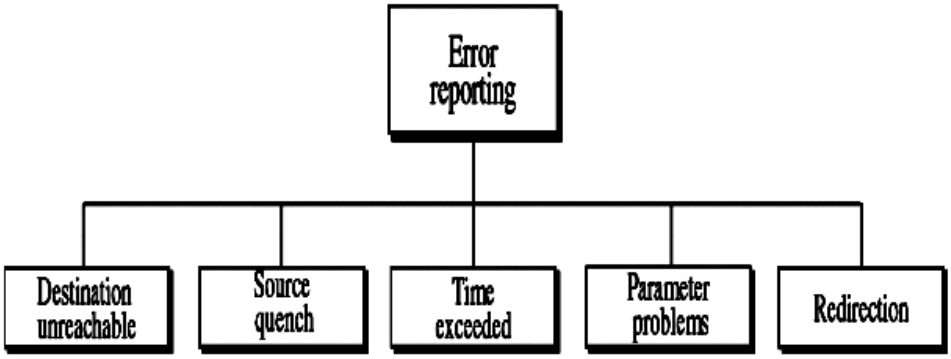


Figure 10.10: Error messages [7]

1. **Destination Unreachable:** If a router or destination host can't deliver a datagram, it drops the message and transmits an ICMP "destination unreachable" message to the sending computer or host that initiated the datagram.
2. **Source Quench:** When the buffer space of a router is full, it rejects the datagram that has arrived and then sends a source quench message to the source. This message notifies the source that the router has discarded the datagram. It also notifies that there is a jam somewhere in the path and therefore the source needs to slow down the process of sending.
3. **Time Exceeded:** When a datagram arrives at a router the value of the TTL (Time To Live) field is decremented by 1. When the value of the TTL field becomes 0, after decrementing, the datagram is rejected by the router. A time-exceeded message is also sent to the original source when the router rejects the datagram. When all the fragments that constitute a message do not reach the destination within a predefined time limit, a time-exceeded message is generated and sent to the source.

4. **Parameter Problem**: If there is any ambiguity in the header portion of a datagram, problems may be created while it is moving through the network. If a router or the destination notices an ambiguous or missing value in any of the datagram's fields, it rejects the datagram and sends to the source a parameter problem message.

5. **Redirection: A** router sends a redirection message to a local host which is located on the same network to inform the host that there is a better path to the destination. Initially the routing table of a host is small. This table is gradually updated and developed. Figure 10.11 below shows how the redirection messages can help in updating routing tables.

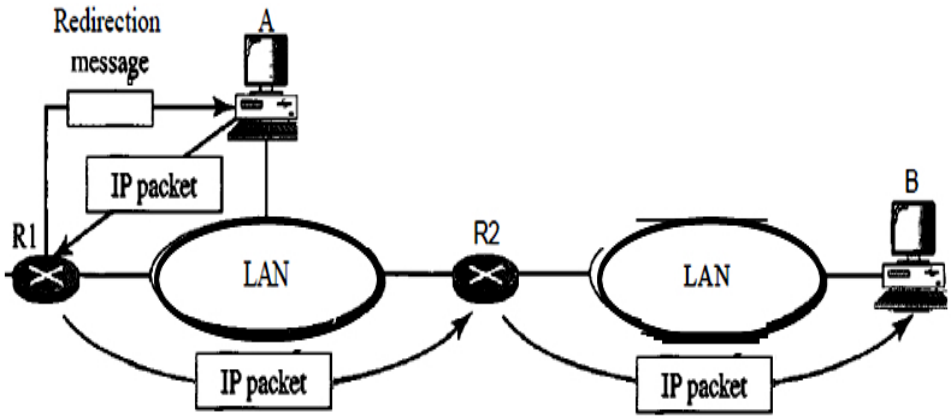


Figure 10.11: Redirection message [7]

Host A wishes to send a datagram to host B. Host A sends an IP packet to router R1. Router R1 checks its routing table and forwards the IP packet to router R2. But it has now learnt that host A should send packets destined for host B directly to router R2. Therefore it also sends a redirection message to host A which updates its table.

ICMP Query Messages

ICMP can also find if there are any problems in the network with the help of query messages. Suppose node X wants to know some specific information from node Y. X sends a query message to Y, which then responds with the reply of the query. There are four types of query messages which have been discussed below.

1. **Echo Request and Reply**

   The echo request and the echo reply message pair is used to check if two nodes (hosts or routers) can talk to each other. If the node that sent an echo request message receives an echo reply message as a response then it infers that the destination is reachable. It also

confirms that all the routers lying between the two nodes are working properly.

2. **Timestamp Request and Reply**

   The timestamp request and timestamp reply message pair is used to determine the round-trip time of an IP datagram to travel between two nodes (hosts or routers). It helps the two nodes in synchronizing their clocks.

3. **Address-Mask Request and Reply**

   A host may be aware of its IP address; however it may not be aware of the corresponding mask. In such a situation it either broadcasts an address-mask request (if it does not know the router's address) or sends the address-mask request straight to the router (if it knows the address of the router). The router responds with an address-mask reply message, which declares the mask for the host.

4. **Router Solicitation and Advertisement**

   A host that wishes to send data to some other network needs to know the addresses of the routers that are connected to its own network. To learn these addresses the host broadcasts a router-solicitation message. All the routers that hear this message respond with router-advertisement messages which contain their routing information.

Figure 10.12 below shows the different types of ICMP query messages.

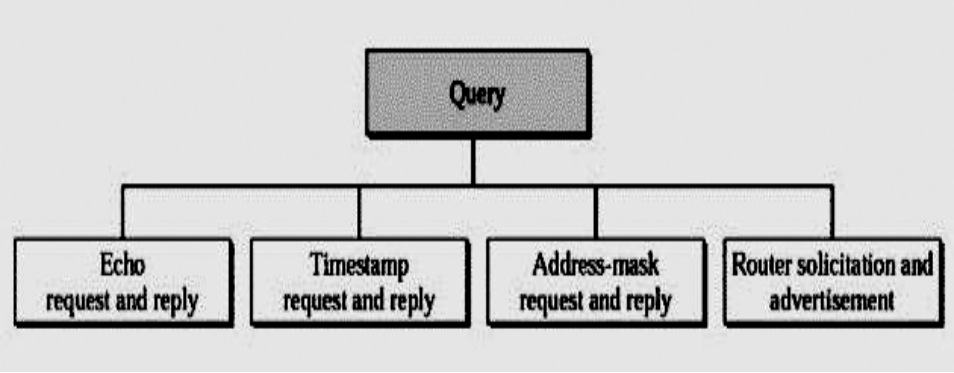


Figure 10.12: ICMP Query Messages [7]

DHCP (Dynamic Host Configuration Protocol) [8]

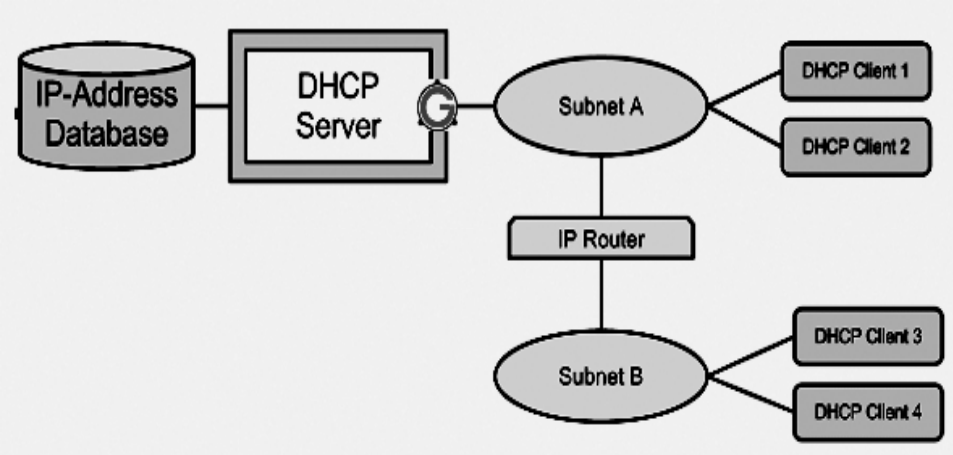
"Computer networks can be of any form like a LAN, WAN etc. If you are connected to a local LAN or an internet connection, the IP addresses form the basis of communication over computer networks. An IP address is the identity of a host or a computer device while connected to any network.

In most of the cases when you connect your computer to a LAN or internet, you'll notice that the IP address and other information like subnet mask etc are assigned to your computer automatically.

As the name suggests, DHCP is used to control the network configuration of a host through a remote server. DHCP functionality comes installed as a default feature in most of the contemporary operating systems. DHCP is an excellent alternative to the time-consuming manual configuration of network settings on a host or a network device.

DHCP works on a client-server model. Being a protocol, it has it's own set of messages that are exchanged between client and server.

Working of DHCP:



Step 1: When the client computer (or device) boots up or is connected to a network, a DHCPDISCOVER message is sent from the client to the server. As there is no network configuration information on the client so the message is sent with 0.0.0.0 as source address and 255.255.255.255 as destination address. If the DHCP server is on local subnet then it directly receives the message or in case it is on different subnet then a relay agent connected on client's subnet is used to pass on the request to DHCP server. The transport protocol used for this message is UDP and the port number used is 67. The client enters the initializing stage during this step.

Step 2: When the DHCP server receives the DHCPDISCOVER request message then it replies with a DHCPOFFER message. This message contains all the network configuration settings required by the client. For example, the yaddr field of the message will contain the IP address to be assigned to client. Similarly the subnet mask and gateway information is filled in the options field. Also, the server fills in the client MAC address in the chaddr field. This message is sent as a broadcast (255.255.255.255) message for the client to receive it directly or if DHCP server is in different subnet then this message is sent to the relay agent that takes care of whether the message is to be passed as unicast or broadcast. In this case also, UDP protocol is used at the transport layer with destination port as 68. The client enters selecting stage during this step.

Step 3: The client forms a DHCPREQUEST message in reply to DHCPOFFER message and sends it to the server indicating it wants to

accept the network configuration sent in the DHCPOFFER message. If there were multiple DHCP servers that received DHCPDISCOVER then client could receive multiple DHCPOFFER messages. But, the client replies to only one of the messages by populating the server identification field with the IP address of a particular DHCP server. All the messages from other DHCP servers are implicitly declined. The DHCPREQUEST message will still contain the source address as 0.0.0.0 as the client is still not allowed to use the IP address passed to it through DHCPOFFER message. The client enters requesting stage during this step.

Step 4: Once the server receives DHCPREQUEST from the client, it sends the DHCPACK message indicating that now the client is allowed to use the IP address assigned to it. The client enters the bound state during this step."

ARP (Address resolution Protocols) [9]

"Address Resolution Protocol (ARP) is one of the major protocol in the TCP/IP suit. Address Resolution Protocol (ARP) resolves an IPv4 address (32 bit Logical Address) to the physical address (48 bit MAC Address). Network Applications at the Application Layer use IPv4 Address to communicate with another device. But at the Datalink layer, the addressing is MAC address (48 bit Physical Address), and this address is burned into the network card permanently. You can view your network card's hardware address by typing the command **ipconfig/all** at the command prompt in Windows Operating Systems.

Working of Address Resolution Protocol (ARP)

Step 1: When a source device want to communicate with another device, source device checks its Address Resolution Protocol (ARP) cache to find it already has a resolved MAC Address of the destination device. If it is there, it will use that MAC Address for communication

Step 2: If ARP resolution is not there in local cache, the source machine will generate an Address Resolution Protocol (ARP) request message, it puts its own data link layer address as the Sender Hardware Address and its own IPv4 Address as the Sender Protocol Address. It fills the destination IPv4 Address as the Target Protocol Address. The Target Hardware Address will be left blank, since the machine is trying to find that.

Step 3: The source broadcast the Address Resolution Protocol (ARP) request message to the local network.

Step 4: The message is received by each device on the LAN since it is a broadcast. Each device compare the Target Protocol Address (IPv4 Address of the machine to which the source is trying to communicate) with its own Protocol Address (IPv4 Address). Those who do not match will drop the packet without any action.

Step 5: When the targeted device checks the Target Protocol Address, it will find a match and will generate an Address Resolution Protocol (ARP) reply message. It takes the Sender Hardware Address and the Sender

Protocol Address fields from the Address Resolution Protocol (ARP) request message and uses these values for the Targeted Hardware Address and Targeted Protocol Address of the reply message.

Step 6: The destination device will update its Address Resolution Protocol (ARP) cache, since it need to contact the sender machine soon.

Step 7: Destination device send the Address Resolution Protocol (ARP) reply message and it will NOT be a broadcast, but a unicast.

Step 8: The source machine will process the Address Resolution Protocol (ARP) reply from destination, it store the Sender Hardware Address as the layer 2 address of the destination.

Step 9: The source machine will update its Address Resolution Protocol (ARP) cache with the Sender Hardware Address and Sender Protocol Address it received from the Address Resolution Protocol (ARP) reply message."

CHECK YOUR PROGRESS

1. Explain internet control messages.
2. When is an ARP request packet generated? What happens when a host receives an ARP request packet?
3. Write down the steps involved in the DHCP process for a client machine. Can DHCP support remote access? Justify the statement.

10.9 SUMMARY

An internetwork can be defined as a group of individual networks, linked by networking devices lying in between, and works as a single large network. Two techniques are used to transfer data over the internet are connection oriented and connection less. The large packet is divided into small packets called fragments. When a datagram is fragmented, it is reassembled only at the destination host's IP layer before delivering to the transport layer. The tunneling strategy is used when two computers based on the same IP protocol want to communicate through a network that operates on some other IP protocol. A firewall is designed to prevent unauthorized access to a networked computer system. It is basically categorized into proxy based firewall and packet filter firewall. IP gives unreliable and connectionless datagram delivery. IP lacks in providing error control and assistance mechanism, this is provided by ICMP protocol. The routers and hosts use ICMP to send network control information to each other.

10.9 TERMINAL QUESTIONS

1. What is difference between connection oriented and connection less service?
2. Discuss ICMP header format.
3. Compute the checksum for the ICMP packet given below-

   Type: Echo Request, Identifier: 123, Sequence number:25, Message: Hello
4. Which two fields in the ICMP header is used for identifying the intent of ICMP message?
5. What are the fields that are changed in an IP header because of fragmentation? What are the IP options that are copied to all the fragments of an IP datagram?
6. What are the common ICMP error reporting messages? Describe in detail the working of the Source Quench message.
7. An IPv4 datagram has arrived whose fragmentation offset is 0 and M bit is also 0. State whether it is a first fragment, a middle fragment, or a last fragment?
8. The Internet at the network layer is a packet-switched connectionless network. Explain this statement.
9. An IPv4 fragment arrives whose offset value is100. How many bytes of data were originally transmitted by the sender prior to the data in this fragment?
10. Explain DHCP in details.
11. Explain working of ARP.

REFERENCES

[1] http://www.cisco.com/cpress/cc/td/cpress/fund/ith/ith01gb.htm#xtocid166841

[2] http://cs.newpaltz.edu/~easwaran/CN/Module5/IPFragmentation.pdf

[3] Behrouz A. Forouzan, Chapter 27, “TCP/IP protocol suite (4th ed.)”.

[4] Behrouz A. Forouzan, Chapter 32, “Data Communications and Networking (4th ed.)”.

[5] Behrouz A. Forouzan, Chapter 30, “TCP/IP protocol suite (4th ed.)”.

[6] http://www.srmuniv.ac.in/ramapuram/sites/ramapuram/files/internetcontrol.pdf

[7] Behrouz A. Forouzan, Chapter 21, “Data Communications and Networking (4th ed.)”.

[8] http://www.thegeekstuff.com/2013/03/dhcp-basics

[9] http://www.omnisecu.com/tcpip/address-resolution-protocol-arp.php

UNIT-11 ROUTING IN NETWORK LAYER

Structure

11.0 INTRODUCTION

This unit starts with the concepts of routing algorithm which is very significant in the network layer. The process of creating static and dynamic routing table is discussed with their application in routing the datagram. After that, the next important concept in the network layer, congestion control and prevention policies have been described. These mechanisms prevent the network to slow down drastically.

The rest of the unit is organized as follows. Section 11.2 presents routing algorithm. Section 11.3 discusses congestion control algorithm and the prevention policies. Section 11.4 presents summary and finally in the end, in section 11.5, some questions have been given.

11.1 OBJECTIVES

After reading this unit, the reader should be able to:

- Learn about the concept of routing and static and dynamic routing table.
- Understand shortest path routing algorithm.
- Learn basic concepts of Flooding, Flow-based routing and Broadcast routing technique.
- Understand different congestion prevention and control policies.

11.2 ROUTING ALGORITHM

In network layer, a packet of data is called a datagram. Routing is a process of moving a datagram from source computer to destination

computer. This is generally performed by a router by analyzing routing table to determine the best path. Routing table lists the routes to particular network destination computers. In Internet, different networks are combined and connected by routers. In a network during moving of a datagram from a source to a destination, datagram passes through many routers until it reaches the router at the destination end. The common field of routing table is shown below in Figure 11.1.

NetMask	Network Address of destination host/network	Next-hop Address	Interface	Flags	Reference Count	Use
……	……	……	……	……	……	……

Figure 11.1: Common fields in a routing table [1]

Where the fields are described as follows:

Netmask: it is used with network address to find out network ID.

Network address: It is destination IP address.

Next-hop address: It tells about address of next-hop router in the direction of Destination.

Interface: It is interface to indicate though which packet will reach.

Flags: There are five flags namely, U (up), G (gateway), H (host-specific), D (added by redirection), and M (modified by redirection). Flags are1/0 to indicate either presence or absence of particular status/devices etc.

(i) U (up): if this flag is 1 then router is up and running else the router is down resulting in discarding packet.

(ii) G (gateway): If this flag is 1 then the destination is in another network that is packet will be delivered to address of the next-hop router for routing table else the destination is in the same network.

(iii) H (host-specific): If it is 1 then the entry in the network address field is a host-specific else the address is only the network address of the destination.

(iv) D (added by redirection):If it is 1 then routing information for this destination has been added to the host routing table by a redirection message from Internet control message protocol (ICMP) else do nothing.

(v) M (modified by redirection): If it is 1 then routing information for this destination has been modified by a redirection message from ICMP else do nothing.

Reference count: It tells that how many users of this route are sending packets to same destination through this route at particular time. For example, if nine users are sending their respective packets to the same host from this router, the value of Reference count is 9.

Use: Indicates the number of packets transmitted through this router for the corresponding destination.

Metrics: To measure or compare routing paths, metrics are used. These metrics are used by routing protocols to determine the best path.

Purpose of a Metric: Routing protocol may determine more than one route between same source and destination and therefore must be able to evaluate and differentiate among available paths; to select the best path. For this purpose, a metric (value used by routing protocols) is used. Each routing protocol assigns metric value in a different way. For example, Routing Information Protocol (RIP) uses hop count, Enhanced Interior Gateway Routing Protocol (EIGRP) uses a combination of bandwidth and delay, and the Cisco implementation of Open Shortest Path First (OSPF) uses bandwidth.

Static versus Dynamic routing table: In static routing table; creation, and maintenance are being done by network administrator. Here, route for each destination into the table is entered by the administrator. Once a table is created, it cannot update automatically when there is a change in the network(s). A static routing table may be used in a network that network topology does not change frequently. On the other hand, dynamic routing table is created, and updated automatically. For example, in the case of shutdown of a router or breaking of a link, the dynamic routing protocols update all the tables in the routers (and eventually in the host) automatically.

Routing Protocol: This type of protocol updates the routing table for any changes. In this, routers to disseminate the information about the internet or their neighborhood. The sharing of information allows a router in Uttar Pradesh to know about the failure of a network in Delhi. There are two types of routing protocols: interior protocol and exterior protocol. Intra-domain routing is handled by an interior protocol and inter-domain routing is handled by an exterior protocol.

As the size of internet has increased, therefore, one routing protocol is not capable to handle routing table of all routers. For this reason, autonomous systems, which are a group of routers and networks authorized by a single administration, have been introduced. Inside an autonomous system, routing is called intra-domain routing. Between autonomous systems, routing is called inter-domain routing. Figure 11.2 below shows Intra-domain and Inter-domain routing protocols. Intra-domain is divided into Distance vector, which uses Routing Information Protocol (RIP) and Link state routing, which uses Open Shortest Path First(OSPF) protocol

whereas Path vector routing, which uses Border Gateway Protocol (BGP) comes under Inter-domain routing protocol.

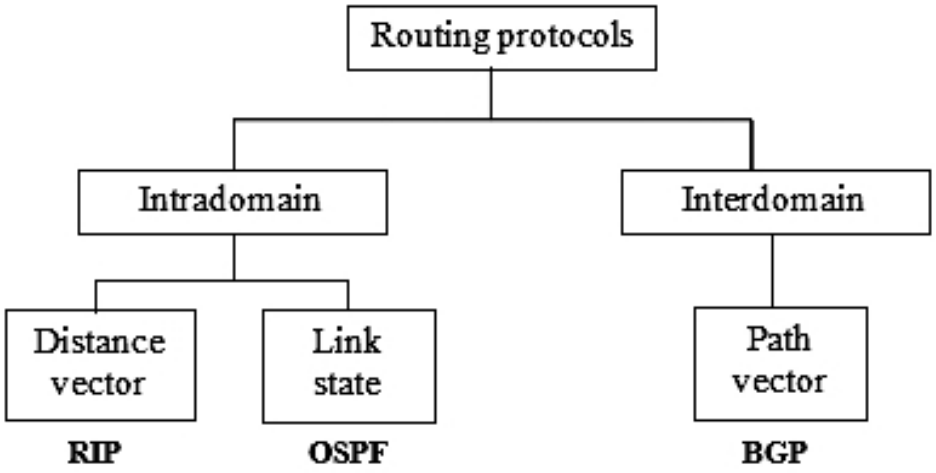


Figure 11.2: Routing protocols [2]

11.2.1 SHORTEST PATH ROUTING

In case of link state routing, each node maintains status like type, cost (metric), and the condition of the links (up or down). Dijkstra algorithm helps in constructing a routing table. Generally, the topology may be dynamic. SO there is a need to update the status of link like, link failure. Initially, no node will have any information about a topology or any change in the network. In linkstate routing, each node has partial knowledge about type, condition, cost etc. of its links. But in due course of time, router will get information of whole topology. Figure 11.3 shows the part of the knowledge belonging to each node.

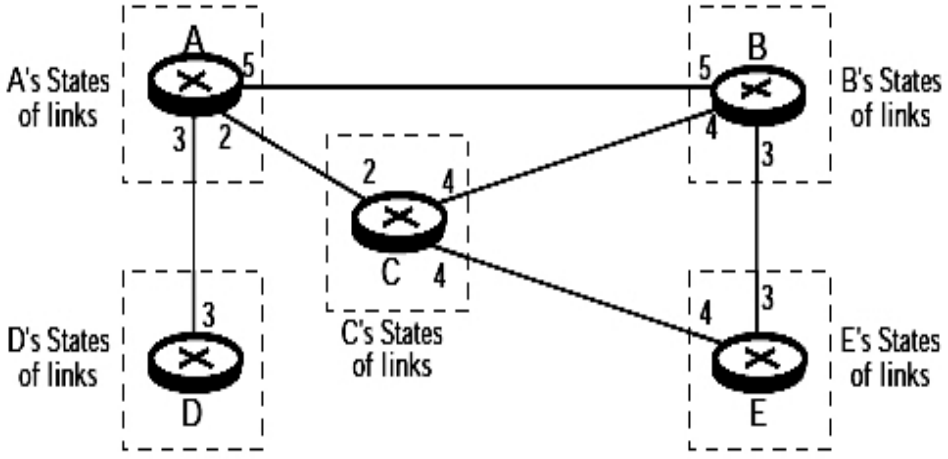


Figure 11.3: Link state knowledge [2]

Node A has information that it is connected to node B with cost 5, to node C with cost 2, and to node D with cost 3. Node C has information that it is

connected to node A with cost 2, to node B with cost 4, and to node E with cost 4. Node D has information that it is connected to node A with cost 3. And so on. Although the knowledge has some overlap but the overlap guarantees the creation of a unique topology.

Building Routing Tables

In link state routing**,** four actions are needed to confirm that every node has the routing table and it has the least-cost node to other nodes.

1. Each node creates states of the links and also called the link state packet or LSP.
2. Link state packets are disseminated to every other router, in a reliable and efficient way, called flooding.
3. Then for each node**,** a shortest path tree is formulated.
4. Based on the shortest path tree a routing table is calculated.

Creation of Link State Packet (LSP)

A link state packet (LSP) is capable to carry large volume of data. Initially it carries a small volume of data: the list of links, the node identity, a sequence number and age. The list of links and node identity are required to make a topology. The sequence number facilitates flooding and it differentiates new LSPs from the old ones. And age prohibits old LSPs from halting in the domain for a long time. LSPs are created on two times.

1. If there is a change in the topology of a domain. Firstly, LSPs are disseminated and immediately informs the other nodes to upgrade its topology.
2. Secondly, to ensure that old information is removed from the domain LSPs are disseminated on a periodic basis. For periodic dissemination, the timer is set generally around of 60 minutes or 2 hours based on implementation. Longer period ensures lesser chance of flooding and do not create too much traffic on the network.

Flooding of LSPs

After a node prepares a link state packet (LSP), it should be disseminated to its neighbors and also all the other nodes. This process is called flooding.

1. If LSP is created by a node, then it sends a copy to each interface.
2. When a node has received a LSP, it compares the copy it may have previously with the newly arrived LSP. If the recently arrived LSP is older than the existing previous one (by checking a sequence number), then it discards the newly arrived LSP. If recently received LSP is new, then the node can do the following.
    a. It keeps the new LSP and discards the old LSP.

b. It sends a copy of new LSP to each interface except the node from which the packet as arrived and assures that somewhere in the domain, flooding stops where anode has only one interface.

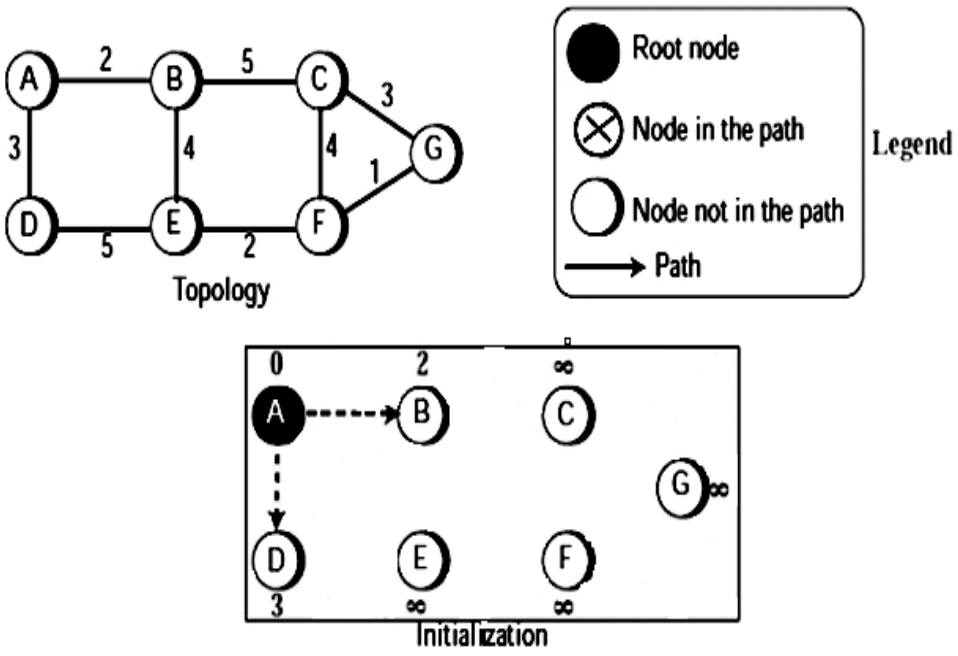
Formation of Shortest Path Tree

Now, all LSPs are received and each and every node has a copy of the whole topology. But the topology is not sufficient to find the shortest path to other nodes and a shortest path tree is required.

A graph of nodes and links, having no loops, is called a tree. Only one node is called the root and from the root we can find a path to other node. In a shortest path tree the path from the root to every other node is the shortest path. The Dijkstra algorithm is applied to a given graph to find a shortest path tree. The algorithm executes the following steps.

1. Initialization: Select a root node to form the tree and add it to the path. Set the smallest distance of the root to zero. Set the shortest distances for all the neighbor nodes reachable from the root to its cost between them.
2. Iteration: Repeat the two steps given below until all nodes are adjusted to the path.
   - **a)** Search the node which is not included in the path and add the new node to the path with minimum shortest distance.
   - **b)** After adding a new node update the shortest distance for all remaining nodes using the shortest distance of the new node.

Figure 11.4given below shows an example.



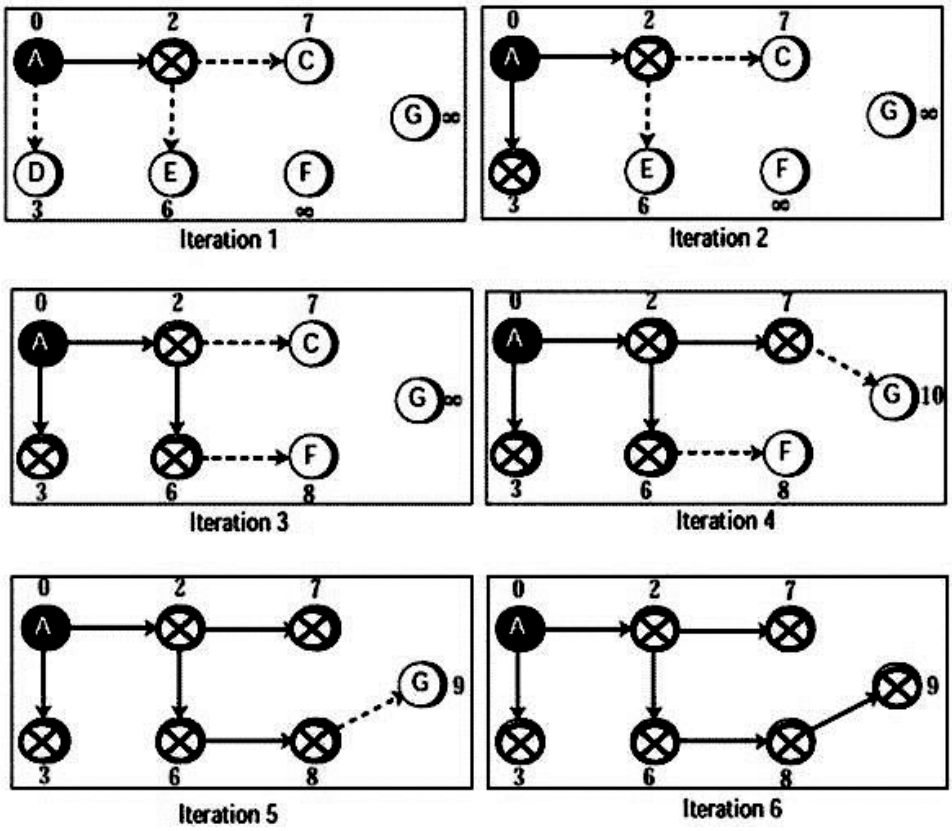


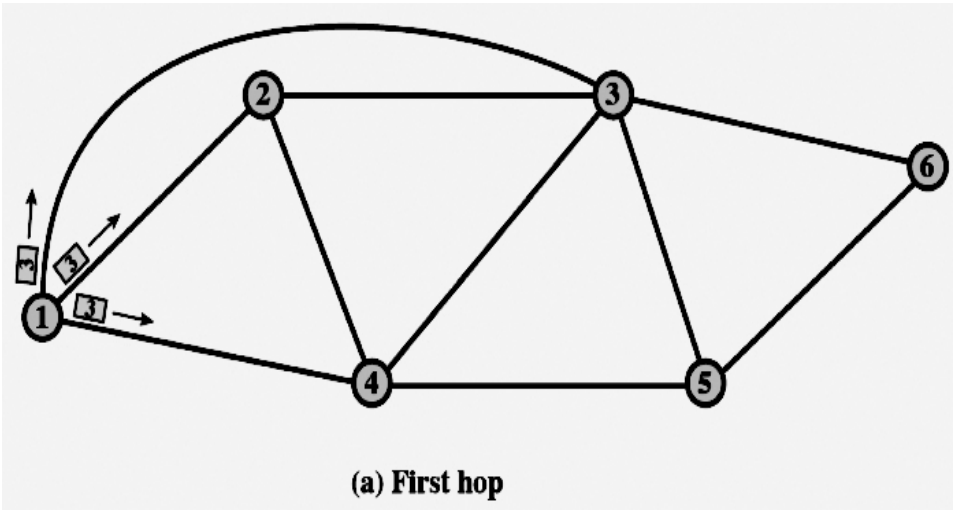
Figure 11.4: Forming shortest path tree for router A from a graph [2]

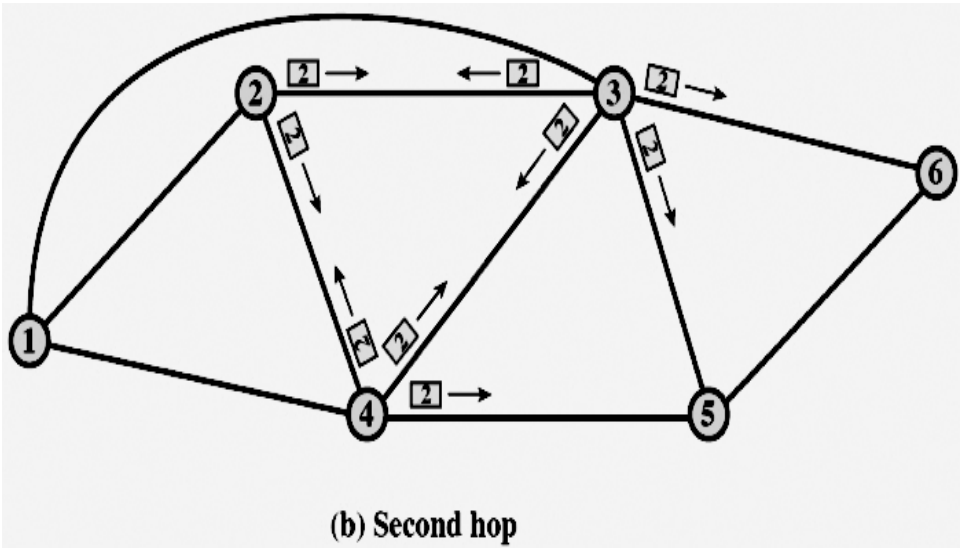
11.2.2 FLOODING

In flooding, each and every router will send out the data packet on all interfaces except the one it arrived on. Flooding produces huge number of duplicate packets, which can be infinite number and some measure should be taken to prevent this.

Flooding is controlled by some of these measures:

1. Sequencing: Source router sets a sequence number in the packet. Each router remembers this identity of the packet it has sent out. If duplicate packet arrives back, then they are discarded.
2. Hop count or TTL (time-to-live) field: Source router initialize a hop count value (as TTL) with each packet. Each time a node passes a packet, it decrements the hope count value by 1. When the hope count value is zero (TTL=0), then the router discards the packet. This is shown below in Figure 11.5.





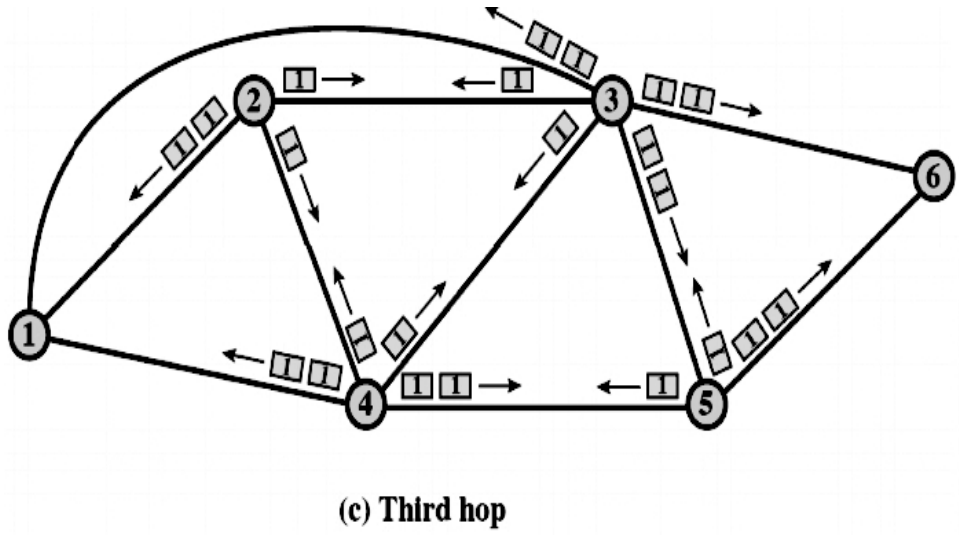


Figure 11.5: TTL value decreases by one after each hop [3]

11.2.3 FLOW BASED ROUTING

Flow based routing takes not only the topology, it also consider the flow of the network. Inflow based routing, for a given line, if the capacity and average flow are known, we are able to compute the mean packet delay on that line from the queuing theory. From the mean delays of all the lines, we can find the mean packet delay for the whole subnet. And it is straightforward to calculate the flow weighted average. In that way the routing problem reduces to find the routing algorithm that generates the minimum average delay for the subnet.

11.2.4 BROADCAST ROUTING

In broadcast routing packet is sent from a source node to every destination simultaneously in the network. Different possible routing mechanisms are provided for broadcasting as described below.

(i) Simplistic approach

It sends separate packet to each destination, but expensive one. Here the source needs to know about all destinations on the network.

(ii) Flooding

It may create too many duplicates and it depends on node connectivity. It also wastes bandwidth of the network. Here, the worse drawback is when a node is connected to more than two nodes it will generates and forwards more than one copies of the broadcast packet. Then each destination node with more neighbors will create more copies of the packet and so on and this results endless multiplication of broadcast packet and is called broadcast storm.

CHECK YOUR PROGRESS

1. What is routing? Discuss static vs. dynamic routing.

2. The routing table of a router is shown below:

Destination	Sub net mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
Default		Eth2

a. On which interfaces will the router forward packets addressed to destinations 128.75.43.16 and 192.12.17.10 respectively?

3. Consider the following routing table of a router.

4.	Prefix	**5.**	Next Hope
6.	192.24.0.0/18	**7.**	D
8.	192.24.12.0/22	**9.**	B

a. Consider the following three IP addresses:

b. 192.24.6.0

c. 192.24.14.32

d. 192.24.54.0

e. How the packets with above three destination IP addresses are forwarded?

11.3 CONGESTION CONTROL ALGORITHMS

Congestion control introduces mechanisms and techniques to either prevent or remove congestion. Congestion control mechanisms may be broadly divided into two major categories namely (i) open-loop congestion control for prevention of congestion, and(ii) closed-loop congestion control for removal of congestion as shown in Figure 11.6.

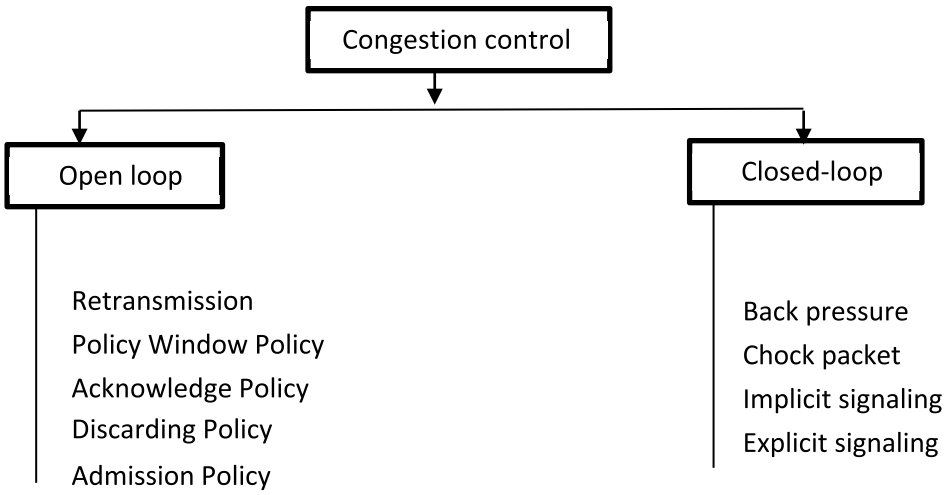


Figure 11.6: Congestion control categories [4]

11.3.1 OPEN LOOP CONGESTION CONTROL

To prevent congestion before it occurs, different policies are applied in open loop congestion control. Here, the source or the destination handles congestion control. A brief list of policies is given below.

(i) Retransmission Policy

Retransmission is sometimes unavoidable. When the sender senses that a sent packet is corrupted or lost, retransmission of the packet is required. But congestion in the network may increase by the retransmission of the packet. However, to prevent congestion a good retransmission policy is needed. To optimize efficiency and prevent congestion at the same time, the retransmission policy and the retransmission timers should be modeled. For example, the retransmission policy used by transmission control protocol (TCP) is designed to prevent congestion.

(ii) Window Policy

At the sender side the type of window can be affected by the congestion. To control congestion, rather than the Go-Back-N window the Selective Repeat window is used. In the Go-Back-N window, for a packet if the timer times out, many of the packets are resent, even some packets are arrived previously safe and sound at the receiver end. This duplication can cause the congestion in the network. However, the Selective Repeat window retransmits only the specific packets that are corrupted or lost.

(iii) Acknowledgment Policy

This policy is introduced by the receiver to affect congestion. If the receiver doesn't transit acknowledgement for every packet it receives, the sender may slow down and this prevent congestion. Certain techniques are considered in that case. A receiver transmits an acknowledgment only when it needs to send a packet or a timer expires. At a time a receiver may send acknowledgment for N packets only. Here the acknowledgments are the part of the load in the network. Sending fewer acknowledgments means imposing lesser loads on the network.

(iv) Discarding Policy

To prevent congestion a good discarding policy can be provided by the routers and at the same time it holds the integrity of the transmission. For example, in case of audio transmission, if the policy is to drop few sensitive packets when congestion occurs, the sound quality is still maintained and congestion is prevented.

(v) Admission Policy

An admission policy is a quality-of-service mechanism and prevents congestion in virtual-circuit networks. In a flow of network, switches of virtual-circuit networks first search the resource requirement of a flow before added it to the network. A router can reject a virtual circuit connection establishment for congestion in the network or for possible future congestion in the network.

11.3.2 CLOSED-LOOP CONGESTION CONTROL

These mechanisms try to reduce congestion after it happens. Different protocols use various mechanisms. Few of them are described below.

(i) Backpressure

Backpressure technique is a node-to-node congestion control mechanism. In this, if any node is congested then it start rejecting further packets from neighbor node in turns the neighbor node gets congested and so on. It gets repeated till source node. This technique is applied only to virtual circuit networks, where each node knows the upstream node from which a flow of data is coming. Figure 11.7 shows the idea.

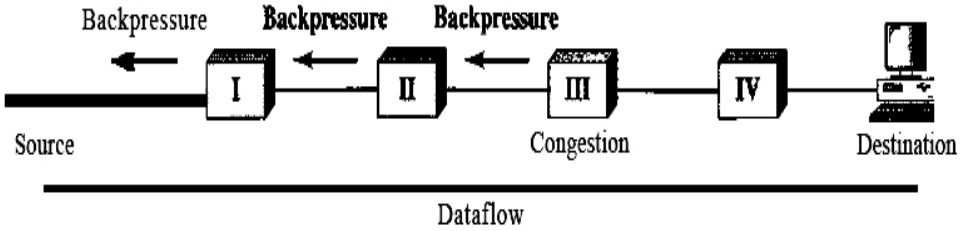


Figure 11.7: Backpressure method [4]

In Figure 11.7 shows that Node III is congested that it cannot handle any further packets. Then it starts rejecting packets from its input buffer and inform to neighbor node II to slow down the rate of sending packets. Further, Node II may be congested in output buffer as Node II has slow down the output flow of packets. Now node II will informs node I to slow down, which in turn is congestion. This process gets repeated at each node till source node. This lightens the congestion.

(ii) Choke Packet

In this method, if router encounters with congestion, then it send choke packet (ICMP Message) directly to the source station to inform about congestion. Here intermediate nodes are not involved to reduce the congestion as it is being done in the case of Backpressure. Internet control massage protocol (ICMP) has this type of control. Figure 11.8 below shows the idea.

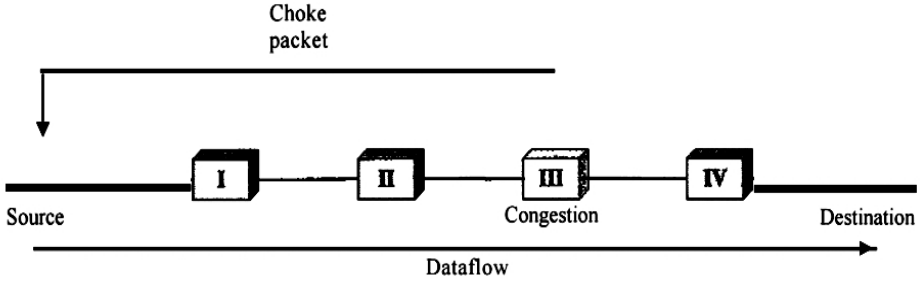


Figure 11.8: Choke packet [4]

(iii) Implicit Signaling

In this method, there is communication between the congested node and the source. If source node does not receive acknowledgement then source node assumes that there is congestion somewhere in the network from other symptoms. And then source starts slow down transmitting packets.

(iv) Explicit Signaling

If a node has experienced congestion then it can explicitly send a signal to the source or destination. This signal is different from the choke packet. It is used in Frame Relay congestion control and may occurs in either of directions that is forward or backward direction.

(v) Backward Signaling

A bit is set in a packet, moving in the direction opposite to the congestion and warns the source for any congestion. To avoid the discarding of packets, the source needs to slow down.

(vi) Forward Signaling

A bit is set in a packet, moving in the direction of the congestion and warns the destination for any congestion in the network. To lighten the congestion, the receiver uses policies like slowing down the acknowledgments.

Traffic shaping

Many times, more number of packets are being generated in the network. Bandwidth available for handling such huge traffic may not be sufficient. That's why we need Traffic shaping. Traffic shaping (also known as packet shaping) is a computer network traffic management technique which delays some or all datagrams to bring them into compliance with a desired traffic profile. It is used to optimize or guarantee performance, improve latency, and/or increase usable bandwidth for some kinds of packets by delaying other kinds.

Leaky Bucket Algorithm

It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network. A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate. Imagine a bucket with a small hole at the bottom. The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate. Thus (as long as water is present in bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket. Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost. (Figure 11.9)

The same concept can be applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 14 Mbps for 5 seconds. Then there is no data for 4 seconds. The source again transmits data at a rate of 11 Mbps for 3 seconds. Thus, in a time span of 12 seconds, 103 Mb (14*5 + 11*3) data has been transmitted.

If a leaky bucket algorithm is used, the data flow will be 6 Mbps for 12 seconds. Thus constant flow is maintained. Assume 6 Mbps is the output data rate of the networking device.

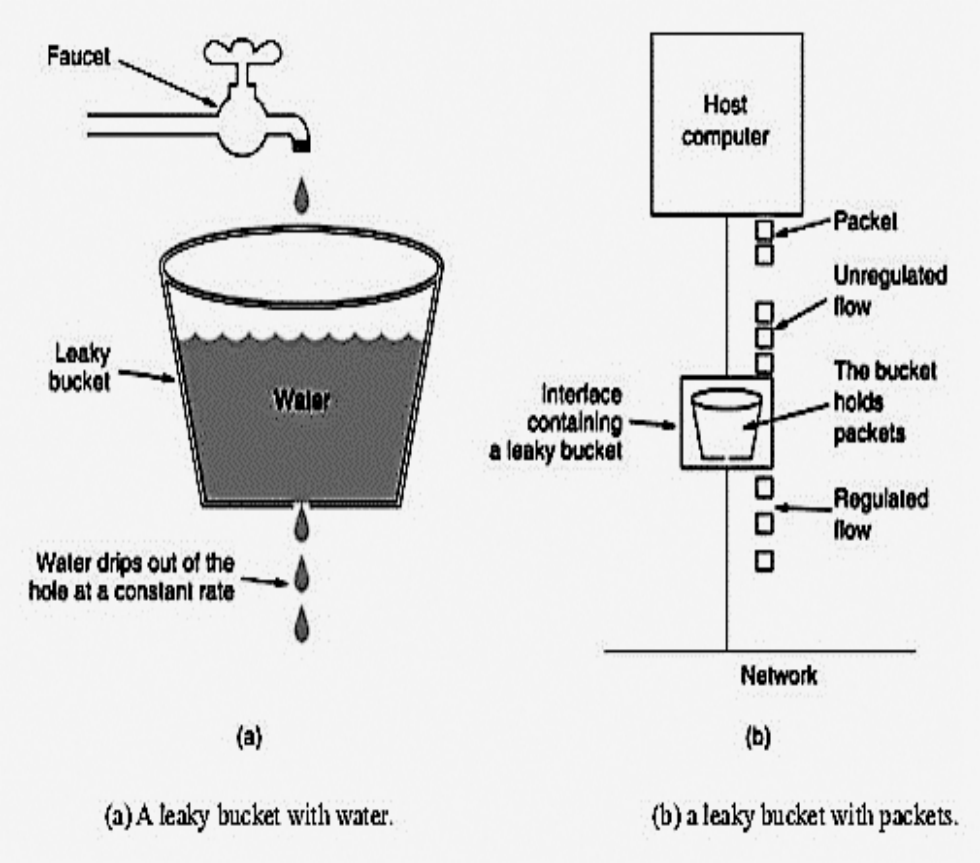


Figure 11.9: Leaky bucket

Token bucket Algorithm

The leaky bucket algorithm allows only an average (constant) rate of data flow. Its major problem is that it cannot deal with bursty data.

A leaky bucket algorithm does not consider the idle time of the host. For example, if the host was idle for 10 seconds and now it is willing to sent data at a very high speed for another 10 seconds, the total data transmission will be divided into 20 seconds and average data rate will be maintained. The host is having no advantage of sitting idle for 10 seconds.

To overcome this problem, a token bucket algorithm is used. A token bucket algorithm allows bursty data transfers.

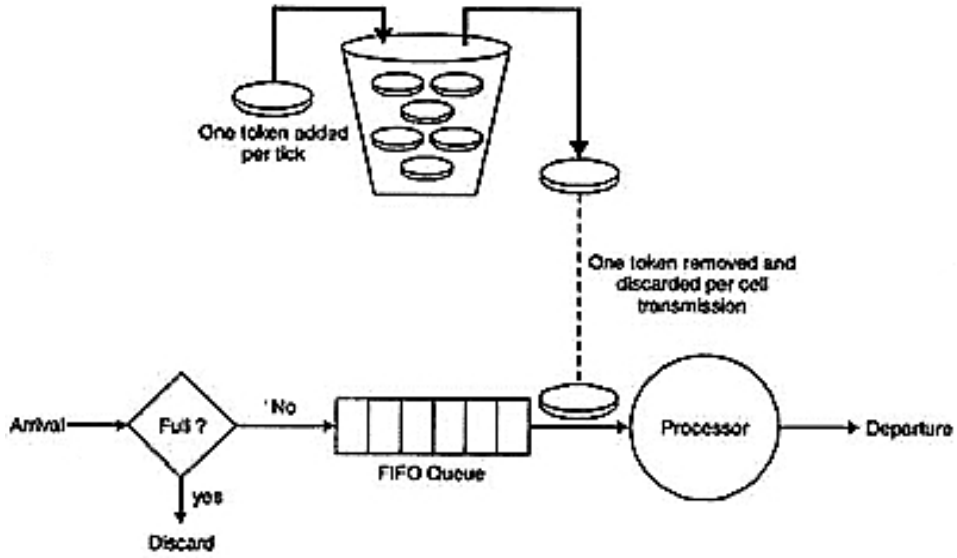


Figure 11.10 Token Bucket Algorithm

A token bucket algorithm is a modification of leaky bucket in which leaky bucket contains tokens. In this algorithm, a token(s) are generated at every clock tick. For a packet to be transmitted, system must remove token(s) from the bucket. Thus, a token bucket algorithm allows idle hosts to accumulate credit for the future in form of tokens. For example, if a system generates 100 tokens in one clock tick and the host is idle for 100 ticks. The bucket will contain 10,000 tokens. Now, if the host wants to send bursty data, it can consume all 10,000 tokens at once for sending 10,000 cells or bytes. Thus a host can send bursty data as long as bucket is not empty.

RSVP (Resource Reservation Protocol)

RSVP (Resource Reservation Protocol) is a set of communication rules that allows channels or paths on the Internet to be reserved for the multicast (one source to many receivers) transmission of video and other high-bandwidth messages. RSVP is part of the Internet Integrated Service (IIS) model, which ensures best-effort service, real-time service, and controlled link-sharing.

Understanding by example: Let's assume that a particular multimedia program is to be multicast at a certain time on Sunday morning. For this you need high bandwidth which may not available at the particular time. So, before the broadcast, you need to send an RSVP request to allocate sufficient bandwidth and priority of packet scheduling for the program. This request will reach to your nearest Internet gateway which has RSVP server. This server will determine whether you are eligible to have such request. If yes, then this server will reserve the requested bandwidth without affecting other's earlier reservations. Then this gateway forwards this request reservation to the next gateway toward the destination. In this

manner, your reservation is ensured between sources to destination. If the reservation can't be made all the way to the destination, then your request will be dropped out.

CHECK YOUR PROGRESS

1. What is choke packet? How is it used for congestion control?
2. Compare and contrast between leaky bucket and token bucket algorithm.

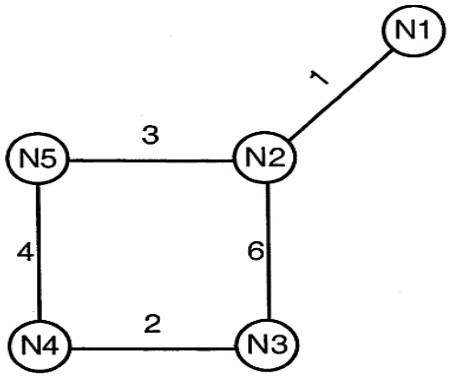
11.4 SUMMARY

Routing is a process of moving a datagram from source computer to destination computer; generally performed by a router by analyzing routing table to determine the best path. In static routing table entries are manual whereas dynamic routing table is updated automatically. Routing protocol is a combination of procedures and rules that let routers to inform each other for any changes. For shortest path routing, the Dijkstra algorithm is used to build a routing table. Flooding produces huge number of duplicate packets, which can be infinite number and some measure to control flooding has been discussed. Flow based routing considers the flow of the network. In broadcast routing, a packet has sent from a source node to every destination at the same time in the network. Congestion control is the mechanism and technique to control congestion. Open-loop congestion control prevents congestion whereas closed-loop congestion control removes congestion and keeps the load below capacity.

11.5 TERMINALQUESTIONS

1. What is routing? Discuss static vs. dynamic routing.

2. Consider a network with five nodes, N1 to N5, as shown below.



The network uses a Distance Vector Routing protocol. Once the routes have stabilized, the distance vectors at different nodes are as following.

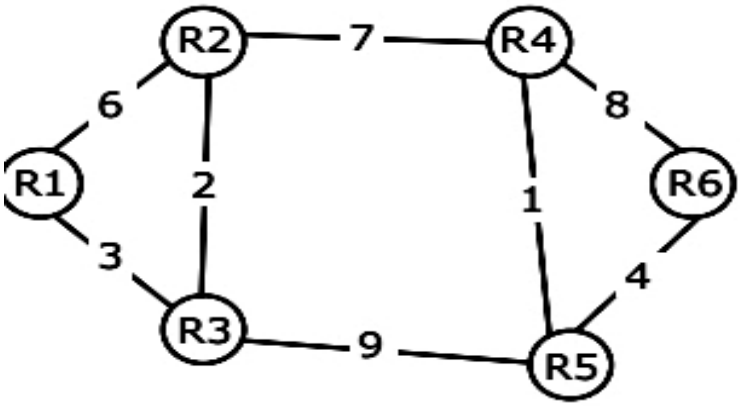
N1: (0, 1, 7, 8, 4), N2: (1, 0, 6, 7, 3), N3: (7, 6, 0, 2, 6), N4: (8, 7, 2, 0, 4) and N5: (4, 3, 6, 4, 0).

Each distance vector is the distance of the best known path at the instance to nodes, N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbors. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors.

(a) The cost of link N2-N3 reduces to 2(in both directions). After the next round of updates, what will be the new distance vector at node, N3?

(b) After the update in the previous question, the link N1-N2 goes down. N2 will reflect this change immediately in its distance vector as cost, ∞. After the NEXT ROUND of update, what will be the cost to N1 in the distance vector of N3?

3. Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram.



(a) All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbor with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

(b) Suppose the weights of all unused links in the previous question are changed to 2 and the distance vector algorithm is used again until all routing tables stabilize. How many links will now remain unused?

4. Classless Inter-domain Routing (CIDR) receives a packet with address 131.23.151.76. The router's routing table has the following entries:

Prefix	Output Interface Identifier
131.16.0.0/12	3
131.28.0.0/14	5
131.19.0.0/16	2
131.22.0.0/15	1

The identifier of the output interface on which this packet will be forwarded is _____.

5. The routing table of a router is shown below :

Destination	Sub net mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
Default		Eth2

On which interfaces will the router forward packets addressed to destinations 128.75.43.16 and 192.12.17.10 respectively?

6. Consider the following table of a router.

Prefix	Next Hope
192.24.0.0/18	D
192.24.12.0/22	B

Consider the following three IP addresses:

1. 192.24.6.0
2. 192.24.14.32
3. 192.24.54.0

How the packets with above three destination IP addresses are forwarded?

7. Suppose that the maximum transmit window size for a TCP connection is 12000 bytes. Each packet consists of 2000 bytes. At some point of time, the connection is in slow-start phase with a current transmitting window of 4000 bytes. Subsequently, the transmitter receives two acknowledgements. Assume that no packets are lost and there are no time-outs. What is the maximum possible value of the current transmit window?

8. Host X has IP address 192.168.1.97 and is connected through two routers R1 and R2 to an-other host Y with IP address 192.168.1.80. Router R1 has IP addresses 192.168.1.135 and 192.168.1.110. R2 has IP addresses 192.168.1.67 and 192.168.1.155. The net mask used in the network is 255.255.255.224. Given the information

above, how many distinct subnets are guaranteed to already exist in the network?

9. Why flooding technique is not commonly used for routing?

10. What is choke packet? How is it used for congestion control?

11. Explain working of leaky bucket and token bucket algorithm.

12. Compare and contrast between leaky bucket and token bucket algorithm.

REFERENCES

[1] Behrouz A. Forouzan, Chapter 21, "Data Communications and Networking (4th ed.)".

[2] Behrouz A. Forouzan, Chapter 11, "TCP/IP protocol suite (4th ed.)".

[3] www.comp.hkbu.edu.hk/~comp2330/lecture/notes/ch11.ppt

[4] Behrouz A. Forouzan, Chapter 24, "Data Communications and Networking (4th ed.)".

Uttar Pradesh Rajarshi Tandon
Open University

Bachelor of Computer Application

BCA-1.13

Computer Network

Block

4

Transport, Session, Presentation and Application Layer

Course Design Committee

Course Preparation Committee

ISBN : 978-93-83328-18-5

Printed and Published by Dr. Arun Kumar Gupta Registrar, Uttar Pradesh Rajarshi Tandon Open University, 2019.

Printed By: Chandrakala Universal Pvt. Ltd. 42/7 Jawahar Lal Neharu Road, Prayagraj.

BCA-1.13/228

BLOCK INTRODUCTION

This is the fourth block on last four layers of OSI layers namely Transport, Session, Presentation and Application Layer. As name of this block indicate that this block will introduce requirement of transport, session and application layers. This block has three units namely, Transport layer, Session & Presentation Layer and Application Layer.

We will begin the first unit on Transport layer. This unit discussed different functions like Transport layer connection management, flow control, error control, congestion control, Establishing and releasing a connection. You will understand that why same work like error control, flow control etc. are being managed at two different layers namely Data link layer and Transport layer. It discussed TCP service model and TCP protocol. The second unit mainly discusses need of Introduction to cryptography and data compression. In the last unit, different applications are being discussed in details. First this unit discussed the theory behind conversion from url to IP address using DNS protocol. Further it also discussed working of most ever used application Email. It discussed different protocol used in sending and receiving emails. As you study the material, you will understand the concept with the help of figures, tables, wherever required. Each unit has been describes using many sections. Every unit has summary and review questions in the end. These questions will help you to review yourself.

UNIT-12 TRANSPORT LAYER

Structure

12.0 INTRODUCTION

This unit starts with the discussion on Transport layer connection management after that Flow control, Error control and Congestion control algorithms has been discussed. And in the end, Connection establishment and termination, TCP service model followed by TCP protocol has been discussed.

The rest of the unit is organized as follows. Section 12.1 lists the objectives of the unit. Section 12.2 discusses transport layer connection management. Sections 12.3 and 12.4 talk about flow control and error control techniques respectively. Section 12.5 describes the TCP congestion control algorithms. Section 12.6 explains the connection establishment and termination procedure. Section 12.7 describes TCP service model and section 12.8 describes TCP protocol. Section 12.9 summarizes the unit and section 12.10 ends it with a few terminal questions for students.

12.1 OBJECTIVE

After reading this unit, the reader should be able to:

- Understand the transport layer services
- Learn Flow control, Error control in this layer
- Learn TCP Congestion Control algorithms

- Learn Connection establishment and termination phases in TCP
- Understand TCP service model and TCP header

12.2 TRANSPORT LAYER CONNECTION MANAGEMENT

One of the important functions of transport-layer protocol is to support the communication between two processes running on two different nodes. A process runs on application-layer. Here it is important to understand the difference between and process-to-process communication and host-to-host communication. The network layer is responsible for host-to-host communication. That is network layer transmits the message to the destination computer only. Once message is reached at network layer of destination machine, transport layer deliver the message to the process. Figure 12.1 shows the area of a network layer and a transport layer.

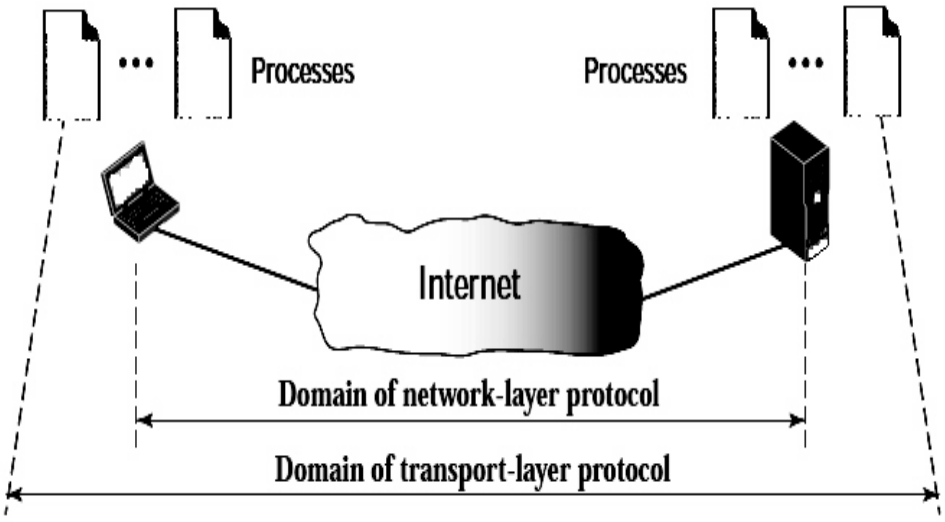


Figure 12.1: Network layer versus transport layer [1]

Port Numbers: This is the number used to uniquely identify the process as there may be more than one process running on the computer at the same time. Port number Process-to-process communication is done mainly through the client-server architecture. A client is a process on the local host, whereas a server is a process on the remote host. Both processes have the same name.

Port number is of 16-bits. Port numbers range from 0 to 65536. Port numbers are divided into three ranges, namely (i) range from 0 to 1023 known as Well Known Ports (ii) range from 1024 to 49151 known as Registered Ports, and (iii) range from 49152 to 65535 known as Dynamic and/or Private Ports. The client program defines itself with a port number is called the ephemeral port number. This port number is recommended to be greater than 1,023 for some client/server programs. The server process

also defines a port number, called well-known port numbers. Some of the port number is as below:

20 FTP -- Data

21 FTP -- Control

22 SSH Remote Login Protocol

23 Telnet

25 Simple Mail Transfer Protocol (SMTP)

53 Domain Name System (DNS)

80 HTTP

110 POP3

115 Simple File Transfer Protocol (SMTP)

443 HTTPS

546 DHCP Client

547 DHCP Server

Socket Addresses: It is combination of the IP address and the port number for a connection. The client socket address uniquely specifies the client process and the server socket address uniquely specifies the server process as shown in Figure 12.2.

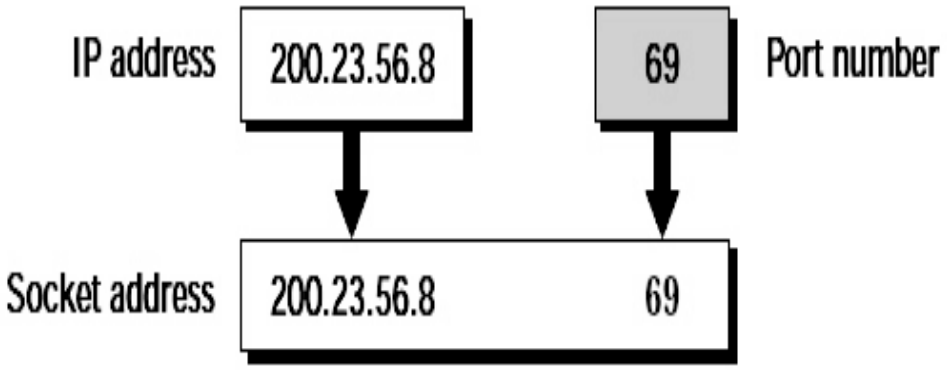


Figure 12.2: Socket address [1]

12.3 FLOW CONTROL [2]

Whenever an object creates items and another object consumes them, the production and consumption between them should be a balance. When the items are created quicker than they can be consumed, the consumer can be overloaded and needs to reject some items. When the items are created slower than they can be consumed, the consumer must

wait and the system becomes not as much of efficient. The first issue is related to flow control. We want to prevent losing the data items at the consumer side.

Pushing or Pulling: Items are delivered from a producer to a consumer can happen in one of the two ways: pushing or pulling. When the sender delivers produced items without the prior request from the consumer the delivery is called pushing. If the producers end the items after the consumer has requested them, then the delivery is called pulling. Figure 12.3 shows these two types of delivery.

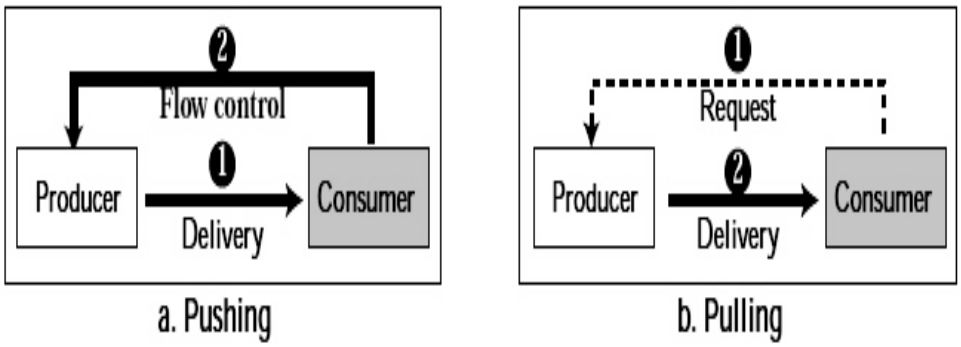


Figure 12.3: Pushing and pulling [1]

If the producer pushes the items, then the consumer may be overloaded and in the opposite direction there is a need for flow control, to prevent the rejecting of the items. That is the consumer is required to warn the producer to stop the delivery and also to inform that it is ready again to receive the items. If the consumer pulls the items, then it will request producer that it is ready to receive items. In second case, there is no need for flow control.

In transport layer, we are concerning with four entities: sender process, sender transport layer, receiver transport layer, and receiver process. At the application layer the sending process is a producer and creates messages and pushes them to the transport layer. The sending transport layer has two roles. It is both a consumer and the producer and consumes the messages pushed by the producer (Application layer). Then it encapsulates the messages in packets and pushes them to the receiving transport layer. The receiving transport layer has also two roles. As a consumer it receives packets from the sender and as a producer: it requires to de-capsulate the messages and sends them to the application layer. However the last delivery is generally a pulling delivery where the transport layer waits for a request from application layer.

Figure 12.4, shows that we require at least two cases of flow control, from the sending transport layer to the sending application layer and from the receiving transport layer to the sending transport layer.

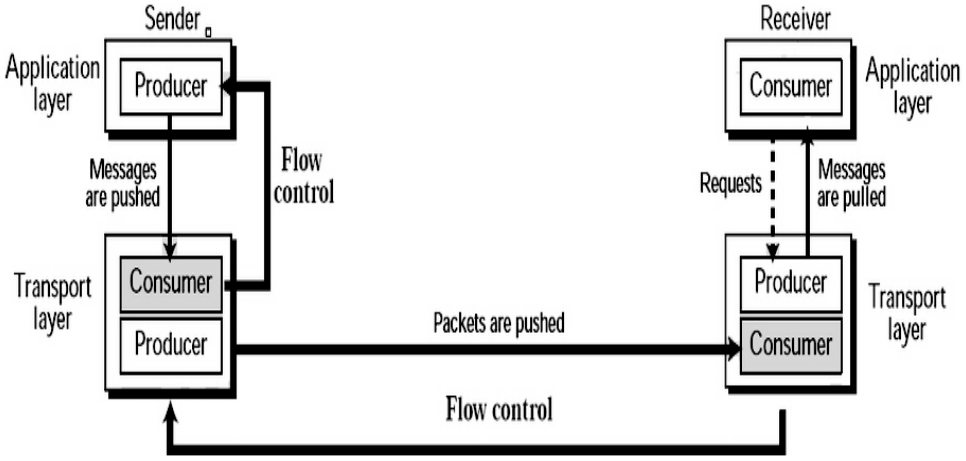


Figure 12.4: Flow control at the transport layer [1]

One of the solutions of flow control is generally to use two buffers: first one at the sending transport layer and the second at the receiving transport layer. A buffer is a collection of memory locations that can hold packets at the sender and receiver site. The flow control communication can happen by sending signals from the consumer to producer. If the buffer of the sending transport layer is full, then it notifies the application layer to stop passing messages. When there are some empty locations, it notifies the application layer that again it can pass messages. If the buffer of the receiving transport layer is full, then it notifies the sending transport layer to stop from sending packets. When there are some empty locations in the buffer, it notifies the sending transport layer that again it can send messages.

12.4 ERROR CONTROL [2]

As we know that network layer (IP) is unreliable and perform the communication based on best-effort policy. Therefore, transport layer takes care of error between host-to-host communications. Error control includes error detection and error recovery mechanisms. The responsibility of error control at the transport layer is to:

(i) Detect and discard corrupted packets.

(ii) Keep track of lost and discarded packets and resend them.

(iii) Recognize duplicate packets and discard them.

(iv) Buffer out-of-order packets until the missing packets arrive.

As we know that both layers Data Link layer and the Transport layer are responsible for Error control. Both layers follow the same principle for

controlling error(s). Immediate question(s) come(s) into mind that why do we need the error control at the both layers? Reason for the same is as follows:

- The data link layer implements error control on host-to-host basis.
- The transport layer implements error control on end-to-end basis. Following errors are being taken care by Transport layer:

Data change from 1 to 0 or 0 to 1, Packets loss, disordered of packets because of queue delay, misroute of packets etc.

Error control in TCP is achieved through the use of checksum, acknowledgment, and time-out.

Checksum: As shown in Figure 12.13, sender calculates the checksum for each segment, which will be used by destination to check for a corrupted segment. Destination recalculates the checksum and compare with the value of checksum field. If both are same then segment is not corrupted otherwise segment is corrupted and hence this segment will be discarded by destination. Such discard is not notified by the destination to source. If source does not receive any acknowledge for the respective segment then it assumes that there may be either loss or packet drop because of error in the segment.

Acknowledgment: To confirm the receipt of data segments, TCP uses acknowledgments. A control segment which carries no data but consume a sequence number are also acknowledged. ACK segments should not be acknowledged. TCP uses another type of acknowledgment called cumulative acknowledgment. In cumulative acknowledgment, the next expected byte is advertised by the receiver, ignoring all segments already received and stored out of order. This is also referred to as ACK or positive cumulative acknowledgment. The word “positive” specifies that no feedback is needed for duplicate, discarded, or lost segments.

Retransmission: Retransmission of segments is the heart of the error control mechanism. When a segment is sent, it has to be stored in a queue until and unless it is acknowledged. A segment is retransmitted if the retransmission timer expires or else the sender receives three duplicate ACKs for the first transmitted segment in the queue.

Retransmission after RTO: For each connection, the sending TCP maintains one retransmission time-out (RTO). When times out occurs, then TCP resends the segment and restarts the timer. In TCP, RTO is dynamic and is updated based on the round-trip time (RTT) of segments. RTT is the time required for a segment to reach a destination and to receive the acknowledgment.

In the following case, it is assumed that the segment has been lost and therefore, a TCP sender retransmits a segment.

(i) Timeout occurs and no ACK has been received.

(ii) For the same segment multiple ACKs have been received.

Generating Acknowledgment:

1. When one end sends a data segment. It must piggyback an acknowledgment to reduce the number of segments needed.
2. Sending an ACK is delayed by the receiver:
   - **(i)** If the receiver has no data to send.
   - **(ii)** If it receives an in-order segment.
   - **(iii)** If the previous segment has already been acknowledged.
   - **(iv)** Until another segment arrives or
   - **(v)** Until a period of time, normally 500 ms, has passed.
3. The receiver immediately sends an ACK when:
   - **(i)** An in-order segment arrives.
   - **(ii)** The previous in-order segment has not been acknowledged.
   - **(iii)** An out-of-order segment having higher sequence number is received.
4. When a missing segment arrives, the receiver sends an ACK.
5. The receiver immediately sends an ACK if a duplicate segment arrives.

Some scenarios occur during the operation of TCP: The Figure 12.5 depicts the scenario of the lost segment.

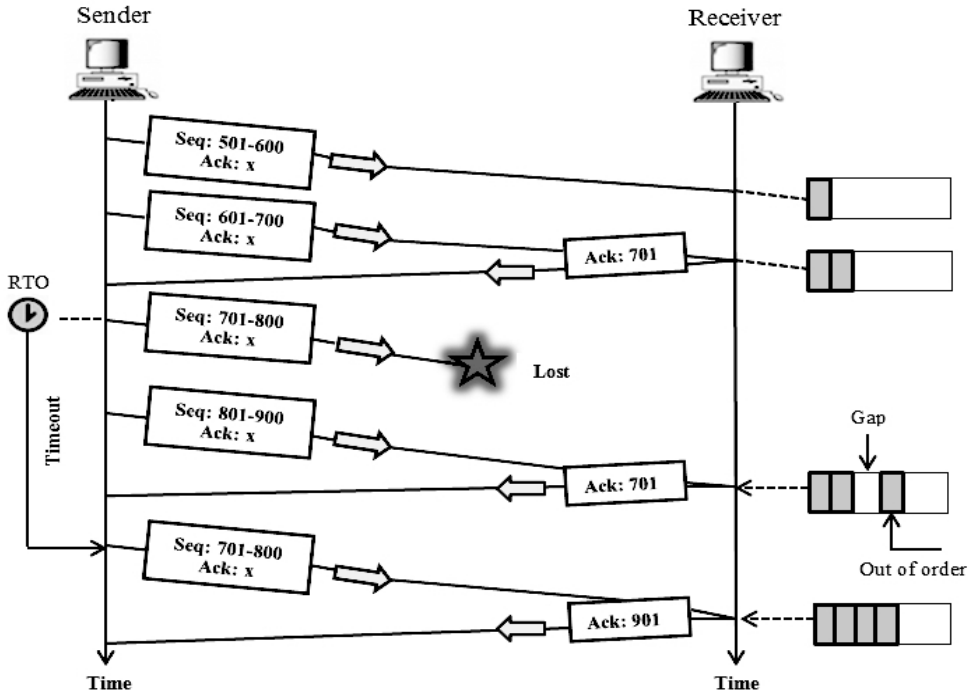


Figure 12.5: Lost segment [2]

Lost or Corrupted Segment: TCP receiver treats both the lost or corrupted segment in the same way. The lost segment is discarded somewhere in the network by router/switch, whereas corrupted segment is discarded by the receiver itself. From Figure 12.5, suppose if segment 3 is lost and receiver receives an out-of-order segment (segment 4). Store it temporary and leave a gap. Send an ACK immediately (ACK number = 701). When the RTO timer matures sender resent segment 3.

Fast Retransmission: As shown in Figure 12.6, when the receiver receives the 4th, 5th, 6th segment, it generates an acknowledgment. Therefore, all the four acknowledgments are same and last three are duplicates. Although the RTO timer for segment 3 has not yet matured but it will invoke fast retransmit for segment 3.

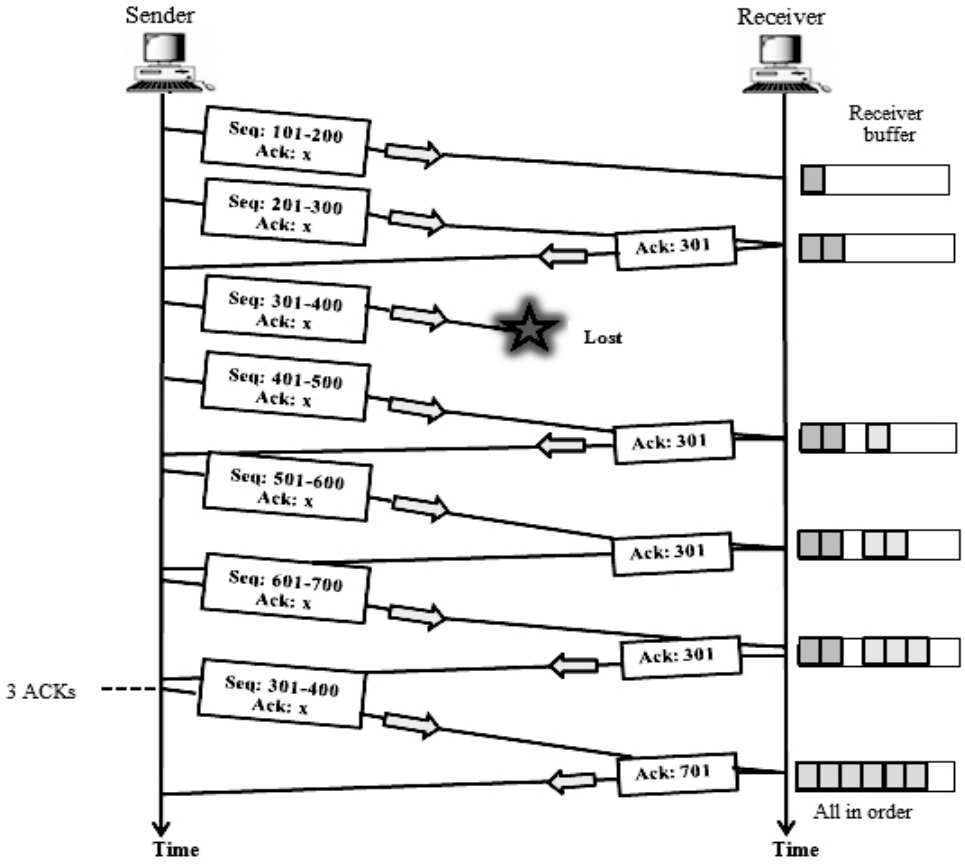


Figure 12.6:Fast retransmission[2]

Duplicate Segment: TCP creates duplicate segment when a segment is delayed and treated as lost by the receiver. If sequence number of a segment that arrives is equal to an already received and stored segment, then it is discarded. In that case an ACK is sent with acknowledgment number of the expected segment.

Lost ACK: Since in TCP acknowledgment mechanism, the source TCP is not even able to notice a lost acknowledgment. This problem is easily sorted out as TCP uses cumulative acknowledgment system; therefore the

next acknowledgment automatically corrects the loss of the acknowledgment. This scenario is depicted by the following Figure 12.7 shown below.

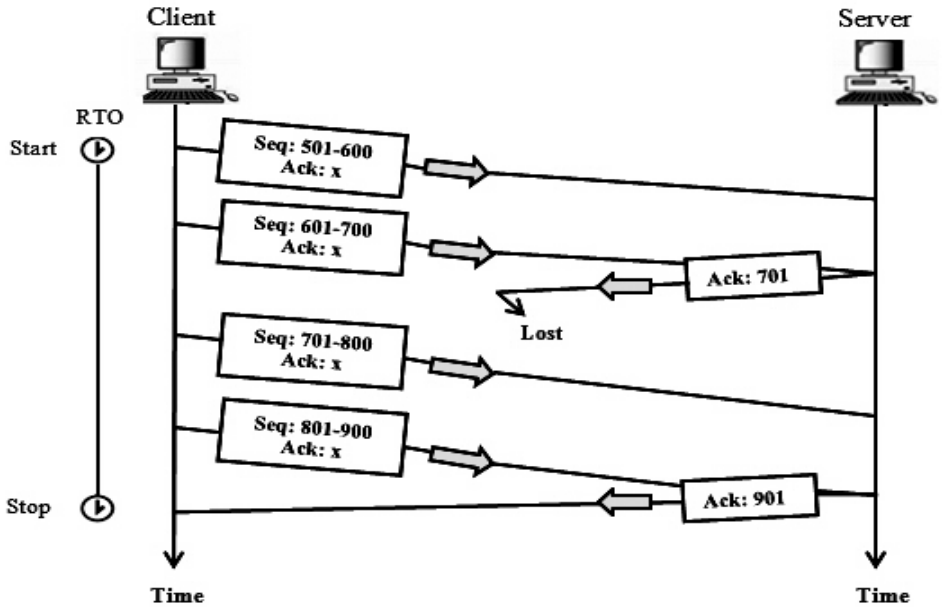


Figure 12.7: Automatically corrected lost acknowledgment [2]

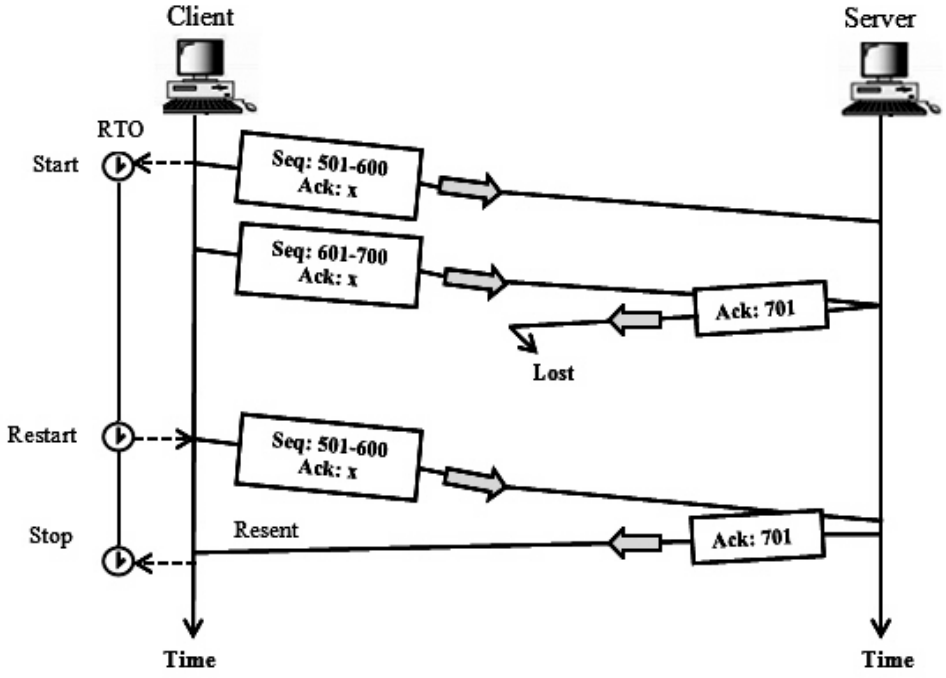


Figure 12.8: Lost nowledgment corrected by resending a segment [2]

However as shown in Figure 12.8, if there is no next acknowledge mentor the next acknowledgment is delayed for a long time, then the correction is triggered by the RTO timer. Now a duplicate segment has to be resent. Now if the receiver receives a duplicate segment, it discards it, and then resends the last ACK immediately to notify the sender that the segment or segments have been received. When the sender receives the retransmitted ACK, the sender recognizes that both segments have been received correctly since the acknowledgment is cumulative.

CHECK YOUR PROGRESS

1. Describe the transport layer services.
2. How do we achieve error control?
3. How do we achieve flow control?

12.5 TCP CONGESTION CONTROL ALGORITHMS [3]

Whenever, the number of packets sent to the network is greater than the number of packets a network can handle, that is, if the load exceeds the capacity of the network then network gets congested. Congestion can occur in a network devises like routers and switches. Routers/switches have input and out queues, buffers to hold the packets. The queues are finite in terms of memory space. Packets are kept in buffers to find out the rout for this packet. In such case, input flow in the queue may be much larger that output flow from the queue. This situation occurs whenever packets are being generated in the network is too high. There are two ways of congestion control.

1. Open-Loop Congestion Control

In this case, policies are applied to prevent congestion before it happens. Here, congestion control is handled by either the source or the destination.

Retransmission Policy: Retransmission is needed if the sender feels that a sent packet is lost or corrupted. Retransmission may in general, increase congestion in the network. However, a good retransmission policy is useful in preventing the congestion. Therefore, retransmission policy and the retransmission timers must be designed to time prevent congestion and to optimize efficiency.

Window Policy: The type of window at the sender also affects congestion. We can easily perceive that the Selective Repeat window is better than the Go- Back-N window for congestion control.

Acknowledgment Policy: Congestion is also affected by the acknowledgment policy imposed by the receiver. Numerous approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent to the sender or a

special timer expires. A receiver may choose to acknowledge only *N* packets at a time. We should consider that the acknowledgments are also part of the load in a network. Therefore, fewer acknowledgments will cause less loads on the network.

2. Closed-Loop Congestion Control

These mechanisms try to alleviate congestion after it happens. So many mechanisms have been used by different protocols. The size of the window at the sender can be flexible. The congestion in the Internet could be used to determine the sender window size. By monitoring the congestion in the Internet, for example, watching the lost packets, strategy can be devised to decrease the window size if the congestion is increasing and vice versa.

TCP is self-regulating: Sender enforces congestion control whereas receiver enforces flow control.

Types of windows:

rws = receiver window size (flow control)

cws = congestion window size (congestion control)

Effective window size: wnd = min (rws, cws)

Receiver doesn't know cws, it only knows that the actual window size is no larger than rws.

Actually TCP may be implemented by using four algorithms:

1. Slow start
2. Congestion avoidance
3. Fast retransmit
4. Fast recovery

Slow start: The sender transmits one segment and waits for its ACK. If that ACK is received, the congestion window is incremented from one to two. Now the sender sends two segments and the congestion window is increased to four, when each of those two segments is acknowledged. This causes an exponential growth, although it is not exactly exponential, as the receiver may delay its ACKs, typically sends one ACK for every two segments that it receives. Figure 12.9 shows the working of TCP slow start algorithm.

Slow start algorithm adds another window to the sender's TCP known as the congestion window (cws). The congestion window is used for controlling the flow imposed by the sender, whereas the advertised window is also used for controlling flow imposed by the receiver. Size of the congestion window is calculated sender based on network congestion

condition whereas the advertised window is calculated based on the amount of available buffer space at the receiver.

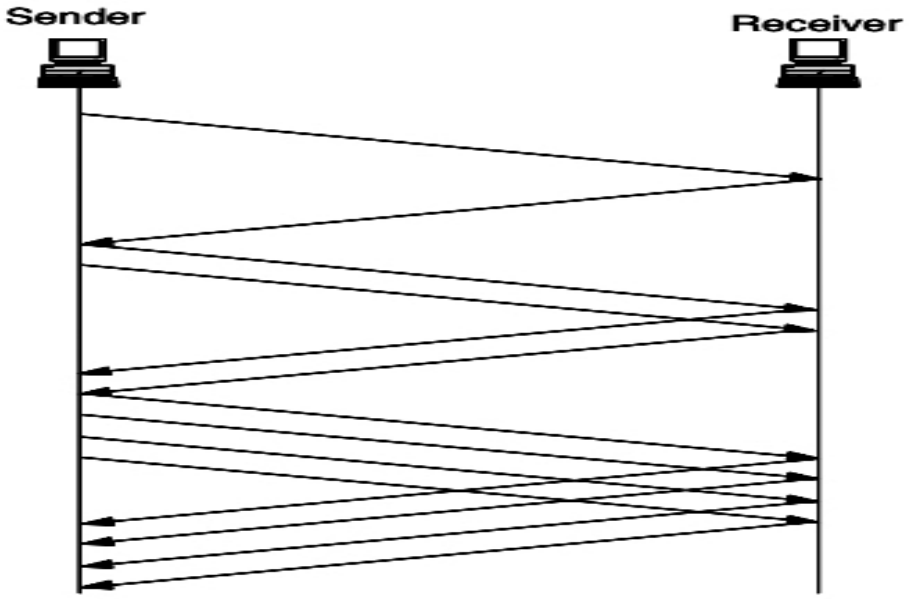


Figure 12.9: TCP slow start [3]

Congestion avoidance: One of the major reasons for packet loss is congestion between source and destination. Packet loss may be indicated by either timeout or duplicate ACKs.

Whenever congestion occurs, the transmission rate of packets into the network must slow down, and invoke slow start again. In practice, they are implemented together. Slow start and congestion avoidance require are implemented by using two variables namely, (1) a congestion window size, cws. And (2) a slow start threshold size, ssthresh.

Working of the combined algorithm is as follows:

1. For a given connection, initialize cws to one segment and ssthresh to 65535 bytes.
2. The sender never sends more than the lower value of cws or the receiver's advertised window.
3. If congestion occurs (timeout or duplicate ACK), then the current window size is reduced to half of ssthresh. If the congestion is indicated by a timeout, then cws is set to one.
4. When data is acknowledged by the other end, then increase cws. If cws is less than or equal to ssthresh, TCP is in slow start; otherwise, TCP is performing congestion avoidance.

Slow start will continue till TCP is halfway to where congestion occurred (that is up to step 3), and then congestion avoidance takes over. Slow start causes cws to begin at one, and incremented by one every time an ACK is received.

Fast retransmission: Fast retransmit, avoids the TCP to wait for a timeout to resend lost segments. In this case, when an out-of-order segment is received, the TCP may generate an immediate acknowledgment (a duplicate ACK) to indicate that destination has received segment which is out-of-order with expected sequence number.

Since there is no way for TCP to know whether a duplicate ACK is caused by a lost segment or just a reordering of segments, it waits for a small number of duplicate ACKs to be received. If there is just a reordering of the segments, then before the reordered segments are processed, it is assumed that there could be only one or two duplicate ACKs. When three or more duplicate ACKs are received in a row, it suggests that a segment has been lost. And then TCP retransmit the missing segment, without waiting for a retransmission timer to expire. Figure 12.10 shows the TCP fast retransmit algorithm.

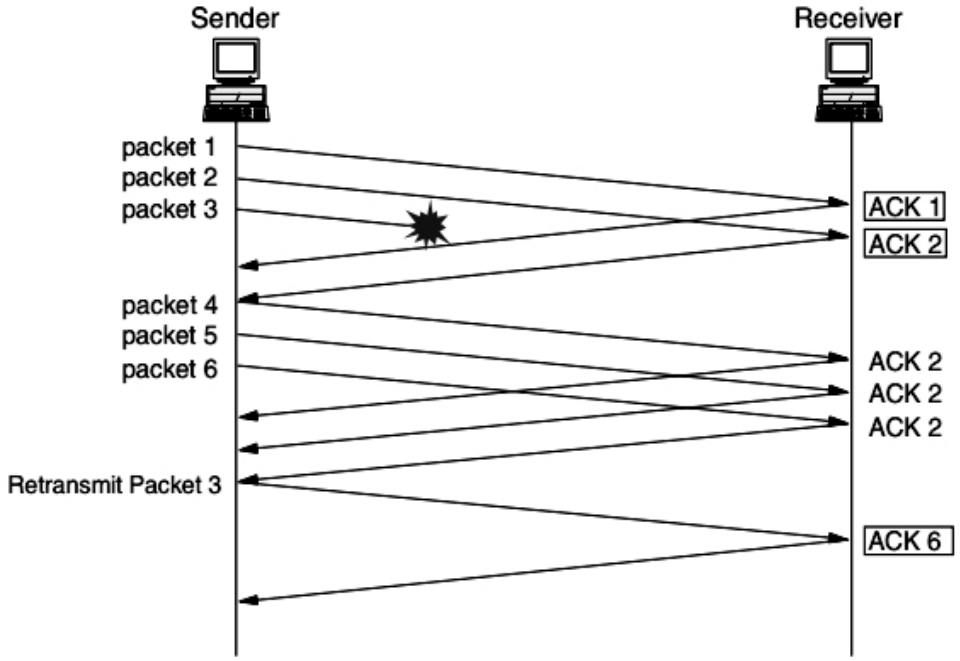


Figure 12.10: TCP fast retransmit [3]

12.6 CONNECTION ESTABLISHMENT AND TERMINATION [5]

In his section we will learn how the TCP connection is established and teardown.

TCP connection establishment: TCP uses three way handshaking protocols for establishing connection. For establishing a

TCP connection, the sender and receiver must “handshake” before exchanging data. This involves two steps:

1. Agree to establish connection (each knowing the other willing to establish connection).
2. Agree on connection parameters (here the parameter is sequence number).

TCP uses three way handshake strategies to establish the connection. This technique is often referred to as "SYN-SYN-ACK" or more accurately SYN, SYN-ACK, ACK because three messages has to be transmitted by TCP to negotiate and start a TCP session between two computers.

The server must first bind to and listen at a port to open it up for connections and only after that the client can attempts to connect with a server: this is called a passive open**.** After the passive open is established, a client may initiate an active open. Three way handshake steps are as follows:

1. **SYN:** Client performs the active open by sending a SYN to the server and sets the segment's sequence number to a random value J.
2. **SYN-ACK:** Server replies with a SYN-ACK in response. The acknowledgment number is set to one more than the received sequence number i.e. J+1, and the server chooses another random number ‘K’ as sequence number for the packet.
3. **ACK:** Lastly, the client sends an ACK back to the server. The sequence number is set to ‘J+1’ which is same as the received acknowledgement number and the acknowledgement number is set to‘K+1’which is one more than the received sequence number.

Above process is a full-duplex communication as both the client and server have received an acknowledgment of the connection. The steps 1, and step 2 establish the sequence number for one direction and it is acknowledged. The steps 2 and step 3 establish the sequence number for the other direction.

Sequence of events for establishing connection: The following are the sequence of events for establishing a connection.

- Host A sends a TCP SYN packet to Host B.
- Host B receives A’s SYN.
- Host B sends an ACK of SYN.
- Host A receives B’s ACK of SYN.
- Host A sends ACK.
- Host B receives ACK.
- TCP connection is established.

Figure 12.11 shows the steps in the connection establishment process.

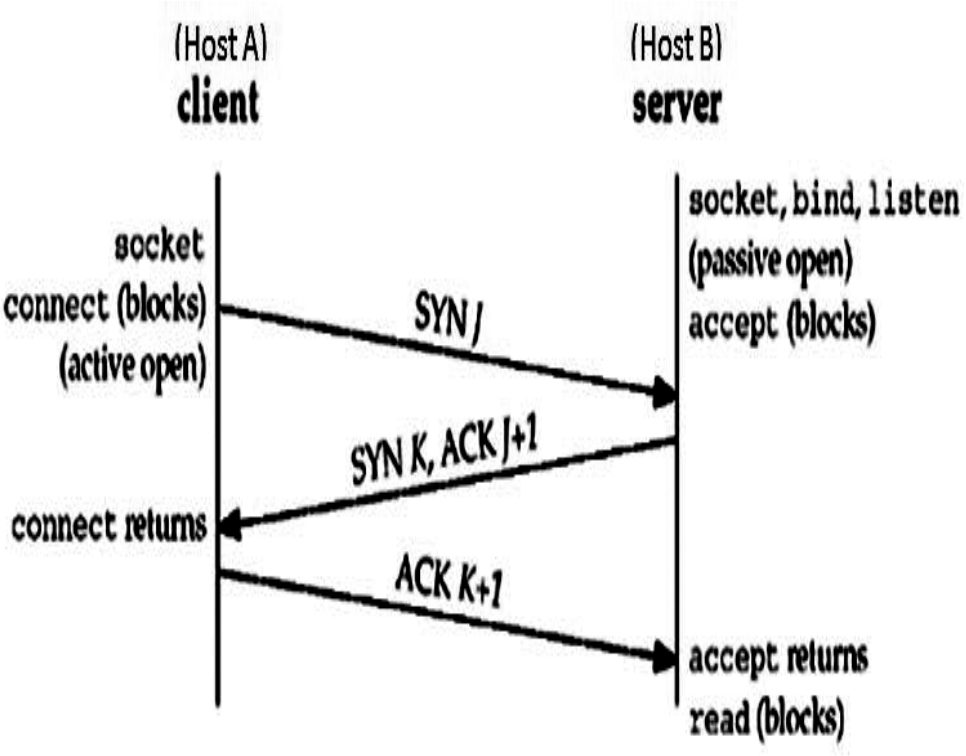


Figure 12.11: Connection establishment process [4]

SYN (synchronize) and ACK (acknowledge) messages are identified by flag bit in TCP header.

TCP connection termination: For connection termination, four-way handshake is used where each side of the connection may be terminating independently. If source or destination wants to terminates the half of the connection. If source (or destination) transmit a FIN packet to the destination (or source), then destination (or source) acknowledges with an ACK. And hence half connection is closed. So tear-down requires a pair of FIN and ACK segments from each TCP endpoint. In such case there is half-open connection. Now, terminated side will not be able send any data to other side, however the other side can. But terminating side will continue to read the data until and unless the other side terminates as well.

The side which sent the first FIN also responds with the final ACK. After sending the first FIN and responding with the final ACK, the sender side has to wait for a timeout before finally closing the connection, during that time the local port is unavailable for new connections; this prevents confusion due to delayed packets being delivered during subsequent connections.

We can also terminate the connection using 3-way handshake, when host A sends a FIN and host B replies with a FIN & ACK (merely combines 2 steps into one) and host A replies with an ACK. Figure 12.12 below depicts the four-way handshake connection termination process.

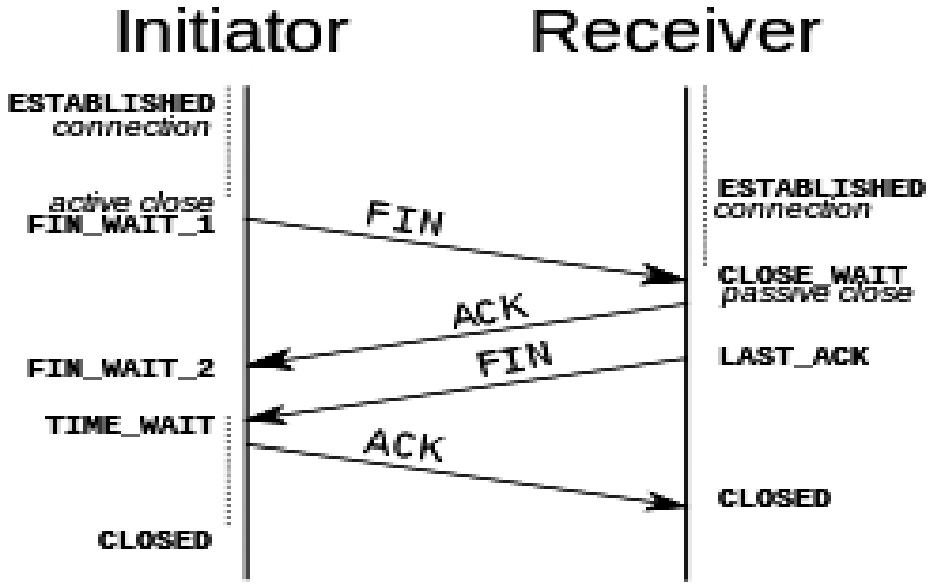


Figure 12.12: Connection termination process [5]

12.7 TCP SERVICE MODEL [2]

The basic purpose of TCP is to provide reliable logical circuit or connection service between pairs of processes. As we know, transport layer lies between the application layer and network layer, therefore it has to provide services to the application layer and receive services from the network layer. TCP provides the following facilities for the applications using it.

1. **Process-to-Process Communication**: A process is a running program in the application layer that uses the services of the transport layer. Process-to-process communication is most commonly achieved through client server paradigm. A process on the local host, called a client, generally need services from a process on the remote host called a client. As we know, the IP addresses define the local host and the remote host whereas port number defines the processes. The client program defines itself with short lived port number, because of the usually short life of the client. TCP/IP uses universal port numbers (also called well-known port numbers) for servers.
2. **Connectionless and Connection-Oriented Services**: In a connectionless service, the sender process, i.e. running program in the application layer, is required to divide its messages into chunks of data and send them to the transport layer one by one. When a chunk arrives from the application layer, the transport layer

encapsulates it in a packet and sends it. Therefore, the chunks may arrive out of order at the receiver process and also some of the chunks may be lost. And finally the server process gets a strange message, because it is out of order or the server process gets incomplete message with some chunks lost. These problems arise because there is no coordination between the two transport layers. Hence no error control, flow control, or congestion control can be effectively employed in a connectionless service. In a connection-oriented service, the client and the server first required to establish a connection between them. They can exchange data only after the connection establishment. After the data exchange, the connection is required to be teardown. The error control, flow control, or congestion control can be implemented in connection oriented service.

3. **Multiplexing and Demultiplexing**: Multiplexing (many to one) happens when an entity receives items from more than one source. Demultiplexing (one to many) happens when an entity has to deliver items to more than one source. Multiplexing is performed by the transport layer at the source and demultiplexing is performed by the transport layer at the destination. Let us understand the following scenario of multiplexing: Suppose three client processes P1, P2, and P3 are running at the client site. The processes P1 and P2 are required to send requests to the corresponding server process running in a server. The client process P3 is required to send a request to the corresponding server process running at another server. At the client site, the transport layer takes three messages from the three processes and produces three packets. Transport layer acts as a multiplexer. To reach the transport layer of the first server, packets 1 and 2 uses the same logical channel and when arrives at the server, the transport layer does the job of a demultiplexer and distributes the messages to two different processes. Similarly, the transport layer at the second server receives packet 3 and delivers it to the corresponding process.

4. **Error Control**: The error control service to the transport layer is used to achieve the reliability. The error control at the transport layer does the following.
   - **(i)** To keep track of lost and discarded packets and resend them.
   - **(ii)** To detect and discard corrupted packets.
   - **(iii)** To recognize duplicate packets and discard them.
   - **(iv)** To buffer out-of-order packets until the missing packets arrive.

Error control involves only the sending and receiving transport layers. However the receiving transport layer is more involved in managing error

control, as it informs the sending transport layer about the problems most of the times. As only sending transport layer knows which packet is to be resent and a duplicate packet or out of order packets is known only to the receiving transport layer. Therefore in order to distinguish the one packet from the other, the error control requires numbering of packets. Numbering is done by adding a field to the transport layer packet to hold the sequence number of the packets. So, when a packet is lost or corrupted, the receiving transport layer informs the sending transport layer to resend that packet using the sequence number. Also, in case of duplicate packets, the two or more received packets have the same sequence number. Similarly the out-of-order packets are recognized by observing gaps in the sequence numbers because the packets are numbered sequentially.

Both positive and negative signals could be used for error control. The receiver sends an acknowledgement (ACK) for each or a collection of packets that have arrived correctly and can simply discard the corrupted packets. The sender detects the lost packets by using a timer. After sending the packets, the sender starts the timer. If an ACK does not arrive before the timer expires then the sender assumes that the packet is lost and resends the packet. The receiver silently discards the duplicate packets. Out-of-order packets is either discarded (which is treated as lost packets by the sender), or stored until the arrival of missing ones.

12.8 TCP PROTOCOL [2]

The various TCP protocol is already discussed in the previous sections: these are

12.2 Transport layer connection management,

12.3 Flow Control,

12.4 Error Control,

12.5 TCP Congestion Control Algorithms and

12.6 Connection Establishment and Termination.

TCP Header Segment: The TCP protocol header segment is described in the Figure 12.13 shown below.

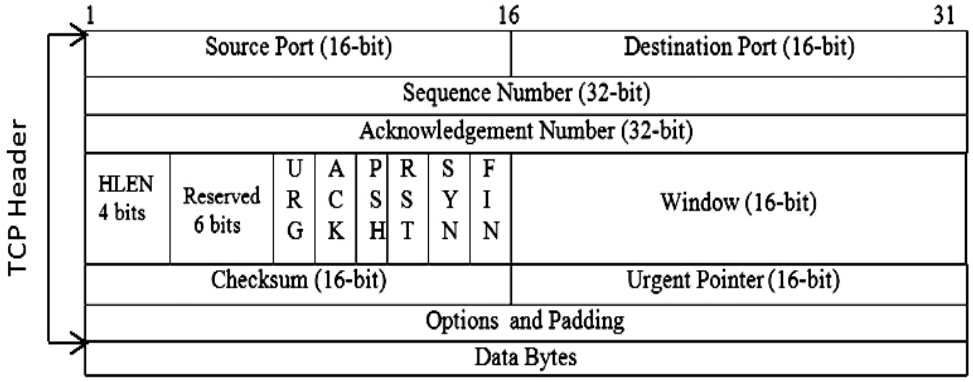


Figure 12.13: TCP-Header segment [6]

Source Port: The 16-bit source port number of application program in the host that is sending the segment. It is used by the receiver to reply.

Destination Port: The port number (16-bit) of the application program in the host that is receiving the segment.

Sequence Number: It is the sequence number (32-bit) of the first byte in data segment. This will help to identify the duplicate packets.

Acknowledgment Number: This not only indicates receiving of packet but also what next expecting packet with sequence number is. If the receiver of the segment has successfully received byte number *N* from the sender, it returns *N*+1 as the acknowledgment number.

Header length (HLEN): It is 4-byte words to indicate only length of header excluding length of data.

Reserved: Six bits reserved for future use. All the bits are set zero.

URG: Urgent pointer is valid

ACK: Specifies that the acknowledgment field is significant in this segment.

PSH: Push function.

RST: Resets the connection.

SYN: Used to synchronize the sequence numbers.

FIN: Terminate the connection.

Window: Specifies the window size of the sending TCP in bytes. As the length of this field is 16 bits, therefore the maximum size of the window is 65,535 bytes. It is usually referred to as the receiving window (*rws*) and hence determined by the receiver.

Checksum: The 16-bit one's complement of the one's complement sum of all 16-bit words in a pseudo-header, the TCP header, and the TCP data. While computing the checksum, the checksum field itself is considered zero. The format of pseudo-header is shown in Figure 12.14 below as already described in the network layer. Pseudo-header is added to the TCP segment at the network layer.

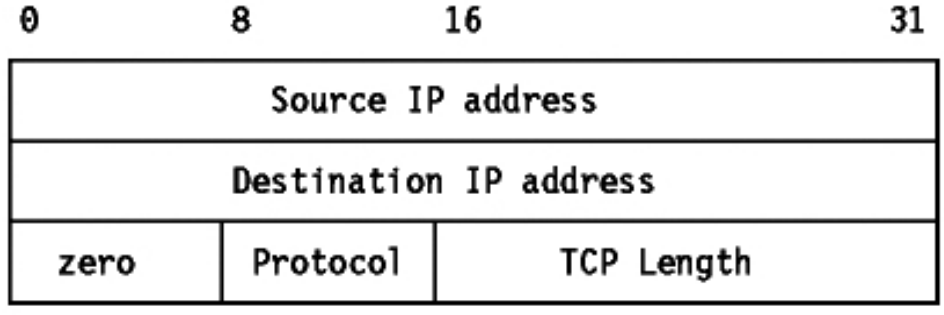


Figure 12.14: Pseudo-header [6]

Urgent pointer: 16-bit field. It is used when the segment contains urgent data.

Options &Padding: TCP header may contain up to 40 bytes of optional information. Padding is added to make the data a multiple of 16 bits.

CHECK YOUR PROGRESS

1. How congestion can be avoided at transport layer?
2. What is the maximum size of the TCP header? What is the minimum size of the TCP header?
3. What is the purpose of TCP push operation?

12.9 SUMMARY

The first duty of a transport-layer protocol is to support a process-to-process communication**.** The combination of an IP address and a port number is called a socket address and is used to achieve process-to-process communication. Whenever an object creates items and another object consumes them, the production and consumption between them should be balance and this is achieved by flow control mechanism. The objective of an error control mechanism is to provide a reliable transfer of data units between systems. Error control includes error detection and error recovery mechanisms. Congestion in a network may occur when the number of packets sent to the network is greater than the number of packets a network can handle, that is, if the load exceeds the capacity of the network. There are two ways of congestion control; open loop congestion control and closed loop congestion control. TCP service model provides process-to-process communication, connection management, multiplexing and demultiplexing, flow and error control mechanism.

12.10 TERMINAL QUESTIONS

1. Explain the TCP header format.
2. Describe the congestion control mechanism.
3. How do we establish and teardown the TCP connection? Explain.
4. What do you mean by open loop congestion control and closed loop congestion control in transport layer?
5. Write down the difference between connection less service and connection oriented Service?
6. How deadlock is created by lost acknowledgment in TCP error control mechanism.
7. What is the purpose of the sequence number in a TCP packet?

8. TCP uses a cumulative acknowledgement system. How does it help TCP in dealing with lost acknowledgements?

REFERENCES

[1] Behrouz A. Forouzan,Chapter 13, "TCP/IP protocol suite (4th ed.)".

[2] Behrouz A. Forouzan,Chapter 15, "TCP/IP protocol suite (4th ed.)".

[3] http://mykeepit.blogspot.in/2012/10/explain-various-steps-in-tcp-congestion.html

[4] http://www.masterraghu.com/subjects/np/introduction/unix_network_programming_v1.3/ch02lev1sec6.html

[5] https://en.wikipedia.org/wiki/Transmission_Control_Protocol

[6] http://networkengineering.stackexchange.com/questions/6396/how-can-a-tcp-socket-be-identified-by-ip-address

UNIT-13 SESSION AND PRESENTATION LAYER

Structure

13.0 INTRODUCTION

In today's world it is very tough to secure information during electronic communication because anyone can listen to the channel and can find some pattern to understand what is being communicated. In this unit, the reader shall learn the cryptographic methods to overcome insecure e-communication and some basic idea about data compression.

The rest of the unit is organized as follows. Section 13.1 lists the objectives of the unit. Section 13.2 gives an introduction of cryptography. Section 13.3 discusses various data compression techniques. Section 13.4 explains the session layer and its functions. Section 13.5 provides an overview of the unit and section 13.6 closes the unit with some terminal questions for students to work out.

13.1 OBJECTIVE

After reading this unit, the reader should be able to:

- Understand the need of cryptography.
- Learn basics of symmetric and asymmetric cryptosystem.
- Learn basics of data compression.

13.2 INTRODUCTION TO CRYPTOGRAPHY

Before understanding the Cryptography and data compression, we need to understand the functions of Presentation Layer.

The main goal of Presentation layer is to handle the syntax and semantics of the message exchanged between two communicating hosts. This layer also ensures that the receiver understand the message and should able to use the data. The presentation layer plays a role of a translator, because the languages of the two communicating systems may be different. Some important tasks of this layer are the following.

1. Translation: Information expressed as characters and numbers needs to be changed to bit streams before transmission. Since different hosts may use different encoding methods, therefore it is the responsibility of this layer to provide interoperability.

2. Encryption: This layer performs encryption at the sender side and decryption at the receiver side.

3. Compression: Data compression is done to reduce the number of bits to be transmitted.

The Figure 13.1 below shows the direction of the data flow among the different layers at the sender and the receiver side.

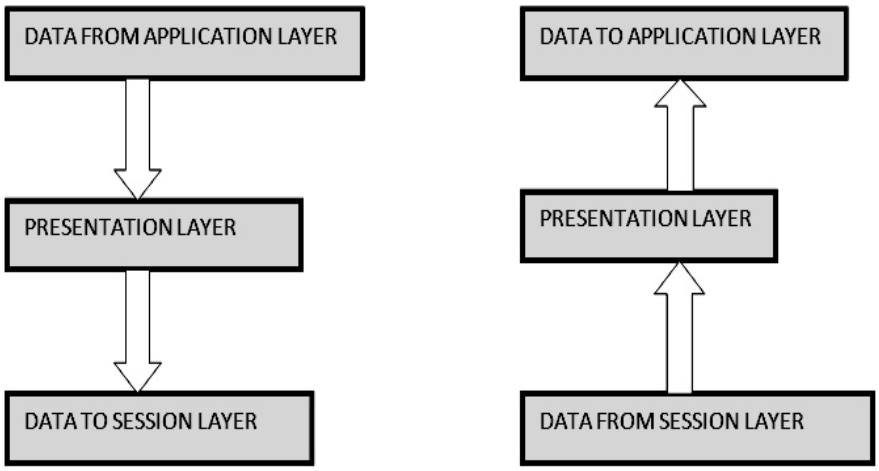


Figure 13.1: Data flow among layers at the sender and receiver side [1]

In today's age, the information can be treated as an asset. The information could be so crucial that you may not want this to be revealed. So your goal is to store the information securely. To secure the information you need to, hide it from unauthorized access (*called Confidentiality*), protect it from unauthorized change (*called Integrity*), and make it available to authorized people when it is required (*called Availability*). But due the revolution in computer network, you can send/retrieve the information from a long distance using computer networks. Therefore, there should also be some technique to maintain its confidentiality when it is transmitted from one computer to another.

Cryptography refers to a technique of transforming information into a secure form while it is being transmitted or stored so that unauthorized users can get no information from the intercepted data.

The interesting fact about modern cryptographic system is that the technique of encryption (and decryption) is standardized and is known to every people. Therefore, there must be some secret information that should prevent the attacker form decrypting the message. This secret information is the key.

There are two types of cryptographic system.

(i) Symmetric key systems

(ii) Asymmetric Key (or Public key systems)

In symmetric key systems, identical keys are used and are secret. In public key systems, a pair of keys is used. One of the keys is known to both the sender and the receiver and is not secret that is known to everybody. The other key is known only to the sender or the receiver.

Symmetric Key Cryptosystem [2]

The general idea behind a symmetric-key cipher has been shown in Figure 13.2. Here, to create the cipher text form the plaintext, Alice has to use an encryption algorithm and a secret key. The key is secret and shared between the Alice and Bob. Bob uses a decryption algorithm and the same secret key to create the plaintext from cipher text.

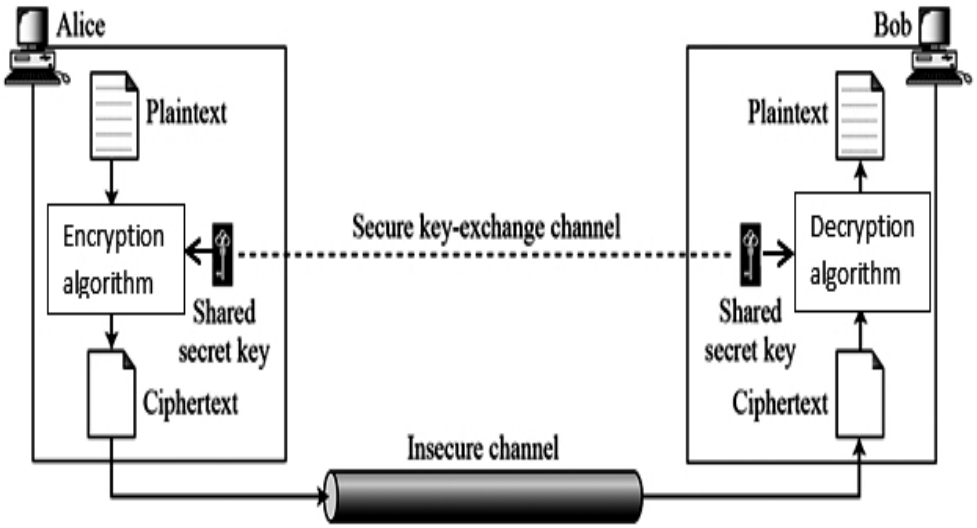


Figure 13.2: General idea of symmetric-key cipher [2]

Plaintext is the original message; **cipher text** is the original message in other form that is sent through the channel.

If P is the plaintext, C is the cipher text, and K is the key,

Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

We assume that Bob creates P_1; we prove that $P_1 = P$

Alice: $C = E_k(P)$

Bob: $P_1 = D_k(C) = D_k(E_k(P)) = P$

Kerckhoff's principle[2]**:** It is always assumed that the attacker knows the encryption/decryption algorithm. Therefore, only the secrecy of the key provides the resistance to attack.

Substitution ciphers [2]**:** Substitution ciphers replace one symbol with another and can be classified into two types: monoalphabetic ciphers or polyalphabetic ciphers.

If, for one symbol in the plaintext there can be only one symbol in the cipher text, that is the relation between the symbol in the plaintext to a symbol in the cipher text is one-to-one, then such ciphers are called monoalphabetic ciphers.

For the plaintext "hello"as shown below the cipher text is "KHOOR" as shown below. This cipher is monoalphabetic because both *l*'s (els) are substituted as *O*'s.

Plaintext: hello Ciphertext: KHOOR

However, in the following example the plaintext is "hello" and the ciphertext is "KHOPR". This cipher is not monoalphabetic because each *l* (el) is substituted by a different character.

Plaintext: hello Ciphertext: KHOPR

Features of symmetric key encryption are [5]**:**

- The common key is required to be shared between the communicating parties before the transmission of the message.
- The key has to be changed regularly to prevent attack.
- There should be a robust mechanism to exchange the key between the communicating parties as the keys have to be changed frequently. Therefore, this mechanism is costly and burdensome.
- The number of keys required for a group of **n** people is **n × (n – 1)/2**.
- Because of the smaller length of the key in symmetric key encryption, it is speedier than asymmetric key encryption.

Issues of Symmetric Key Cryptosystem [5]

The following are the issues in symmetric key cryptography.

- **Key establishment:** Both the sender and the receiver should decide upon a symmetric key that is secret prior to the communication.
- **Trust Issue:** There should be trust factor between the sender and the receiver. It is so because the secret key that is shared between

them may be lost to an attacker without the sender knowing about it.

Today, information is frequently exchanged between non-trusted entities. This situation may arise when a customer is communicating with an online vendor. These problems with symmetric key encryption make it vulnerable. Therefore, asymmetric key encryption is a better choice in such scenarios.

Public Key or Asymmetric Key Cryptosystem [5]

Public key encryption or Asymmetric key encryption uses two different keys – one for encryption and the other for decryption. Even if the keys are different, they are mathematically correlated. Therefore, the retrieval of plaintext from ciphertext seems practical.

Features of this encryption scheme are as follows [5]**:**

- Each user in this system requires having a pair of dissimilar keys, private key and public key. When one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- Public key is placed in public repository and the private key is secret.
- Although public and private keys are related, but it is not computationally easy to find one from another.
- Due to large length of keys (number of bits) in this encryption, the process of encryption-decryption is slower than symmetric key encryption.
- To run asymmetric algorithm, the required processing power of computer system is higher.

Issues of Public Key Cryptosystem [5]

One significant challenge of public key cryptosystems is that, the user has to trust that the public key that he/she is using in communications with a legitimate person and has not been spoofed by an attacker. Public Key Infrastructure (PKI) is being used in such case.PKI uses a trusted third party. The third party securely manages and attests to the authenticity of public keys. When requested to provide the public key, the third party is trusted to provide the correct public key for any communicating person X.

The third party uses the process of attestation to satisfy itself about user identity, notarization, or some other process - that X is the one and only, or globally unique, X.

CHECK YOUR PROGRESS

1. Explain symmetric and asymmetric key cryptosystem.

2. Explain the significance of cryptography.

3.3 DATA COMPRESSION [3]

Data compression is presentation layer functionality in OSI reference model. It causes the reduction in the number of bits contained in the multimedia data. This is done to maximize the use of bandwidth across a network or to optimize disk space when storing data. There are two main types of data compression algorithms. There are two types of compression as shown in Figure 13.3.

1. Lossless compression
2. Lossy compression

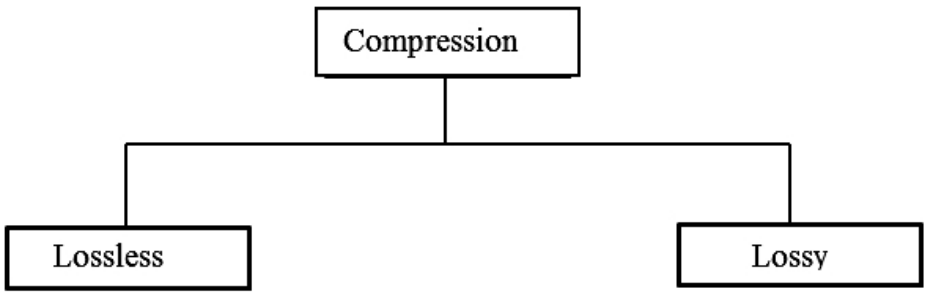


Figure 13.3: Types of compression [3]

1. Lossless Compression

This technique compresses the data without loss of data. It is used to compress data like text files, executable code, and numeric data, since programs that process such data cannot tolerate mistakes in the data.

But in contrast to Lossless compression does not compress data as much as lossy compression techniques and generally takes more processing power for compression.

Lossless Compression Algorithms

The following algorithms are used for lossless data compression.

(i) Run length encoding (RLE)

(ii) Differential pulse code modulation

(iii) Dictionary based encoding

(i) Run length encoding (RLE)

- **RLE** replaces the consecutive occurrences of a given symbol with only one copy of the symbol along with a count of how many times that symbol occurs. Therefore the names ‘run length'.
- For example, the string AAABBBBCDDD would be encoded as 3A4BIC3D.
- Fax machine **uses RLE** encoding. Most faxes are white sheets with the fewer black text. Therefore, it takes each line and transmits a

code for white then the number of pixels, then the code for black and the number of pixels and so on.

- If the data does not have lot of repetition then it is possible the run length encoding scheme would actually increase the size of a file. Therefore, this method of compression must be used very carefully.

(ii) Differential pulse code modulation

- In this method, we first place a reference symbol. Then for every symbol in the data, we place the difference between that symbol and the reference symbol used.
- For example, if A is used as a reference symbol, the string AABBCDDD would be encoded as AOOl12333. B has a difference of 1 from the reference symbol A and so on.

(iii) Dictionary based encoding

- Lempel-Ziv (LZ) compression algorithm is best known dictionary based encoding algorithms. It is also known as substitution coder.
- First, this scheme builds a dictionary (table) of variable length strings (common phrases) that are expected to occur in data.
- If any of these strings occur in the data, then they will be replaced with the corresponding index to the dictionary.
- Here, instead of working with individual characters in text data, each word is treated as a string and output the index in the dictionary for that word.
- For example, let us assume that the word "information" has the index 3905 in one particular dictionary. During compression, the word information will be replaced by 3905 wherever it appears in the data.

2. Lossy Compression

Lossy compression compresses the data with loss of some information. After compression there is no way to retrieve the data which was removed during compression. And hence generally this technique is used compress images, audio and video. These algorithms achieve much improved compression ratios than the lossless algorithms.

Audio Compression

It is used for speech or music. For speech, 64 KHz digitized signal has to be compressed; for music, 1.411 MHz signal has to be compressed.

Techniques used for audio compression are:

1. Predictive encoding
2. Perceptual encoding

Figure 13.4 shows the two Audio compression techniques.

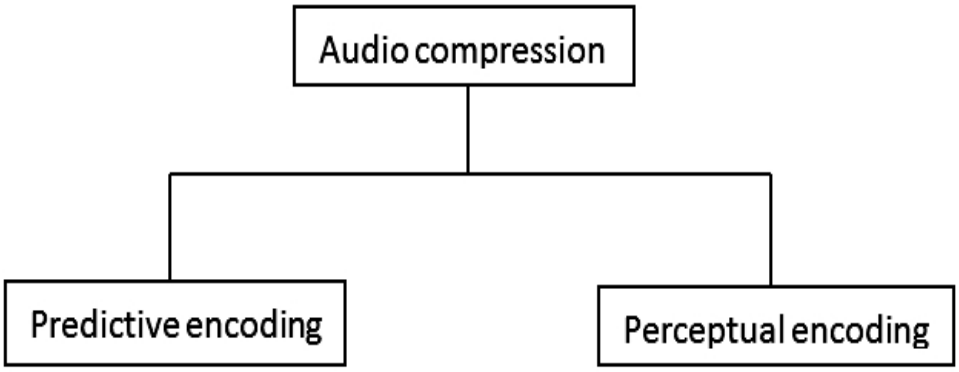


Figure 13.4: Techniques of audio compression [3]

1. Predictive encoding

- In predictive encoding, the differences between the samples are encoded rather than encoding all the sampled values.
- This is normally used for compression of speech.
- There are many standards like GSM (13 kbps), G.723.3 (6.4 or 5.3 kbps) and G. 729 (8 kbps).

2. Perceptual encoding

- This scheme is used to create a CD-quality audio which requires a transmission bandwidth of 1.411 Mbps.
- Perceptual encoding is used by MP3 (a part of MPEG standard).
- It is based on the science of psychoacoustics (a study of how people perceive sound).
- Exploits certain flaws in the human auditory system for encoding a signal in such a way that it sounds the same to a human listener despite of it look quite different on an oscilloscope.
- The most important property of this coding scheme is that some sounds can mask other sound. For example, suppose you are broadcasting a live sitar concert and suddenly some unpleasant sound start like hammering on metal that generates more vibration and heavy sound. Then you would not be able to hear the sitar because the sound has been masked by the heavy sound generated by hammer.
- The above technique is known as frequency masking. In such masking sound (may be louder) in one frequency band hides a sound (soft) in another frequency band.
- Time can also be used for masking. For example: the sitar will be not be audible for some period of time even if the hammering is over because temporal masking in which the ears turn down its gain when they start and take a finite time to turn up again.

MP3

- The above two phenomena is used byMP3, *i.e.* frequency masking and temporal masking to compress audio signals.
- In this system, the technique analyses and divides the spectrum into many groups.
- Zero bits are assigned to the frequency ranges that are totally masked whereas small number of bits is allocated to the frequency ranges that are partially masked and larger number of bits is allocated to the frequency ranges that are not masked.
- MP3 produces three data rates 96kbps, 128 kbps and 160 kbps based on the range of frequencies in the original analog audio.

13.4 SESSION LAYER [4]

Its main aim is to establish, maintain and synchronize the interaction between communicating systems. Session layer manages and synchronize the conversation between two different applications. Transfer of data from one destination to another session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided. Function of the session layer is depicted below in Figure 13.5.

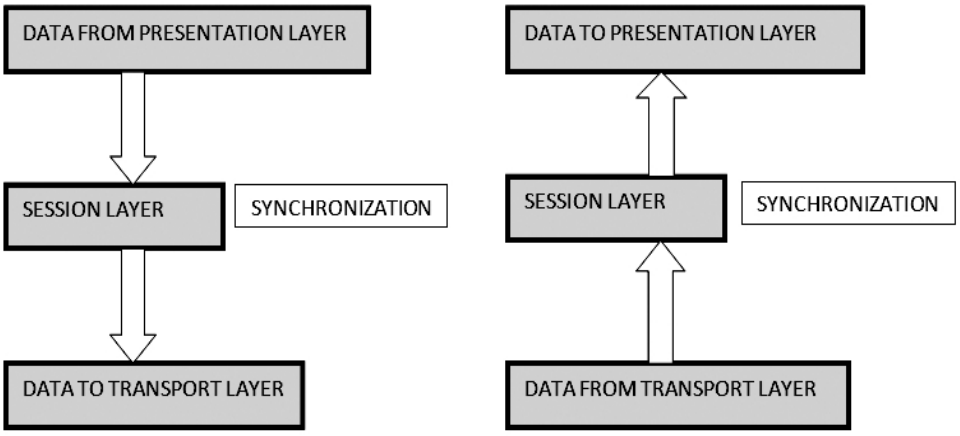


Figure 13.5: Function of session layer [4]

Main Functions of Session Layer are given below:

1. Dialog Control: This layer allows two systems to start communication with each other either in half-duplex or full-duplex.

2. Synchronization: This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints

after every 50 pages is recommended. This ensures that 50 page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.

CHECK YOUR PROGRESS

1. What is the need of data compression?
2. What is Run Length Encoding? For the string AAABBBCDDDDE what would be the compressed output?
3. Explain the functions of session layer in brief.

13.5 SUMMARY

To secure the information you need to, hide it from unauthorized access (*called Confidentiality*), protect it from unauthorized change (*called Integrity*), and make it available to authorized people when it is required (*called Availability*). Cryptography is a technique to secure the information from unauthorized access while it is being stored or transmitted. There are two types of cryptography; symmetric and asymmetric. There are two main types of data compression algorithms; lossless and lossy compression. For lossless data compression the algorithms are run length encoding, differential pulse code modulation and dictionary based encoding. Lossy compressions are used to compress images, audio and video. Techniques used for audio compression are predictive encoding and perceptual encoding.

13.6 TERMINAL QUESTIONS

1. Explain the functions of session layer in brief.

2. Explain the functions of presentation layer in brief.

3. What is Cryptography? Why it is important?

4. Explain symmetric and asymetric key cryptosystem?

5. Explain the significance of cryptography.

6. What is the need of data compression?

7. What are the different data compression techniques?

8. Explain lossless compression algorithms.

9. Explain lossy compression algorithms.

10. Define the following terms in relation to Cryptography:

(i) Plain text

(ii) Cipher text

(iii) Encryption

(iv) Decryption

(v) Key

11. What is Run Length Encoding? For the string AAABBBCDDDDE what would be the compressed output?

12. Differentiate between Predictive encoding and Perceptual encoding techniques in Audio compression.

REFERENCES

[1] http://www.studytonight.com/computer-networks/osi-model-presentation-layer

[2] Behrouz A. Forouzan, Chapter 3, "Cryptography and Network security".

[3] http://ecomputernotes.com/computer-graphics/basic-of-computer-graphics/data-compression

[4] http://www.studytonight.com/computer-networks/osi-model-session-layer

[5] http://www.tutorialspoint.com/cryptography/cryptosystems.htm

UNIT-14 THE APPLICATION LAYER

Structure

14.0 INTRODUCTION

In this unit, after a brief introduction of network security, the concepts of domain name system and E-mail has been discussed in detail.

The rest of the unit is organized as follows. Section 14.1 enlists the objectives of the unit. Section 14.2 discusses the aspects of network security. Section 14.3 explains DNS and its functions. Section 14.4 describes electronic mail and its working procedure. Section 14.5 captures the summary of the unit and section 14.6 marks the end of the unit with a few terminal questions for students.

14.1 OBJECTIVE

After reading this unit, the reader should be able to:

- Understand network security and the security services for E-mail.
- Learn DNS naming tree, operations, name resolution and message formats.
- Learn E-mail architecture, Message formats, Message transfer process.
- Learn about message transfer agent (MTA), message access agent (MAA).

14.2 NETWORK SECURITY [1]

Network security can be understood with the help of following example.

Suppose two people Alice and Bob wants to communicate "securely". Basic requirements for their communication are:

1. Alice has sent a message to the Bob, and she wants that only Bob should understand the message. However, as the communication is taking place over an insecure medium; therefore an attacker may intercept the message being transmitted from Alice to Bob.
2. Bob received a message from Alice. Now Bob wants to make sure that "is it the same message that was sent by Alice". Also Alice wants to make sure that "is she communicating with Bob or someone else".
3. Both Alice and Bob want to make sure that there is no modification or alteration in the contents of their messages.
4. They also want the assurance, that whenever they are required to communicate, they should be able to do so. That is no one should be able to deny them the access to the resources needed to communicate.

Therefore the desirable properties of secure communication are:

1. **Confidentiality:** Only authorized parties are able to access the data.
2. **Authenticity:** The identity of a user should be verified by a host or service.
3. **Integrity:** Only authorized parties should be able to modify the data.
4. **Availability:** The data should always be available to authorized parties.

Intruder may want to get unauthorized access to information during transmission. This is known as attack. There are two types of security attacks, namely (i) Passive attack and (ii) Active attack.

Passive Attacks: This attack is also referred to as eavesdropping. This attack attempts to learn or make use of information from the system without disturbing the system resources. The aim of the attacker is to get the information that is being transmitted. Examples of passive attack are Release of message contents, Traffic analysis etc.

Release of message contents: A telephone conversation, an electronic mail message, or a transmitted file may contain sensitive or confidential information. We have to prevent an attacker to learn the contents of these transmissions.

Traffic analysis: Traffic analysis is a special type of inference attack technique that looks at communication patterns between entities in a system. Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. In this If we mask the information traffic or the contents of messages so that even if the attacker captured the message, could not extract the

information from the message. Encryption is the common technique for masking contents. Even if the traffic or message is encrypted, an attacker may still be able to detect the pattern of these messages. The attacker could determine the location and identity of communicating hosts and could detect the frequency and length of messages being exchanged. This information might be useful to guess the nature of the communication that was taking place. These attacks are very difficult to detect because they do not involve any alteration/modification of the data. Hence there is no way to understand that somebody observed and learnt the traffic or messages. Therefore this attack can only be prevented.

Active Attacks: Involve some modification in the data or the creation of a false data. Examples of active attack are: **masquerade, modification of messages, replay, and denial of service etc.**

In a masquerade attack, the attacker achieves some unauthorized privileges by pretending to be a genuine user or entity. This is done by the use of stolen passwords or login IDs, to find security holes in programs or they may bypass the authentication mechanism.

Replay is a security attack in which information is stored and then retransmitted to produce unauthorized effect such as false identification or authentication. For example, messages from a user who is logging into a network can be captured by an attacker and resent (replayed) later on.

In a message modification attack, the attacker change the packet header addresses to send a packet to several destinations or can modify the data in a machine.

In a denial of service (DoS) attack, users are unable to access the network or web resource. This is done by creating very large traffic at the target machine.

For example, an attacker may send thousands of messages to a particular destination; this prevents the network access to the genuine user. The attacker can also disable the entire network or a server. This is done by deactivating the network server or by overloading it with messages.

One of the important goals of the network security is to secure data against attacks while it is being transmitted on a network. To achieve this goal, several security protocols have been designed. All such protocols need to provide the following primary objectives.

- To authenticate each other, the parties can negotiate interactively.
- To create a secret session key before exchanging information on network.
- To encrypt the messages before sending it to the network.

E-Mail Security services: E-mail communication needs certain basic security services as the following.

Confidentiality: Only intended recipient should be able to read e-mail message.

Authentication: The identity of the e-mail sender should be verified by the recipient.

Integrity: To guarantee the recipient that the e-mail message is same as the one sent by the sender.

Non-repudiation: E-mail recipient should be able to prove to a third party that “this message is really sent by the sender”.

Proof of submission: E-mail sender must get the confirmation whether it has been delivered to the mail delivery system or not.

Proof of delivery: E-mail sender must get the confirmation whether the recipients have received the message or not.

14.3 DOMAIN NAME SYSTEM [2][3][4]

To identify a computer over the internet, TCP/IP protocol uses unique internet protocol (IP) address. But people always prefer name rather than numeric address. Therefore computer system requires a mapping technique from name to address or address to name.

Previously, a host file is used as a mapping technique. This has two columns: name and address. Every computer or host over the internet could store host file and updating it, after consulting with master host file. When a user has wrote a name to a host. The host consulted with the host file and finds the mapping. But the host file is too large to store in a computer or host and it is not possible to update all host file when there is a change.

One idea is to store entire host file in one computer and other hosts are allowed to access it for mapping. But these create huge amount of traffic on the internet.

Another idea, is used today is divide one piece of large host file into smaller parts and each part stores into different computer. When a host or computer needs mapping can interact with the closest computer holding the information. Domain name system (DNS) used same method.

The domain name system (DNS) is the networking system which resolves human-friendly names to unique is IP address. For example, "google.com" is a domain name. When we type "google.com" into our browsers, it is the domain name system that allows us to reach the Google servers.

Domain Name System (DNS) authorize us to use hierarchical names to easily identify computers and other resources on an internet protocol (IP) network. The Domain Name System provides a standard naming convention for finding IP-based computers.

There are two types of naming system that are used in DNS: Hierarchical and logical tree structure. It indicates the name syntax and rules for assigning authority over names and the implementation of computing system that logically map names to addresses.

DNS Syntax: Set of labels separated by delimiter character.

Example: in the URL (universal resource locator) *das.nitp.edu, nitp.edu* is also a domain and *edu* is top-level domain.

Top-Level Domain

A top-level domain (TLD), is the most common part of the domain. It is the rightmost part (as separated by a dot). For example, "com", "net", "org", "gov", "edu", and "io", as shown in Table 14.1 below.

Hosts

The owner of the domain can define individual hosts or resource, within a domain. The domain name owner generally allows web servers accessible through the exposed domain (webopedia.com) and by the "host" definition "www" (www.webopedia.com).

We could have ftp access by defining a host called "ftp" (ftp.webopedia.com). The host names can be arbitrary and they are unique for the domain.

Domain Name

Every node in a tree has a domain name. A complete domain name is a sequence of labels separated by dots (.). A domain name always read from the leave up to the root of the tree. Figure 14.1 shows some domain name.

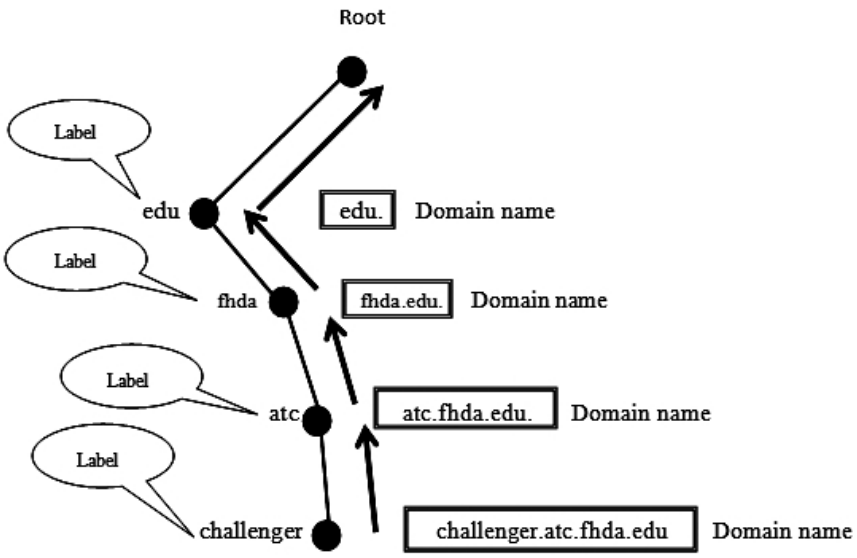


Figure 14.1: Domain names and labels [4]

Sub Domain: A "subdomain" is the part of a larger domain. E. g: "fhda.edu" is a subdomain of domain "edu". A domain can control "subdomains" that are located under it. A host specifies a computer or resource, whereas a subdomain expands the parent domain.

Fully qualified domain name (FQDN): Fully Qualified Domain Name starts from a node and it does reach the root, i.e. a full name of a host. It must be stated with a trailing dot. For example, www.yahoo.com., where www is the host, yahoo is the second-level domain, and the top level domain is .com.

Partially qualified domain name (PQDN): A partially qualified domain name can starts from any node and do not reaches to the DNS root. It can be simply a hostnames, i.e.

challenger or atc.fhda.edu, fhda.edu.

DNS database: In a name space tree each node and leaf has information (e.g., IP address, type of resource) that is stored in a resource record (RR).The collection of all resource records is organized into a database.

Name servers: Information of domain name space and the associated RRs must be stored among many computers called Name server. We have hierarchical name server shown in Figure 14.2. i.e., domains are divided into subdomains.

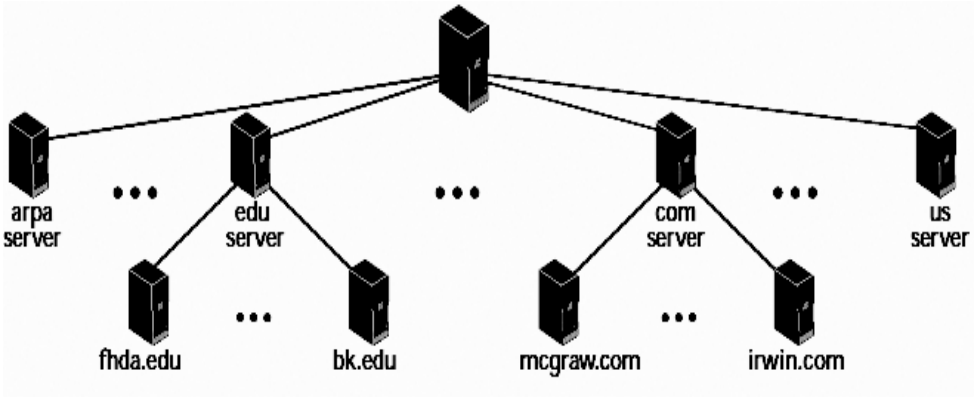


Figure 14.2: Hierarchy of name servers [4]

Resolvers: When a client requests for a name, resolver extract information from name servers. Basically these are the programs of DNS client that needs to map an address to a name or a name to an address by accessing closest DNS server with mapping request. When the DNS server does not satisfy the request, it refers the resolver to the other servers to provide the information.

Zones: Depending on the administration of the zone manager, a DNS zone consists of only one domain, or of many domains and sub-domains. Zone manager can create additional zone over any zone. Authority over the new zone is given to a designated name server.

Internet protocol (IP) address has two elements: a network number which identifies a network on the Internet, and a host or computer address, which identifies a unique host on a network. But IP address has two problems.

First, packet forwarding by the router into the network is done by using network number. The management of the tables becomes troublesome and time consuming, if each router wants to keep a master table that listed every network and the preferred path to that network. It is better to group

the networks in such a way that make the routing easier. Second, The 32-bit address pattern is effective for processing in computer but is not easily to remember for users.

The above mentioned problems are addressed by the concept of domain which is organized hierarchically. Figure 14.3 shows a portion of the domain naming tree.

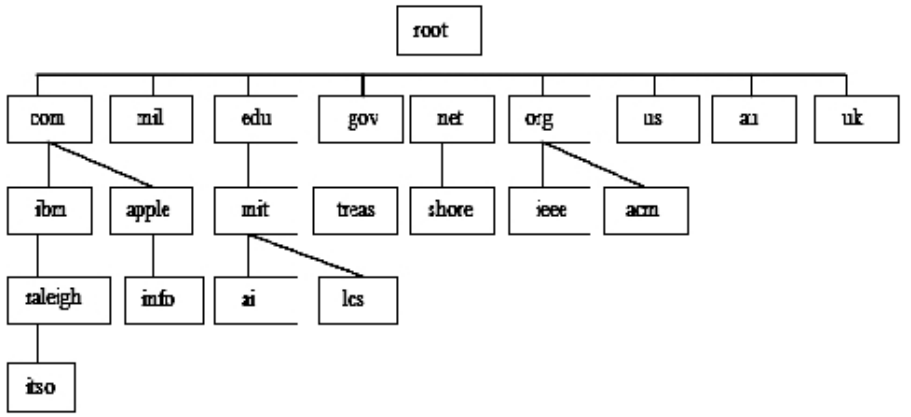


Figure 14.3: Domain naming tree [2]

Table 14.1: Top-level Internet domains [2]

Domain	Contents
com	Commercial organizations
edu	Educational institutions
gov	U.S. federal government agencies
mil	U.S. military
net	Network support centers, Internet service providers, and other network-related organizations
org	Nonprofit organizations
us	U.S. state and local government agencies, schools, libraries, and museums
Country code	ISO standard 2-letter identifier for country-specific domains (e.g., au, ca, uk)
biz	Dedicated exclusively for private businesses
info	Unrestricted use
name	Individuals, for email addresses and personalized domain names.
museum	restricted to museums, museum organizations, and individual members of the profession
coop	Member-owned cooperative organizations, such as credit unions
aero	Aviation community
pro	Medical, legal, and accounting

The DNS Database: Domain name system is based on a hierarchical database containing **resource records (RRs),** consisting the name, IP address, and other information about hosts. The various features of the database are as follows:

Variable depth hierarchy for names: There is no restriction of levels in DNS and it uses the period (.) as a level delimiter in names.

Distributed database: It is the DNS servers, where database resides, which is distributed throughout the Internet and private intranets. Private intranets area computer network with restricted access.

Distribution controlled by the database: Database of domain name system is divided into thousands of separately managed zones, which are managed by separate administrators. Software of the database controls the distribution and updating the records. This database is used by DNS servers to provide a name-to-address directory service for network applications and locate specific servers.

Figure 14.4 shows the structure of DNS Resource record.

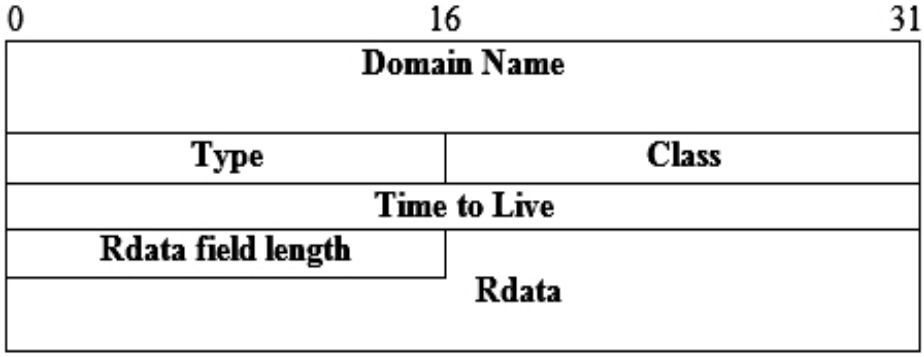


Figure 14.4: DNS Resource record form [2]

Resource Record (RR) consists of the following elements:

Domain Name: The domain name in a resource record must be in human readable form. It consists of a series of labels of alphanumeric characters or hyphens, with each pair of labels separated by a period.

Type: It indicates the type of resource in this resource record. The various types are listed in Table 14.2.

Class: It defines the family of a protocol. Most commonly used value is IN, for the Internet.

Time to Live: When a resource record is retrieved from a name server, the retriever caches the resource record to prevent repeated query to the name server. This field indicates the time interval for which the resource record is cached before the source of the information is again referred. A zero value indicates that the resource record can only be used for the operation in progress and should not be cached.

Rdata Field Length: It is the length of the Rdata field in octets.

Rdata: It is a variable-length string of octets and it describes the resource. According to the type of the resource record, the format varies. For example, for type A (Address), the Rdata is a 32-bit IP address is a 4-octet integer, and for the CNAME (Canonical name) type, the Rdata is a domain name.

Type	Description
A	A host addresses. This RR type maps the name of a system to its IP address. Some systems e.g., routers have multiple addresses, and there is separate RR for each.
CNAME	Canonical name. Specifies an alias name for a host and maps this to the canonical (true) name.
HINFO	Host information. Designates the processor and operating system used by the host.
MINFO	Mailbox or mail list information. Maps a mail box or mail list name to a host name.
MX	Mail exchange. Identifies the systems that relay mail into the organization.
NS	Authoritative name server for this domain.
PTR	Domain name pointer. Points to another part of the domain name space.
SOA	Start of a zone of authority (which part of name hierarchy is implemented). Includes parameter related to this zone.
SRV	For a given service provides name of server or servers in domain that provide that service.
TXT	Arbitrary text. Provides a way to add text comment to a database.
WKS	Well known services. May list the application services available at this host.

Table 14.2: Resource record types [2]

DNS Operation: Domain name system operation normally consists following steps.

1. One user program requests an internet protocol (IP) address for a domain name.
2. The resolver module in the local host composes a query for a local name server in the same domain.
3. First, the local name server searches the name in its local database or cache. If the name is found, then local name server returns the IP address to the user. Otherwise, the name server requests to other available name servers. This starts from the root of the DNS tree or as high up the tree as possible.
4. Having received the response at the local name server, it stores the name or address mapping in its local cache. And this entry is maintained for the specified amount of time, equal to the value given in the time to live field of the retrieved resource record.
5. The user program will be given the IP address or an error message.

Figure 14.5 shows how DNS translates domain names into IP addresses.

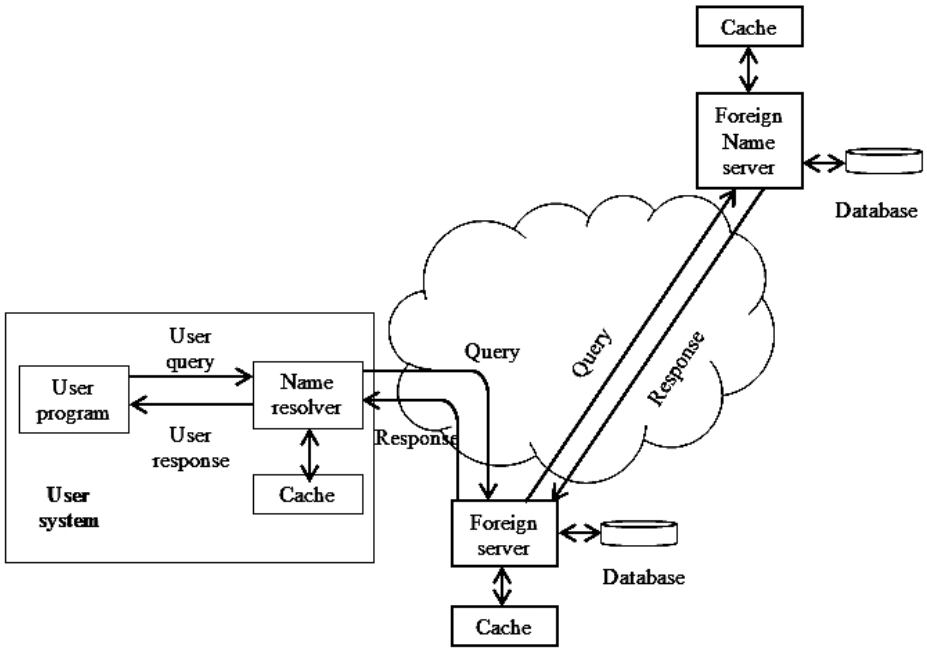


Figure 14.5: DNS operation [2]

Let us consider a query by a program on a user host for **amit.ibm.com**. This query is sent to the local server and the following steps occur:

1. The local server returns the IP address, if it has the IP address for **amit.ibm.com** in its local cache.
2. If the local name server's cache does not have the IP address, then it sends the query to a root server. The root server then forwards the request to a server with a name server record for **ibm.com**. If this server has the information for **amit.ibm.com**, then the IP address is returned by it.
3. If there is a name server just for **amit.ibm.com**, then the **ibm.com** name server forwards the request to the **amit.ibm.com** name server, which then returns the IP address.

Name Resolution: Queries for a group of names are passed over transmission control protocol (TCP), whereas single queries are passed over user datagram protocol (UDP).

Two methods are used to forward the query and return the result as described below.

Recursive Resolution: Here, the client (resolver) asks for a recursive answer from a name server. So, client expects from the server to give the absolute answer. If the server is the authority for the domain name, then it will look into its database and respond. If the server is not the authority for the domain name, then it will refer the request usually to the parent server and waits for a reply. Now, if the authority is parent, then it replies a response. And if parent is not the authority, then it forwards the query to yet another server and so on. Finally, query is resolved and the response travels back to reach the requesting client. Figure 14.6 shows the concept of recursive resolution.

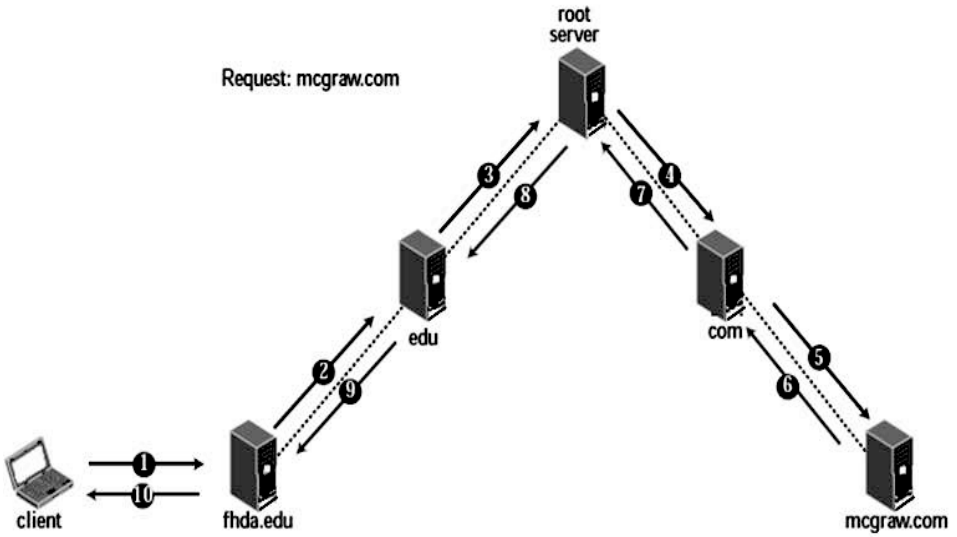


Figure 14.6: Recursive resolution [4]

Iterative Resolution: It is used when the client does not query for a recursive answer. Here, on requesting the root server for the name, the root server sends the answer If it is authority for the name, otherwise it sends the IP address of another server to the client that it considers resolve the query. Then the client repeats the query to this second server. If this server can resolve the query, then it will respond the query with the IP address. Otherwise, it will once again send the IP address of a new server. Now the client again repeats the same query to the third server. In iterative resolution, the client repeats the same query to multiple servers until it gets the result. As shown in Figure 14.7, the client queries five servers and finally it gets an answer from the mcgraw.com server.

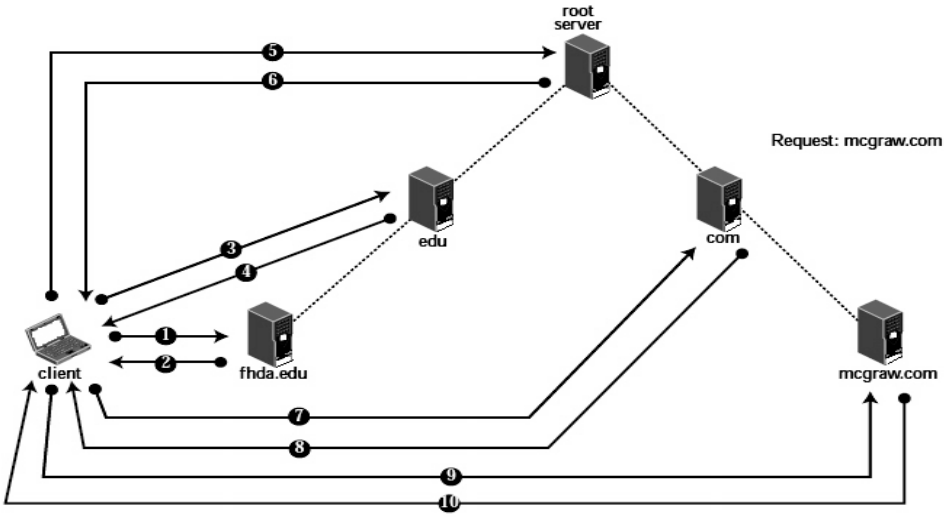


Figure 14.7: Iterative resolution [4]

DNS Messages: The domain name system messages format is shown in Figure 14.8 below. The different possible sections of the header are: header, question, answer, authority, and additional records. The various fields of the header section are as described below.

- Identifier: This is assigned by the program. For all response, same identifier is used and it enables the sender to match queries and responses.
- Query Response: Used to specify whether a message is a query or response.
- Opcode: Used to indicate the type of query. The query could be a standard query, an inverse query (address to name), or a server status request.
- Authoritative Answer: Valid in case of a response. This specifies whether the responding name server is an authority for the domain name.
- Truncated: The response message is truncated if its length is greater than permitted on the transmission channel. The requestor will use a transmission control protocol (TCP) connection to resend the query.
- Recursion Desired: Used to instruct the server to query recursively.
- Recursion Available: Used to denote whether recursive query support is available in the name server or not.
- Response Code: This field can take the following possible value: server failure, no error, name error (domain name does not exist), format error (server unable to interpret query),refused (for policy reasons), and not implemented (this type of query not supported).

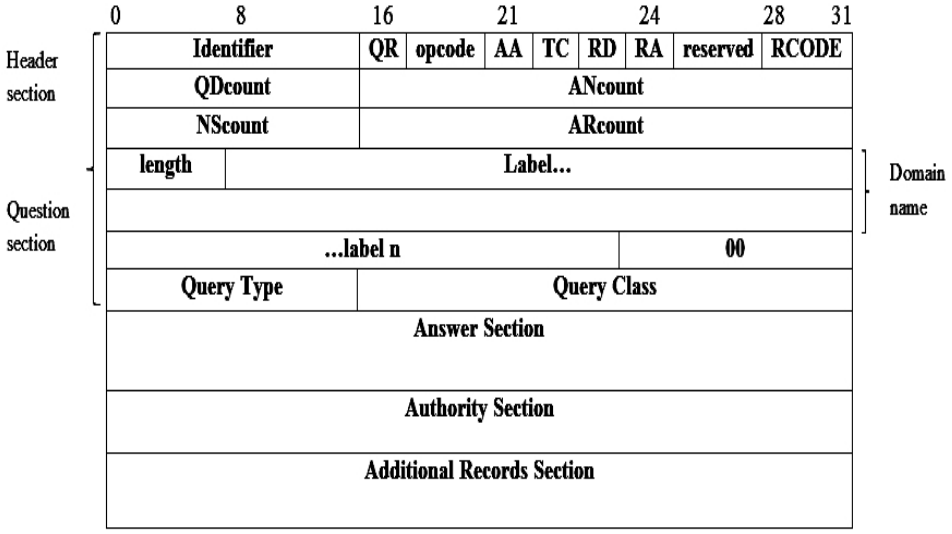


Figure 14.8: DNS message format [2]

QR - query/response bit

AA - authoritative answer

TC - truncated

RD - recursion desired

RA - recursion available

QDcount: Number of entries in question section (zero or more).

ANcount: Number of RRs in answer section (zero or more).

NScount: Number of RRs in authority section (zero or more).

ARcount: Number of RRs in additional records section (zero or more).

The question section contains only one entry. Each entry contains the following fields.

Domain Name: The domain name in a resource record must bein human readable form. It consists of a series of labels of alphanumeric characters or hyphens, with each pair of labels separated by a period.

Query Type: specifies the type of query. This field includes all values valid for the Type field in the resource record format (Figure 14.4).

Query Class: It indicates the class of query, typically Internet.

Answer Section: It contains resource records that answer the question.

Authority Section: It contains resource records that point toward an authoritative name server.

Additional Records Section: It consist resource records that relate to the query but are not strictly answers for the question.

CHECK YOUR PROGRESS

1. What do mean by DNS? Discuss the DNS operations.
2. Why do we need a DNS system when we can directly use an IP address?

14.4 ELECTRONIC MAIL [5][6]

There are many different email services available. Two most popular, free email services are Gmail and Yahoo Mail that allows you to create an email account, to send and receive email.

Nowadays, E-mail allows a message to include audio and video along with the text. Also you can send a message to one or more recipients.

The architecture of an e-mail system and its three main components: user agent, message transfer agent, and message access agent have been described below.

Architecture: Architecture of e-mail can be understood with the help of four scenarios.

1. In the first scenario, the sender and receiver of the Email users are directly connected to a shared system. The received messages are stored in a mailbox, which is created by the administrator for each user. A mailbox is a part of a local hard drive and a specific file with permission restrictions. Only the owner of the mailbox can access it. When Alice (a user) wants to send a message to Bob (another user). To prepare the message, Alice executes a user agent (UA) program and stores it in Bob's mailbox. The message contains the address of the sender and recipient mailbox. Now using a user agent at any time Bob can retrieve and read the contents of his mailbox. Figure 14.9 shows the concept.

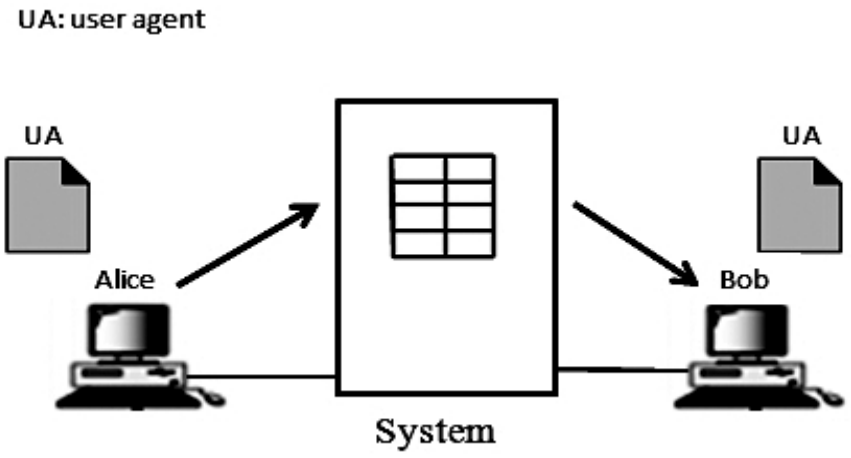


Figure 14.9: First scenario [5]

2. In the second scenario, the sender and the receiver of the e-mail users are on two different systems and the messages have to be sent over the Internet. Figure 14.10shows the concept. In this case we need user agents (UAs) and message transfer agents (MTAs) at both the site. Now, as shown in Figure 14.10, the message is to be sent from Alice's site to Bob's site through the Internet. Alice sends her message to a system at her own site by using a user agent program. The mail server at Alice's site has a queue (to store messages) and the MTA client. At the Bob's site there is also a user agent program (to retrieve messages) and MTA server. The messages are retrieved by the Bob from the mailbox at the Bob's site. Since, at any time the client can ask for a connection, the server is running all the time. On the other hand, when a message in the queue is to be sent, the system (mail server) will alert the client.

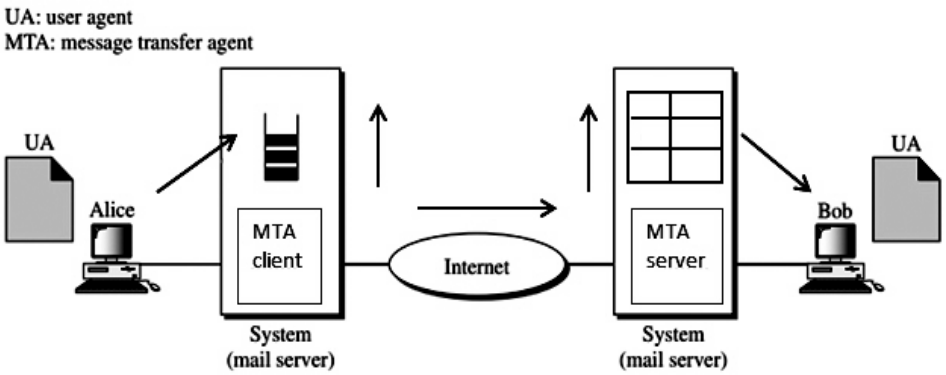


Figure 14.10: Second scenario [5]

3. In the third scenario, initially, Alice is detached from her system and she connects to the system via a point-to-point WAN, like as a cable modem or a dial-up modem, or through a LAN in an organization, which is one mail server to handle e-mails. However, Bob is connected directly to the system. Figure 14.11 shows this situation.

Alice, after preparing her message with the help of user agent sends the message through the LAN or WAN, by using a pair of message transfer agents, MTA client and MTA server. The user agent at the Alice's site calls the MTA client. This MTA client establishes a connection with the MTA server on the system, which runs all the time. All the messages sent by the Alice are stored in a queue at Alice's site system. To send the messages to the system at Bob's site, the Alice's site system uses an MTA client. The Bob's site system receives the message and stores it in Bob's mailbox. Now, Bob uses his user agent to retrieve the message and reads it. Here, it is important to note that we require two pairs of MTA client/server programs.

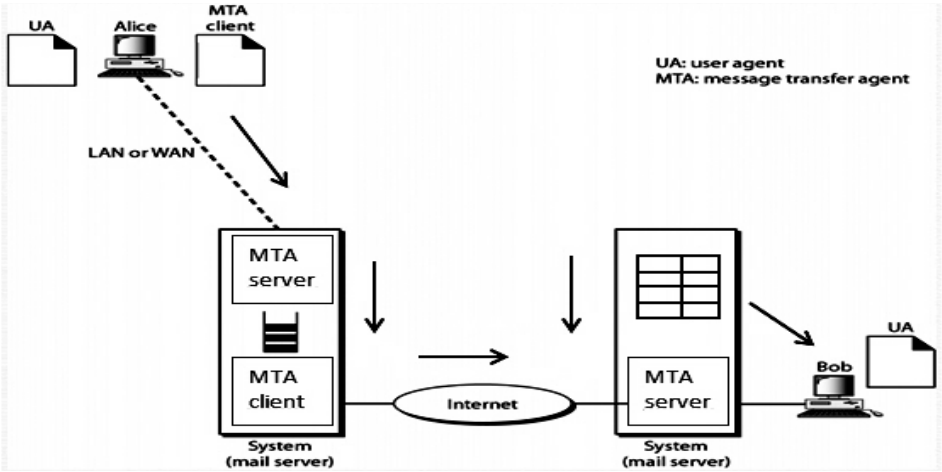


Figure 14.11: Third scenario [5]

4. The fourth one is the most common scenario, where Bob is always connected to his mail server by a LAN or a WAN. When a message has reached at Bob's mail server then Bob needs to download it. Here, we require another set of client/server agents, called message access agents (MAAs). Now Bob access an MAA client to see his messages. T is a client has sent a request to the MAA server (running all the time) and requests to transfer of the messages. The situation is shown in Figure 14.12. Here Bob's MTA server is running all the time at his site because at any time a message will arrive. Note that Bob requires another pair of client/server programs: message access programs. Because of an MTA client/server program is a push program, where the client pushes a message to the server. But Bob requires a pull program, where the client requires pulling the message from the server.

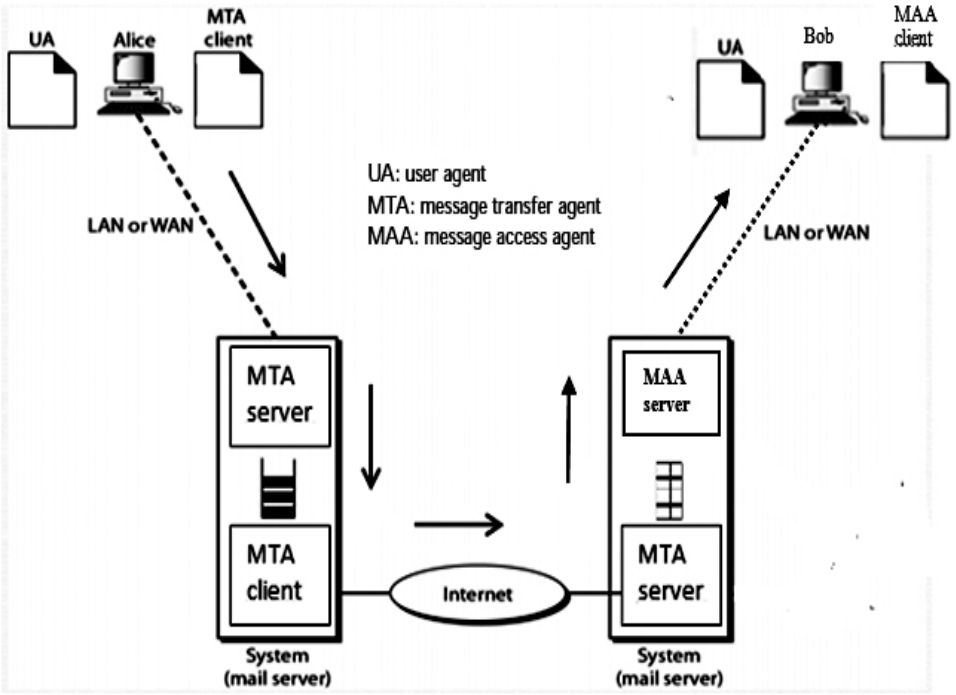


Figure 14.12: Fourth scenario [5]

User Agent: The various services provided by the user agent are: Composing messages, reading messages, replying to messages, forwarding messages and handling mailboxes. Figure 14.13shows the services of a user agent.

Composing Messages: t includes creation of template on the screen, which is to be filled by the user. There is a built-in editor for grammar checking, spell checking and other tasks. The user can also use word processor or text editor of his/her choice to create the message and can be imported into the user agent template.

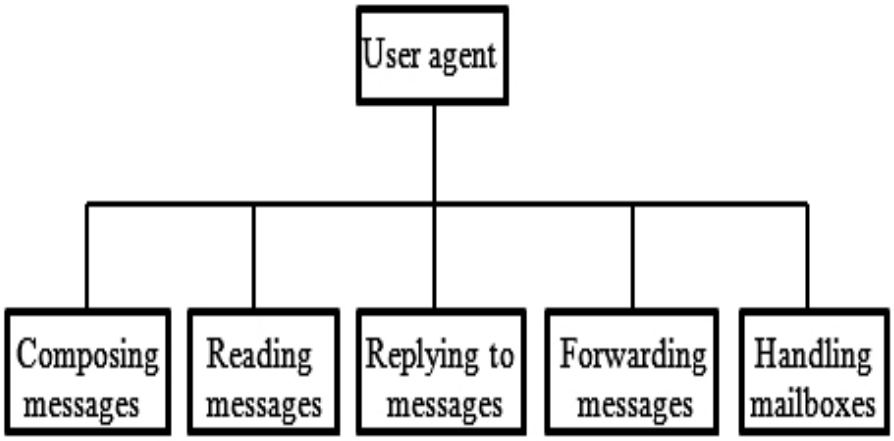


Figure 14.13: Services of user agent [5]

Reading messages: On invoking, a user agent first checks the mail in the incoming mailbox. It generally displays a one line summary of each and every received mail. The various fields each E-mail has been described below.

1. A flag field displays the status of the mail like new, previously read but not replied to, or read and replied to.
2. A number field.
3. The size of the message.
4. The optional subject field.
5. The sender.

Replying messages: User agent allows the user for replying to the sender of the message. User agent also allows or to reply to all the recipients of the message. The reply message consists of both the new message and original message.

Forwarding messages: It means sending a message to third person. The forwarding message may or may not include extra comments.

Handling mailboxes: A user agent creates two types of mailboxes: inbox and outbox. Each and every box is a file with a special format and handled by a user agent. The inbox keeps all the received e-mails until and unless deleted by the user. Sent e-mails are stored in outbox until they are deleted by the user.

User Agent Types: There are two types of user agents: (i) Command-driven and (ii) GUI-based. Outlook, Eudora and Netscape are examples GUI-based user agents whereas pine, mail and elm are examples of command-driven user agents.

Sending Mail: User agent sends mail like a postal, which contains envelope and a message.

Figure 14.14(a) shows the structure of a postal mail and Figure 14.14(b) shows the structure of an E-mail.

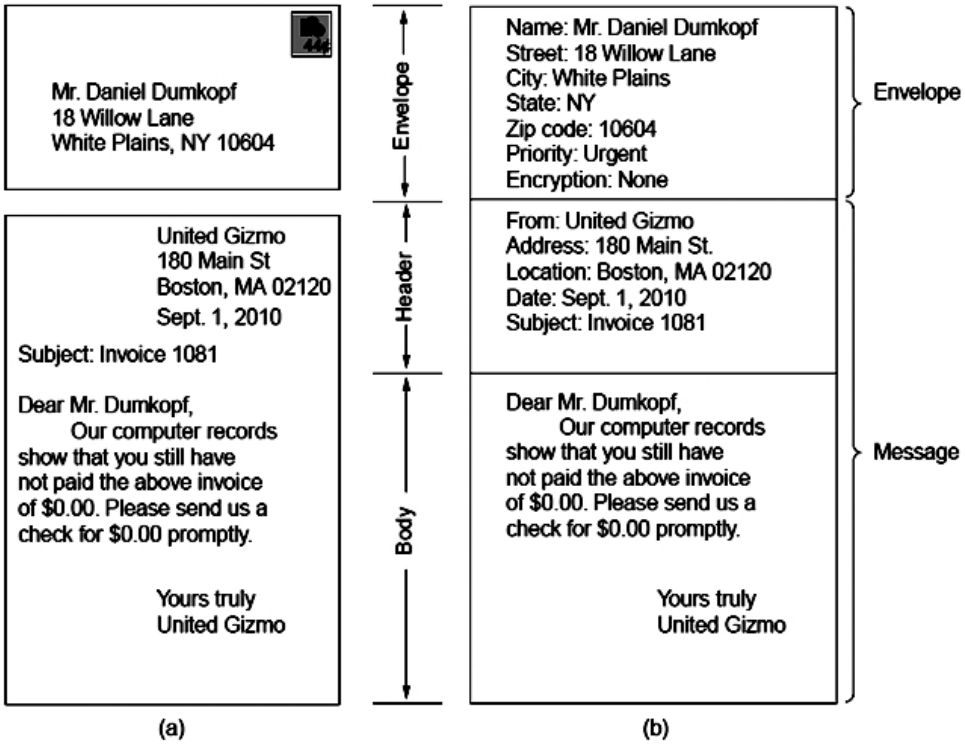


Figure 14.14: Format of an E-mail (a) Postal mail (b) E-mail [6]

Envelope: It contains addresses of the sender and the receiver.

Message: The message is the collection of header and a body. The various information under header part are: (i) the receiver, (ii) the sender, (iii) the subject of the message, and (iv) other information like encoding type. The body part contains the actual information.

Receiving Mail: The user agent is triggered by a timer. If a user has mail, the user agent notifies the user. After the user is ready to read the mail, for a particular message in the mailbox, a list is displayed where each and every line consists of a summary of the information. The summary generally comprises the subject, the sender mail address and the time when the mail was received or sent. The user only selects any of the messages and then displays the contents on the screen.

Addresses: To deliver a mail, a mail handling system uses an addressing system with unique addresses. Internet address is a combination of two parts: a local part and a domain name and are separated by an @ sign as shown in Figure 14.15.

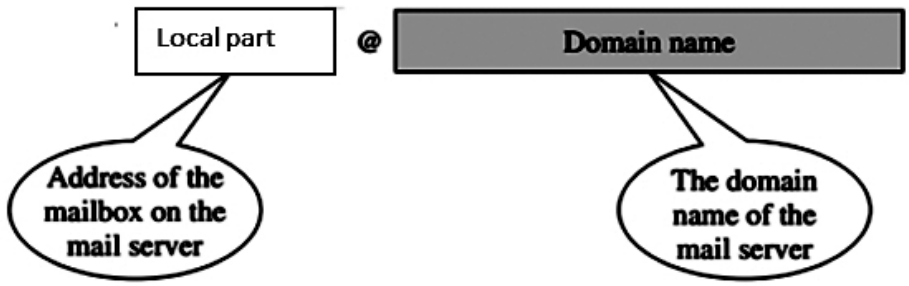


Figure 14.15: E-mail address [5]

Mailing List: Email has a mailing list, which allows one name (that is an alias), that represents many different e-mail addresses. Each time a message is to be sent, the system checks the name of the recipient in the alias database. If there is a mailing list for a particular alias, then separate messages for each entry in the list is prepared and handed to the message transfer agent.

MESSAGE TRANSFER AGENT: Simple Mail Transfer Protocol (SMTP)

The actual mail transfer is done by message transfer agents. Simple Mail Transfer Protocol (SMTP) characterizes the MTA client and server. Figure 14.16 shows the range of SMTP.

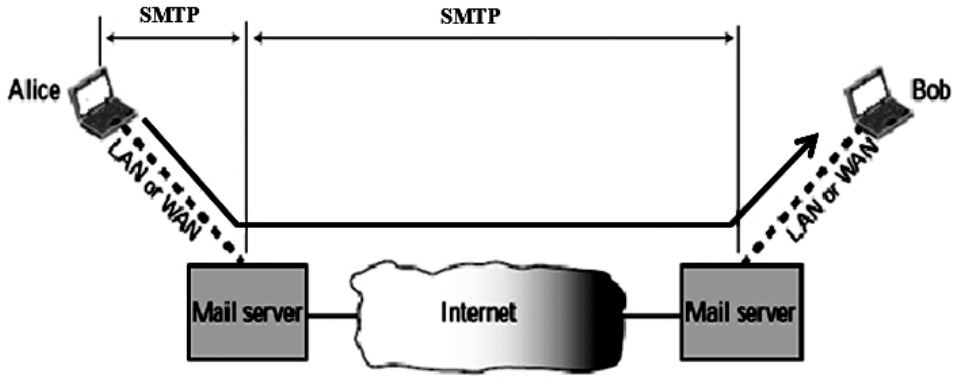


Figure 14.16: SMTP range [6]

To transfer messages, between a MTA client and a MTA server. Various commands and responses are required.

Command: Commands are sent from a client to a server. The formats of a command sent by the client to the server are described below.

HELO: It is used for client's self-identification.

MAIL FROM: To identify the sender of the message. This argument is the sender's e-mail address.

RCPT TO: Used to identify the expected recipient of the message. The argument is the recipient's e-mail address. This command is repeated for multiple recipients.

DATA: It is used to send the actual message.

QUIT: It terminates the message.

RSET: The current mail transaction is aborted by this command and it also deletes the stored information about the recipient and sender.

VRFY: Used to verify the address of the recipient.

NOOP: To check the status of the recipient the client uses this command. It always needs an answer from the recipient.

HELP: This command always asks the recipient to send information about the command sent as the argument.

SEND FROM: It indicates that the mail is to be delivered to the recipient's terminal, not the mailbox. If the recipient is already logged out, then mail is bounced back. The address of the sender is the argument.

SMAL FROM: It specifies that the mail is to be delivered to the recipient's terminal and mailbox. In this case, if the recipient is logged out, then mail is delivered to the mailbox only otherwise the mail is delivered to both the terminal and mailbox.

Responses: This is always sent from a server to the client. Table 14.3 lists some of the responses.

Code	Description
Positive Completion Reply	
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
Positive Intermediate reply	
354	Start mail input
Transient negative Completion Reply	
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted: inefficient storage
Permanent Negative completion Reply	
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mail box unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

Table 14.3: Responses [6]

MESSAGE ACCESS AGENT: POP AND IMAP

In the last phase as shown in Figure 14.17, the client pulls messages from the mail server. The direction of the data is from the server to the client.

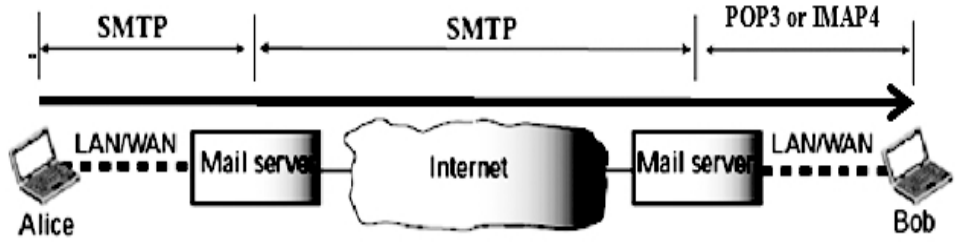


Figure 14.17: POP3 and IMAP[6]

Post Office Protocol, version 3 (POP3): The mail server has the server POP3 software and the client has client POP3 software. The interaction of the client POP3 and server POP3has been shown in Figure 14.18 below. The client starts mail access by opening a connection to the server on TCP port number 110. After that the client sends its user name and password to access the mailbox. Now, the user can list and retrieve the mail messages.

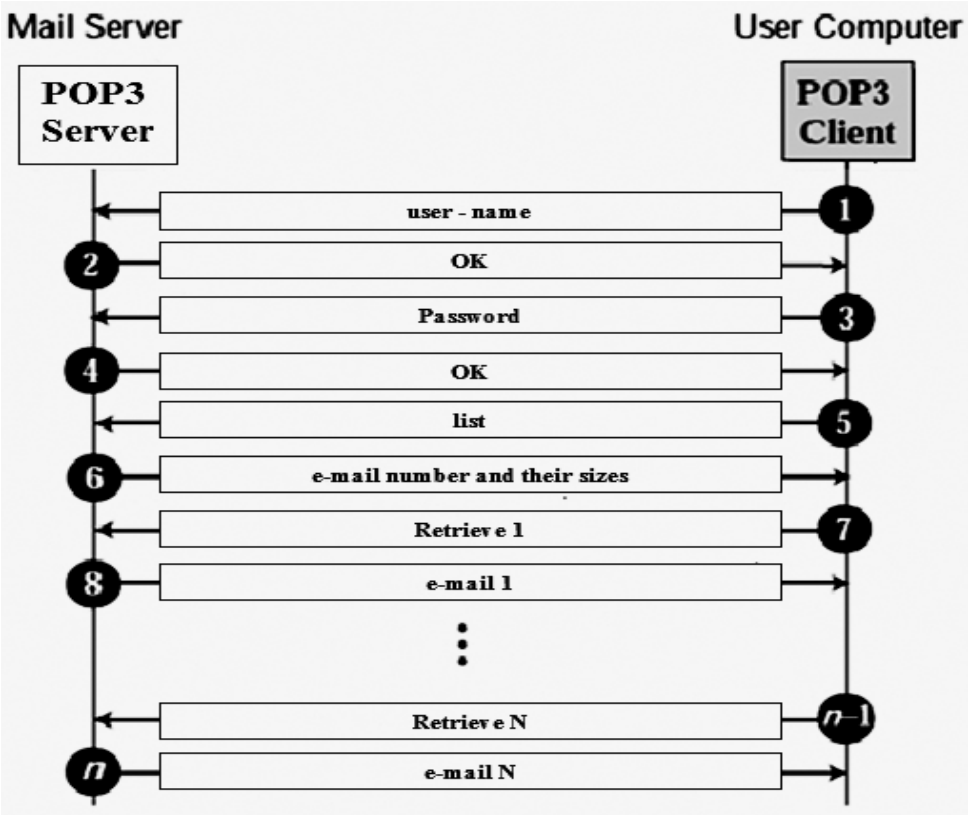


Figure 14.18: POP3 [6]

After retrieval of mail by the client, there are two strategies to decide whether we have to delete the retrieved mail from the mailbox or to keep the retrieved mail in the mailbox. In first case (delete mode) the mail is deleted from the mailbox and in second case (keep mode) mail remains in the mailbox.

Internet Mail Access Protocol, version 4 (IMAP4): It is more powerful but complex. POP3 do not allow the user to organize mail on the server. For example, before downloading the mail, the user cannot check the contents of the mail. However, IMAP4 provides the following.

- The header of the E-mail can be checked by the user prior to downloading.
- The user can delete, create, or rename mailboxes on the mail server.
- The user can also generate a hierarchy of mailboxes for e-mail storage.
- The user can search the E-mail contents for an intended string of characters prior to downloading.
- The user can partly download the E-mail. This is useful when the bandwidth is limited.

Mail Transfer Phases: The process sending the mail message can be done in three phases: connection establishment, mail transfer, and connection termination.

Connection Establishment: After the creation of Transmission control protocol (TCP) connection to the port number 25 by the client, connection phase is started by the SMTP server. The SMTP server starts the connection phase in the following three steps.

1. First, service ready code (code 220) is sent by the server to the client to indicate the client that server is ready to receive mail. And servers ends service not available code (code 421), if it is not ready.
2. After that the client sends the HELO message to identify itself by using its domain name address. The receiver and sender know each other by their IP addresses.
3. And finally to know the receiver, the server responds with code 250 and it completes the request for the command.
   Figure 14.19 shows the connection establishment process between an MTA client and an MTA server.

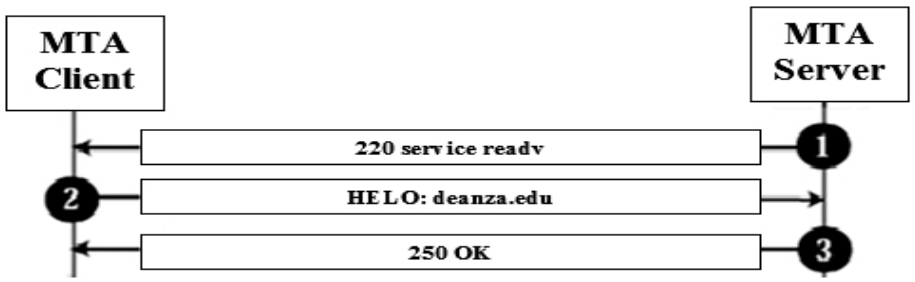


Figure 14.19: Connection establishment [6]

Message Transfer: After establishing the connection between the SMTP client and server, only one message between a sender and one or many recipients could be exchanged.

1. To introduce the sender of the message the client sends the MAIL FROM message. It attaches the sender's mail address (the domain name and mailbox).To return errors and reporting messages this step is required to give the server a return mail address.
2. The response code of the server is code 250.
3. The RCPT TO (recipient) message has sent by the client and includes the recipient's mail address.
4. Again the response code of the server is code 250.To initialize the message transfer the client sends the DATA message.
5. The response code of the server is code 354 (start mail input).
6. In consecutive lines the client sends the message contents. Each and every line is terminated using an end-of-line token. The message is terminated by a line with just one period.
7. The response code of the server is code 250 (OK).

Repeat steps 3 and 4, when there is greater than one recipient.

Connection Termination: This phase has two steps:

1. QUIT command has sent by the client.
2. The response code of the server is code 221.

The following Figure 14.20 depicts the connection termination process.

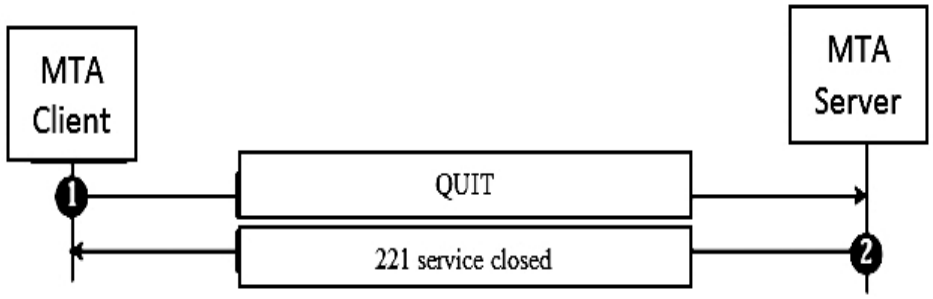


Figure 14.20: Connection termination [6]

At the end of the connection termination phase, the TCP connection should be closed.

CHECK YOUR PROGRESS

1. Briefly describe the email security services.
2. How the User agent gives services to the user?
3. Explain the architecture of E-mail. Why do we need POP3 or IMAP4 for electronic mail?

14.4 SUMMARY

Confidentiality, Authenticity, Integrity, Availability are the desirable properties for security. There are two types of security attacks; passive attacks and active attacks. Domain name system is a mapping technique from name to address. Resolvers are the programs of DNS client that needs to map an address to a name. Information of domain name space and the associated resource records must be stored among many computers called Name server. Name resolution has two methods by which queries are forwarded and results are returned; recursive resolution and iterative resolution. The three main components of E-mail system are: user agent, message transfer agent, and message access agent.

14.5 TERMINAL QUESTIONS

1. What do you mean by network security? Describe security services and attacks.
2. Write short note: a) SMTP b) POP3.
3. How does recursive resolution differ from iterative resolution?
4. Describe the DNS message format.
5. Do you think a recursive resolution is normally faster than an iterative one?
   Explain.
6. A domain name is hello.customer.info. Is this a generic domain or a country
   domain? State the reason.
7. Why is a connection establishment for mail transfer needed if TCP has already
   established a connection?
8. With the help of a neat and labelled diagram show the connection establishment
   phase between an MTA client and an MTA server.

REFERENCES

[1] Behrouz A. Forouzan, Chapter 29, “TCP/IP protocol suite (4th ed.)”.

[2] WilliamStallings, Chapter 23, “Data and Computer Communications (8th ed.)”.

[3] Behrouz A. Forouzan, Chapter 25, “Data Communications and Networking (4th ed.)”.

[4] Behrouz A. Forouzan, Chapter 19, “TCP/IP protocol suite (4th ed.)”.

[5] Behrouz A. Forouzan, Chapter 26, “Data Communications and Networking (4th ed.)”.

[6] Behrouz A. Forouzan, Chapter 23, “TCP/IP protocol suite (4th ed.)”.