Data Communications

Data communications is the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

l. **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. **Accuracy:** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. **Timeliness:** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.

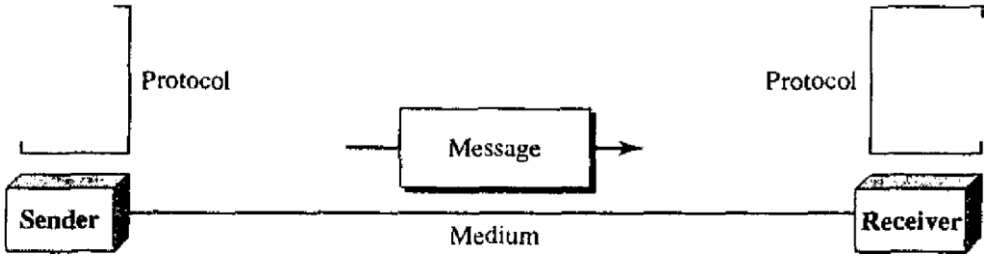
4. **Jitter:** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40- ms delay, an uneven quality in the video is the result.

Components

A data communications system has five components (see Figure 1.1).

Figure 1.1 *Five components of data communication*

Rule l. Rule 2: Rule n:



1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. Transmission medium. The transmission medium is the path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiberoptic cable, and radio waves.
5. Protocol. A protocol is a set of rules that govern data communications. It sents an agreement between the communicating devices. Without a protocol, devices may be connected but not communicating, just as a person speaking Fr cannot be understood by a person who speaks only Japanese.

Data Representation

Information today comes in different forms such as text, numbers, images, audio, and video.

Text

In data communications, text is represented as a bit pattern, a sequence of bits (Is). Different sets of bit patterns have been designed to represent text symbols. Each is called a code, and the process of representing symbols is called coding. Today prevalent coding system is called Unicode, which uses 32 bits to represent a symbol character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not *t* to represent numbers; the number is directly converted to a binary number to simple mathematical operations.

Images

Images are also represented by bit patterns. In its simplest form, an image is compound of a matrix of pixels (picture elements), where each pixel is a small dot. The size of pixel depends on the resolution. For example, an image can be divided into 1000 pi: or 10,000 pixels. In the second case, there is a better representation of the image (be resolution), but more memory is needed to store the image.

After an image is divided into pixels, each pixel is assigned a bit pattern. The value of the pattern depends on the image. For an image made of only black and-white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel.

If an image is not made of pure white and pure black pixels, you can increase size of the bit pattern to include gray scale. For example, to show four levels of g scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark g pixel by 01, a light gray pixel by 10, and a white pixel by 11.

There are several methods to represent color images. One method is called RGB so called because each color is made of a combination of three primary colors: red green, and blue. The intensity of each color is measured, and a bit pattern is assignee it. Another method is called YCM, in which a color is made of a combination of the other primary colors: yellow, cyan, and magenta.

Audio

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

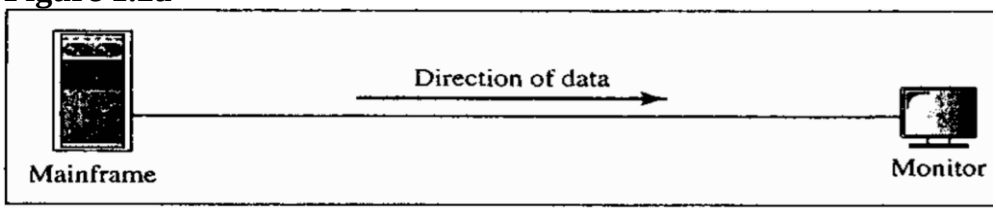
Video

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow

Communication between two devices can be simplex, half-duplex, or full - duplex as shown in Figure 1.2. (a, b & c)

Figure 1.2a



Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.

The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. half-duplex transmission, the entire capacity of a channel is taken over by whichever the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communicate, in both directions at the same time; the entire capacity of the channel can be utilized each direction.

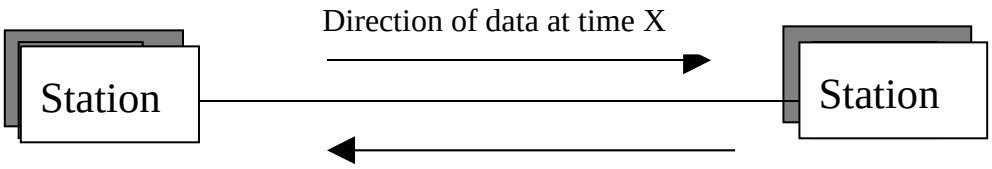


Figure 1.2 b

Full-Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c). The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share capacity of the link with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, for sending and the other for receiving; or the capacity of the channel is division between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at same time.

The full-duplex mode is used when communication in both directions is requires all the time. The capacity of the channel, however, must be divided between the t directions.

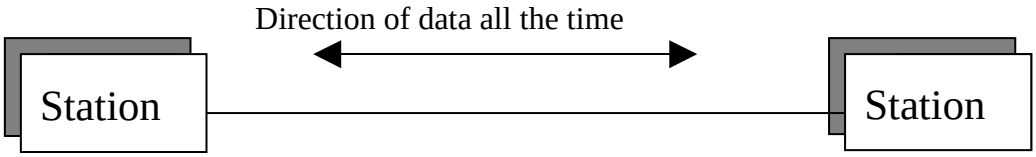


Figure 1.2 c

UNIT 2 NETWORKS
INTRODUCTION

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and, receiving data generated by other nodes on the network.

Distributed Processing

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of process, separate computers (usually a personal computer or workstation) handle subset.

Network Criteria

A network must be able to meet a certain number of criteria. The most important these are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time. Transmit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, zinc) the efficiency of the software.

Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay. However, these two criteria are often contradictory, If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

Point-to-Point

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 1,3a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

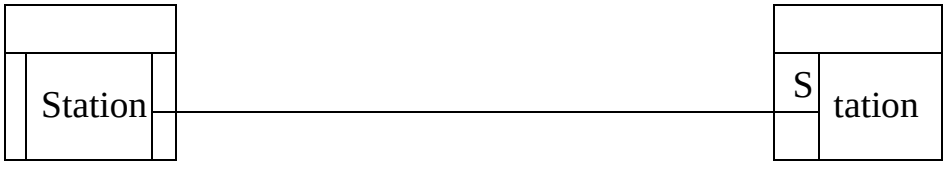
Multipoint

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.36).

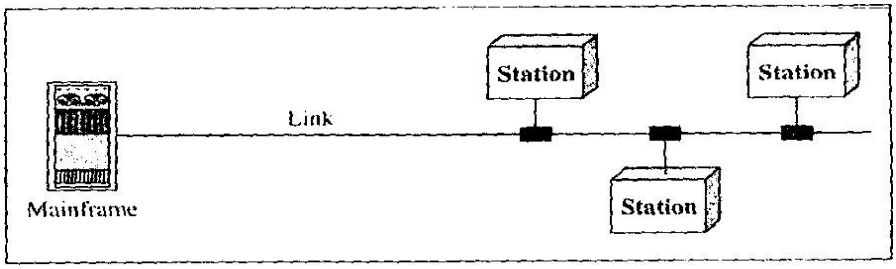
In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. It' sever al devices can use the link simultaneously; it is a *spatially shared* connection. If users must take turns, it is a timeshared connection.

Physical Topology

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link: two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the line linking devices (usually called nodes) to one another. There are four basic tope possible: mesh, star, bus, and ring (see Figure 1.4). *Figure 1.3 Types of connections: point-to-point and multipoint*



a. point-to-point



b. Multipoint

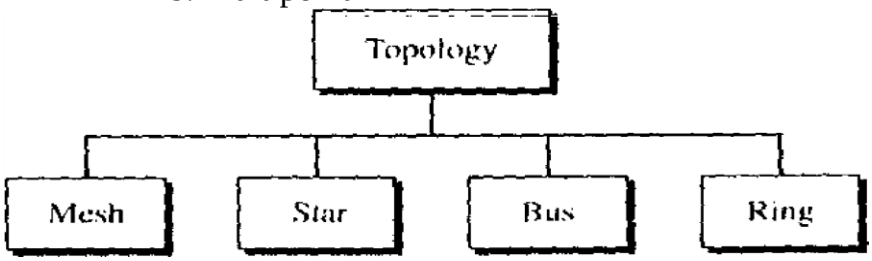


Figure 1.4 Categories of topology

UNIT 3 PROTOCOLS

INTRODUCTION

In this unit, we define two widely used terms: protocols and standards. First we define protocol, which is synonymous with rule. Then we discuss standards, with agreed-upon rules.

OBJECTIVES

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

- understand Protocols

Protocols

In computer networks, communication occur between entities in different system entity is anything capable of sending or receiving information. However, two entities not simply send bit streams to each other and expect to be understood. For communicate to occur, the entities must agree on a protocol. A protocol is a set of rules that govern communications. A protocol defines what is communicated, how it is communicate when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax:** The term *syntax* refers to the structure or format of the data, meaning order in which they are presented. For example, a simple protocol might expect first 8 bits of data to be the address of the sender, the second 8 bits to be the at of the receiver, and the rest of the stream to be the message itself.
- **Semantics:** The word *semantics* refers to the meaning of each section o How is a particular pattern to be interpreted, and what action is to be taken on that interpretation? For example, does an address identify the route to be or the final destination of the message?
- **Timing:** The term *timing* refers to two characteristics: when data should b and how fast they can be sent. For example, if a sender produces data at 100 but the receiver can process data at only I Mbps, the transmission will overload receiver and some data will be lost.

MODULE 2 MODELS OF COMMUNICATION

UNIT 1 OSI: PHYSICAL LAYER

INTRODUCTION

The **Open System Interconnection Reference Model (OSI Reference Model or OSI Model)** is an abstract description for layered communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative. In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the **OSI Seven Layer Model**.

A layer is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. On each layer an *instance* provides services to the instances at the layer above and requests service from the layer below. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path. Conceptually two instances at one layer are connected by a horizontal protocol connection on that layer.

OBJECTIVES

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

- discuss OSI Seven Layer Model
- explain the Physical layer
- explain the Physical signaling sub-layer
- understand the relationship between the physical Layer of OSI model and the TCP/IP model

Physical Layer

The Physical Layer is the first and lowest layer in the seven-layer OSI model of computer networking. The Physical Layer consists of the basic hardware transmission

technologies of a network. It is a fundamental layer underlying the logical data structures of the higher level functions in a network. Due to the plethora of available hardware technologies with widely varying characteristics, this is perhaps the most complex layer in the OSI architecture. The implementation of this layer is often termed PHY.

The Physical Layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes. The bit stream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a hardware transmission medium. The Physical Layer provides an electrical, mechanical, and procedural interface to the transmission medium. The shapes and properties of the electrical connectors, the frequencies to broadcast on, the modulation scheme to use and similar low-level parameters, are specified here.

Within the semantics of the OSI network architecture, the Physical Layer translates logical communications requests from the Data Link Layer into hardware-specific operations to effect transmission or reception of electronic signals.

List of Physical Layer Services

The major functions and services performed by the Physical Layer are:

- Bit-by-bit or symbol-by-symbol delivery
- Providing a standardized interface to physical transmission media, including ○ Mechanical specification of electrical connectors and cables, for example maximum cable length
    - Electrical specification of transmission line signal level and impedance
    - Radio interface, including electromagnetic spectrum frequency allocation and specification of signal strength, analog bandwidth, etc.
    - Specifications for IR over optical fiber or a wireless IR communication link
- Modulation
- Line coding
- Bit synchronization in synchronous serial communication
- Start-stop signaling and flow control in asynchronous serial communication
- Circuit switching
- Multiplexing ○ Establishment and termination of circuit switched connections
- Carrier sense and collision detection utilized by some level 2 multiple access protocols
- Equalization filtering, training sequences, pulse shaping and other signal processing of physical signals
- Forward error correction [2] for example bitwise convolution coding
- Bit-interleaving and other channel coding

The Physical Layer is also concerned with

- Bit rate
- Point-to-point , multipoint or point-to-multipoint line configuration
- Physical network topology, for example bus, ring, mesh or star network
- Serial or parallel communication
- Simplex , half duplex or full duplex transmission mode
- Auto negotiation

Physical Layer Examples

- Telephone network modems- V.92
- IRDA Physical Layer
- USB Physical Layer
- EIA RS-232, EIA-422, EIA-423, RS-449, RS-485
- Ethernet physical layer Including 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX and other varieties
- Varieties of 802.11 Wi-Fi Physical Layers
- DSL
- ISDN
- T1 and other T-carrier links, and E1 and other E-carrier links
- SONET/SDH
- GSM Um radio interface physical layer
- Bluetooth Physical Layer
- ITU Recommendations: see ITU-T
- Firewire
- TransferJet Physical Layer
- Etherloop
- ARINC 818 Avionics Digital Video Bus
- G.hn /G.9960 Physical Layer 4 Hardware Equipment (Network Node) Examples

- Network adapter
- Repeater
- Network hub
- Modem
- Fiber Media Converter

Relation to TCP/IP Model

The TCP/IP model is a high-level networking description used for the Internet and similar networks. It does not define an equivalent layer that deals exclusively with hardware-level specifications, as this model does not concern itself directly with physical interfaces. It specifies a functioning host operating system with a facility to transmit packets onto

the local network via a local area network encapsulation method (e.g., RFC 1042). and simply absorbs all hardware specific components of the operating system and interface firmware into the Link Layer without detailed specifications. The TCP/IP model is not a top/down comprehensive design reference for general networks and networking hardware, but an architectural description of the suite of methods and requirements used in the Internet Protocol Suite to achieve internetworking between disparate local area networks.

Self-Review Question

1. What is OSI?
2. What are the major functions and services performed by the Physical Layer?

UNIT 2 OSI: DATA LINK LAYER

INTRODUCTION

The Data Link Layer is Layer 2 of the seven-layer OSI model of computer networking. It corresponds to or is part of the link layer of the TCP/IP reference model.

OBJECTIVES

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

• discuss the Data link layer

• explain it's r**elation to TCP/IP model**

Data Link Layer

The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-toPoint Protocol (PPP), HDLC and ADCCP for point-to-point (dual-node) connections.

The Data Link Layer is concerned with local delivery of frames between devices on the same LAN. Data Link frames, as these protocol data units are called, do not cross the boundaries of a local network. Inter-

network routing and global addressing are higher layer functions, allowing Data Link protocols to focus on local delivery, addressing, and media arbitration. In this way, the Data Link layer is analogous to a neighborhood traffic cop; it endeavors to arbitrate between parties contending for access to a medium.
When devices attempt to use a medium simultaneously, frame collisions occur. Data Link protocols specify how devices detect and recover from such collisions, but it does not prevent them from happening.

Delivery of frames by layer 2 devices is effected through the use of unambiguous hardware addresses. A frame's header contains source and destination addresses that indicate which device originated the frame and which device is expected to receive and process it. In contrast to the hierarchical and routable addresses of the network layer, layer 2 addresses are flat, meaning that no part of the address can be used to identify the logical or physical group to which the address belongs.

The data link thus provides data transfer across the physical link. That transfer can be reliable or unreliable; many data link protocols do not have acknowledgments of successful frame reception and acceptance, and some data link protocols might not even have any form of checksum to check for transmission errors. In those cases, higher-level protocols must provide flow control, error checking, and acknowledgments and retransmission.

In some networks, such as IEEE 802 local area networks, the Data Link Layer is described in more detail with Media Access Control (MAC) and Logical Link Control (LLC) sublayers; this means that the IEEE 802.2 LLC protocol can be used with all of the IEEE 802 MAC layers, such as Ethernet, token ring, IEEE 802.11, etc., as well as with some non-802 MAC layers such as FDDI. Other Data Link Layer protocols, such as HDLC, are specified to include both sublayers, although some other protocols, such as Cisco HDLC, use HDLC's low-level framing as a MAC layer in combination with a different LLC layer. In the ITU-T G.hn standard, which provides a way to create a high-speed (up to 1 Gigabit/s) Local area network using existing home wiring (power lines, phone lines and coaxial cables), the Data Link Layer is divided into three sub-layers (Application Protocol Convergence, Logical Link Control and Medium Access Control).

Within the semantics of the OSI network architecture, the Data Link Layer protocols respond to service requests from the Network Layer and they perform their function by issuing service requests to the Physical Layer.

Sub-layers of the Data Link Layer

Logical Link Control sublayer

The uppermost sublayer is *Logical Link Control* (LLC). This sublayer multiplexes protocols running atop the Data Link Layer, and optionally provides flow control, acknowledgment, and error notification. The LLC provides addressing and control of the data link. It specifies which mechanisms are to be used for addressing stations over the transmission medium and for controlling the data exchanged between the originator and recipient machines.

Media Access Control sublayer

The sublayer below it is *Media Access Control* (MAC). Sometimes this refers to the sublayer that determines who is allowed to access the media at any one time (usually CSMA/CD). Other times it refers to a frame structure with MAC addresses inside.

There are generally two forms of media access control: distributed and centralized. Both of these may be compared to communication between people. In a network made up of people speaking, i.e. a conversation, we look for clues from our fellow talkers to see if any of them appear to be about to speak. If two people speak at the same time, they will back off and begin a long and elaborate game of saying "no, you first".

The Media Access Control sublayer also determines where one frame of data ends and the next one starts. There are four means of doing that: time based, character counting, byte stuffing and bit stuffing.

- The *time based* approach simply puts a specified amount of time between frames. The major drawback of this is that new gaps can be introduced or old gaps can be lost due to external influences.
- *Character counting* simply notes the count of remaining characters in the frame's header. This method, however, is easily disturbed if this field gets faulty in some way, thus making it hard to keep up synchronization.
- *Byte stuffing* precedes the frame with a special byte sequence such as DLE STX and succeeds it with DLE ETX. Appearances of DLE (byte value 0x10) has to be escaped with another DLE. The start and stop marks are detected at the receiver and removed as well as the inserted DLE characters.
- Similarly, *bit stuffing* replaces these start and end marks with flag consisting of a special bit pattern (e.g. a 0, six 1 bits and a 0). Occurrences of this bit pattern in the data to be transmitted is

avoided by inserting a bit. To use the example where the flag is 01111110, a 0 is inserted after 5 consecutive 1's in the data stream. The flags and the inserted 0's are removed at the receiving end. This makes for arbitrary long frames and easy synchronization for the recipient. Note that this stuffed bit is added even if the following data bit is 0, which could not be mistaken for a sync sequence, so that the receiver can unambiguously distinguish stuffed bits from normal bits.

Interfaces

The Data Link Layer is often implemented in software as a "network card driver". The operating system will have a defined software interface between the data link and the network transport stack above. This interface is not a layer itself, but rather a definition for interfacing between layers.

List of Data Link Layer services

- Encapsulation of network layer data packets into frames
  - Frame synchronization
  - Logical link control (LLC) sublayer:
    - Error control (automatic repeat request,ARQ), in addition to ARQ provided by some Transport layer protocols, to forward error correction (FEC) techniques provided on the Physical Layer, and to error-detection and packet canceling provided at all layers, including the network layer. Data link layer error control (i.e. retransmission of erroneous packets) is provided in wireless networks and V.42 telephone network modems, but not in LAN protocols such as Ethernet, since bit errors are so uncommon in short wires. In that case, only error detection and canceling of erroneous packets are provided.
    - Flow control, in addition to one provided on the Transport layer. Data link layer error control is not used in LAN protocols such as Ethernet, but in modems and wireless networks.
- Media access control (MAC) sublayer:
    - Multiple access protocols for channel-access control, for example CSMA/CD protocols for collision detection and retransmission in Ethernet bus networks and hub networks, or the CSMA/CA protocol for collision avoidance in wireless networks. ○ Physical addressing (MAC addressing)
    - LAN switching (packet switching) including MAC filtering and spanning tree protocol
    - Data packet queuing or scheduling

- Store-and-forward switching or cut-through switching
- Quality of Service (QoS) control
- Virtual LANs (VLAN)

Protocol Examples

- ARCnet
- ATM
- Cisco Discovery Protocol (CDP)
- Controller Area Network (CAN)
- Econet
- Ethernet
- Ethernet Automatic Protection Switching (EAPS)
- Fiber Distributed Data Interface (FDDI)
- Frame Relay
- High-Level Data Link Control (HDLC)
- IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers)
- IEEE 802.11 wireless LAN
- Link Access Procedures, D channel (LAPD)
- LocalTalk
- Multiprotocol Label Switching (MPLS)
- Point-to-Point Protocol (PPP)
- Serial Line Internet Protocol (SLIP) (obsolete)
- Spanning tree protocol
- StarLan
- Token ring
- Unidirectional Link Detection (UDLD)
- and most forms of serial communication.

Relation to TCP/IP model

In the frame work of the TCP/IP (Internet Protocol Suite) model, OSI's Data Link Layer, in addition to other components, is contained in TCP/IP's lowest layer, the Link Layer. The Internet Protocol's Link Layer only concerns itself with hardware issues to the point of obtaining hardware addresses for locating hosts on a physical network link and transmitting data frames onto the link. Thus, the Link Layer is broader in scope and encompasses all methods that affect the local link, which is the group of connections that are limited in scope to other nodes on the local access network.

The TCP/IP model is not a top/down comprehensive design reference for networks. It was formulated for the purpose of illustrating the logical groups and scopes of functions needed in the design of the suite of internetworking protocols of TCP/IP, as needed for the operation of the Internet. In general, direct or strict comparisons of the OSI and TCP/IP models should be avoided, because the layering in TCP/IP is

not a principal design criterion and in general considered to be "harmful" (RFC 3439). In particular, TCP/IP does not dictate a strict hierarchical sequence of encapsulation requirements, as is attributed to OSI protocol

SRQ

1. What is Data link layer?
2. Outline 7 protocols of the data link layer

UNIT 3 OSI: NETWORK LAYER AND TRANSPORT LAYER

INTRODUCTION

The Network Layer is Layer 3 of the seven-layer OSI model of computer networking.

The Network Layer is responsible for end-to-end (source to destination) packet delivery including routing through intermediate hosts, whereas the Data Link Layer is responsible for node-to-node (hop-to-hop) frame delivery on the same link.

OBJECTIVES

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

- define the Network layer
- discuss the functions of the network layer
- explain the relation of the Network layer with TCP/IP
- discuss the Transport layer.

Network Layer

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination host via one or more networks while maintaining the quality of service and error control functions.

Functions of the Network Layer include:

- **Connection model:** connection-oriented and connectionless communication.

For example, snail mail is connectionless, in that a letter can travel from a sender to a recipient without the recipient having to do anything. On the other hand, the telephone system is connection-oriented, because the other party is required to pick up the phone before communication can be established. The OSI Network Layer protocol can be either connection-oriented, or connectionless. In contrast, the TCP/IP Internet Layer supports only the connectionless Internet Protocol (IP); but connectionoriented protocols exist higher at other layers of that model.

- **Host addressing:** Every host in the network needs to have a unique address which determines where it is. This address will normally be assigned from a hierarchical system, so you can be "Fred Murphy" to people in your house, "Fred Murphy, Main Street 1" to Dubliners, or "Fred Murphy, Main Street 1, Dublin" to people in Ireland, or "Fred Murphy, Main Street 1, Dublin, Ireland" to people anywhere in the world. On the Internet, addresses are known as Internet Protocol (IP) addresses.

- **Message forwarding:** Since many networks are partitioned into sub networks and connect to other networks for wide-area communications, networks use specialized hosts, called gateways or routers to forward packets between networks. This is also of interest to mobile applications, where a user may move from one location to another, and it must be arranged that his messages follow him. Version 4 of the Internet Protocol (IPv4) was not designed with this feature in mind, although mobility extensions exist. IPv6 has a better designed solution.

Within the service layering semantics of the OSI network architecture the Network Layer responds to service requests from the Transport Layer and issues service requests to the Data Link Layer.

Relation to TCP/IP Model

The TCP/IP model describes the protocol suite of the Internet. This model has a layer called the Internet Layer, located above the Link Layer. In many text books and other secondary references the Internet Layer is often equated with OSI's Network Layer. However, this is misleading as the allowed characteristics of protocols (e.g., whether they are connection-oriented or connection-less) placed into these layer are different in the two models. The Internet Layer of TCP/IP is in fact only a subset of functionality of the Network Layer. It only describes one type of network architecture, the Internet.

In general, direct or strict comparisons between these models should be avoided, since the layering in TCP/IP is not a principal design criterion and in general is considered to be "harmful".

Transport Layer

The **Transport Layer** provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state and connection oriented. This means that the Transport Layer can keep track of the segments and retransmit those that fail.

Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the Transport Layer, typical examples of Layer 4 are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Of the actual OSI protocols, there are five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the least error recovery) to class 4 (TP4, designed for less reliable networks, similar to the Internet). Class 0 contains no error recovery, and was designed for use on network layers that provide errorfree connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the Session Layer. Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries, both of which TCP is incapable. Detailed characteristics of TP0-4 classes are shown in the following table:

Feature Name	TP0	TP1	TP2	TP3	TP4
Connection oriented network	Yes	Yes	Yes	Yes	Yes
Connectionless network	No	No	No	No	Yes
Concatenation and separation	No	Yes	Yes	Yes	Yes
Segmentation and reassembly	Yes	Yes	Yes	Yes	Yes
Error Recovery	No	Yes	No	Yes	Yes
Reinitiate connection (if an excessive number of PDUs are unacknowledged)	No	Yes	No	Yes	No

multiplexing and demultiplexing over a single virtual circuit	No	No	Yes	Yes	Yes
Explicit flow control	No	No	Yes	Yes	Yes
Retransmission on timeout	No	No	No	No	Yes
Reliable Transport Service	No	Yes	No	Yes	Yes

Perhaps an easy way to visualize the Transport Layer is to compare it with a Post Office, which deals with the dispatch and classification of mail and parcels sent. Do remember, however, that a post office manages the outer envelope of mail. Higher layers may have the equivalent of double envelopes, such as cryptographic presentation services that can be read by the addressee only. Roughly speaking, tunneling protocols operate at the Transport Layer, such as carrying non-IP protocols such as IBM's SNA or Novell's IPX over an IP network, or end-to-end encryption with IPsec. While Generic Routing Encapsulation (GRE) might seem to be a Network Layer protocol, if the encapsulation of the payload takes place only at endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete frames or packets to deliver to an endpoint. L2TP carries PPP frames inside transport.

UNIT 3 OSI: SESSION LAYER

INTRODUCTION

The Session Layer is Layer 5 of the seven-layer OSI model of computer networking. The Session Layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e. a semi-permanent dialogue.

OBJECTIVES

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

- define the Session layer
- list the Session layer services
- outline the Session layer Protocols
- compare the Session layer with TCP/IP model.

Session Layer

The Session Layer is Layer 5 of the seven-layer OSI model of computer networking.

Communication sessions consist of requests and responses that occur between applications. Session Layer services are commonly used in application environments that make use of remote procedure calls (RPCs).

An example of a Session Layer protocol is the OSI protocol suite Session Layer Protocol, also known as X.225 or ISO 8327. In case of a connection loss this protocol may try to recover the connection. If a connection is not used for a long period, the Session Layer Protocol may close it and re-open it. It provides for either full duplex or half-duplex operation and provides synchronization points in the stream of exchanged messages.[1]

Other examples of Session Layer implementations include Zone Information Protocol (ZIP) – the AppleTalk protocol that coordinates the name binding process, and Session Control Protocol (SCP) – the DECnet Phase IV Session Layer protocol.

Within the service layering semantics of the OSI network architecture, the Session Layer responds to service requests from the Presentation Layer and issues service requests to the Transport Layer.

Session Layer Services

- Authentication
- Permissions
- Session restoration (check pointing and recovery).

The Session Layer of the OSI model is responsible for session checkpointing and recovery. It allows information of different streams, perhaps originating from different sources, to be properly combined or synchronized.

An example application is web conferencing, in which the streams of audio and video must be synchronous to avoid so-called lip synch problems. Floor control ensures that the person displayed on screen is the current speaker.

Another application is in live TV programs, where streams of audio and video need to be seamlessly merged and transitioned from one to the other to avoid silent airtime or excessive overlap.

Session Layer Protocols

- ADSP, AppleTalk Data Stream Protocol
- ASP, AppleTalk Session Protocol
- H.245, Call Control Protocol for Multimedia Communication
- ISO-SP, OSI Session Layer Protocol (X.225, ISO 8327)
- iSNS, Internet Storage Name Service
- L2F, Layer 2 Forwarding Protocol
- L2TP, Layer 2 Tunneling Protocol
- NetBIOS, Network Basic Input Output System
- PAP, Password Authentication Protocol
- PPTP, Point-to-Point Tunneling Protocol
- RPC, Remote Procedure Call Protocol
- RTCP, Real-time Transport Control Protocol
- SMPP, Short Message Peer-to-Peer
- SCP, Secure Copy Protocol
- SSH, Secure Shell
- ZIP, Zone Information Protocol
- SDP, Sockets Direct Protocol

Comparison with TCP/IP Model

The TCP/IP reference model does not concern itself with the OSI model's details of application or transport protocol semantics and therefore does not consider a Session Layer. OSI's session management in connection with the typical transport protocols (TCP, SCTP), is contained in the Transport Layer protocols, or otherwise considered the realm of the Application Layer protocols. TCP/IP's layers are *descriptions* of operating scopes (application, host-to-host, network, link) and not detailed *prescriptions* of operating procedures or data semantics.

Session Layer services include; Authentication, Permissions, and Session restoration (check pointing and recovery)

UNIT 4 OSI: PRESENTATION LAYER AND APPLICATION LAYER

INTRODUCTION

The Presentation Layer is Layer 6 of the seven-layer OSI model of computer networking.

The Presentation Layer is responsible for the delivery and formatting of information to the application layer for further processing or display. It relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems. An example of a presentation service would be the conversion of an EBCDIC-coded text file to an ASCII-coded file.

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model.

OBJECTIVES

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

- discuss the Presentation Layer
- explain CASE and SASE Layer services • list Presentation Layer Protocol
- discuss Application Layer.

Presentation Layer

The Presentation Layer is the lowest layer at which application programmers consider data structure and presentation, instead of simply sending data in form of datagrams or packets between hosts. This layer deals with issues of string representation - whether they use the Pascal method (an integer length field followed by the specified amount of bytes) or the C/C++ method (null-terminated strings, i.e. "`thisisastring\0`"). The idea is that the application layer should be able to point at the data to be moved, and the Presentation Layer will deal with the rest.

Encryption is typically done at this level too, although it can be done at the Application, Session, Transport, or Network Layers; each having its own advantages and disadvantages. Another example is representing structure, which is normally standardized at this level, often by using XML. As well as simple pieces of data, like strings, more complicated things are standardized in this layer. Two common examples are

'objects' in object-oriented programming, and the exact way that streaming video is transmitted.

In many widely used applications and protocols, no distinction is made between the presentation and application layers. For example, HTTP, generally regarded as an application layer protocol, has Presentation Layer aspects such as the ability to identify character encoding for proper conversion, which is then done in the Application Layer.

Within the service layering semantics of the OSI network architecture, the Presentation Layer responds to service requests from the Application Layer and issues service requests to the Session Layer.

Presentation Layer Services

- Encryption
- Compression

Sublayers

The Presentation Layer is composed of two sublayers:

- **CASE** (Common Application Service Element)
- **SASE** (Specific Application Service Element)

CASE

The **CASE sublayer** provides services for the Application Layer and request services from the Presentation Layer. It provides support for common application services, such as:

- ACSE (Association Control Service Element)
- ROSE (Remote Operation Service Element)
- CCR (Commitment Concurrency and Recovery)
- RTSE (Reliable Transfer Service Element)

SASE

The **SASE sublayer** provides application specific services (protocols), such as

- FTAM (File Transfer, Access and Manager)
- VT (Virtual Terminal)
- MOTIS (Message Oriented Text Interchange Standard)
- CMIP (Common Management Information Protocol)
- JTM (Job Transfer and Manipulation) a former OSI standard
- MMS (Manufacturing Messaging Service)

- RDA (Remote Database Access)
- DTP (Distributed Transaction Processing)
- Tel Net(a remote terminal access protocol)

Presentation Layer Protocol Examples

- AFP, Apple Filing Protocol
- ASCII, American Standard Code for Information Interchange
- EBCDIC, Extended Binary Coded Decimal Interchange Code
- ICA, Independent Computing Architecture, the Citrix system core protocol
- LPP, Lightweight Presentation Protocol
- NCP, NetWare Core Protocol
- NDR, Network Data Representation
- RDP, Remote Desktop Protocol
- XDR, eXternal Data Representation
- X.25 PAD, Packet Assembler/Disassembler Protocol

Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network resources for the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer. Some examples of application layer implementations include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and X.400 Electronic Mail.

Examples

Layer		OSI protocols	TCP/IP Protocols	Signaling System 7	Apple Talk	IPX	SNA	UMTS	Misc. examples
#	Name								

7	Application	FTAM, X.400, X.500, DAP, ROSE, RTSE, ACSE	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, DHCP, SMPP, SMTP, SNMP, Telnet, RIP, BGP	INAP, MAP, TCAP, ISUP, TUP	AFP, ZIP, RTMP, NBP	RIP SAP	APPC		HL7, Modbus

UNIT 5 TCP/IP MODEL

INTRODUCTION

- The TCP/IP model or Internet reference model, sometimes called the DoD [(Department of Defense) model or the ARPANET reference model, is a layered abstract description for communications and computer network protocol design.
- It was created in the 1970s by DARPA for use in developing the Internet's protocols.
- It is a suite of protocols among which TCP and IP are the two main protocols, hence the name.
- This model was developed before the OSI Reference Model, and the Internet Engineering Task Force (IETF), which is responsible for the model and protocols developed under it, has never felt obligated to be compliant with OSI.
- The model is composed of 5 layers ○ Physical ○ Data Link ○ Network ○ Transport ○ Application

OBJECTIVES

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

- discuss the TCP/IP model • outline TCP/IP Services and Protocols
- discuss the Internet Protocol (IP).

The TCP/IP Advantage

The reasons that TCP/IP has become the most widely used protocol are as follows:

- The flexible addressing scheme of TCP/IP allows data to be routed over even very large networks.
- Virtually all operating systems and platforms can use TCP/IP.
- TCP/IP offers a very large number of utilities and tools.
- The I/internet communication is based on TCP/IP.

3.1.2 TCP/IP Services and Protocols

Layer	Services	Protocols	Devices
Physical Layer	• Dictates Signal Characteristics • Data Transmission Signal Multiplexing • Dictates Network L/O • Dictates Media Characteristics • Switching	• HSSI • X.21	• Repeaters • Hubs • Modems
Data Link Layer	• Error Detection and Correction • Flow and Error Control • Media Access Control • Virtual Circuit Switching	• HDLC • ARP/RARP • SLIP • PPP	• Bridges • Switches
Network Layer	• Internetworking Logical Addressing • Routing Datagram Switching •	• Routed Protocols o IGMP o IP o ICMP • Routing Protocols o RIP o IGRP o BGP	• Routers • Gateways

		○ OSF	
Transport Layer	• Process-to-Process Delivery • Congestion Control • Quality of Service	• TCP • UDP	N/A
Application Layer	• • WWW • Mail Multimedia	• • TFTP • • • HTTP FTP • SMTP SNMP POP3	• Application Gateways

3.2 The Internet Protocol (IP)

- The IP component of TCP/IP determines where packets of data are to be routed based on their destination addresses, and IP has certain characteristics related to how it handles this function.
- The functioning of an IP based communication is analogous to Delivering Mail Through the Postal Service.

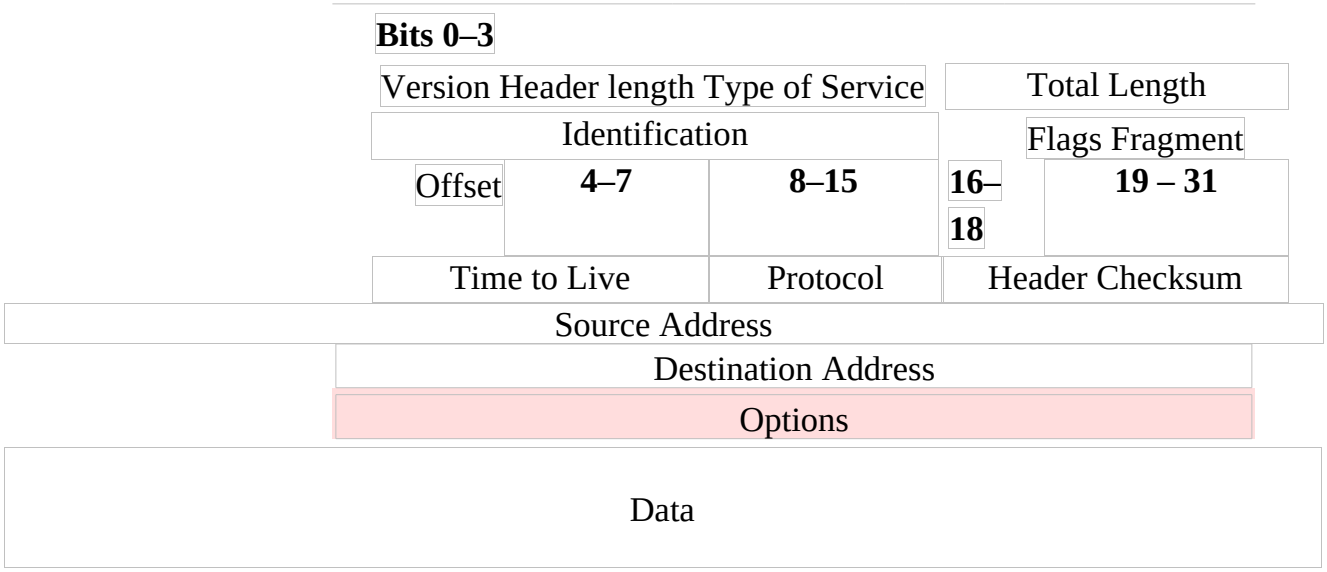
3.2.1 IP Characteristics

- Operates at network layer
- Connectionless protocol- The destination device receives the data and does not return any status information to the sending device
- Packets treated independently- A packet can be misdirected, duplicated, or lost on the way to its destination.
- Hierarchical addressing
- Best-effort delivery
- No data recovery features- does not provide any special features that recover corrupted packets

3.2.2 IP Packet Format

- The header consists of 12 fields + 1 optional field
- *Version(4bits)* :For IPv4, this has a value of 4 (hence the name IPv4).
- *Internet Header Length(4bits)* : tells the number of 32-bit words in the header. In IPv4, this field specifies the size of the header.

- *Type of Service (8bits)* ○ bits 0-2: precedence ○ bit 3: 0 = Normal Delay, 1 = Low Delay



  - ○ bit 4: 0 = Normal Throughput, 1 = High Throughput
  - ○ bit 5: 0 = Normal Reliability, 1 = High Reliability
  - ○ bits 6-7: Reserved for future use or for Differentiated services or for Explicit Congestion Notification
- *Total Length(16bits)* : defines the entire datagram size, including header and data, in bytes.
- *Identification* : primarily used for uniquely identifying fragments of an original IP datagram.
- *Flags(3bits)* : used to control or identify fragments. They are (in order, from high order to low order):
  - ○ Reserved; must be zero. ○ Don't Fragment (DF)
  - ○ More Fragments (MF)
- *Fragment Offset(13bits)* : specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram.
- *Time To Live(8bits) : helps prevent datagrams from persisting in an internetwork. When the TTL field hits zero, the packet is no longer forwarded by a packet switch and is discarded.*
- *Protocol* : defines the protocol used in the data portion of the IP datagram.
- *Header Checksum(16bits)* :used for error-checking of the header.
- *Source address* : An IP address is a group of 4, 8-bit octets for a total of 32 bits. The value for this field is determined by taking the binary value of each octet and concatenating them together to make a single 32-bit value.
- *Destination address* : indicates the address of the packet receiver.

- *Options* : Additional header fields may follow the destination address field, but these are not often used. Note that the value in the IHL field must include enough extra 32-bit words to hold all the options (plus any padding needed to ensure that the header contains an integral number of 32-bit words)

3.2.3 IP Addressing

- Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnetwork.
- Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts:
  - the network number- identifies a network, assigned by InterNIC or an ISP
  - the host number-identifies a host on a network, assigned by the local network administrator.
- IPv4 Address representations

Notation	Value	Conversion from dotdecimal
Dot-decimal notation	192.0.2.235	N/A
Dotted Hexadecimal	0xC0.0x00.0x02.0xEB	Each octet is individually converted to hex
Dotted Octal	0300.0000.0002.0353	Each octet is individually converted into octal
Hexadecimal	0xC00002EB	Concatenation of the octets from the dotted hexadecimal
Decimal	3221226219	The hexadecimal form converted to decimal
Octal	030000001353	The hexadecimal form converted to octal

- IP Address Classes
  - The IPV4 addresses are divided into five different address classes: A, B,C, D, and E.

IP Address Class	Format	Purpose	HighOrder Bit(s)	Address Range	No. Bits Network/Host	Max. Hosts
A	N.H.H.H	Few large organizations	0	1.0.0.0 to 126.0.0.0	7/24	167772142 (2^{24} - 2)
B	N.N.H.H	Medium-size organizations	1, 0	128.1.0.0 to 191.254.0.0	14/16	65534 (2^{16} - 2)

C	N.N.N.H	Relatively small organizations	1, 1, 0	192.0.1.0 to 223.255.254.0	21/8	254 (2^8 - 2)
D	N/A	Multicast groups (RFC 1112)	1, 1, 1, 0	224.0.0.0 to 239.255.255.255	N/A (not for commercial use)	N/A
E	N/A	Experimental	1, 1, 1, 1	240.0.0.0 to 254.255.255.255	N/A	N/A

4.0 CONCLUSION

The TCP/IP has become the most widely used protocol for the following reasons: it has a flexible addressing scheme which allows data to be routed over even very large networks. Virtually all operating systems and platforms can use TCP/IP. It offers a very large number of utilities and tools. The fact that internet communication is based on TCP/IP, show it's high relevance.

5.0 SUMMARY

The TCP/IP model or Internet reference model, sometimes called the DoD [(Department of Defense) model or the ARPANET reference model, is a 5 layered abstract description for communications and computer network protocol design.

The flexible addressing scheme of TCP/IP allows data to be routed over even very large networks. Internet communication is based on TCP/IP. In IP Packet Format, the header consists of 12 fields + 1 optional field Internet Header Length (4bits): tells the number of 32-bit words in the header.

6.0 TUTOR-MARKED ASSIGNMENT

1. Compare the OSI model with the TCP/IP model.

7.0 REFERENCES/FURTHER READING

Computer Networks, Fourth Edition, Andrew S.Tanenbaum, Prentice Hall, ISBN: 0130661023.

MODULE 3 ANALOG AND DIGITAL SIGNAL TRANSMISSION

Unit 1 Analog Signal
Unit 2 Digital Signal

UNIT 1 ANALOG SIGNAL PROCESSING

CONTENTS

1.0 Introduction

Analog signal processing is any signal processing conducted on analog signals by analog means. "Analog" indicates something that is mathematically represented as a set of continuous values. This differs from "digital" which uses a series of discrete quantities to represent signal. Analog values are typically represented as a voltage, electric current, or electric charge around components in the electronic devices. An error or noise affecting such physical quantities will result in a corresponding error in the signals represented by such physical quantities.

Examples of analog signal processing include crossover filters in loudspeakers, "bass", "treble" and "volume" controls on stereos, and "tint" controls on TVs. Common analog processing elements include capacitors, resistors, inductors and transistors.

2.0 Objectives

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

- Explain Analog Signal processing
- Discus tools used in analog signal processing
- Discuss Domains
- Explain Signals
- Discuss Systems

3.1 Tools used in analog signal processing

A system's behavior can be mathematically modeled and is represented in the time domain as h(t) and in the frequency domain as H(s), where s is a complex number in the form of s = a+ib, or s = a+jb in electrical engineering terms (electrical engineers use j because current is

represented by the variable i). Input signals are usually called x(t) or X(s) and output signals are usually called y(t) or Y(s).

3.1.1 Convolution

Convolution is the basic concept in signal processing that states an input signal can be combined with the system's function to find the output signal. It is the integral of the product of two waveforms after one has reversed and shifted; the symbol for convolution is *.

$$y(t) = (x * h)(t) = \int_a^b x(\tau)h(t-\tau)\,d\tau$$

That is the convolution integral and is used to find the convolution of a signal and a system; typically a = -∞ and b = +∞.

Consider two waveforms f and g. By calculating the convolution, we determine how much a reversed function g must be shifted along the xaxis to become identical to function f. The convolution function essentially reverses and slides function g along the axis, and calculates the integral of their (f and the reversed and shifted g) product for each possible amount of sliding. When the functions match, the value of (f*g) is maximized. This occurs because when positive areas (peaks) or negative areas (troughs) are multiplied, they contribute to the integral.

3.1.2 Fourier transform

The Fourier transform is a function that transforms a signal or system in the time domain into the frequency domain, but it only works for certain ones. The constraint on which systems or signals can be transformed by the Fourier Transform is that:

$$\int_{-\infty}^{\infty} |x(t)|\,dt < \infty$$

This is the Fourier transform integral:

$$X(j\omega) = \int_{-\infty}^{\infty} x(t)e^{-j\omega t}\,dt$$

Most of the time the Fourier transform integral isn't used to determine the transform. Usually a table of transform pairs is used to find the Fourier transform of a signal or system. The inverse Fourier transform is used to go from frequency domain to time domain:

$$x(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} X(j\omega)e^{j\omega t}\,d\omega$$

Each signal or system that can be transformed has a unique Fourier transform; there is only one time signal and one frequency signal that goes together. **3.1.3 Laplace transform**

The Laplace transform is a generalized Fourier transform. It allows a transform of any system or signal because it is a transform into the complex plane instead of just the jω line like the Fourier transform. The major difference is that the Laplace transform has a region of convergence for which the transform is valid. This implies that a signal in frequency may have more than one signal in time; the correct time

signal for the transform is determined by the region of convergence. If the region of convergence includes the jω axis, jω can be substituted into the Laplace transform for s and it's the same as the Fourier transform.

The Laplace transform is:

$$X(s) = \int_{-\infty}^{\infty} x(t)e^{-st}\,dt$$

and the inverse Laplace transform is:

$$x(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} X(s)e^{st}\,ds$$

3.1.4 Bode plots

Bode plots are plots of magnitude vs. frequency and phase vs. frequency for a system. The magnitude axis is in Decibel (dB). The phase axis is in either degrees or radians. The frequency axes are in a logarithmic scale. These are useful because for sinusoidal inputs, the output is the input multiplied by the value of the magnitude plot at the frequency and shifted by the value of the phase plot at the frequency.

3.2 Domains

3.2.1 Time domain

This is the domain that most people are familiar with. A plot in the time domain shows the magnitude of a signal at a point in time.

3.2.12 Frequency domain

This is the domain that engineers are glad exists. It's unfamiliar to most people, but makes the math associated with analog signal processing much easier than if it's analyzed in the time domain. A plot in the frequency domain shows either the phase shift or magnitude of a signal at each frequency that it exists at. These can be found by taking the Fourier transform of a time signal and are plotted similarly to a bode plot.

3.3 Signals

While any signal can be used in analog signal processing, there are many **types of signals** that are used very frequently.

3.3.1 Sinusoids

Sinusoids are the building block of analog signal processing. Theorem states that all real world signals can be represented by a sum of sinusoids. A sinusoid can be represented by a complex exponential, e^{st}.

3.3.2 Impulse

An impulse (Dirac delta function) is defined as a signal that has an infinite magnitude and an infinitesimally narrow width with an area under it of one, centered at zero. An impulse can be represented as an infinite sum of sinusoids that includes all possible frequencies. It is not, in reality, possible to generate such a signal, but it can be sufficiently approximated with a large amplitude, narrow pulse, to produce the theoretical impulse response in a network to a high degree of accuracy. The symbol for an impulse is δ(t). If an impulse is used as an input to a system, the output is known as the impulse response. The impulse response defines the system because all possible frequencies are represented in the input.

3.3.3 Step

A unit step function, also called the Heaviside step function, is a signal that has a magnitude of zero before zero and a magnitude of one after zero. The symbol for a unit step is u(t). If a step is used as the input to a system, the output is called the step response. The step response shows how a system responds to a sudden input, similar to turning on a switch. The period before the output stabilizes is called the transient part of a signal. The step response can be multiplied with other signals to show how the system responds when an input is suddenly turned on. The unit step function is related to the Dirac delta function by;

$$\mathrm{u}(t) = \int \delta(t).dt$$

3.4 Systems

3.4.1 Linear time-invariant (LTI)

Linearity means that if you have two inputs and two corresponding outputs, if you take a linear combination of those two inputs you will get a linear combination of the outputs. An example of a linear system is a first order low-pass or high-pass filter. Linear systems are made out of analog devices that demonstrate linear properties. These devices don't have to be entirely linear, but must have a region of operation that is linear. An operational amplifier is a non-linear device, but has a region of operation that is linear, so it can be modeled as linear within that region of operation. Time-invariance means it doesn't matter when you start a system, the same output will result. For example, if you have a system and put an input into it today, you would get the same output if you started the system tomorrow instead. There aren't any real systems that are LTI, but many systems can be modeled as LTI for simplicity in determining what their output will be. All systems have

some dependence on things like temperature, signal level or other factors that cause them to be non-linear or non-time-invariant, but most are stable enough to model as LTI. Linearity and time-invariance are important because they are the only types of systems that can be easily solved using conventional analog signal processing methods. Once a system becomes non-linear or non-time-invariant, it becomes a non-linear differential equations problem, and there are very few of those that can actually be solved. (Haykin & Van Veen 2003)

3.4.2 Common systems

Some common systems used in everyday life are filters, AM/FM radio, electric guitars and musical instrument amplifiers. Filters are used in almost everything that has electronic circuitry. Radio and television are good examples of everyday uses of filters. When a channel is changed on an analog television set or radio, an analog filter is used to pick out the carrier frequency on the input signal. Once it's isolated, the television or radio information being broadcast is used to form the picture and/or sound. Another common analog system is an electric guitar and its amplifier. The guitar uses a magnet with a coil wrapped around it (inductor) to turn the vibration of the strings into a small electric current. The current is then filtered, amplified and sent to a speaker in the amplifier. Most amplifiers are analog because they are easier and cheaper to make than making a digital amplifier. There are also many analog guitar effects pedals, although a large number of pedals are now digital (they turn the input current into a digitized value, perform an operation on it, then convert it back into an analog signal).

4.0 Conclusion

Analog" indicates something that is mathematically represented as a set of continuous values. This differs from "digital" which uses a series of discrete quantities to represent signal. Analog values are typically represented as a voltage, electric current, or electric charge around components in the electronic devices.

5.0 Summary

Input signals are usually called x(t) or X(s) and output signals are usually called y(t) or Y(s).

Convolution is the basic concept in signal processing that states an input signal can be combined with the system's function to find the output signal.

The Fourier transform is a function that transforms a signal or system in the time domain into the frequency domain, but it only works for certain ones. The constraint on which systems or signals can be transformed by the Fourier Transform is that: Most of the time the

Fourier transform integral isn't used to determine the transform. Usually a table of transform pairs is used to find the Fourier transform of a signal or system. The inverse Fourier transform is used to go from frequency domain to time domain:

Each signal or system that can be transformed has a unique Fourier transform; there is only one time signal and one frequency signal that goes together.

The Laplace transform is a generalized Fourier transform. Bode plots are plots of magnitude vs. frequency and phase vs. frequency for a system.
A plot in the time domain shows the magnitude of a signal at a point in time.
While any signal can be used in analog signal processing, there are many types of signals that are used very frequently.
Sinusoids are the building block of analog signal processing. If an impulse is used as an input to a system, the output is known as the impulse response. The impulse response defines the system because all possible frequencies are represented in the input.
If a step is used as the input to a system, the output is called the step response. The step response can be multiplied with other signals to show how the system responds when an input is suddenly turned on. Linear systems are made out of analog devices that demonstrate linear properties.

6.0 TMA

1 . Write the Laplace transform and the inverse Laplace transform.

7.0 Reference & Further Reading

- Haykin, Simon, and Barry Van Veen. Signals and Systems. 2nd ed. Hoboken, NJ: John Wiley and Sons, Inc., 2003.
-
- McClellan, James H., Ronald W. Schafer, and Mark A. Yoder. Signal Processing First. Upper Saddle River, NJ: Pearson Education, Inc., 2003.

Unit 2 Digital Signal Processing (DSP)

1.0 Introduction
2.0 Objectives
3.0 Main content
3.1 DSP domains
3.2 Domains
3.3 Signal Sampling

1.0 Introduction

Digital signal processing (DSP) is concerned with the representation of the signals by a sequence of numbers or symbols and the processing of these signals. Digital signal processing and analog signal processing are subfields of signal processing. DSP includes subfields like: audio and speech signal processing, sonar and radar signal processing, sensor array processing, spectral estimation, statistical signal processing, digital image processing, signal processing for communications, biomedical signal processing, seismic data processing, etc.

Since the goal of DSP is usually to measure or filter continuous realworld analog signals, the first step is usually to convert the signal from an analog to a digital form, by using an analog to digital converter. Often, the required output signal is another analog output signal, which requires a digital to analog converter. Even if this process is more complex than analog processing and has a discrete value range, the stability of digital signal processing thanks to error detection and correction and being less vulnerable to noise makes it advantageous over analog signal processing for many, though not all, applications.

DSP algorithms have long been run on standard computers, on specialized processors called digital signal processors (DSPs), or on purpose-built hardware such as application-specific integrated circuit (ASICs). Today there are additional technologies used for digital signal processing including more powerful general purpose microprocessors, field-programmable gate arrays (FPGAs), digital signal controllers (mostly for industrial apps such as motor control), and stream processors, among others.

2.0 Objectives

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

- Explain Digital Signal Processing
- Explain Digital Signal Domain

- Discuss Signal sampling
- Discuss Time and Space Domains
- Explain Frequency Domain

3.1 DSP domains

In DSP, engineers usually study digital signals in one of the following domains: time domain (one-dimensional signals), spatial domain (multidimensional signals), frequency domain, autocorrelation domain, and wavelet domains. They choose the domain in which to process a signal by making an informed guess (or by trying different possibilities) as to which domain best represents the essential characteristics of the signal. A sequence of samples from a measuring device produces a time or spatial domain representation, whereas a discrete Fourier transform produces the frequency domain information, that is the frequency spectrum. Autocorrelation is defined as the cross-correlation of the signal with itself over varying intervals of time or space.

3.2 Signal sampling

With the increasing use of computers the usage of and need for digital signal processing has increased. In order to use an analog signal on a computer it must be digitized with an analog to digital converter (**ADC**). Sampling is usually carried out in two stages, discretization and quantization. In the discretization stage, the space of signals is partitioned into equivalence classes and quantization is carried out by replacing the signal with representative signal of the corresponding equivalence class. In the quantization stage the representative signal values are approximated by values from a finite set.
The Nyquist–Shannon sampling theorem states that a signal can be exactly reconstructed from its samples if the sampling frequency is greater than twice the highest frequency of the signal. In practice, the sampling frequency is often significantly more than twice the required bandwidth.

A digital to analog converter (DAC) is used to convert the digital signal back to analog. The use of a digital computer is a key ingredient in digital control systems.

3.3 Time and space domains

The most common processing approach in the time or space domain is enhancement of the input signal through a method called filtering. Filtering generally consists of some transformation of a number of surrounding samples around the current sample of the input or output signal. There are various ways to characterize filters; for example:

- A "linear" filter is a linear transformation of input samples; other filters are "non-linear." Linear filters satisfy the superposition condition, i.e. if an input is a weighted linear combination of different signals, the output is an equally weighted linear combination of the corresponding output signals.
- A "causal" filter uses only previous samples of the input or output signals; while a "non-causal" filter uses future input samples. A non-causal filter can usually be changed into a causal filter by adding a delay to it.
- A "time-invariant" filter has constant properties over time; other filters such as adaptive filters change in time.
- Some filters are "stable", others are "unstable". A stable filter produces an output that converges to a constant value with time, or remains bounded within a finite interval. An unstable filter can produce an output that grows without bounds, with bounded or even zero input.
- A "finite impulse response" (FIR) filter uses only the input signal, while an "infinite impulse response" filter (IIR) uses both the input signal and previous samples of the output signal. FIR filters are always stable, while IIR filters may be unstable.

Most filters can be described in Z-domain (a superset of the frequency domain) by their transfer functions. A filter may also be described as a difference equation, a collection of zeroes and poles or, if it is an FIR filter, an impulse response or step response. The output of an FIR filter to any given input may be calculated by convolving the input signal with the impulse response. Filters can also be represented by block diagrams which can then be used to derive a sample processing algorithm to implement the filter using hardware instructions.

3.4 Frequency domain

Signals are converted from time or space domain to the frequency domain usually through the Fourier transform. The Fourier transform converts the signal information to a magnitude and phase component of each frequency. Often the Fourier transform is converted to the power spectrum, which is the magnitude of each frequency component squared.
The most common purpose for analysis of signals in the frequency domain is analysis of signal properties. The engineer can study the spectrum to determine which frequencies are present in the input signal and which are missing.

Filtering, particularly in non realtime work can also be achieved by converting to the frequency domain, applying the filter and then converting back to the time domain. This is a fast, O(n log n) operation,

and can give essentially any filter shape including excellent approximations to brickwall filters.

There are some commonly used frequency domain transformations. For example, the cepstrum converts a signal to the frequency domain through Fourier transform, takes the logarithm, then applies another Fourier transform. This emphasizes the frequency components with smaller magnitude while retaining the order of magnitudes of frequency components.

Frequency domain analysis is also called *spectrum-* or *spectral analysis*.

3.5 Applications

The main applications of DSP are audio signal processing, audio compression, digital image processing, video compression, speech processing, speech recognition, digital communications, RADAR, SONAR, seismology, and biomedicine. Specific examples are speech compression and transmission in digital mobile phones, room matching equalization of sound in Hifi and sound reinforcement applications, weather forecasting, economic forecasting, seismic data processing, analysis and control of industrial processes, computer-generated animations in movies, medical imaging such as CAT scans and MRI, MP3 compression, image manipulation, high fidelity loudspeaker crossovers and equalization, and audio effects for use with electric guitar amplifiers.

3.6 Implementation and Techniques

Digital signal processing is often implemented using specialised microprocessors such as the DSP56000, the TMS320, or the SHARC. These often process data using fixed-point arithmetic, although some versions are available which use floating point arithmetic and are more powerful. For faster applications FPGAs [3] might be used. Beginning in 2007, multicore implementations of DSPs have started to emerge from companies including Freescale and Stream Processors, Inc. For faster applications with vast usage, ASICs might be designed specifically. For slow applications, a traditional slower processor such as a microcontroller may be adequate.

3.6.1 Techniques

- Bilinear transform
- Discrete Fourier transform
- Discrete-time Fourier transform
- Filter design
- LTI system theory

- Minimum phase
- Transfer function
- Z-transform
- Goertzel algorithm
- s-plane

4.0 Conclusion

With the increasing use of computers the usage of and need for digital signal processing has increased. In order to use an analog signal on a computer it must be digitized with an analog to digital converter (**ADC**).

5.0 Summary

In DSP, engineers usually study digital signals in one of the following domains: time domain (one-dimensional signals), spatial domain (multidimensional signals), frequency domain, autocorrelation domain, and wavelet domains.

The most common processing approach in the time or space domain is enhancement of the input signal through a method called filtering. A "linear" filter is a linear transformation of input samples; other filters are "non-linear." A "causal" filter uses only previous samples of the input or output signals; while a "non-causal" filter uses future input samples. A "time-invariant" filter has constant properties over time; other filters such as adaptive filters change in time.

A "finite impulse response" (FIR) filter uses only the input signal, while an "infinite impulse response" filter (IIR) uses both the input signal and previous samples of the output signal. FIR filters are always stable, while IIR filters may be unstable.

Signals are converted from time or space domain to the frequency domain usually through the Fourier transform. The Fourier transform converts the signal information to a magnitude and phase component of each frequency. The most common purpose for analysis of signals in the frequency domain is analysis of signal properties. Frequency domain analysis is also called *spectrum-* or *spectral analysis*.

The main applications of DSP are audio signal processing, audio compression, digital image processing, video compression, speech processing, speech recognition, digital communications, RADAR, SONAR, seismology, and biomedicine. Bilinear transform.

6.0 TMA

1 . Outline the techniques involved in Digital Signal Processing

7.0 References and Further reading

1. ^ James D. Broesch, Dag Stranneby and William Walker. *Digital Signal Processing: Instant access*. Butterworth-Heinemann. p. 3.
- Jonathan Yaakov Stein, *Digital Signal Processing, a Computer Science Perspective*, Wiley, ISBN 0-471-29546-9

MODULE 4 COMPUTER NETWORKING

Unit 1 Networking Methods
Unit 2 Network Topology
Unit 3 VOIP

UNIT 1 NETWORKING METHODS and DEVICES

CONTENTS

1.0 INTRODUCTION

Networking is a complex part of computing that makes up most of the IT Industry. Without networks, almost all communication in the world would cease to happen. It is because of networking that telephones, televisions, the Computer networking devices are units that mediate data in a computer network.. Computer networking devices are also called network equipment, Intermediate Systems (IS) or InterWorking Unit (IWU). Units which are the last receiver or generate data are called hosts or data terminal equipment internet, etc. work.

2.0 OBJECTIVES

At the end of this unit you should be able to;

- Networking Methods
- Network Devices

3.1 NETWORKING METHODS

One way to categorize computer networks is by their geographic scope, although many real-world networks interconnect Local Area Networks (LAN) via Wide Area Networks (WAN) and wireless networks[WWAN]. These three (broad) types are:

3.1.1 LOCAL AREA NETWORK (LAN)

A local area network is a network that spans a relatively small space and provides services to a small number of people.

A peer-to-peer or client-server method of networking may be used. A peer-to-peer network is where each client shares their resources with other workstations in the network. Examples of peer-to-peer networks are: Small office networks where resource use is minimal and a home network. A client-server network is where every client is connected to

the server and each other. Client-server networks use servers in different capacities. These can be classified into two types:

1. Single-service servers
2. print server, where the server performs one task such as file server, ; while other servers can not only perform in the capacity of file servers and print servers, but they also conduct calculations and use these to provide information to clients (Web/Intranet Server). Computers may be connected in many different ways, including Ethernet cables, Wireless networks, or other types of wires such as power lines or phone lines. The ITU-T G.hn standard is an example of a technology that provides high-speed (up to 1 Gbit/s) local area networking over existing home wiring (power lines, phone lines and coaxial cables).

3.1.2 WIDE AREA NETWORK (WAN)

A wide area network is a network where a wide variety of resources are deployed across a large domestic area or internationally. An example of this is a multinational business that uses a WAN to interconnect their offices in different countries. The largest and best example of a WAN is the Internet, which is a network composed of many smaller networks. The Internet is considered the largest network in the world. The PSTN (Public Switched Telephone Network) also is an extremely large network that is converging to use Internet technologies, although not necessarily through the public Internet.

A Wide Area Network involves communication through the use of a wide range of different technologies. These technologies include Pointto-Point WANs such as Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC), Frame Relay, ATM (Asynchronous Transfer Mode) and Sonet (Synchronous Optical Network). The difference between the WAN technologies is based on the switching capabilities they perform and the speed at which sending and receiving bits of information (data) occur.

3.1.3 METROPOLITAN AREA NETWORK (MAN)

A metropolitan network is a network that is too large for even the largest of LAN's but is not on the scale of a WAN. It also integrates two or more LAN networks over a specific geographical area (usually a city) so as to increase the network and the flow of communications. The LAN's in question would usually be connected via "backbone" lines.

3.1.4 WIRELESS NETWORKS (WLAN, WWAN)

A wireless network is basically the same as a LAN or a WAN but there are no wires between hosts and servers. The data is transferred over sets of radio transceivers. These types of networks are beneficial when it is too costly or inconvenient to run the necessary cables. For more

information, see Wireless LAN and Wireless wide area network. The media access protocols for LANs come from the IEEE.

The most common IEEE 802.11 WLANs cover, depending on antennas, ranges from hundreds of meters to a few kilometers. For larger areas, either communications satellites of various types, cellular radio, or wireless local loop (IEEE 802.16) all have advantages and disadvantages. Depending on the type of mobility needed, the relevant standards may come from the IETF or the ITU.

3.2 COMPUTER NETWORKING DEVICE

3.2.1 Common Basic Networking Devices :

- **Gateway :** device sitting at a network node for interfacing with another network that uses different protocols. Works on OSI layers 4 to 7.
- **Router :** a specialized network device that determines the next network point to which to forward a data packet toward its destination. Unlike a gateway, it cannot interface different protocols. Works on OSI layer 3.
- **Bridge :** a device that connects multiple network segments along the data link layer. Works on OSI layer 2.
- **Switch :** a device that allocates traffic from one network segment to certain lines (intended destination(s)) which connect the segment to another network segment. So unlike a hub a switch splits the network traffic and sends it to different destinations rather than to all systems on the network. Works on OSI layer 2.
- **Hub :** connects multiple Ethernet segments together making them act as a single segment. When using a hub, every attached device shares the same broadcast domain and the same collision domain. Therefore, only one computer connected to the hub is able to transmit at a time. Depending on the network topology, the hub provides a basic level 1 OSI model connection among the network objects (workstations, servers, etc). It provides bandwidth which is shared among all the objects, compared to switches, which provide a dedicated connection between individual nodes. Works on OSI layer 1.
- **Repeater :** device to amplify or regenerate digital signals received while setting them from one part of a network into another. Works on OSI layer 1.

3.2.2 Hybrid Network Devices :

- **Multilayer Switch :** a switch which, in addition to switching on OSI layer 2, provides functionality at higher protocol layers.

- **Protocol Converter :** a hardware device that converts between two different types of transmissions, such as asynchronous and synchronous transmissions.
- **Bridge Router (Brouter):** Combine router and bridge functionality and are therefore working on OSI layers 2 and 3.
- Digital media receiver : Connects a computer network to a home theatre

3.2.3 Software for Networks or Dial-up connections :

- **Proxy :** computer network service which allows clients to make indirect network connections to other network services
- **Firewall :** a piece of hardware or software put on the network to prevent some communications forbidden by the network policy
- **Network Address Translator :** network service provide as hardware or software that converts internal to external network addresses and vice versa

3.2.4 Other Hardware for Networks or Dial-up connections :

- **Multiplexer :** device that combines several electrical signals into a single signal
- **Network Card :** a piece of computer hardware to allow the attached computer to communicate by network
- **Modem :** device that modulates an analog "carrier" signal (such as sound), to encode digital information, and that also demodulates such a carrier signal to decode the transmitted information, as a computer communicating with another computer over the telephone network
- **ISDN terminal adapter (TA):** a specialized gateway for ISDN
- **Line Driver :** a device to increase transmission distance by amplifying the signal. Base-band networks only.

4.0 Conclusion

Without networks, almost all communication in the world would cease to happen. Computer networking devices mediate data in a computer network.

5.0 Summary

It is because of networking that telephones, televisions, the Computer networking devices are units that mediate data in a computer network. Computer networking devices are also called network equipment, Intermediate Systems (IS) or InterWorking Unit (IWU). Networking Methods.

One way to categorize computer networks is by their geographic scope, although many real-world networks interconnect Local Area Networks (LAN) via Wide Area Networks (WAN) and wireless networks[WWAN].

Common Basic Networking Devices:

Gateway: device sitting at a network node for interfacing with another network that uses different protocols. Works on OSI layer 3.

Bridge: a device that connects multiple network segments along the data link layer. Works on OSI layer 2.

Switch: a device that allocates traffic from one network segment to certain lines (intended destination(s)) which connect the segment to another network segment. Depending on the network topology, the hub provides a basic level 1 OSI model connection among the network objects (workstations, servers, etc).

Hybrid Network Devices:

Digital media receiver: Connects a computer network to a home theatre Software for Networks or Dial-up connections:

Proxy: computer network service which allows clients to make indirect network connections to other network services.

Network Address Translator: network service provide as hardware or software that converts internal to external network addresses and vice versa.

Other Hardware for Networks or Dial-up connections:
Network Card: a piece of computer hardware to allow the attached computer to communicate by network.

6.0 Tutor-Marked Assignment

1 . List and define five Common Basic Networking Devices **7.0**

References/Further Reading

http://en.wikipedia.org/wiki/DARPA
http://www.darpa.mil/DARPA50thevent/history.html

UNIT 2 NETWORK TOPOLOGY

CONTENTS

1.0 INTRODUCTION

The network topology defines the way in which computers, printers, and other devices are connected, physically and logically. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.

2.0 OBJECTIVES

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

Explain Bus, Ring, Star, Tree and mesh network Topologies.

3.2 NETWORK TOPOLOGY

Network topology has two types:

- Physical
- logical

Commonly used topologies include:

- Bus
- Star
- Tree (hierarchical)
- Linear
- Ring
- Mesh
    - partially connected
    - fully connected (sometimes known as *fully redundant*) The network topologies mentioned above are only a general representation of the kinds of topologies used in computer network and are considered basic topologies.

3.2.1 Topology in Network Design

Think of a topology as a network's virtual shape or structure. This shape does not necessarily correspond to the actual physical layout of the devices on the

network. For example, the computers on a home LAN may be arranged in a circle in a family room, but it would be highly unlikely to find a ring topology there.

Network topologies are categorized into the following basic types:

- bus
- ring
- star
- tree
- mesh

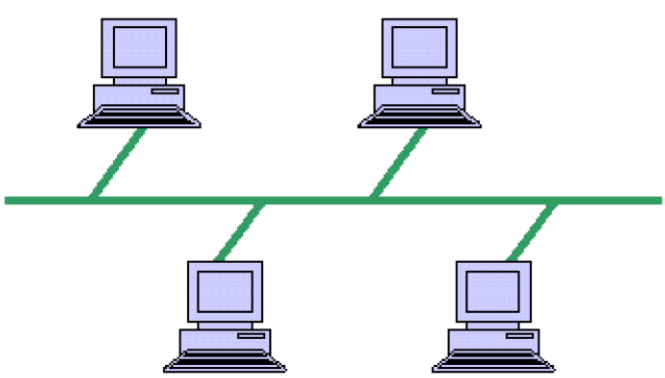
More complex networks can be built as hybrids of two or more of the above basic topologies.

3.2.1.1 Bus Topology

Bus networks (not to be confused with the system bus of a computer) use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

Ethernet bus topologies are relatively easy to install and don't require much cabling compared to the alternatives. 10Base-2 ("ThinNet") and 10Base-5 ("ThickNet") both were popular Ethernet cabling options many years ago for bus topologies. However, bus networks work best with a limited number of devices. If more than a few dozen computers are added to a network bus, performance problems will likely result. In addition, if the backbone cable fails, the entire network effectively becomes unusable.

This diagram illustrates the bus network topology. A bus topology such as 10Base-2 or 10Base-5 Ethernet uses a single communication backbone for all devices. Bus Network Topology

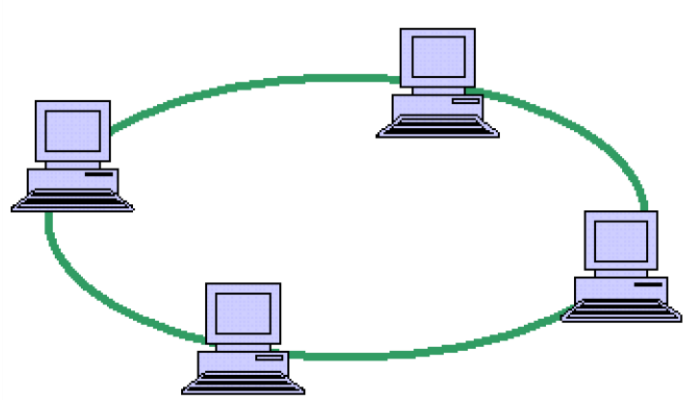


3.2.1.2 Ring Topology

In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or device breaks the loop and can take down the entire network.

To implement a ring network, one typically uses FDDI, SONET, or Token Ring technology. Ring topologies are found in some office buildings or school campuses.

This diagram illustrates the ring network topology. A ring topology such as FDDI or SONET sends messages clockwise or counterclockwise through the shared link.



Ring Network Topology

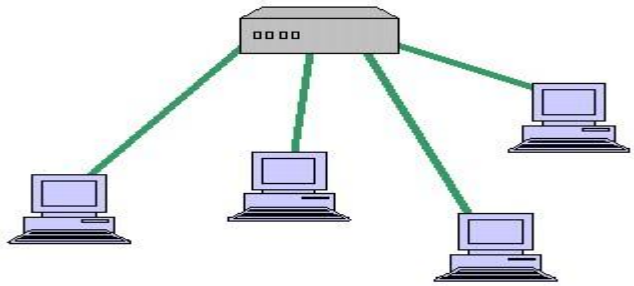
3.2.1.3 STAR TOPOLOGY

Many home networks use the star topology. A star network features a central connection point called a "hub" that may be a hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.

Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one

computer's network access and not the entire LAN. (If the hub fails, however, the entire network also fails.)

This diagram illustrates the star network topology. A star topology typically uses a network hub or switch and is common in home networks.

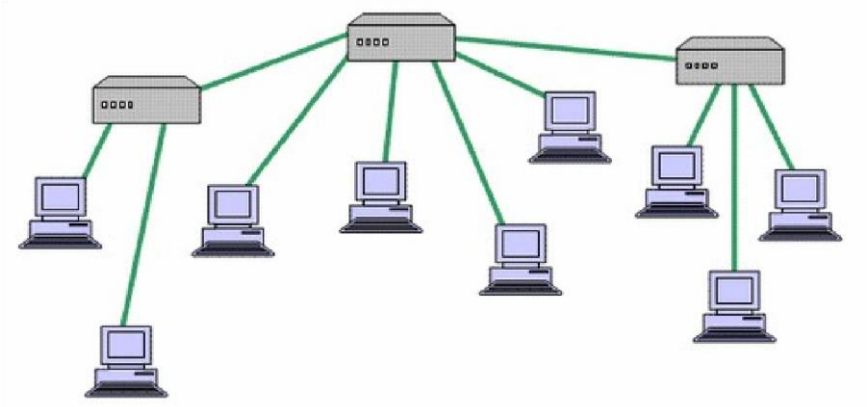


Star Network Topology

3.2.1.4 TREE TOPOLOGY

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the "root" of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.

This diagram illustrates the tree network topology. A tree topology integrates the star and bus topologies in a hybrid approach to improve network scalability.



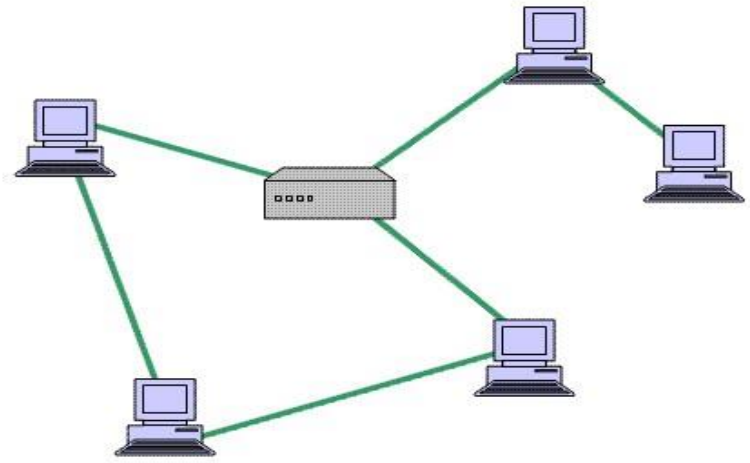
Tree Network Topology

3.2.1.5 MESH TOPOLOGY

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths exist, messages can only travel in one direction.) Some WANs, most notably the Internet, employ mesh routing.

A mesh network in which every device connects to every other is called a full mesh. As shown in the illustration below, partial mesh networks also exist in which some devices connect only indirectly to others.

This diagram illustrates the mesh network topology. A mesh topology provides redundant communication paths between some or all devices (partial or full mesh).



Mesh Network Topology

4.0 Conclusion

The network topologies mentioned in this unit are only a general representation of the kinds of topologies used in computer network and are considered basic topologies. They are; Bus, Ring, Star, Tree, Mesh.

5.0 Summary

Network topology has two types:

- Physical
- logical

Commonly used topologies include:

- Bus
- Star
- Tree (hierarchical)
- Linear

- Ring
- Mesh
    - partially connected
    - fully connected (sometimes known as *fully redundant*) The network topologies mentioned above are only a general representation of the kinds of topologies used in computer network and are considered basic topologies.

6.0 TMA

1. what is Network Topology?
2. Explain the Mesh Network Topology

7.0 Reference & Further reading

http://en.wikipedia.org/wiki/DARPA
http://www.darpa.mil/DARPA50thevent/history.html

UNIT 3 VOICE OVER INTERNET PROTOCOL (VOIP)

CONTENTS

1.0 Introduction

Internet telephony refers to communications services—voice, facsimile, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). The basic steps involved in originating an Internet telephone call are conversion of the analog voice signal to digital format and compression/ translation of the signal into Internet protocol (IP) packets for transmission over the Internet; the process is reversed at the receiving end.

2.0 Objectives

At the end of this unit we should be able to;
- Discourse Internet Telephony
- Explain the Technical Barriers in VOIP
- discourse the future of VOIP

3.0 . Internet Telephony

Although progressing rapidly, Internet telephony still has some problems with reliability and sound quality, due primarily to limitations both in Internet bandwidth and current compression technology. As a result, most corporations looking to reduce their phone bills today confine their Internet-telephony applications to their intranets. With more predictable bandwidth available than the public Internet, intranets can support full-duplex, real-time voice communications. Corporations generally limit their Internet voice traffic to half-duplex asynchronous applications (e.g., voice messaging).

Internet telephony within an intranet enables users to save on longdistance bills between sites; they can make point-to-point calls via gateway servers attached to the local-area network (LAN). No PC–based telephony software or Internet account is required.

For example, User A in New York wants to make a (point-to-point) phone call to User B in the company's Geneva office. He picks up the phone and dials an extension to connect with the gateway server, which is equipped with a telephony board and compression-conversion software; the server configures the private branch exchange (PBX) to digitize the upcoming call. User A then dials the number of the London office, and the gateway server transmits the (digitized, IP–packetized) call over the IP–based wide-area network (WAN) to the gateway at the Geneva end. The Geneva gateway converts the digital signal back to analog format and delivers it to the called party.

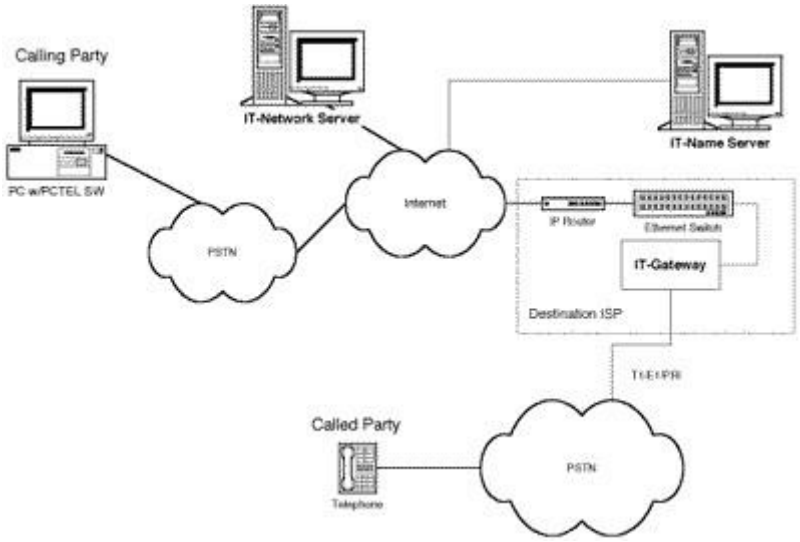


Figure 7. PC–to-Phone Connection

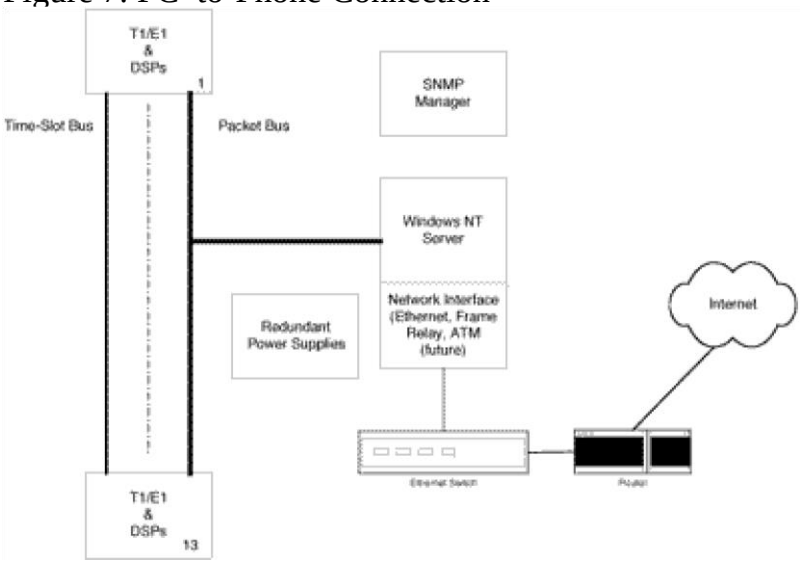


Figure 8. Internet Telephony Gateway

This version of Internet telephony also enables companies to transmit their (digitized) voice and data traffic together over the intranet in support of shared applications and white boarding.

3.1 Technical Barriers

The ultimate objective of Internet telephony is, of course, reliable, highquality voice service, the kind that users expect from the PSTN. At the moment, however, that level of reliability and sound quality is not available on the Internet, primarily because of bandwidth limitations that lead to packet loss. In voice communications, packet loss shows up in the form of gaps or periods of silence in the conversation, leading to a clipped-speech effect that is unsatisfactory for most users and unacceptable in business communications.

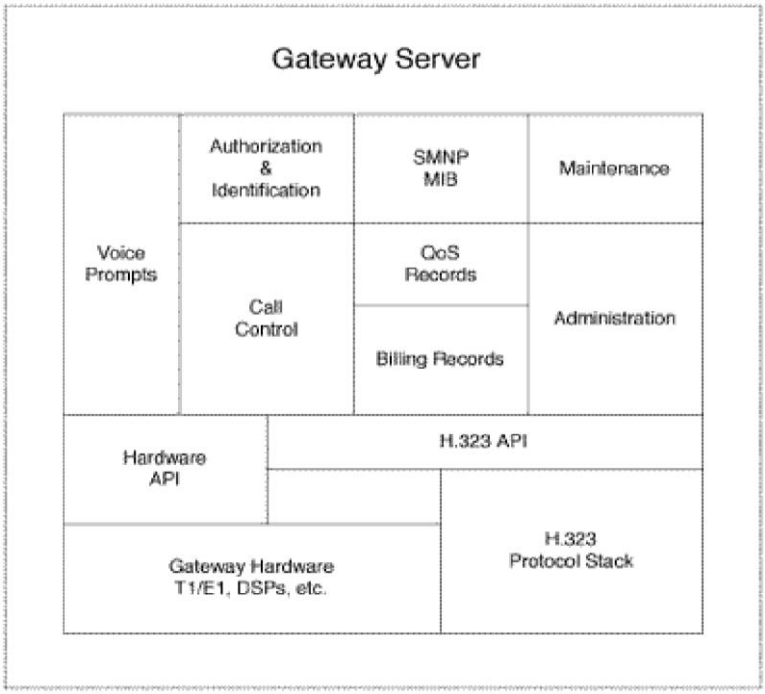


Figure 9. Internet Telephony

The Internet, a collection of more than 130,000 networks, is gaining in popularity as millions of new users sign on every month. The increasingly heavy use of the Internet's limited bandwidth often results in congestion which, in turn, can cause delays in packet transmission. Such network delays mean packets are lost or discarded.

In addition, because the Internet is a packet-switched or connectionless network, the individual packets of each voice signal travel over separate network paths for reassembly in the proper sequence at their ultimate destination. While this makes for a more efficient use of network resources than the circuit-switched PSTN, which routes a call over a single path, it also increases the chances for packet loss.

Network reliability and sound quality also are functions of the voiceencoding techniques and associated voice-processing functions of the gateway servers. To date, most developers of Internet-telephony software, as well as vendors of gateway servers, have been using a variety of speech-compression protocols. The use of various speechcoding algorithms—with their different bit rates and mechanisms for reconstructing voice packets and handling delays—produces varying levels of intelligibility and fidelity in sound transmitted over the Internet. The lack of standardized protocols also means that many Internet-telephony products do not interoperate with each other or with the PSTN.

3.1 Standards

Over the next few years, the industry will address the bandwidth limitations by upgrading the Internet backbone to asynchronous transfer mode (ATM), the switching fabric designed to handle voice, data, and video traffic. Such network optimization will go a long way toward eliminating network congestion and the associated packet loss. The Internet industry also is tackling the problems of network reliability and sound quality on the Internet through the gradual adoption of standards. Standards-setting efforts are focusing on the three central elements of Internet telephony: the audio codec format; transport protocols; and directory services.

In May 1996, the International Telecommunications Union (ITU) ratified the H.323 specification, which defines how voice, data, and video traffic will be transported over IP–based local area networks; it also incorporates the T.120 data-conferencing standard (see Figure 10). The recommendation is based on the real-time protocol/real-time control protocol (RTP/RTCP) for managing audio and video signals.

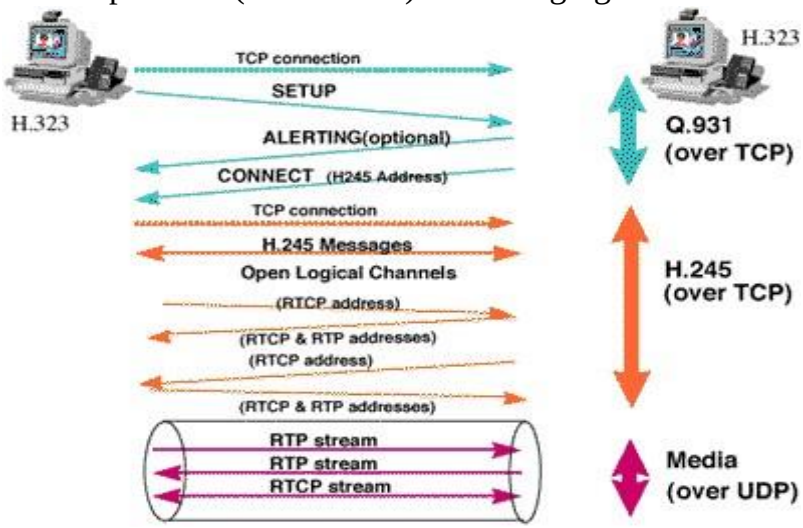


Figure 10. H.323 Call Sequence

As such, H.323 addresses the core Internet-telephony applications by defining how delay-sensitive traffic, (i.e., voice and video), gets priority

transport to ensure real-time communications service over the Internet. (The H.324 specification defines the transport of voice, data, and video over regular telephony networks, while H.320 defines the protocols for transporting voice, data, and video over integrated services digital network (ISDN).

H.323 is a set of recommendations, one of which is G.729 for audio codecs, which the ITU ratified in November 1995. Despite the ITU recommendation, however, the Voice over IP (VoIP) Forum in March 1997 voted to recommend the G.723.1 specification over the G.729 standard. The industry consortium, which is led by Intel and Microsoft, agreed to sacrifice some sound quality for the sake of greater bandwidth efficiency—G.723.1 requires 6.3 kbps, while G.729 requires 7.9 kbps. Adoption of the audio codec standard, while an important step, is expected to improve reliability and sound quality mostly for intranet traffic and point-to-point IP connections. To achieve PSTN–like quality, standards are required to guarantee Internet connections.

The transport protocol RTP, on which the H.323 recommendation is based, essentially is a new protocol layer for real-time applications; RTP–compliant equipment will include control mechanisms for synchronizing different traffic streams. However, RTP does not have any mechanisms for ensuring the on-time delivery of traffic signals or for recovering lost packets. RTP also does not address the so-called quality of service (QoS) issue related to guaranteed bandwidth availability for specific applications. Currently, there is a draft signaling-protocol standard aimed at strengthening the Internet's ability to handle real-time traffic reliably (i.e., to dedicate end-to-end transport paths for specific sessions much like the circuit-switched PSTN does). If adopted, the resource reservation protocol (RSVP), will be implemented in routers to establish and maintain requested transmission paths and quality-of-service levels.

Finally, there is a need for industry standards in the area of Internettelephony directory services. Directories are required to ensure interoperability between the Internet and the PSTN, and most current Internet-telephony applications involve proprietary implementations. However, the lightweight directory access protocol (LDAP v3.0) seems to be emerging as the basis for a new standard.

3.4 Future VoIP

Several factors will influence future developments in VoIP products and services. Currently, the most promising areas for VoIP are corporate intranets and commercial extranets. Their IP–based infrastructures enable operators to control who can—and cannot—use

the network. Another influential element in the ongoing Internet-telephony evolution is the VoIP gateway. As these gateways evolve from PC–based platforms to robust embedded systems, each will be able to handle hundreds of simultaneous calls. Consequently, corporations will deploy large numbers of them in an effort to reduce the expenses associated with high-volume voice, fax, and videoconferencing traffic. The economics of placing all traffic— data, voice, and video—over an IP– based network will pull companies in this direction, simply because IP will act as a unifying agent, regardless of the underlying architecture (i.e., leased lines, frame relay, or ATM) of an organization's network.

Commercial extranets, based on conservatively engineered IP networks, will deliver VoIP and facsimile over Internet protocol (FAXoIP) services to the general public. By guaranteeing specific parameters, such as packet delay, packet jitter, and service interoperability, these extranets will ensure reliable network support for such applications.

VoIP products and services transported via the public Internet will be niche markets that can tolerate the varying performance levels of that transport medium. Telecommunications carriers most likely will rely on the public Internet to provide telephone service between/among geographic locations that today are high-tariff areas. It is unlikely that the public Internet's performance characteristics will improve sufficiently within the next two years to stimulate significant growth in VoIP for that medium.

However, the public Internet will be able to handle voice and video services quite reliably within the next three to five years, once two critical changes take place:

- an increase by several orders of magnitude in backbone bandwidth and access speeds, stemming from the deployment of IP/ATM/synchronous optical network (SONET) and ISDN, cable modems, and x digital subscriber line (xDSL) technologies, respectively
- the tiering of the public Internet, in which users will be required to pay for the specific service levels they require

On the other hand, FAXoIP products and services via the public Internet will become economically viable more quickly than voice and video, primarily because the technical roadblocks are less challenging. Within two years, corporations will take their fax traffic off the PSTN and move it quickly to the public Internet and corporate Intranet, first through FAXoIP gateways and then via IP–capable fax machines. Standards for IP–based fax transmission will be in place by the end of this year.

Throughout the remainder of this decade, videoconferencing (H.323) with data collaboration (T.120) will become the normal method of

corporate communications, as network performance and interoperability increase and business organizations appreciate the economics of telecommuting. Soon, the video camera will be a standard piece of computer hardware, for full-featured multimedia systems, as well as for the less-than-$500 network-computer appliances now starting to appear in the market. The latter in particular should stimulate the residential demand and bring VoIP services to the mass market—including the roughly 60 percent of American households that still do not have a PC.

4.0 Conclusion

This unit discussed the ongoing but rapid evolution of Internet telephony, the market forces fueling that evolution and the benefits that users can realize, as well as the underlying technologies. It also examined the hurdles that must be overcome before Internet telephony can be adopted on a widespread basis.

5.0 Summary

Internet telephony refers to communications services—voice, facsimile, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). Corporations generally limit their Internet voice traffic to half-duplex asynchronous applications (e.g., voice messaging).
The Internet industry also is tackling the problems of network reliability and sound quality on the Internet through the gradual adoption of standards. Directories are required to ensure interoperability between the Internet and the PSTN, and most current Internet-telephony applications involve proprietary implementations.

6.0 TUTOR MARKED ASSIGNMENT

1. What is VOIP?
2. Discourse the technical barriers in VOIP

7.0 Reference & Further Reading http://en.wikipedia.org/wiki/DARPA
http://www.darpa.mil/DARPA50thevent/history.html

MODULE 5 TYPES OF COMMUNICATION MEDIA

Unit 1 Guided Media

Unit 2 Unguided Media
Unit 3 Transmission Impairment

UNIT 1 GUIDED MEDIA

CONTENTS

1.0 Introduction

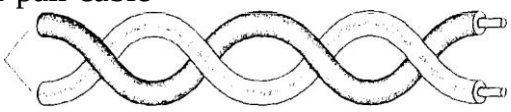
Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

2.0 Objectives

At the end of this unit you should be able to;
- Explain guided media of communication
- Discuss un-guided media of communication

3.1 Twisted-Pair Cable

A twist pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together as shown in figure 7.3. Figure 7.3 Twisted-pair cable



One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

In addition to the signal sent by the sender on one of the wires, interference (muse) and crosstalk may affect both wires and create unwanted signals.

If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are al different locations relative to the noise or crosstalk sources (e.g one is closer and the other is farther). This results in a difference at the receiver. By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is Farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out. From the above discussion, it is clear that the number of twists per unit of length inch) has some effect on the quality of the cable.

3.1.1 Unshielded versus Shielded twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive. Figure 7.4 shows the difference between UTP and STP. Our discussion focuses primarily on UTP because STP is seldom used outside of IBM.

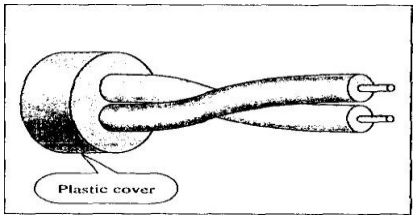
Categories

The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with I as the lowest and 7 as the highest. Each EIA category is suitable lot specific uses. Table 7.1 shows these categories.

Connectors

The most common UTP connector is 8,145 (RJ stands for- registered jack), as shown in Figure 7.5. The 8.145 is a keyed Connector, meaning the connector can be inserted in only one way.

Figure 7.4 UTP *and STP cables*



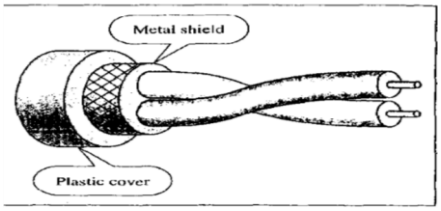


Table *7.1 Categories of unshielded twisted-pair cables*

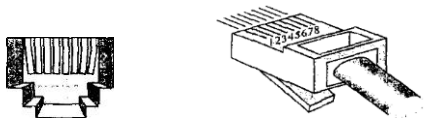
Category	Specification	Data Rate (MBPS)	Use

1	Unshielded twisted-pair used in telephone	<0.1	Telephone
2	Unshielded twisted-pair originally used in T-line	2	T-1 line
3	Improved CAT 2 used in LANS	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that include extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometime called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increase the data rate.		

Performance

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. A twisted-pair cable can pass a wide range of frequencies. However, with increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz. Note that guage is a measure of the thickness of the wire.

Figure 7.5 *UTP connector*



Applications

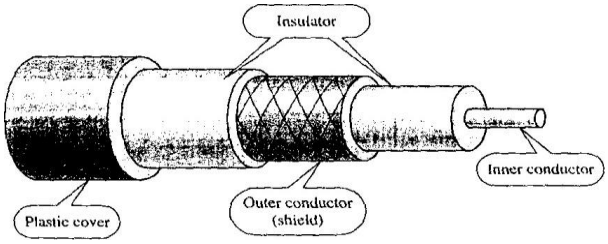
Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office-commonly consists of unshielded twistedpair cables. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

3.2 Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover (see Figure 7.7).

Figure 7.7 Coaxial cable



3.2.1 Coaxial Cable Standards

Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in Table 7.2.

Table 7.2 Categories of coaxial cables

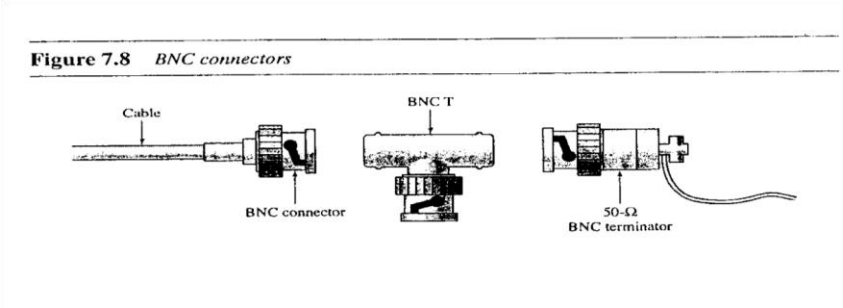
Category	*Impedance*	*Use*
RG-59	75	Cable TV
RG-58	50	Thin Ethernet
RG-11	50	Thick Ethernet

3.2.2 Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-NeillConcelman (13NC), connector. Figure 7.8 shows three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator.

The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

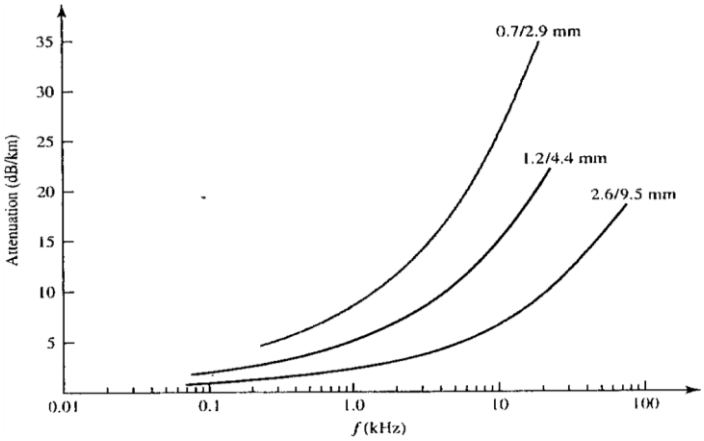
Figure 7.8 BNC Connector



Performance

As we did with twisted-pair cables, we can measure the performance of a coaxial cable. We notice in Figure 7.9 that the attenuation is much higher in coaxial cables than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Figure 7.9 *coaxial cable performances*



Applications

Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiber-optic cable.

Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable.

Another common application of coaxial cable is in traditional Ethernet LANs. Because of its high bandwidth, and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs. The I OBase-2, or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10 Mbps with a range of 185 m. The 10Base5, or Thick Ethernet, uses RG-l l (thick coaxial cable) to transmit 10 Mbps with a range of 5000 m. Thick Ethernet has specialized connectors.

3.3 Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction.

If the angle of incidence I (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface. If the

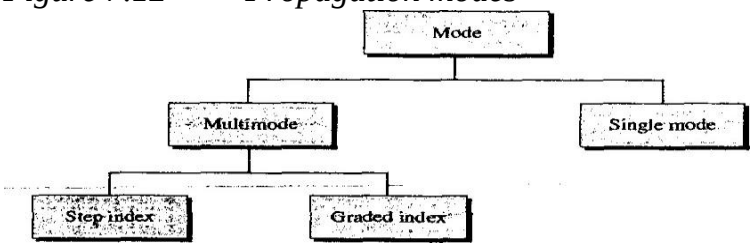
angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance. Note that the critical angle is a property of the substance, and its value differs from one substance to another.

Optical fibers use reflection to guide light through a channel. A glass or plastic-core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

Propagation Modes

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index (see Figure 7.12).

Figure 7.12 Propagation modes



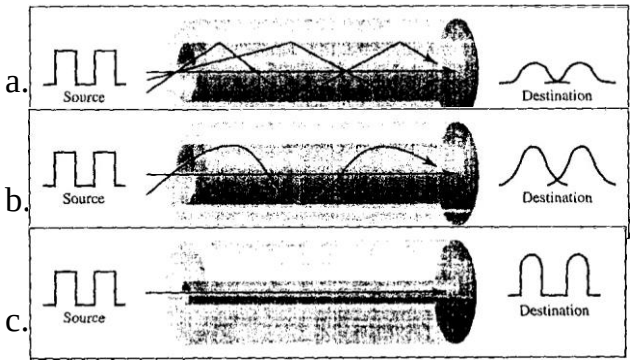
Multimode Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core, as shown in Figure 7.13.

In multimode step-index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term *step index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

A second type of fiber, called multimode graded-index fiber, decreases this distortion of the signal through the cable. The word *index* here refers to the index of refraction. As we saw above, the index of refraction is related to density. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge. Figure 7. 13 shows the impact of this variable density on the propagation of light beams.

Single-Mode Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction). The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible. All the beams arrive at the destination "together" and can be recombined with little distortion to the signal (see Figure 7.13).

Figure 7.13 *Modes*



Fiber Sizes

Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers. The common sizes are shown in Table 7.3. Note that the last size listed is for singlemode only.

Table 7.3 *Fiber types*

Type	*Core(µm)*	*Cladding (µm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

Cable Composition

Figure 7.14 shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the

fiber. The fiber is at the center of the cable, and it consists of cladding and core.

3.3.1 Fiber-Optic Cable Connectors

There are three types of connectors for fiber-optic cables, as shown in Figure 7.15.

Figure 7.14 *Fiber construction*

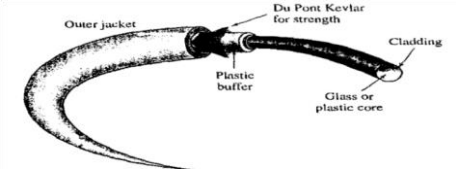
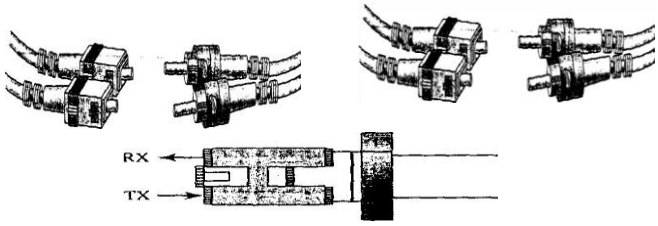


Figure 7.15 *Fiber-optic cable connectors*



The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. MT RJ is a connector that is the same size as RJ45.

Performance

The plot of attenuation versus wavelength shows a very interesting phenomenon in fiber-optic cable. Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer (actually 10 times less) repeaters when we use fiberoptic cable.

Applications

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides the connection to the user premises. This is a cost-effective configuration since the

narrow bandwidth requirement at the user end does not justify the use of optical fiber.

Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000 Base-X also use fiber-optic cable.

3.3.2 Advantages and Disadvantages of Optical Fiber

Advantages Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

- Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.
- Less signal attenuation. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.
- Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.
- Light weight. Fiber-optic cables are much lighter than copper cables.
- Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages.

There are some disadvantages in the use of optical fiber.

- Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- Cost. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

4.0 Conclusion

Guided media, which are those that provide a conduit from one device to another coveys signals in different media which is directed and

contained by the physical limits of the medium. These limitations informs our decision on which media to opt for.

5.0 Summary

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP).

A twisted-pair cable can pass a wide range of frequencies. Twistedpair cables are used in telephone lines to provide voice and data channels.

3.2 Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently.
As we did with twisted-pair cables, we can measure the performance of a coaxial cable.

Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable.

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Optical fibers use reflection to guide light through a channel. A second type of fiber, called multimode graded-index fiber, decreases this distortion of the signal through the cable.

The subscriber channel (SC) connector is used for cable TV. Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides the connection to the user premises. Local-area

networks such as 100Base-FX network (Fast Ethernet) and 1000BaseX also use fiber-optic cable.

Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Less signal attenuation. We need repeaters every 5 km for coaxial or twisted-pair cable. Electromagnetic noise cannot affect fiber-optic cables.

Light weight. Fiber-optic cables are much lighter than copper cables. Fiber-optic cables are more immune to tapping than copper cables. Fiber-optic cable is a relatively new technology. Unidirectional light propagation.

6.0 TMA

1. compare and contrast the guided and unguided media of communication

7.0 Reference & Further Reading

http://en.wikipedia.org/wiki

UNIT 2 UNGUIDED MEDIA: WIRELESS

1.0 Introduction

Unguided media transport electromagnetic waves without using a physical conductor. This type o f communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

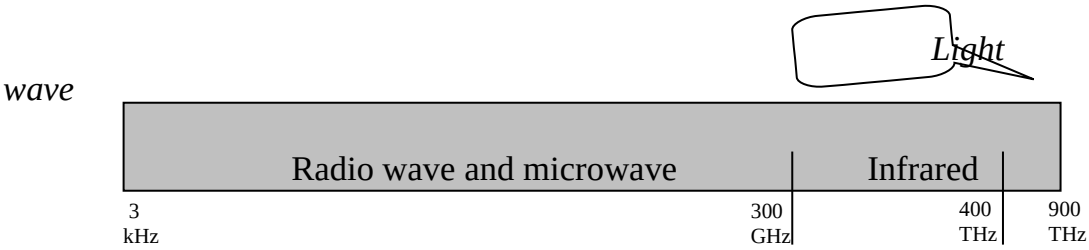
Figure 7.17 shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

2.0 Objectives

At the end of this Unit you should be able to;

- discuss unguided media of network communication
- Explain Radio wavs, Microwaves and Infrared

Figure 7.17: *Electromagnetic spectrum for wireless communication*



Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure 7.18. In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance. In sky propagation, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power. In line-of-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

The section of the electromagnetic spectrum defined as radio waves and microwaves is divided into eight ranges, called *bands*, each regulated by government authorities. These bands are rated from *very low frequency* (VLF) to *extremely high frequency* (EHF). Table 7.4 lists these bands, their ranges, propagation methods, and some applications.

Ground Propagation (Below 2 MHz) Sky Propagation (2-30 MHz) Line-of-sight propagation (above 30 MHz)

Band	*Range*	*Propagation*	*Application*

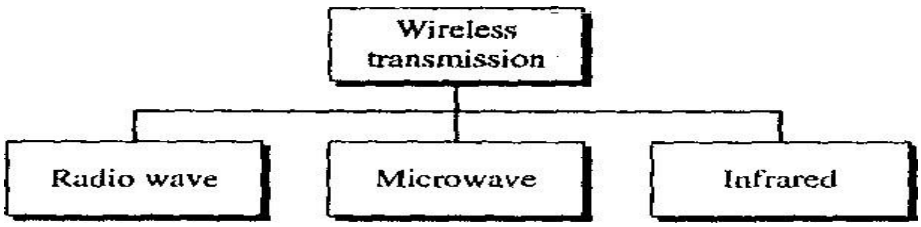
Figure 7.18 Propagation methods

VLF (very low frequency)	3-30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30-300 kHz	Ground	Radio beacons and navigation locators
MF (middle frequency)	300 kHz-3 MHz	Sky	AM radio
HF (high frequency)	3-30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30-300 MHz	Sky and line-ofsight	VHFTV, FM radio
UHF (ultrahigh frequency)	300 MHz-3 GHz	Line-of-sight	UHFTV, cellular phones, paging, satellite
SHF (super high frequency)	3-30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30-300 GHz	Line-of-sight	Radar, satellite

Table 7.4 Bands

We can divide wireless transmission into three broad groups: radio waves, microwaves, and infrared waves. See Figure 7.19.

Figure 7.19 *Wireless transmission waves*



3.1 Radio Waves

Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves. However, the behavior of the waves, rather than the frequencies, is a better criterion for classification.

Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna. The omnidirectional property has a disadvantage, too. The

radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.

Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building. The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into subbands, the subbands are also narrow, leading to a low data rate for digital communications.

Almost the entire band is regulated by authorities. Using any part of the band requires permission from the authorities.

3.1.1 Omni-directional Antenna

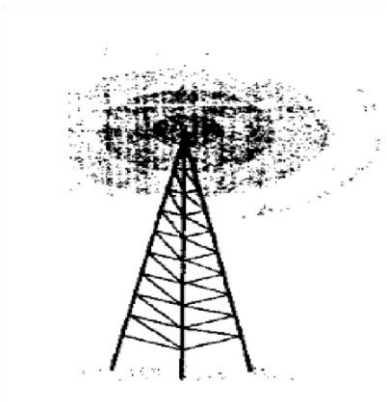
Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure 7.20 shows an omnidirectional antenna.

3.1.2 Applications

The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Figure 7.20 *Unidirectional antenna*

Radio waves are used for multicast communications,' such as radio and television, and paging systems.



3.2 Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. The following describes some characteristics of microwave propagation:

- Microwave propagation is line-of-sight. Since the towers with the mount6d antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for long distance communication.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities.

3.2.1 Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn (see Figure 7.21).

A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus. The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaves hit the dish and are deflected outward in a reversal of the receipt path.

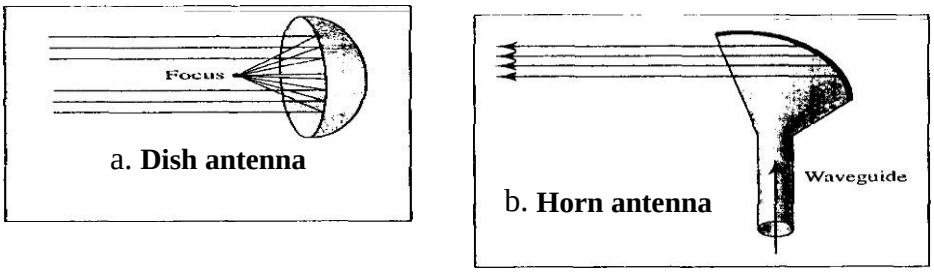
A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem (resembling a handle) and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a

manner similar to the parabolic dish, and are deflected down into the stem.

3.2.2 Applications

Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks, and wireless LANs.

Figure 7.21 *Unidirectional antennas*



3.3 Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from I mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

3.3.1 Applications

The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate. The *Infrared Data Association* (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers. For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC. The standard originally

defined a data rate of 75 kbps for a distance up to 8 m. The recent standard defines a data rate of 4 Mbps.

Infrared signals defined by IrDA transmit through line of sight; the IrDA port on the keyboard needs to point to the PC for transmission to occur. Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

4.0 CONCLUSION

Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

5.0 SUMMARY

- Transmission media lie below the physical layer.
- A guided medium provides a physical conduit from one device to another. Twisted-pair cable, coaxial cable, and optical fiber are the most popular types of guided media.
- Twisted-pair cable consists of two insulated copper wires twisted together. Twisted-pair cable is used for voice and data communications.
- Coaxial cable consists of a central conductor and a shield. Coaxial cable can carry signals of higher frequency ranges than twisted-pair cable. Coaxial cable is used in cable TV networks and traditional Ethernet LANs.
- Fiber-optic cables are composed of a glass or plastic inner core surrounded by cladding, all encased in an outside jacket. Fiberoptic cables carry data signals in the form of light. The signal is propagated along the inner core by reflection. Fiberoptic transmission is becoming increasingly popular due to its noise resistance, low attenuation, and high-bandwidth capabilities. Fiber-optic cable is used in backbone networks, cable TV networks, and Fast Ethernet networks.
- Unguided media (free space) transport electromagnetic waves without the use of a physical conductor.
- Wireless data are transmitted through ground propagation, sky propagation, and line-of-sight propagation. Wireless waves can be classified as radio waves, microwaves, or infrared waves. Radio waves are omnidirectional; microwaves are unidirectional.

Microwaves are used for cellular phone, satellite, and wireless LAN communications.

- Infrared waves are used for short-range communications such as those between a PC and a peripheral device. It can also be used for indoor LANs.

6.0 TUTOR-MARKED ASSIGNMENT

1. Name the two major categories of transmission media.
2. How do guided media differ from unguided media?

7.0 Reference & Further Reading

http://www.sintef.no/content/page1
http://en.wikipedia.org/wiki/Wireless

UNIT 3 TRANSMISSION IMPAIRMENT

CONTENTS

1.0 INTRODUCTION

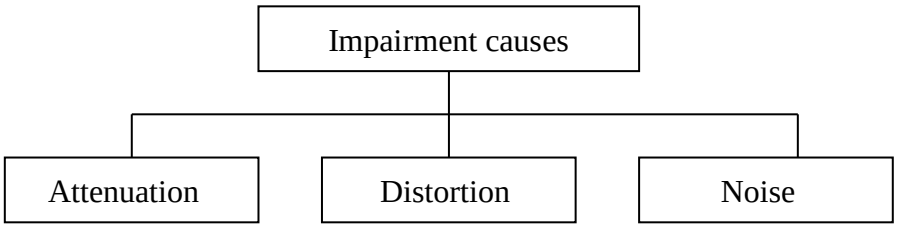
Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise (see Figure 3.25).'

2.0 Objectives

At the end of this unit you should be able to;

- Discuss Transmission impairment
- Explain Attenuation, Distortion and Noise

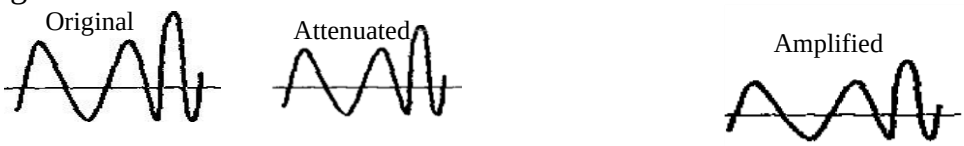
Figure 3.25 *Causes of impairment*



3.1 Attenuation

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal. Figure 3.26 shows the effect of attenuation and amplification.

Figure 3.26 *Attenuation*



3.1.1 Decibel

To show that a signal has lost or gained strength, engineers use the unit of the decibel. The decibel (dB) measures the relative strengths of two signals or one signal at two different points. Note that the decibel is negative if a signal is attenuated and positive if a signal is amplified. dB $=10\log_{10} P^2/ P_1$

Variables P_1 and P_2 are the powers of a signal at points 1 and 2, respectively. Note that some engineering books define the decibel in terms of voltage instead of power. In this case, because power is proportional to the square of the voltage, the formula is dB = 20 log to (V_2/V_1) . In this text, we express dB in terms of power.

Example 3.26

Suppose a signal travels through a transmission medium and its power is reduced to one-half. This means that $P_2= ½ P_1$. In this case, the attenuation (loss of power) can be calculated as

$10\log_{10} P^2/P_1= 10\log_{10} 0.5P^1/P_1 = 10\log_{10} 0.5= 10 (-0.3) = -3$ dB

A loss of 3 dB (-3 dB) is equivalent to losing one-half the power.

Example 3.27

A signal travels through an amplifier, and its power is increased 10 times. This means that $P_2 =$
$10P_1$. In this case, the amplification (gain of power) can be calculated as:

$101og_{10}\ P^2/P_1 = 10log_{10}\ 10P^1/P_1 = 10log_{10}\ 10 = 10(1) = 10$ dB

Example 3.28 Sometimes the decibel is used to measure signal power

in milliwatts.

In this case, it is referred to as dB_m and is calculated as $dB_m = 10\ log_{10}\ P_m$ where P_m is the power in milliwatts. Calculate the power of a signal if its dB_m =-30.
Solution
We can calculate the power in the signal as
$dB_m = 101og10\ Pm = -30$
$log\ P_m.=-3 \qquad P_m=10^{-3}$
mW

Example 3.29

The loss in a cable is usually defined in decibels per kilometer (dB/km). If the signal at the beginning of a cable with -0.3 dB/km has a power of 2 mW, what is the power of the signal at 5 km?

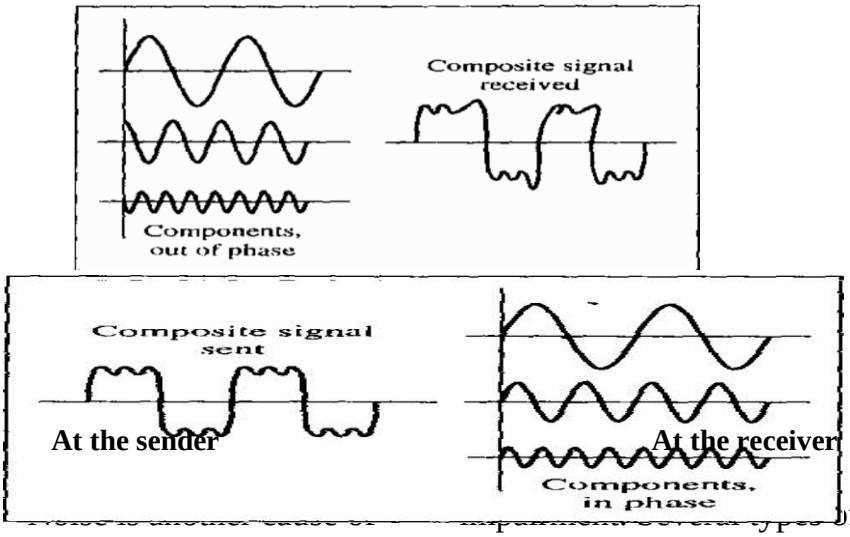
Solution

The loss in the cable in decibels is 5 x (-0.3) =-1.5 dB. We can calculate the power as $dB = 10log_{10}\ P^2/P_1 = -1.5$
$P_2/P_1 = 10^{-0.1.5} = 0.71$
$P_2 = 0.71\ P_1 = 0.7x2=1.4mW$

3.2 Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed (see the next section) through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same. Figure 3.28 shows the effect of distortion on a composite signal.

Figure 3.28 *Distortion*



f noise,

Such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna. 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 noise is a :spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on. Figure 3.29 shows the effect of noise on a signal.

3.3.1 Signal- to- Noise Ratio (SNR)

As we will see later, to find the theoretical bit rate limit, we need to know the ratio of the signal power to the noise power. The signal-to-noise ratio is defined as

$$SNR = \frac{\text{average signal power}}{\text{average noise power}}$$

We need to consider the average signal power and the average noise power because these may change with time. Figure 3.30 shows the idea of SNR.

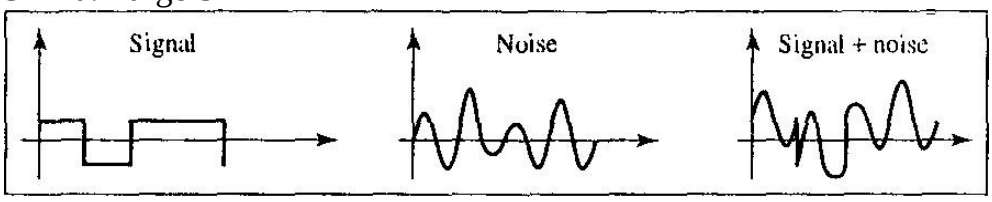
SNR is actually the ratio of what is wanted (signal) to what is not wanted (noise). A high SNR means the signal is less corrupted by noise; a low SNR means the signal is more corrupted by noise. Because SNR is the ratio of two powers, it is often described in decibel units, SNR_{dB}, defined as:

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

Example 3.30

The power of a signal is 10 mW and the power of the noise is µ*W;* what are the values of SNR and SNR_{dB}?

Figure 3.30 Two cases of SNR: a high SNR and a low SNR a. Large SNR



Solution

The values of SNR and SNR_{dB} can be calculated as follows:

$$SNR = \frac{10{,}000\,\mu W}{1\ mW} = 10{,}000$$

$$SNR_{dB} = 10\log_{10} 10{,}000 = 10 \log_{10} 10^4 = 40$$

Example 3.31

The values of SNR and SNR_{dB} for a noiseless channel are

$$SNR = \frac{\text{signal power}}{0} = \infty$$

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

We can never achieve this ratio in real life; it is an ideal.

4.0 Conclusion

Three causes of impairment are attenuation, distortion, and noise

5.0 Summary

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment.

The decibel (dB) measures the relative strengths of two signals or one signal at two different points. $dB = 10\log_{10} P^2/P_1$

$10\log_{10} P^2/P_1 = 10\log_{10} 0.5P^1/P_1 = 10\log_{10} 0.5 = 10\ (-0.3) = -3$ dB

A signal travels through an amplifier, and its power is increased 10 times. Sometimes the decibel is used to measure signal power in milliwatts. Calculate the power of a signal if its $dB_m = -30$. We can calculate the power in the signal as $\log P_m = -3$ $P_m = 10^{-3}$ *mW*

If the signal at the beginning of a cable with -0.3 dB/km has a power of 2 mW, what is the power of the signal at 5 km? $dB = 10\log_{10} P^2/P_1$ *=-1.5*

Several types of noise, Such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. The signalto-noise ratio is defined as

SNR = average signal power
average noise power

We need to consider the average signal power and the average noise power because these may change with time. A high SNR means the signal is less corrupted by noise; a low SNR means the signal is more corrupted by noise.

6.0 Tutor-Marked Assignment

1. What is attenuation?
2. Explain Distortion?

7.0 Reference & Further Reading

Peterson L.L and Davies B.S. Computer Network: A System Approaches, Morgan Kaufmann, 1996

MODULE 6 APPLICATION OF COMPUTER IN DATA TRANSMISSION AND SECURITY

Unit 1 Network Operating Systems (NOS)
Unit 2 Switching Technology
Unit 3 Cryptography
Unit 4 Network Security

UNIT 1 NETWORK OPERATING SYSTEMS (NOS)

CONTENTS

6.0 TMA

7.0 Reference & Further Reading

1.0 Introduction

Specialized software, called Network Operating Systems (NOS), is needed to control LANs. However there are Personal Computers (PC) without Network operating systems this is discussed in section 3.2 while those with NOS is discussed in section 3.1.

A Network Operating System (NOS) transfers files between computers, and between computers and print servers. Often when a user is using a program, such as a word processor, and requests a file, the user is not aware that the file was not residing on his or her machine's hard drive.

A Network Operating System (NOS) transfers files between computers, and between computers and print servers.

The NOS monitors who logs in and that the user employs the correct password. The latest NOS versions have elaborate methods of hacker/intruder detection, monitoring, and disabling the hacker.

2.0 Objectives

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

Define a Network Operating System (NOS)
Compare a Computer with a NOS to a Computer without a NOS and a Network Interface Card (NIC) Discuss
Peer-to-peer and Client/Server LAN
Explain what a NOS does and
Discuss Network monitoring

3.0 Main Content

3.1 PC with Network Operating systems

When a NOS is added to a computer, a major addition is the Redirector as shown in fig 6.1.When the Redirector receives a command from the application program, the Redirector determines if the command is intended for the computer Operating System (OS) and BIOS, or for the network. If the command is a network command, it will be directed to the LAN software and hardware.

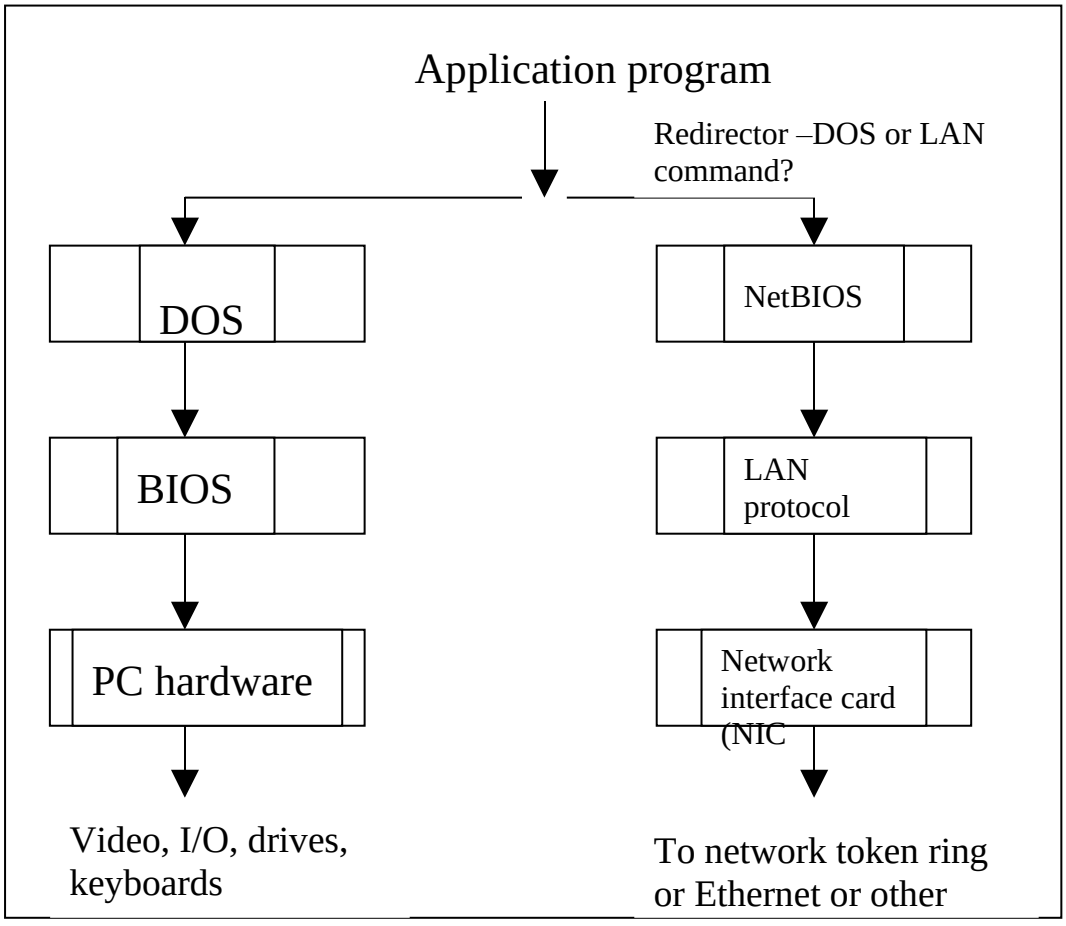
A network command will go first to the NetBIOS (Network Basic Input Output System) software, then to the LAN protocol software. The LAN protocol software is unique to the type of LAN. Token Ring software will be different from 10Base5 software, and so forth. The LAN protocol software converts the NetBIOS command to a command that the network Interface card (NIC) can understand. The NIC is a card that plugs into the computer and is the hardware that connects the computer to the LAN. Generally each type of LAN (10Base5 or Token Ring) requires a different type of NIC, but some NICs can support both 10Base2 and 10 BaseT. Newer NICs translate between 10BaseT and 100BaseT.

Fig 6.1 PC software and LAN software

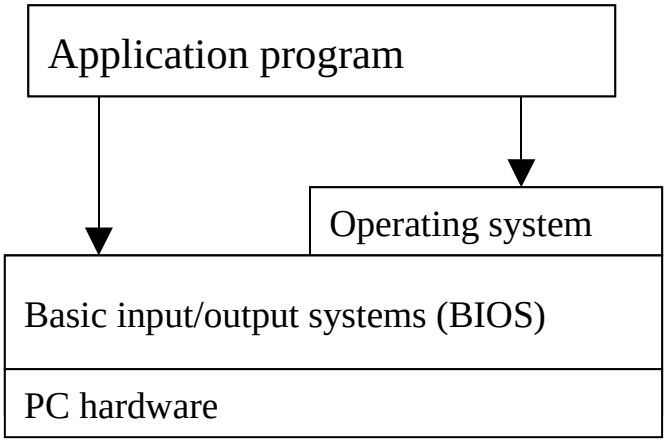
3.2 PC without Network Operating systems

Figure 6.2 shows the organization of an operating System (OS) based IBM PC without a NOS. The OS can be DOS or Windows. A command in an application program will call either an OS command, an input device (keyboard) or an output device (printer), or an input/output device (disk drive). If an input, or output, or input/output device is called, the command will be routed to the Basic Input Output System (BIOS) and then to the PC hardware.

The BIOS is software written or 'burned' into a read only Memory (ROM) that converts program commands to commands the PC



hardware can understand. A ROM stores data even if the power is turned off.



NT Windows 95, etc
Software control of video, I/O, keyboard, drives

Fig 6.2 PC software without LAN software

3.3 Peer-to-Peer versus Client/Server

Peer-to peer means there is no dedicated server, yet all workstations within the work group can communicate with each other via the network. No workstation is a server, and all workstations are considered equals or peers. All workstations share resources. A server is a computer dedicated to sending files (serving) to workstations requesting those files; the server allows other computers on the network to use its resources. A client is the computer requesting files from the server.

3.4 NOS Functions

A Network Operating System (NOS) transfers files between computers, and between computers and print servers. Often when a user is using a program, such as a word processor, and requests a file, the user is not aware that the file was not residing on his or her machine's hard drive. When a user commands his or her word processor to print a file, the user also is unaware of the file transfer to a print server. The file transfers are 'transparent' to the user.

3.4.1 Network Monitoring

The NOS monitors who logs in and that the user employs the correct password. The latest NOS versions have elaborate methods of

hacker/intruder detection, monitoring, and disabling (shutting out) the hacker.

NOSs will monitor and log the users for their time on the net. It is possible to monitor a user's e-mail, and the U.S courts have ruled that an employee provides the equipment and connection to the Internet, the company has the right to monitor what is being sent over the net.

NOSs monitor traffic and are useful to find traffic bottleneck and equipment failures.

4.0 Conclusion

We can now easily differentiate between PC with NOS and PC without NOS. We also saw the difference between Peer-to-Peer and Client/Server networks. Finally we looked at NOS Functions of which the key is monitoring network users and the network traffic.

5.0 Summary

The redirector is the key piece of software in a computer with a NOS. The redirector examines a command to see if it is part of the normal Operating System or a network command. If the command is an Operating System command, the computer operates as usual. If the command is a network command, the command will go to the NOS. The NOS will perform the proper network function.

A NOS does file serving, print serving and network monitoring. Network monitoring, keeps track of traffic levels, types of traffic, sources and destinations, what users are logged in, what users will be allowed to log in, and hackers and intruders.

6.0 Tutor-Marked Assignment

1. What is a Network Operating System (NOS)?
2. Compare a computer without a NOS to One with a NOS

7.0 Reference & Further Reading

Milan Milenkovic, Operating Systems and Design, Second Edition. Tata McGraw - Hill

Unit 2 SWITCHING TECHNOLOGY

1.0 Introduction

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one –to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). These methods are impractical when applied to very large networks. The number and length of the links require too much infrastructure to be cost efficient and most of those links will be frequently idle. Other topologies employing multipoint connections, such as a bus, are ruled out because the distances between devices and the total number of devices increase beyond the capacities of media and equipment. A better solution is **switching.** A switched network consists of a series of interlinked nodes, called **switches.** Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network some of these nodes are connected to the end systems (e.g. computers or telephones) others are used only for routing.

2.0 Objectives

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

- explain the methods of switching
- understand the concept of Switching Computers
- discuss extensively the structure and component of switchs.

3.0 Methods of switching

Three methods of switching exist: **circuit switching, packet switching, and message switching.** The first two are commonly used today. Naturally this divides today's networks into three broad categories: circuit-switched networks, packet-switched networks, and message-switched networks. Packet-switched networks can further be divided

into two subcategories; virtual-circuit networks and datagram networks. Networks route the first packet based on the datagram addressing idea, but then create a virtual-circuit network for the rest of the packets coming from the same source and going to the same direction. In message switching, each switch stores the whole message and forwards it to the next switch.

3.1 Switching Computers

Switching is done by special purpose computers, designed specifically for switching. The software can easily be replaced and updated. The actual switching is handled by the software, or Stored Program Control (SPC).

The "workhorses" of the switching computers are the Electronic Switching System (ESS). The Switching Computers or ESS of the Lucent Technologies are the 4ESS and 5ESS. They can handle up to 1,200,000 calls per hour and 200,000 calls per hour respectively. The 4ESS is used in high demand areas, and the 5ESS is used in lower usage in lower usage areas.

The trunks interconnecting the computers carry voice, data, and video. The signaling is handled by separate circuits.

3.2 Structure of A Switch

We use switches in circuit-switched and packet-switched networks. In this section, we discuss the structures of the switches used in each type of network.

Structure of Circuit Switches

Circuit switching today can use either of two technologies: the spacedivision switch or the time-division switch.

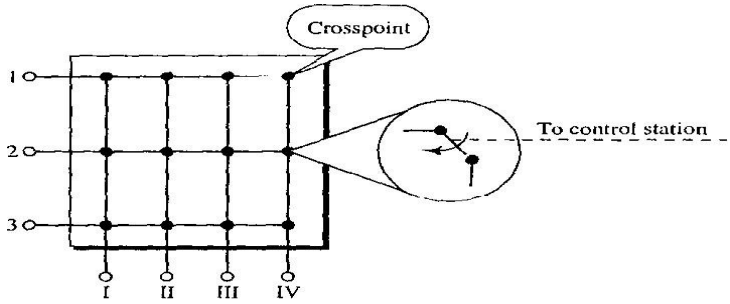
Space-Division Switch

In space-division switching, the paths in the circuit are separated from one another spatially. This technology was originally designed for use in analog networks but is used currently in both analog and digital networks. It has evolved through a long history of many designs.

Crossbar Switch A crossbar switch connects n inputs to m outputs in a grid, using electronic microswitches (transistors) at each cross point (sec Figure 6.17). The major limitation of this design is the number of crosspoints required. To connect n inputs to to outputs using a crossbar switch requires n x m crosspoints. For example, to connect,, 1000 inputs to 1000 outputs requires a switch with 1,000,000 crosspoints. A

crossbar with this number of crosspoints is impractical. Such a switch is also inefficient because statistics show that, in practice, fewer than 25 percent of the crosspoints are in use are in use at any given time. The rest are idle.

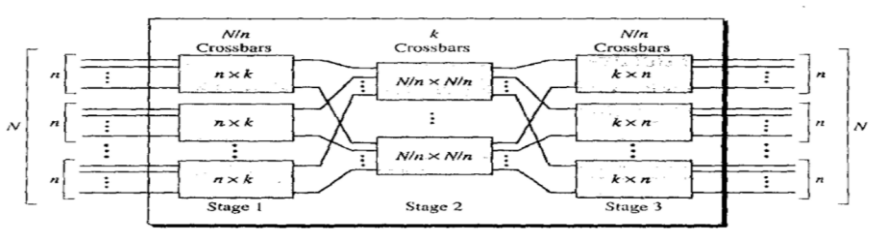
Figure 6.3 Cross switch with three



Multistage Switch The solution to the limitations of the crossbar switch is the multistage switch, which combines crossbar switches in several (normally three stages, as shown in Figure 6.4. In a single crossbar switch, only one row or column (one path) is active for any connection. So we need N x N cross points. If we can allow multiple paths inside the switch, we can decrease the number of cross points.

Each cross point in the middle stage can be accessed by multiple cross points in the first or third stage.

Figure 6.5 Multistage switch



To design a three-stage switch, we follow these steps:

l. We divide the N input lines into groups, each of n lines. For each group, we use one crossbar of size n x k, where k is the number of crossbars in the middle stage. In other words, the first stage has N/n crossbars of n x k crosspoints.

2. We use k crossbars, each of size (N/n) x (N/n) in the middle stage.

3. We use N/n crossbars, each of size k x n at the third stage.

We can calculate the total number of crosspoints as follows:

N/n (n x k) + (N/n x N/n) + N/n (k x n) 2kN + k (N/n)2

In a three-stage switch, the total number of crosspoints is 2kN+k (N/n)2 which is much smaller than the number of crosspoints in a single-stage switch (N2).

Example 6.3

Design a three-stage, 200 x 200 switch (N = 200) with k = 4 and n = 20.

Solution

In the first stage we have N/n or 10 crossbars, each of size 20 x 4. In the second stage, we have 4 crossbars, each of size 10 x 10. In the third stage, we have 10 crossbars, each of size 4 x 20. The total number of crosspoints is 2kN + k(Nln)2, or 2000 crosspoints. This is 5 percent of the number of crosspoints m a single-stage switch (200x200=40,000).

The multistage switch in Example 6.3 has one drawback-blocking during periods of heavy traffic. The whole idea of multistage switching is to share the crosspoints in the middle-stage crossbars. Sharing can cause a lack of availability if the resources are limited and all users want a connection at the same time. Blocking refers to times when one input cannot be connected to an output because there is no path available between them-all the possible intermediate switches are occupied.

In a single-stage switch, blocking does not occur because every combination of input and output has its own crosspoint; there is always a path. (Cases in which two inputs are trying to contact the same- output do not count. That path is not blocked; the output is merely busy.) In the multistage switch described in Example 6.3, however, only 4 of the first 20 inputs can use the switch at a time, only 4 of the second 20 inputs can use the switch at a time, and so on. The small number of crossbars at the middle stage creates blocking.

In large systems, such as those having 10,000 inputs and outputs, the number of stages can be increased to cut down on the number of crosspoints required. As the number of stages increases, however, possible blocking increases as well. Many people have experienced blocking on public telephone systems in the wake of a natural disaster when the calls being made to check on or reassure relatives far outnumber the regular load of the system.

Clos investigated the condition of nonblocking in multistage switches and came ap with the following formula. In a nonblocking switch, the number of middle-stage switches must be at least 2n -1.In other words, we need to have k≥ 2n 1.

Note that the number of crosspoints is still smaller than that in a singlestage switch. Now we need to minimize the number of crosspoints with a fixed N by using the Clos criteria. We can take the derivative of the equation with respect to n (the only variable) and find the value of n that makes the result zero. This n must be equal to or greater than (N/2)1/2. In this case, the total number of crosspoints is greater than or equal to 4N [(2N) v' - 11. In other words, the minimum number of crosspoints according to the Clos criteria is proportional to N3/2.

According to Clos criterion:

n --
(N/2)1/2 k
>2n-1
Total number of crosspoints ≥ 4N [(2N)1/2 -1]

Example 6.4

Redesign the previous three-stage, 200 X 200 switch, using the Clos criteria with a minimum number of crosspoints.

Solution

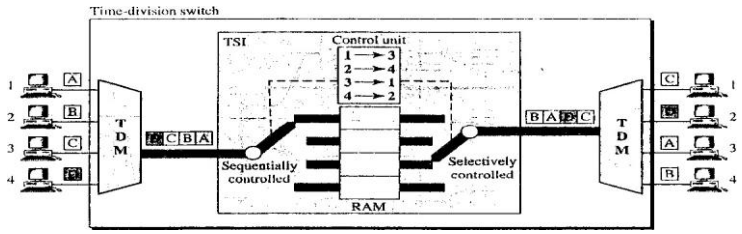
We let n = (200/2)1/2, or n = 10. We calculate k = 2n - 1 = 19. In the first stage, we have 200/10, or 20, crossbars, each with 10 X 19 crosspoints. In the second stage, we have 19 crossbars, each with 10 X 10 crosspoints. In the third stage, we have 20 crossbars each with 19 X 10 crosspoints. The total number of crosspoints is 20(10 x 19) + 19(10 x l0) + 20(19 x10) _ 9500. If we use a single-stage switch, we need 200 x 200 = 40,000 crosspoints. The number of crosspoints in this three-stage switch is 24 percent that of a single-stage switch. More points are needed than in Example 6.3 (5 percent). The extra crosspoints are needed to prevent blocking.

A multistage switch that uses the Clos criteria and a minimum number of crosspoints still requires a huge number of crosspoints. For example, to have a 100,000 input/output switch, we need something close to 200 million crosspoints (instead of l0 billion). This means that if a telephone company needs to provide a switch to connect 100,000 telephones in a city, it needs 200 million crosspoints. The number can be reduced if we accept blocking. Today, telephone companies use time-division switching or a combination of space- and time-division switches, as we will see shortly.

Time-Division Switch

Time-division switching uses time-division multiplexing (TDM) inside a switch. The most popular technology is called the time-slot interchange (TSI). Time-Slot InterchangeFigure 6.6 shows a system connecting four input lines to four output lines. Imagine that each input line wants to send data to an output line according to the following pattern: 1-3 2 – 4 3 – 1 4 - 2

Figure 6.6Time-slot interchange



The figure combines a TDM multiplexer, a TDM demultiplexer, and a TSI consisting of random access memory (RAM) with several memory locations. The size of each location is the same as the size of a single time slot. The number of locations is the same as the number of inputs (in most cases, the numbers of inputs and outputs are equal). The RAM fills up with incoming data from time slots in the order received. Slots are then sent out in an order based on the decisions of a control unit.

Time and Space-Division Switch Combinations

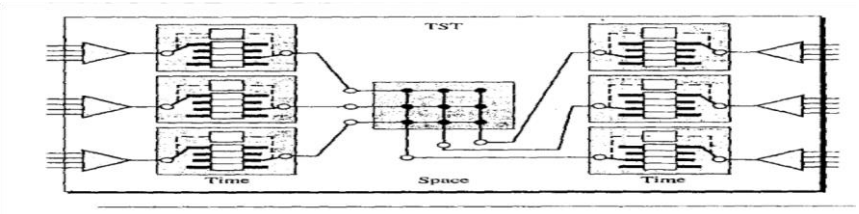
When we compare space-division and time-division switching, some interesting facts emerge. The advantage of space-division switching is that it is instantaneous. Its disadvantage is the number of cross points required to make space-division switching acceptable in terms of blocking.

The advantage of time-division switching is that it needs no crosspoints. Its disadvantage, in the case of TSI, is that processing each connection creates delays. Each time slot must be stored by the RAM, then retrieved and passed on.

In a third option, we combine space-division and time-division technologies to take advantage of the best of both. Combining the two results in switches that are optimized both physically (the number of crosspoints) and temporally (the amount of delay). Multistage switches of this sort can be designed as time-space-time (TST)

Switch

Figure 6.7 shows a simple TST switch that consists of two time stages and one space stage and has 12 inputs and 12 outputs. Instead of one time-division switch, it divides the inputs into three groups (of four inputs each) and directs them to three time slot interchanges. The result is that the average delay is one-third of what would result from using one time-slot interchange to handle all 12 inputs.
The last stage is a mirror image of the first stage. The middle stage is a space division switch (crossbar) that connects the TSI groups to allow connectivity between all possible input and output pairs (e.g., to connect input 3 of the first group to output 7 of the second group).
Figure 6.7 Time-space-time switch



3.2.1 Structure of Packet Switches

A switch used in a packet-switched network has a different structure from a switch used in a circuit-switched network. We can say that a packet switch has four components: input ports, output ports, the routing processor, and the switching fabric, as shown in Figure 6.7

Figure 6.7 Packet switch components

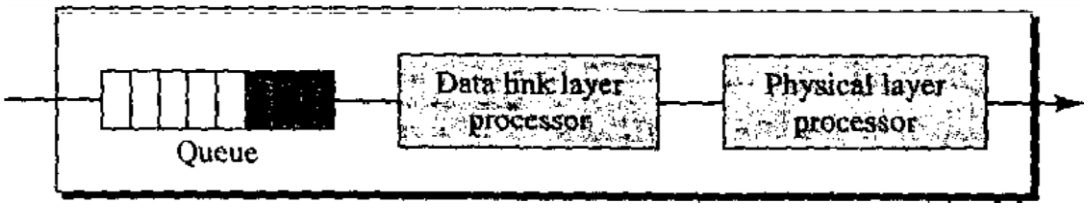
Input Ports

An input port performs the physical and data link functions of the packet switch. The bits are constructed from the received signal. The packet is decapsulated from the frame. Errors are detected and corrected. The packet is now ready to be routed by the network layer. In addition to a physical layer processor and a data link processor, the input port has buffers (queues) to hold the packet before it is directed to the switching fabric.

Output Port

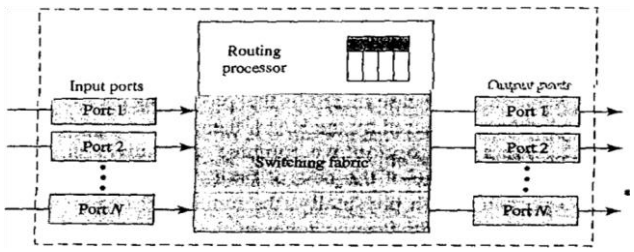
The output port performs the same function, as the input port, but in the reverse order. First the outgoing packets are queued, then the packet is encapsulated in a frame, and finally the physical layer functions are applied to the frame to create the signal to be sent on the line. Figure 6.8 shows a schematic diagram of an output port.

Figure 6.8 Output port



Routing Processor

The routing processor performs the functions of the network layer. The destination address is used to find the address of the next hop and, at



the same time, the output port number from which .the, packet is sent-out. This activity is sometimes referred to as table lookup because the routing processor searches the routing table. In the newer packet switches, this function of the routing processor is being moved to the input ports to facilitate and expedite the process.

3.2.2 Switching Fabrics

The most difficult task in a packet switch is to move the packet from the input queue to the output queue. The speed with which this is done affects the size of the input/output queue and the overall delay in packet delivery. In the past, when a packet switch was actually a dedicated Computer, the memory of the computer or a bus was used as the switching fabric. The input port stored the packet in memory; the output port retrieved the packet from memory. Today, packet switches are specialized mechanisms that use a variety of switching fabrics. We briefly discuss some of these fabrics here.

Crossbar Switch The simplest type of switching fabric is the crossbar switch, discussed in the previous section.

Banyan Switch A more realistic approach than the crossbar switch is the banyan switch (named after the banyan tree). A banyan switch is a multistage switch with micro switches at each stage that route the packets based on the output port represented as a binary string. For n inputs and n outputs, we have log2n stages with nit micro switches at each stage. The first stage routes the packet based on the high-order bit of the binary string. The second stage routes the packet based on the second high-order bit, and so on. Figure 6.9 shows a banyan switch with eight inputs and eight outputs. The number of stages is log2 (8) = 3.
Figure 6.9 A banyan switch

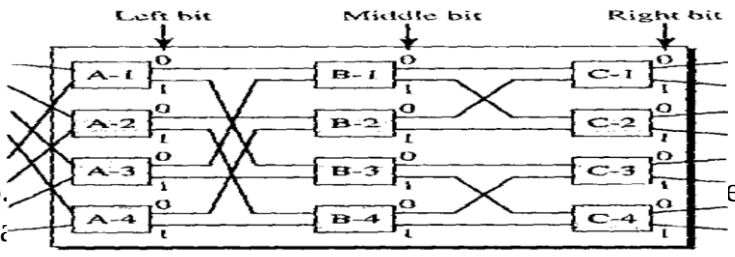
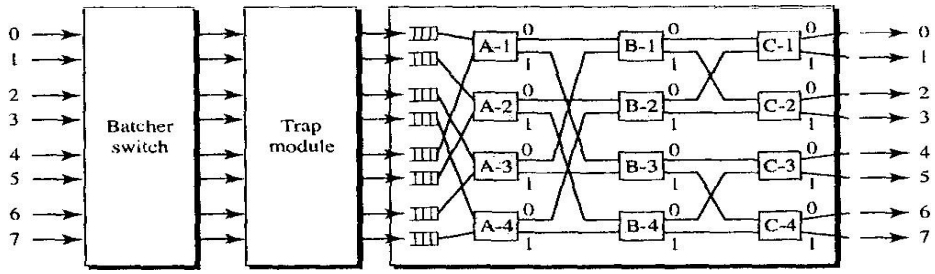


Figure 6. ed at input port 1 The first microsw the second microswitch (B-4) routes the packet based on the second bit (1), and the third microswitch (C-4) routes the packet based on the third bit (0).-~ In part b, a packet has arrived at input port 5 and must go to output port 2 (0) 0 in - binary). The first microswitch (A-2) routes the packet based on the first bit (0), the second microswitch (B-2) routes the packet based on the second bit (t), and the third microswitch (C-2) routes the packet based on the third bit (0).

Figure 6.10 Examples of routing in a banyan switch
Figure 6.11 Butcher-banyan switch

Banyan switch



Batcher-Banyan Switch The problem with the banyan switch is the possibility of internal collision even when two packets are not heading for the same output port. We can solve this problem by sorting the arriving packets based on their destination port.

K. E. Batcher designed a switch that comes before the banyan switch and sorts the incoming packets according to their final destinations. The combination is called the Batcher-banyan switch. The sorting switch uses hardware merging techniques, but we do not discuss the details here. Normally, another hardware module called a trap is added between the Batcher switch and the banyan switch (see Figure 6.11) The trap module prevents duplicate packets (packets with the same output destination) from passing to the banyan switch simultaneously. Only one packet for each destination is allowed at each tick; if there is more than one, they wait for the next tick.

4.0 CONCLUSION

Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network some of these nodes are connected to the end systems (e.g. computers or telephones) others are used only for routing.

Whenever we have multiple devices, we have the problem of how to connect them to make one –to-one communication possible. We employ Switches to address this problem. It's cost effective.

5.0 SUMMARY

A switched network consists of a series of interlinked nodes, called switches. Traditionally, three methods of switching have been important: circuit switching, packet switching, and message switching.

We can divide today's networks into three broad categories: circuitswitched networks, packet-switched networks, and message-

switched. Packet-switched networks can also be divided into two subcategories: virtual-circuit networks and datagram networks.

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels. Circuit switching takes place at the physical layer. In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer phase until the teardown phase.

In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand.

In a datagram network, each packet is treated independently of all others. Packets in this approach are referred to as datagrams. There are no setup or teardown phases. A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

Circuit switching uses either of two technologies: the space-division switch or the time-division switch.

A switch in a packet-switched network has a different structure from a switch used in a circuit-switched network. We can say that a packet switch has four types of components: input ports, output ports, a routing processor, and switching fabric.

6.0 TMA

1. Describe the need for switching and define a switch.
2. List the three traditional switching methods. What are the most common today?
3. What are the two approaches to packet-switching? **7.0 Reference & Further Reading**

Open content License (http:/www.pencontent.org/)

Peterson L.L and Davies B.S. Computer Network: A System Approaches, Morgan Kaufmann, 1996

Unit 3 Cryptography and Security

CONTENTS

1.0 INTRODUCTION

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Network security is mostly achieved through the use of cryptography, a science based on abstract algebra.

The original message, before being transformed, is called plaintext. After the message is transformed, it is called cipher text. An encryption algorithm transforms the plaintext into cipher text; a decryption algorithm transforms the cipher text back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

2.0 Objectives

At the end of this unit you should be able to
- define various terms in cryptography
- differentiate between Symmetric-Key Cryptography and Asymmetric-Key Cryptography

3.1 DEFINITION OF TERMS

Cipher

We refer-to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for a secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key. and the plaintext. These create the cipher text. To decrypt a message, we need a decryption algorithm, a decryption key, and the cipher text. These reveal the original plaintext.

Alice, Bob, and Eve

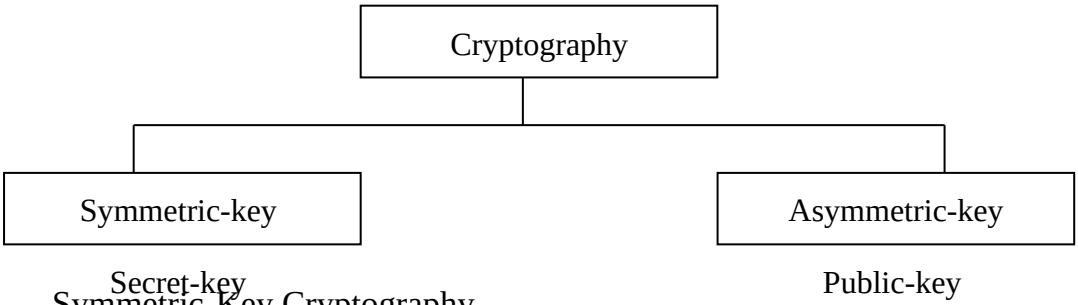
In cryptography, it is customary to use three characters in an information exchange scenario; we use Alice, Bob, and Eve. Alice is the person who needs to send secure data. Bob is the recipient of the data. Eve is the person who somehow disturbs the communication between Alice and Bob by intercepting messages to uncover the data or by sending her own disguised messages. These three names represent computers or processes that actually send or receive data. or intercept or change data.

Two Categories

We can divide all the cryptography algorithms (ciphers) into two groups: symmetric key (also called secret-key) cryptography algorithms and asymmetric (also called public-key) cryptography algorithms.

Figure 3.2 shows the taxonomy.

Figure 3.2Categories of cryptography



Symmetric-Key Cryptography

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data (see Figure 3.3).

Figure 3.3Symmetric-key cryptography

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Asymmetric-Key Cryptography

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public. In Figure 3.4, imagine Alice wants to send a message to Bob. Alice uses the public key to encrypt the

message. When the message is received by Bob, the private key is used to decrypt the message.

Figure 3.4 Asymmetric-key cryptography

In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public; the private key is available only to an individual.

Three Types of Keys

The reader may have noticed that we are dealing with three types of keys in cryptography:

the secret key, the public key, and the private key. The first, the secret key, is the shared key used in symmetric-key cryptography. The second and the third are the public and private keys used in asymmetrickey cryptography.

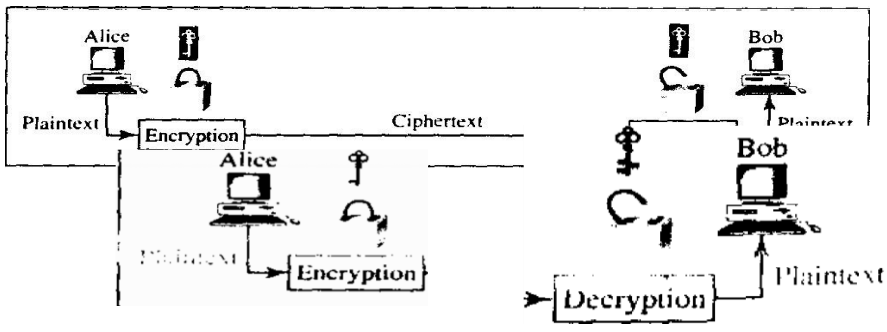
Figure 3.5 Keys used in cryptography
Symmetric-key cryptography Asymmetric-key cryptography

Comparison

Let us compare symmetric-key and asymmetric-key cryptography. Encryption can be thought of as electronic locking; decryption as electronic unlocking. The sender puts the message in a box and locks the box by using a key; the receiver unlocks the box with a key and takes out the message. The difference lies in the mechanism of the locking and unlocking and the type of keys used.

In symmetric-key cryptography, the same key locks and unlocks the box. In asymmetric-key cryptography, one key locks the box, but another key is needed to unlock it. Figure 3.6 shows the difference.

Figure 3.6 Comparison between two categories of cryptography
Symmetric-key cryptography and Asymmetric-key cryptography



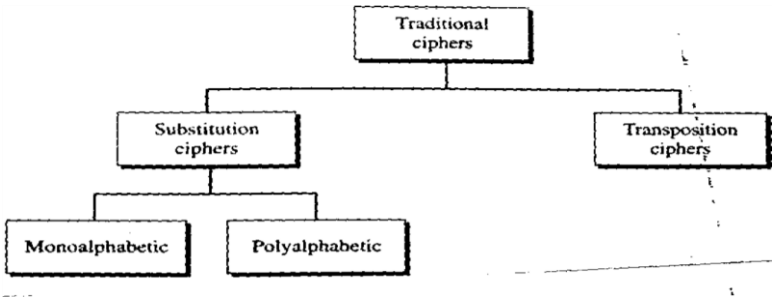
3.1 SYMMETRIC-KEY CRYPTOGRAPHY

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security. However, today's ciphers are much more complex. Let us first discuss traditional algorithms, which were character-oriented. Then we discuss the modern ones, which are bit-oriented.

3.1.1 Traditional Ciphers

We briefly introduce some traditional ciphers, which are characteroriented. Although these are now obsolete, the goal is to show how modern ciphers, evolved from them. We can divide traditional symmetric-key ciphers into two broad categories: substitution ciphers and transposition ciphers, as shown in Figure 3.7.

Figure 3.7Traditional ciphers



A substitution cipher substitutes one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another. For example, we can replace character A with D, and character T with Z. If the symbols are digits (0 to 9), we can replace 3 with 7, and 2 with 6. Substitution ciphers can be categorized as either monoalphabetic or polyalphabetic ciphers.

A substitution cipher replaces one symbol with another.
In a monoalphabetic cipher, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text. For example, if the algorithm say that character. A in the plaintext is changed to character D, every character A is changed to character D. In other words, the relationship between characters in the plaintext and the ciphertext is a one-to-one relationship.In a polyalphabetic cipher, each occurrence of a character can have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is a one-to-many relationship. For example, character A could be changed to D in the beginning of the text, but it could be changed to N at the middle. It is obvious that if the relationship between plaintext characters and

ciphertext characters is one-to many, the key must tell us which of the many possible characters can be chosen for encryption. To achieve this goal, we need to divide the text into groups of characters and use a set of keys. For example, we can divide the text "THISISANEASYTASK" into groups of 3 characters and then apply the encryption using a set of 3 keys. We then repeat the procedure for the next 3 characters.

The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic?

Plaintext: HELLO
Ciphertext: KHOOR

Solution

The cipher is probably monoalphabetic because both occurrences of L's are encrypted as O's.

Example 3.2

The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic? Plaintext: HELLO
Ciphertext: ABNZF

Solution

The cipher is not monoalphabetic because each occurrence of L is encrypted by a different character. The first L is encrypted as N: the second as Z.

Shift Cipher The simplest monoalphabetic cipher is probably the shift cipher. We assume that the plaintext and ciphertext consist of uppercase letters (A to Z) only. hi this cipher, the encryption algorithm is "shift key characters down," with key equal to some number. The decryption algorithm is "shift key characters up." For example, if the key is 5, the encryption algorithm is "shift 5 characters down" (toward the end of the alphabet). The decryption algorithm is "shift 5 characters up" (toward the beginning of the alphabet). Of course, if we reach the end or beginning of the alphabet, we wrap around.

Julius Caesar used the shift cipher to communicate with his officers. For this reason, the shift cipher is sometimes referred to as the Caesar cipher. Caesar used a key of 3 for his communications.

Example 3.3

Use the shift cipher with key = 15 to encrypt the message "HELLO."

Solution

We encrypt one character at a time. Each character is shifted 15 characters down. Letter H is encrypted to W. Letter E is encrypted to T. The first L is encrypted to A. The second L is also encrypted to A. And O is encrypted to D. The cipher text is WTAAD.

Example 3.4

Use the shift cipher with key = 15 to decrypt the message "WTAAD,"

Solution

We decrypt one character at a time. Each character is shifted 15 characters up. Letter W is decrypted to H. Letter T is decrypted to E. The first A is decrypted to L. The second A is decrypted to L. And, finally, D is decrypted to 0. The plaintext is HELLO.

Transposition Ciphers

In a transposition cipher, there is no substitution of characters; instead, their locations change. A character in the first position of the plaintext may appear in the tenth position of the Cphertext. A character in the eighth position may appear in the first position. In other words, a transposition cipher reorders the symbols in a block of symbols.

A transposition cipher reorders (permutes) symbols in a block of symbols.

Key In a transposition cipher, the key is a mapping between the position of the symbols in the plaintext and cipher text. For example, the following shows the key using a block of four characters:

Plaintext: 2 4 1 3
Ciphertext: 1 2 3 4

In encryption, we move the character at position 2 to position 1, the character at position 4 to position 2, and so on. In decryption, we do the reverse. Note that to be more effective, the key should be long, which means encryption and decryption of long blocks of data. Figure 30.8 shows encryption and decryption for our four-character block using the above key. The figure shows that the encryption and decryption use the same key. The encryption applies it from downward while decryption applies it upward.

Figure 3.8Transposition cipher

Example 3.5

Encrypt the message “HELL DEAR,” using the above key.

Solution

We first remove the spaces in the message. We then divide the text into blocks of four characters. We add a bogus character Z at the end of the third block. The result is HELL OMYD EARZ. We create a three-block ciphertext ELHLMDOYAZER.

Example 3.6

Using Example 3.5, decrypt the message “ELHLMDOYAZER”.

Solution

The result is HELL OMYD EARZ. After removing the bogus character and combining the characters, we get the original message “HELLO
MY
DEAR:’
Simple Modern Ciphers
The traditional ciphers we have studied so far are character-oriented. With the advent of the computer, ciphers need to be bit-oriented. This is so because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data. It is convenient to convert these types of data into a stream of bits, encrypt the stream, and then send the encrypted stream. In addition, when text is treated at the bit level, each character is replaced by 8 (or 16) bits, which means the number of symbols becomes 8 (or 16). Mingling and mangling bits provides more security than mingling and mangling characters. Modern ciphers use a different strategy than the traditional ones. A modern symmetric cipher is a combination of simple ciphers. In other words, a modern cipher uses several simple ciphers to achieve its goal. We first discuss these simple ciphers.

XOR Cipher

Modern ciphers today are normally made of a set of simple ciphers, which are simple’ predefined functions in mathematics or computer science. The first one discussed here is called the XOR cipher because it uses the exclusive-or operation as defined in computer science. Figure 30.9 shows an XOR cipher. Figure 30.9 XOR cipher

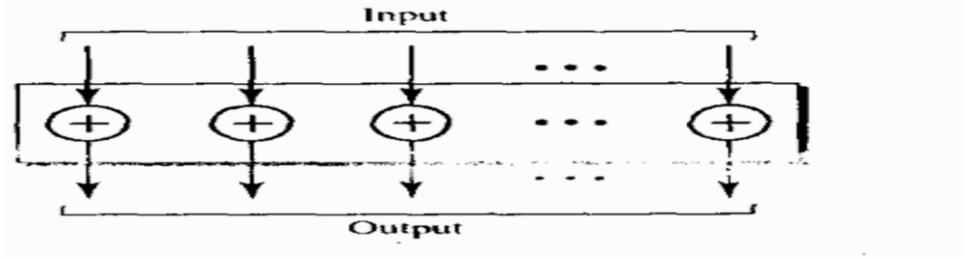


Figure 3.9 XOR cipher

An XOR operation needs two data inputs plaintext, as the first and a key as the second. In other words, one of the inputs is the block to be the encrypted, the other input is a key; the result is the encrypted block. Note that in an XOR cipher, the size of the key, the plaintext, and the ciphertext are all the same. XOR ciphers have a very interesting property: the encryption and decryption are the same.

Rotation Cipher

Another common cipher is the rotation cipher, in which the input bits are rotated to the left or right. The rotation cipher can be keyed or keyless. In keyed rotation, the value of the key defines the number of rotations; in keyless rotation the number of rotations is fixed. The rotation cipher can be considered a special case of the transpositional cipher using bits instead of characters.

The rotation cipher has an interesting property. If the length of the original stream is N, after N rotations, we get the original input stream. This means that it is useless to apply more than N- I rotations. In other words, the number of rotations must be between 1 and N- I .

The decryption algorithm for the rotation cipher uses the same key and the opposite rotation direction. If we use a right rotation in the encryption, we use a left rotation in decryption and vice versa.

Substitution Cipher: S-box

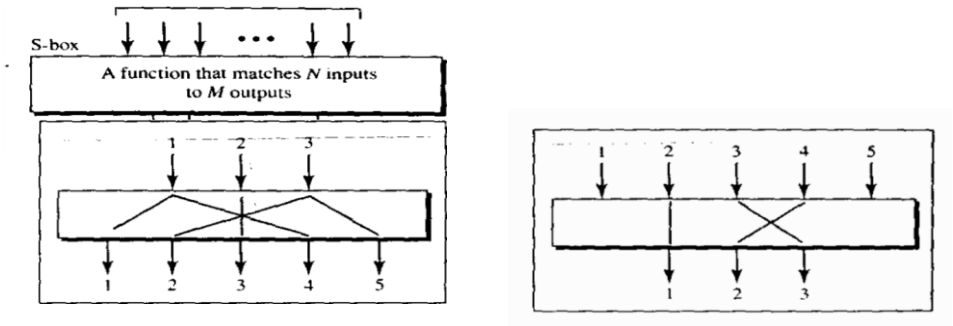
An S-box (substitution box) parallels the traditional substitution cipher for characters. The input to an S-box is a stream of bits with length N; the result is another stream of bits with length M. And N and M are not necessarily the same.

The S-box is normally keyless and is used as an intermediate stage of encryption or decryption. The function that matches the input to the output may be defined mathematically or by a table.

Transposition Cipher: P-box

A P-box (permutation box) for bits parallels the traditional transposition cipher for characters. It performs a transposition at the bit level; it transposes bits. It can be implemented in software or hardware, but hardware is faster. P-boxes, like S-boxes, are normally keyless. We can have three types of permutations in P-boxes: the straight permutation, expansion permutation, and compression permutation as shown in Figure 3.12.

Figure 3.12 P-boxes: straight, expansion, and compression



b. Expansion c. Compression

A straight permutation cipher or a straight P-box has the same number of inputs as outputs. In other words, if the number of inputs is N, the number of outputs is also N. In an expansion permutation cipher, the number of output ports is greater than the number of input ports. In a compression permutation cipher, the number of output ports is less than the number of input ports.

Modern Round Ciphers

The ciphers of today are called round ciphers because they involve multiple rounds, where each round is a complex cipher made up of the simple ciphers that we previously, described. The key used in each round is a subset or variation of the general key called the round key. If the cipher has N rounds, a key generator produces N keys, K1, K2……KN, where K1 is used in round l, K2 in round 2, and so on.

In this section, we introduce two modem symmetric-key ciphers: DES and AES. These ciphers are referred to as block ciphers because they divide the plaintext into blocks and use the same key to encrypt and decrypt the blocks. DES has been the de facto standard until recently. AES is the formal standard now.

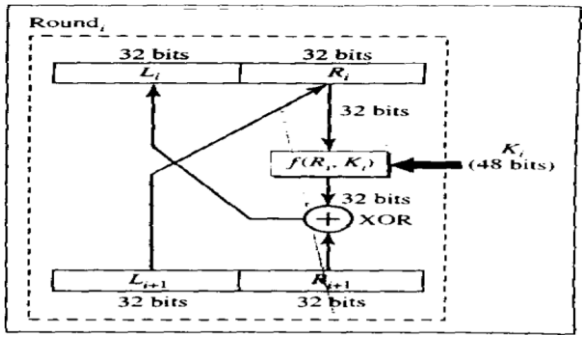
Data Encryption Standard (DES)

One example of a complex block cipher is the Data Encryption Standard 6 l-bit key

DES has two transposition blocks (B boxes) and 16 complex round ciphers (they are repeated). Although the 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key.

The initial and final permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64-bit input and permutes them according to predefined values.

Each round of DES is a complex round cipher, as shown in Figure 30.14. Note that the structure of the encryption round ciphers is different from that of the decryption one. Figure 3.14 One round in DES ciphers



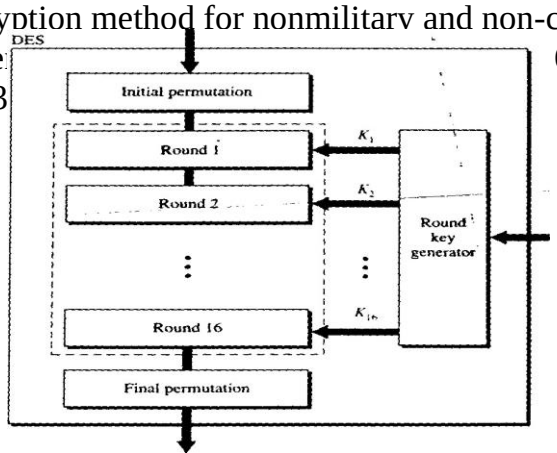
a. Encryption round b. Decryption round
DES Function The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits Ri to produce a 32bit output. This function is made up of four operations: an XOR, an expansion permutation. a group of S-boxes, and a straight permutation.

Triple DES

Critics of DES contend that the key is too short. To lengthen the key, Triple DES or 3DES has been proposed and implemented. This uses

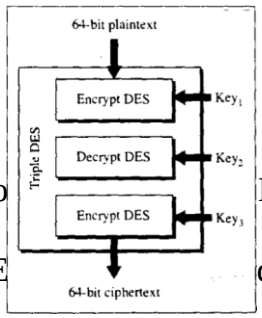
(DES). DES was designed by IBM and adopted by the U.S. government as the standard encryption method for nonmilitary and non-classified use. The algorithm e 64-bit key, as shown in Figure 3

Figure 30.13 DES 6t-bit ciphertext

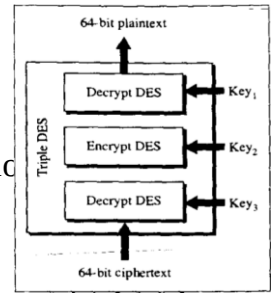


three DES blocks, as shown in Figure 3.16. Note that the encrypting block uses an encryption-decryption-encryption combination of DESs, while the decryption block uses a decryption-encryption-decryption combination. Two different versions of 3DES are in use: 3DES with two keys and 3DES with three keys. To make the key size 112 bits and at the same time protect DES from attacks such as the man-in-the-middle attack, 3DES with two keys was designed. In this version, the first and the third keys are the same (Key I = Key3). This has the advantage in that a text encrypted by a single DES block can be decrypted by the new 3DES. We just set all keys equal to Key I. Many algorithms use a 3DES cipher with three keys. This increases the size of the key to 168 bits.

Figure 3.16 Triple DES



a. Encryptio



Decryptic

Advanced E d (AES)

The Advanced Encryption Standard (AES) was designed because DES's key was too small. Although Triple DES (3DES) increased the key size, the process was too slow. The National Institute of Standards and Technology (NIST) chose the Rijndael algorithm, named after its two

Belgian inventors, Vincent Rijmen and Joan Daemen, as the basis of AES. AES is a very complex round cipher. AES is designed with three key sizes: 128, 192, or 256 bits.

AES has three different configurations with respect to the number of rounds and key size.

In this text, we discuss just the 10-round, 128-bit key configuration. The structure and operation of the other configurations are similar. The difference lies in the key generation. The general structure is shown in Figure 3.17. There is an initial XOR operation followed by 10 round ciphers. The last round is slightly different from the preceding rounds; it is missing one operation.

Although the 10 iteration blocks are almost identical, each uses a different key

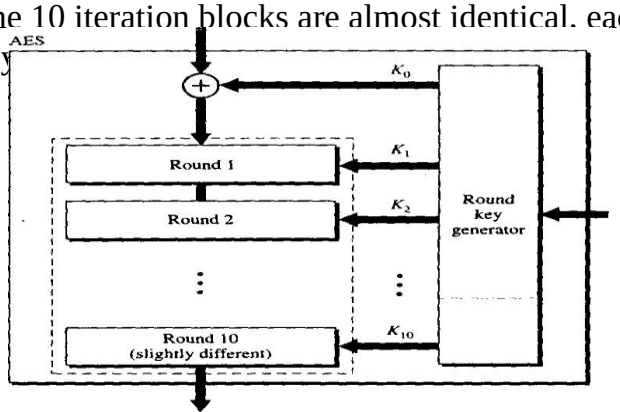


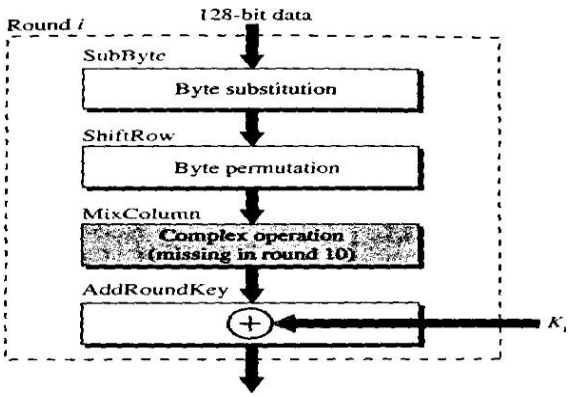
Figure 3.17

Structure of Each Round Each round of AES, except for the last, is a cipher with four, operations that are invertible. The last round has only three operations. Figure 3.18 11E a flowchart that shows the operations in each round. Each of the four operations used id each round uses a complex cipher; this topic is beyond the scope of this book.

Other Ciphers

During the last two decades, a few other symmetric block ciphers been designed and used. Most of these ciphers have similar characteristics to the two ciphers we discussion in this chapter (DES and AES). The difference is usually in the size of the block or key, number of rounds, and the functions used. The principles are the same. In order not burden the user with the details of these ciphers, we give a brief description of each.

Figure 3.18 Structure of each round



IDEA The International Data Encryption Algorithm (IDEA) was developed by Xuejia Lai and James Massey. The block size is 64 and the key size is 128. It can be implemented in both hardware and software. Blowfish was developed by Bruce Schneier. The block size is 64 and the key size between 32 and 448.

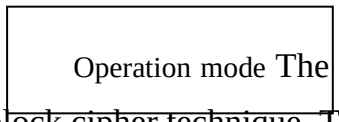
CAST-12% CAST 129 was developed by Carlisle Adams and Stafford Tavares. It is a Feistel cipher with 16 rounds and a block size of 64 bits; the key size is 128 bits.

RC5 RCS was designed by Ron Rivest. It is a family of ciphers with different block sizes, key sizes, and numbers of rounds.

Mode of Operation

A mode of operation is a technique that employs the modem block ciphers such as DES and AES that we discussed earlier (see Figure 3.19).

Figure 3.19 Modes of operation for block ciphers



The electronic code book (ECB) mode is a purely block cipher technique. The plain$_{ECB}$ text is divided into blocks of N bits. The ciphertext$_{CBC\ CFB\ OFB}$ is made of blocks of N bits. The value of N depends on the type of cipher used. Figure 3.20 shows the method.

Figure 3.20 ECB Mode

We mention four characteristics of this mode:

1. Because the key and the encryption/decryption algorithm are the same, equal blocks in the plaintext become equal blocks in the ciphertext. For example, if plaintext blocks 1, 5, and 9 are the same, ciphertext blocks 1, 5, and 9 are also the same. This can be a security problem; the adversary can guess that the plaintext blocks are the same if the corresponding ciphertext blocks are the same.
2. If we reorder the plaintext block, the ciphertext is also reordered.
3. Blocks are independent of each other. Each block is encrypted or decrypted independently. A problem in encryption or decryption of a block does not affect other blocks.
4. An error in one block is not propagated to other blocks. If one or more bits are corrupted during transmission, it only affects the bits in the corresponding plaintext after decryption. Other plaintext blocks are not affected. This is a real advantage if the channel is not noise-free.

Cipher Block Chaining

The cipher block chaining (CBC) mode tries to alleviate some of the problems in ECB by including the previous cipher block in the preparation of the current block. If the current block is i, the previous ciphertext block Ci-1 is included in the encryption of block t‘ In other words, when a block is completely enciphered, the block is sent, but a copy of it is kept in a register (a place where data can be held) to be used in the encryption of the next block. The reader may wonder about the initial block. There is no ciphertext block. 11 before the first block. In this case, a phony block called the initiation vector (IV) is used. Both

the sender and receiver agree upon specific predetermined IV. In other words, the IV is used instead of the nonexistent Co. Figure 30.21 shows the CBC mode.

The reader may wonder about the decryption. Does the configuration shown in figure guarantee the correct decryption? It can be proven that it does, but we leave proof to a textbook in network security.

The following are some characteristics of CBC.

l. Even though the key and the encryption/decryption algorithm are the same, equal blocks in the plaintext do not become equal blocks in the ciphertext. For example, if plaintext blocks 1, 5, and 9 are the same, ciphertext blocks 1, 5, and 9 will not be the same. An adversary will not be able to-guess from the ciphertext that two blocks are the same.

2. Blocks are dependent on each other. Each block is encrypted or decrypted based on a previous block. A problem in encryption or decryption of a block affects other blocks.

3. The error in one block is propagated to the other blocks. If one or more bits are corrupted during the transmission, it affects the bits in the next blocks of the plaintext after decryption.

Cipher Feedback

The cipher feedback (CFB) mode was created for those situations in which we need to send or receive r bits of data, where r is a number different from the underlying block size of the encryption cipher used. The value of r can be 1, 4, 8, or any number of bits. Since all block ciphers work on a block of data at a time, the problem is how to encrypt just r bits. The solution is to let the cipher encrypt a block of bits and use only the first r bits as a new key (stream key) to encrypt the r bits of user data. Figure 30.22 shows the configuration.

The following are some characteristics of the CFB mode:

1. If we change the IV from one encryption to another using the same plaintext, the ciphertext is different.
2. The ciphertext Ci depends on both Pi and the preceding ciphertext block.
3. Error in one or more ciphertext block affects the next ciphertext blocks.

Output Feedback

The output feedback (OFB) mode is very similar to the. CFB mode with one difference. Each bit in the ciphertext is independent of the previous bit or bits. This avoids error propagation. If an error occurs in transmission, it does not affect the future bits. Note that, as in CFB, both the sender and the receiver use the encryption algorithm. Note also that

in OFB, block ciphers such as DES or AES can only be used to create the key stream. The feedback for creating the next bit stream comes from the previous bits of the key stream instead of the ciphertext. The ciphertext does not take part in creating the key stream. Figure 30.23 shows the OFB mode.

Figure 30.23 OFB mode

The following are some of the characteristics of the OFB mode

1. If we change the IV from one encryption to another using the same plaintext, tile, ciphertext will be different.
2. The ciphertext Ci depends on the plaintext Pi.
3. Errors in one or more bits of the ciphertext do not affect future ciphertext blocks.

3.2 ASYMMETRIC-KEY CRYPTOGRAPHY

In the previous sections, we discussed symmetric-key cryptography. In this section we introduce asymmetric-key (public key cryptography). As we mentioned before, an asymmetric-key (or public-key) cipher uses two keys: one private and one public. We discuss two algorithms: RSA and Diflie-Heliman.

RSA

The most common public key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). It uses two numbers, e and d, as the public and private keys, as shown in Figure 3.24.

Figure 3.24 RSA

The two keys, e and d, have a special relationship to each other, a discussion of this relationship is beyond the scope of this book. We just show how to calculate the keys without proof.

Selecting Keys

Bob use the following steps to select the private and public keys:

1. Bob chooses two very large prime numbers p and q. Remember that a prime number is one that can be divided evenly only by 1 and itself.
2. Bob multiplies the above two primes to find n, the modulus for encryption and decryption. In other words, $n = p \times q$.
4. Bob chooses a random integer e. He then calculates d so that $d \times e = 1 \bmod \varphi$.
5. Bob announces e and n to the public; he keeps φ and d secret.

In RSA, e and n are announced to the public; d and φ are kept secret.

Encryption

Anyone who needs to send a message to Bob can use n and e. For example, if Alice needs to send a message to Bob, she can change the message, usually a short one, to an integer. This is the plaintext. She then calculates the ciphertext, using e and n.

C = Pe (mod n)

Alice sends C, the ciphertext, to Bob.

Decryption

Bob keeps φ and d private. When he receives the ciphertext, he uses his private key d to decrypt the message:

P = C'd (mod n)

Restriction

For RSA to work, the value of P must be less than the value of n. If P is a large number, the plaintext needs to be divided into blocks to make P less than it.

Example 3.7

Bob chooses 7 and 1 I as p and q and calculates n = 7 - I I = 77. The value of φ = (7 - 1) (11 - 1) or 60. Now he chooses two keys, e and d. If he chooses e to be 13, then d is 37. Now imagine Alice sends the plaintext 5 to Bob. She uses the public key 13 to encrypt 5.

Plaintext: 5

C=513=26 mod 77

Ciphertext: 26

Bob receives the ciphertext 26 and uses the private key 37 to decipher the ciphertext: Ciphertext: 26

P = 2637 = 5 mod 77

Plaintext: 5

The plaintext 5 sent by Alice is received as plaintext 5 by Bob

Example 3.8

Jennifer creates a pair of keys for herself. She chooses p = 397 and q = 401. She calculates n 159,197 and φ = 396 400 = 153.400. She then chooses e = 343 and d = 12,007. Show how Ted can send a message to Jennifer if he knows e and n.

Solution

Suppose Ted wants to send the message "NO- to Jennifer. He changes each character to a uwui" (front 00 to 25) with each character coded as two digits. He then concatenates the two coded characters and gets a four-digit number. The plaintext is 1314. Ted then uses e and n to encrypt the message. The ciphertext is 13143't3 = 33,677 mod 159,197. Jennifer receives the message.

33,677 and uses the decryption key d to decipher it as 33,67712,007 = 1314 mod 159,197. Jennifer then decodes 1314 as the message “NO”.
Figure 3.25 shows the process.
Figure 3.25 Example 3.8
Example 3.9
Let us give a realistic example. We choose a -512-bit p and q. We calculate n and φ. We then choose e and test for relative primeness with φ(n). We calculated. Finally, we show the results of encryption and decryption. We have written a program written in Java to do so: this type of calculation cannot be done by a calculator.

We randomly chose an integer of 512 bits. The integerp is a 159-digit number.

P=961303453135835045741915812806154279093098455949962158225831508796479404550564706384912571601803475031209866660649242019180878066742109606335421992666120 9
The integer q is a 160-digit-number.
q=120601919572314469182767942044508960015559250546370339360617983217314821484837646592153894532091752252732268301071206956046025138871455249690003596600456 17
We calculate n. It has 309 digits.
n=115935041739676149688925098646158875237714573754541447754855261376147885408326350817276878815968325168468849300625485764111250162417552339182927162507656772727460097082714127730434960500556347274566628060099924037102991424472292215772798531727033839381334692684137327622000966676671831831088373420823444370953
We calculate φ. It has 309 digits:
φ=98646158875237714573754541447754855261376147885408326350817276878815968325168468849300625485764111250162-114552339 1829
271625076567510542336084929167520344826279881175547876570139234444057169895817281960982263610754672118646121713591073586406140088851702653772 7264467341066243857664128 We choose e = 35,535. We then find d. e = 35535
d=58008302860037763936093661289677917594669062089650962180
42286611138059385282235873170628691003002171085904433840 21
70729869087600611530620252495988444804756824096624708148581713046324064407770483313401085094738529564507193677406119732655742423721761767462077637164207600337085333288532144708859551 36670294831

Alice wants to send the message “THIS IS A TEST” which can be changed to a numeric value by using the 00-26 encoding scheme (26 is the space character).
P = 19070818260818260026190418 19
The ciphertext calculated by Alice is C = Pe, which is
C=47530912364622682720636555061054518094237179607049171 65
23239243054452960613199328566617843418359114151197411252 00
56829797945717360361012782188478927415660904800235071907 15
27718591497518846588863210114835410336165789846796838676 37
33765777465625079280521148141844048141844308127730590046 92
874248559166462108656
Bob can recover the plaintext from the ciphertext by using P = Cd, which is
P = 19070818260818260026190418 19
The recovered plaintext is THIS IS A TEST after decoding.

Applications

Although RSA can be used to encrypt and decrypt actual messages, it is very slow if the message is long. RSA, therefore, is useful for short messages such as a small message digest (see Chapter 31) or a symmetric key to be used for a symmetric-key cryptosystem.’ In particular, we will see that RSA is used in digital signatures and other cryptosystems that often need to encrypt a small message without having access to a symmetric ke RSA is also used for authentication as we will see later.

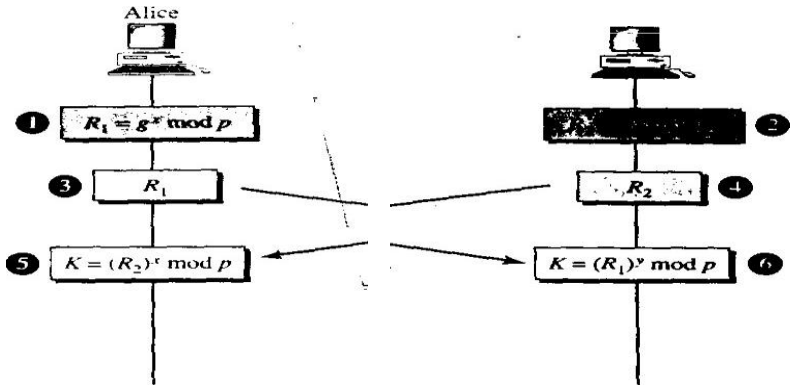
Diffie-Hellman

RSA is a public-key cryptosystem that is often used to encrypt and decrypt symmetric keys. Diffie-Hellman, on the other hand, was originally designed for key exchange. They do not have tom meet to agree on the key; it can be done through the Internet. Let us see how the protocol w when Alice and Bob need a symmetric key to communicate.

Before establishing a symmetric key, the two parties need to choose two numbers p and g. The first number, p, is a large prime number on the order of 300 decimal digits (1024 bits). The second number is a random number. These two numbers need not be confidential. They can be sent through the Internet; they can be public.

Procedure

Figure 3.26 shows the procedure. The steps are as follows:
Figure 3.26 Diffie-Hellman method



Step 1: Alice chooses a large random number x and calculates R, = gx mod p.
Step 2: Bob chooses another large random number y and calculates R2 = gy mod p.
Step 3: Alice sends RI to Bob. Note that Alice does not send the value of x; she sends only R1
Step 4: Bob sends R2, to Alice. Again, note that Bob does not send the value of y, he sends only R
Step 5: Alice calculates K = (R2)3 mod p.
Step 6: Bob also calculates K= (R1) mod p.

The symmetric key for the session is K,
(gx mod pyy mod p = (gy mod pyx mod p = gxy mod p =

3. Bob chooses y, calculates R3 = gy. mod p, and sends R3 to Alice; R3 is intercepted by Eve and never reaches Alice.
4. Alice and Eve calculate K1 = gxz mod p, which becomes a shared key between Alice and Eve. Alice, however, thinks that it is a key shared between Bob and herself.
5. Eve and Bob calculate K2 = gzy mod p, which becomes a shared key between Eve and Bob. Bob, However, thinks that it is a key shared between Alice and himself.

In other words, two keys, instead of one, are created: one between Alice and Eve and one between Eve and Bob. When Alice sends data to Bob encrypted with Kt (shared by Alice and Eve), it can be deciphered and read by Eve. Eve can send the message to Bob encrypted by K2 (shared key between Eve and Bob); or she can even change the message or send a totally new message. Bob is fooled into believing that the message has come from Alice. A similar scenario can happen to Alice in the other direction.

This situation is called a man-in-the-middle attack because Eve comes in between and intercepts R1, sent by Alice to Bob, and R3, sent by Bob to Alice. It is also known as a bucket brigade attack because it resembles

a short line of volunteers passing a bucket of water from person to person.

Authentication

The man-in-the-middle attack can be avoided if Bob and Alice first authenticate each other. In other words, the exchange key process can be combined with an authentication scheme to prevent a man-in-the-middle attack:

6.0 CONCLUSION
7.0

Cryptography algorithms (ciphers) are divide into two groups: symmetric key (also called secret-key) cryptography algorithms and asymmetric (also called public-key).

5.0 SUMMARY

Cryptography is the science and art of transforming messages to make them secure and immune to attacks.

The plaintext is the original message before transformation; the ciphertext is the message after transformation.

An encryption algorithm transforms plaintext to ciphertext; a decryption algorithm transforms ciphertext to plaintext.

A combination of an encryption algorithm and a decryption algorithm is called a cipher.

The key is a number or a set of numbers on which the cipher operates.
We can divide all ciphers into two broad categories: symmetric-key ciphers and asymmetric-key ciphers.

In a symmetric-key cipher, the same key is used by both the sender and receiver. The key is called the secret key.

In an asymmetric-key cipher, a pair of keys is used. The sender uses the public key; the receiver uses the private key. A substitution cipher replaces one character with another character.

Substitution ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.

The shift cipher is tile simpicst nionoalphabctic cipher. It uses modular arithmetic with a modulus of 26. The Caesar cipher is a shift cipher that has a key of 3.

The transposition cipher reorders the plaintext characters to create a ciphertext. An XOR cipher is the simplest cipher which is selfinvertible.

A rotation cipher is an invertible cipher.

An S-box is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream.

A P-box is a keyless transposition cipher with N inputs and M outputs that uses a table to define the relationship between the input stream and the output stream. A P-box is invertible only if the numbers of inputs and outputs are the same. A P-box can use a straight permutation, a compression permutation, or an expansion permutation.

DES uses a key generator to generate sixteen 48-bit round keys.

Triple DES was designed to increase the size of the DES key (effectively 56 bits) for better security.

AES is a round cipher based on the Rijndael algorithm that uses a 128bit block of data. AES has three different configurations: 10 rounds with a key size of 128 bits, 12 rounds with a key size of 192 bits, and 14 rounds with a key size of 256 bits.

Mode of operation refers to techniques that deploy the ciphers such as DES or AES. Four common modes of operation are ECB, CBC, CBF, and OFB. ECB and CBC are block ciphers; CBF and OFB are stream ciphers.

One commonly used public-key cryptography method is the RSA algorithm, invented by Rivest, Shamir, and Adleman.

RSA chooses n to be the product of two primes p and q.
The Diffie-Hellman method provides a one-time session key for two parties.

The man-in-the-middle attack can endanger the security of the DiffieHellman method if two parties are not authenticated to each other.

Network Security

In this unit, we introduced the science of cryptography. Cryptography has several applications in network security. We first introduce the security services we typically expect in a network. We then show how

these services can he provided using cryptography. At the end of the Unit, we also touch on the issue of distributing symmetric and asymmetric keys.

6.0 Tutor-marked Assignment

1. What is a Cipher?
2. Outline the three types of Keys in Cryptography?
3. Differentiate between Symmetric-Key Cryptography and symmetric-Key Cryptography.

7.0 References/Further Reading

M. Millenkovic, Operating Systems: Concepts and Design, Second Edition, Tata McGraw –Hill.
R.O Ayeni, Computer Fundamentals

UNIT 4 NETWORK SECURITY

CONTENTS

1.0 OBJECTIVES

At the end of this unit you should be able to;

- Explain the services provided by network security.
- Discuss Message in a network and
- Explain Entity Integrity

2.0 INTRODUCTION

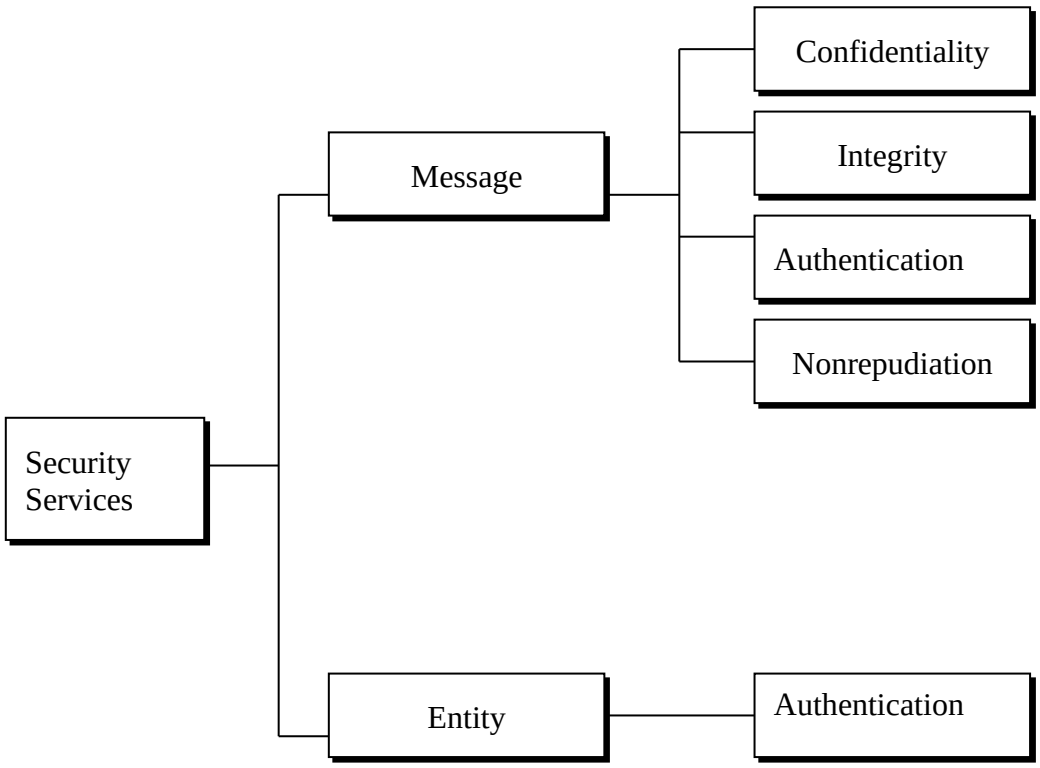
In this unit we first introduce the security services common in most networks. We then show how these services can be provided using cryptography. At the

end of the unit, we also touch on the issue of distributing symmetric and asymmetric keys.

3.1 Security Services

Network Security can provide one of the five services as shown in Figure 6.4.1. Four of these services are related to the message exchanged using the network: message confidentiality, integrity, authentication, and nonrepudiation. The fifth services provides entity authentication on identification.

Figure 6.4.1 Security services related to the message or entity



3.2 Message Exchanged Security

3.2.1 Message Confidentiality

Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

3.2.2 Message Integrity

Message Integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally or maliciously. For instance it will be disastrous if a request for transferring ₦ 300,000 is changed to ₦ 3,000,000.

3.2.3 Message Authentication

Message authentication is a service beyond message integrity. In message authentication the receiver is to be sure of the sender's identity and that an imposter has not sent the message.

3.2.4 Message Non repudiation

Message nonrepudiation means that a sender must not be able to deny sending a message that he or she did send. The burden of proof falls on the receiver. For example when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested the this transaction.

3.3 Entity Authentication

In entity authentication the entity or user is verified prior to access to the system resources. For example, a student who needs to access her university resources needs to be authenticated during the logging process. This protects the interest of the university and the student.

4.0 CONCLUSION

In this unit we have learnt security services in a network for the message: its confidentiality, integrity, authentication and nonrepudiation and also for an entity, such as the user, to protect him and the agency his transacting with.

5.0 SUMMARY

Network security can provide five services. Four of these are related to the message between two parties. The fifth is related to the entity trying to access a system for using its resources.

Message confidentiality means that the sender and the receiver expects privacy. Message integrity means that the data must arrive at the receiver exactly as sent. Message authentication means that the receiver is ensured that the message is coming from the intended sender, not an imposter. Nonrepudiation means that a sender must not be able to deny sending a message that he sent. Entity authentication means to prove the identity of the entity that tries to access the system's resources.

6.0TUTOR-MARKED ASSIGNMENT

1 . Discuss the five services provided by Network security.

7.0REFERENCES/FURTHER READING

Schiller, B. Mobile Communications. Reading, MA: Addison-Wesley, 2003.