DATA COMMUNICATION

[As per Choice Based Credit System (CBCS) scheme]

(Effective from the academic year 2016 -2017)

SEMESTER – IV

Subject Code	15CS46	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Comprehend the transmission technique of digital data between two or more computers and a computer network that allows computers to exchange data.
- Explain with the basics of data communication and various types of computer networks;
- Illustrate TCP/IP protocol suite and switching criteria.
- Demonstrate Medium Access Control protocols for reliable and noisy channels.
- Expose wireless and wired LANs along with IP version.
- Illustrate basic computer network technology.
- Identify the different types of network topologies and protocols.
- Enumerate the layers of the OSI model and TCP/IP functions of each layer.
- Make out the different types of network devices and their functions within a network

Contents	Teaching Hours
Module 1	
Introduction: Data Communications, Networks, Network Types, Internet History, Standards and Administration, **Networks Models**: Protocol Layering, TCP/IP Protocol suite, The OSI model, **Introduction to Physical Layer-1:** Data and Signals, Digital Signals, Transmission Impairment, Data Rate limits, Performance, **Digital Transmission**: Digital to digital conversion (Only Line coding: Polar, Bipolar and Manchester coding).	**10 Hours**
Module 2	
Physical Layer-2: Analog to digital conversion (only PCM), Transmission Modes, **Analog Transmission**: Digital to analog conversion, **Bandwidth Utilization**: Multiplexing and Spread Spectrum, **Switching**: Introduction, Circuit Switched Networks and Packet switching.	**10 Hours**
Module 3	
Error Detection and Correction: Introduction, Block coding, Cyclic codes, Checksum, Forward error correction**, Data link control**: DLC services, Data link layer protocols, HDLC, and Point to Point protocol (Framing, Transition phases only).	**10 Hours**
Module 4	
Media Access control: Random Access, Controlled Access and Channelization, **Wired LANs Ethernet**: Ethernet Protocol, Standard Ethernet, Fast Ethernet, Gigabit Ethernet and 10 Gigabit Ethernet, **Wireless LANs:** Introduction, IEEE 802.11 Project and Bluetooth.	**10 Hours**
Module 5	
Other wireless Networks: WIMAX, Cellular Telephony, Satellite networks, **Network layer Protocols** : Internet Protocol, ICMPv4,Mobile IP, **Next generation IP**: IPv6 addressing, The IPv6 Protocol, The ICMPv6 Protocol and Transition from IPv4 to IPv6.	**10 Hours**

Course Outcomes: The students should be able to:

- Illustrate basic computer network technology.
- Identify the different types of network topologies and protocols.
- Enumerate the layers of the OSI model and TCP/IP functions of each layer.
- Make out the different types of network devices and their functions within a network
- Demonstrate the skills of subnetting and routing mechanisms.

Graduate Attributes

1. Engineering Knowledge
2. Design Development of solution(Partly)
3. Modern Tool Usage
4. Problem Analysis 10904383

Question paper pattern:

The question paper will have ten questions. There
will be 2 questions from each module.
Each question will have questions covering all the topics under a module.
The students will have to answer 5 full questions, selecting one full question from each module.

Text Book:

Behrouz A. Forouzan, Data Communications and Networking 5E, 5th Edition, Tata McGraw-Hill, 2013. (Chapters 1.1 to 1.5, 2.1 to 2.3, 3.1, 3.3 to 3.6, 4.1 to 4.3, 5.1, 6.1, 6.2, 8.1 to 8.3, 10.1 to 10.5, 11.1 to 11.4, 12.1 to 12.3, 13.1 to 13.5, 15.1 to 15.3, 16.1 to 16.3, 19.1 to 19.3, 22.1 to 22.4)

Reference Books:

1. Alberto Leon-Garcia and Indra Widjaja: Communication Networks - Fundamental Concepts and Key architectures, 2nd Edition Tata McGraw-Hill, 2004.
2. William Stallings: Data and Computer Communication, 8th Edition, Pearson Education, 2007.
3. Larry L. Peterson and Bruce S. Davie: Computer Networks – A Systems Approach, 4th Edition, Elsevier, 2007.
4. Nader F. Mir: Computer and Communication Networks, Pearson Education, 2007

MODULE 1

Chapter 1

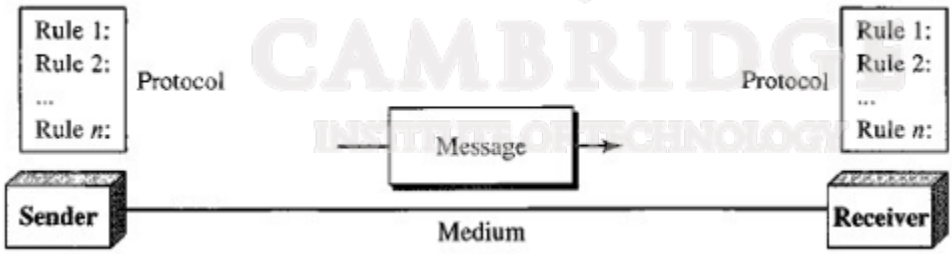
Introduction

1.1 DATA COMMUNICATIONS

Data communications are 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.

1. 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:



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 physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair

wire,coaxial cable, fiber-optic cable, and radio waves.
5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

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 (0s or 1s).Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.

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

Images
Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better 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 size and the value of the pattern depend 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.

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.

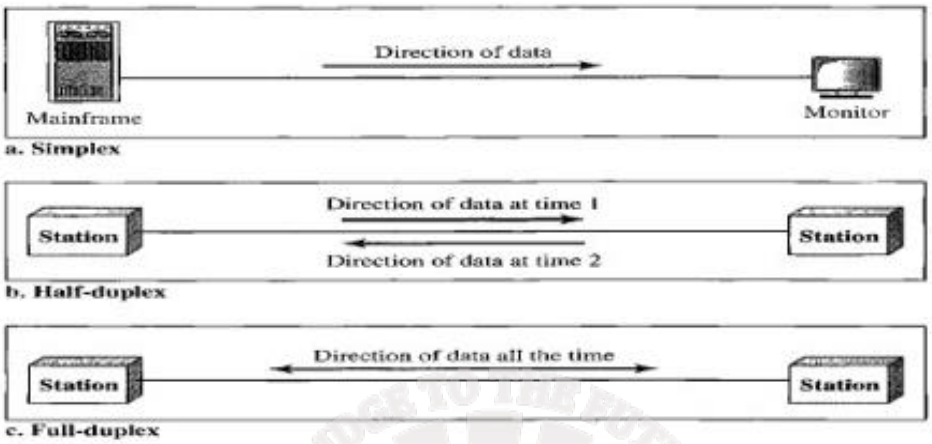
Audio
Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

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.



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. 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. In a half-duplex transmission,the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

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

Full-Duplex

In full-duplex made (also, called duplex), both stations can transmit and receive simultaneously.In full-duplex mode, signals going in one direction share the 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, one for sending and the other for receiving; or the capacity of the channel is divided between signals travelling in both directions.

One common example of full-duplex communication is the telephone network. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

1.2 NETWORKS

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/or receiving data generated by other nodes on the network. A device can also be a connecting device such as a

router, which connects the network to other networks, a switch, which connects devices together, a modem (modulator-demodulator), which changes the form of data, and so on. These devices in a network are connected using wired or wireless transmission media such as cable or air.

Network Criteria

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

Performance

Performance can be measured in many ways, including transit time and response time. Transit 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, and the efficiency of the software. Performance is often evaluated by two networking metrics: throughput and delay.We often need more throughput and less delay.

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

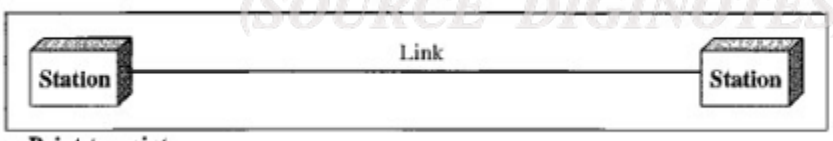
Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Physical Structures

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 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.

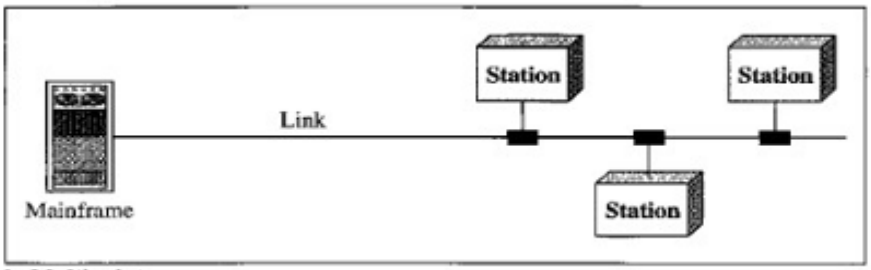
Point-to-Point A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.



a. Point-to-point

Multipoint A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is

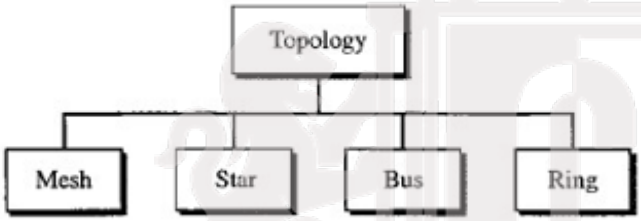
shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



b. Multipoint

Physical Topology

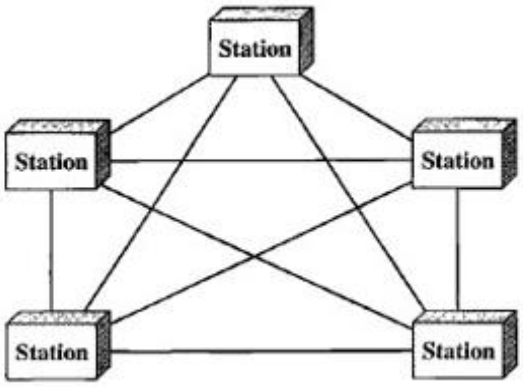
The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.



Mesh In a mesh topology, every device has a dedicated point-to-point link to every other device.The term dedicated means that the link carries traffic only between the two devices it connects.To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n-1 nodes, node 2 must be connected to n-1 nodes, and finally node n must be connected to n-1 nodes. We need n(n-1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need

$$n(n - 1) / 2$$

duplex-mode links.



A mesh offers several **advantage**s over other network topologies.

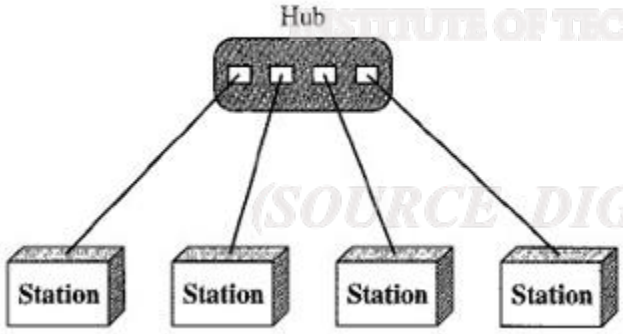
1 .The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

The main **disadvantage**s of a mesh are related to the amount of cabling and the number of I/O ports required.

1. Because every device must be connected to every other device, installation and reconnection are difficult.
2. The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
3. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

Star Topology In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.



Advantages:

1. A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and

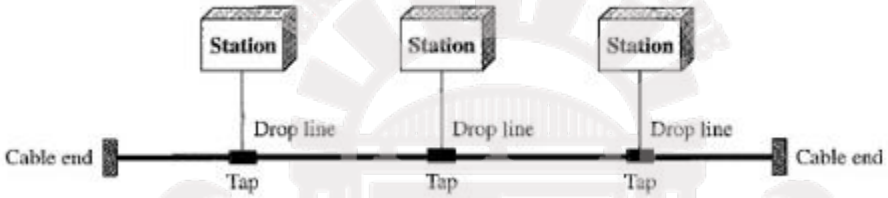
reconfigure. Far less cabling needs to be housed, and additions, moves,and deletions involve only one connection: between that device and the hub.

2. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active.This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:

1. One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
2. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies.

Bus Topology The preceding examples all describe point-to-point connections. A bus topology,on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.



Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

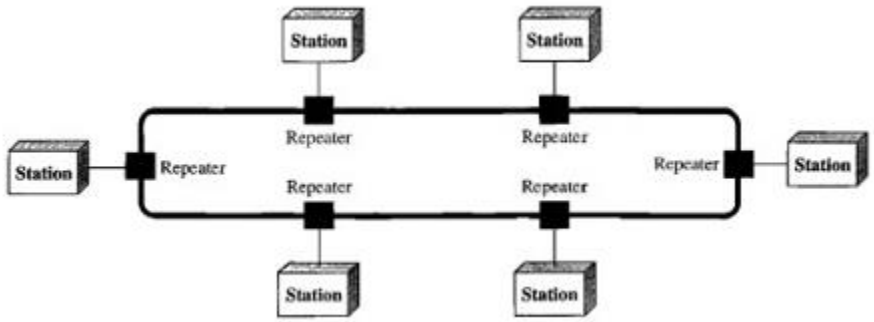
Advantages:

1. Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.
2. In a bus, redundancy is eliminated. Only the backbone cable stretches through the entiry facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages:

1. Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
2. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.
3. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring Topology In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



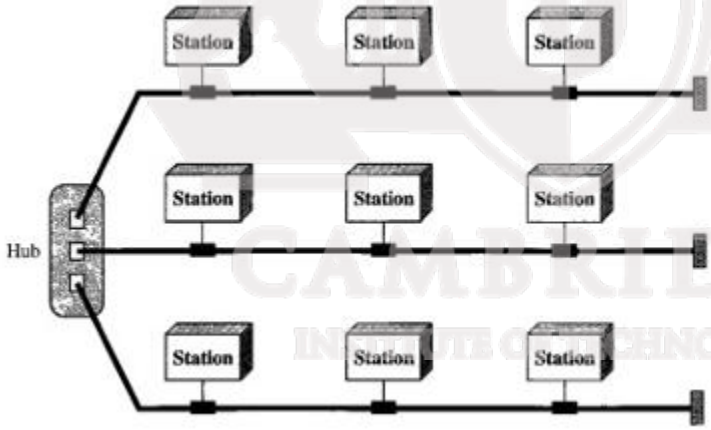
Advantages:

1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors.
2. To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices).
3. In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

1. Unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using as dual ring or a switch capable of closing off the break.

Hybrid Topology A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown:



1.3 NETWORK TYPES

1.3.1 Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office,building, or campus. Depending on the needs of an organization and the type of technology used,a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

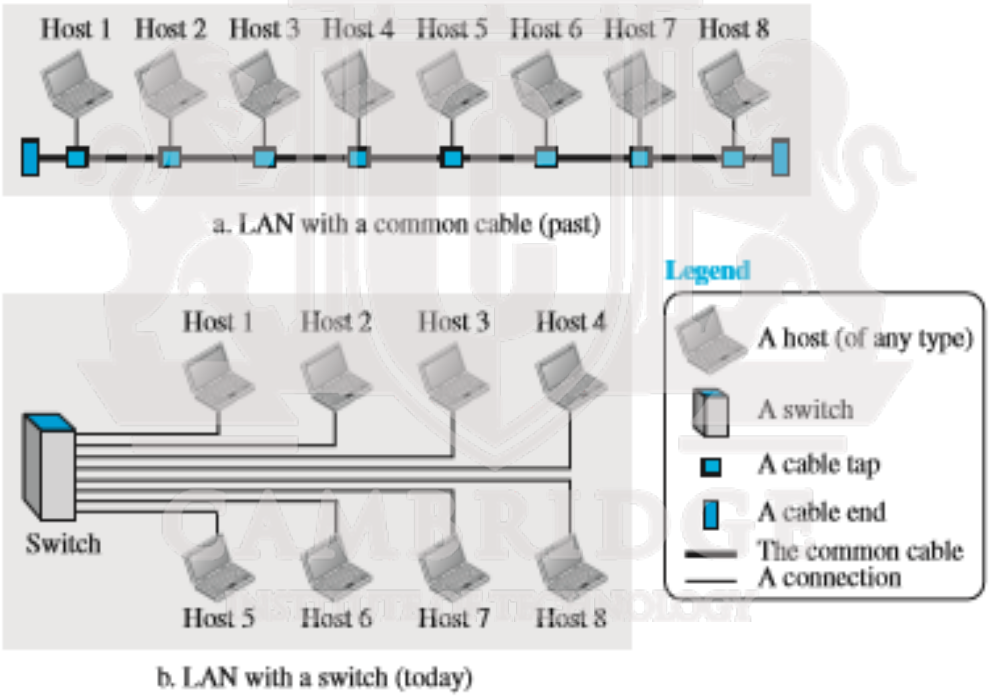
LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. A

common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium.The most common LAN topologies are bus, ring, and star.

In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet. Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts. The switch alleviates the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them. Note that the above definition of a LAN does not define the minimum or maximum number of hosts in a LAN. Figure 1.8 shows a LAN using either a common cable or a switch.

Figure 1.8 *An isolated LAN in the past and today*



1.3.2 Wide Area Network

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home

computer to the Internet. We see two distinct examples of WANs today: point-to-point WANs and switched WANs.

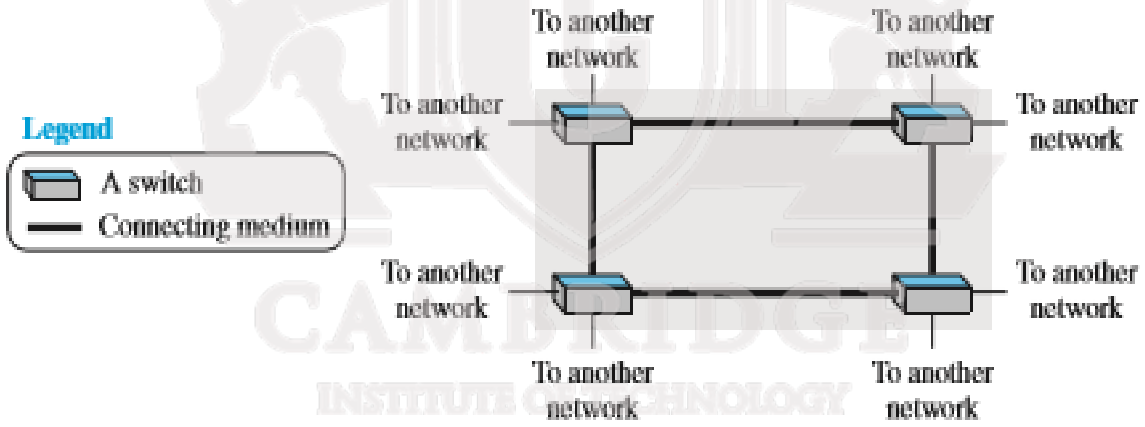
A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air). We will see examples of these WANs when we discuss how to connect the networks to one another. Figure 1.9 shows an example of a point-to-point WAN.

Figure 1.9 *A point-to-point WAN*

A switched WAN is a network with more than two ends. A switched WAN, as we will see shortly, is used in the backbone of global communication today. We can say that a switched WAN is a combination of several point-to-point WANs that are connected by switches. Figure 1.10 shows an example of a switched WAN.

LANs

Figure 1.10 *A switched WAN*

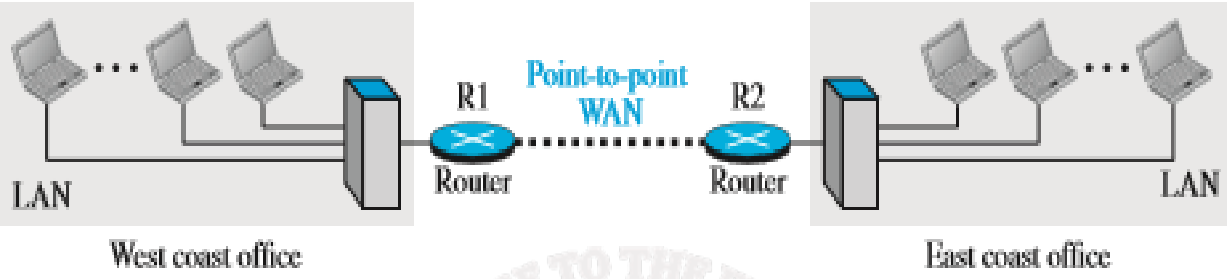


Interconnection of Networks: Internetwork

Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are connected to one another. When two or more networks are connected, they become an internetwork, or internet.

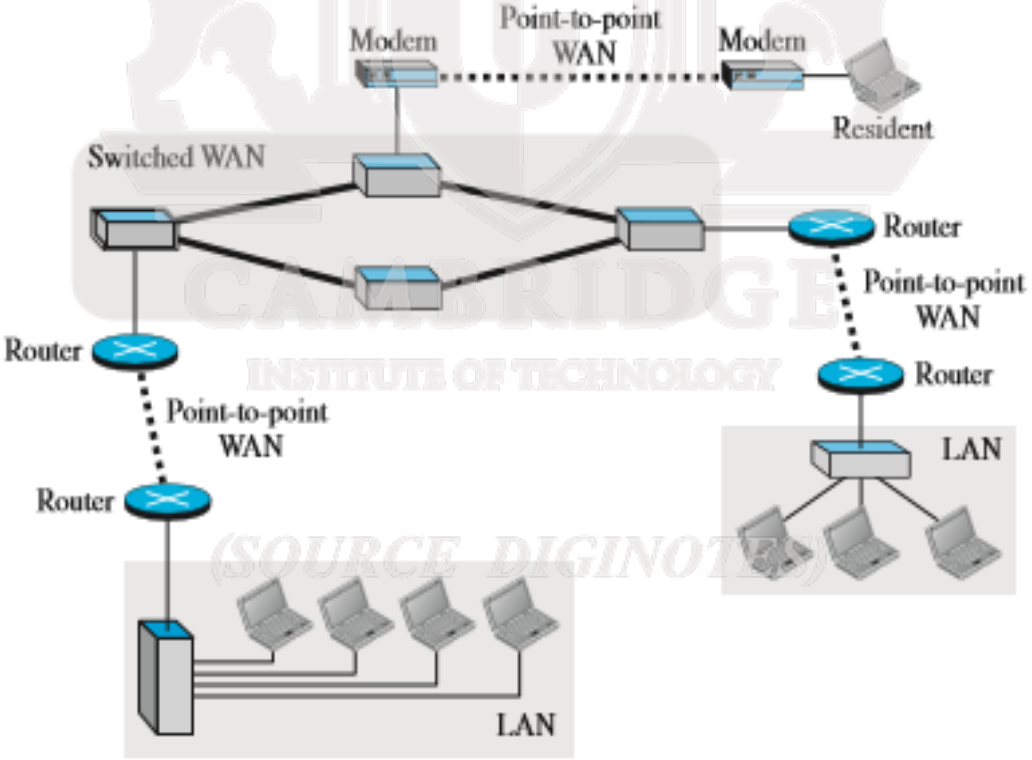
As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. Each office has a LAN that allows all employees in the office to communicate with each other. To make the communication between employees at different offices possible, the management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs. Now the company has an internetwork, or a private internet.Communication between offices is now possible. Figure 1.11 shows this internet.

Figure 1.11 *An internetwork made of two LANs and one point-to-point WAN*



When a host in the west coast office sends a message to another host in the same office, the router blocks the message, but the switch directs the message to the destination. On the other hand, when a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination. Figure 1.12 shows another internet with several LANs and WANs connected. One of the WANs is a switched WAN with four switches.

Figure 1.12 *A heterogeneous network made of four WANs and three LANs*



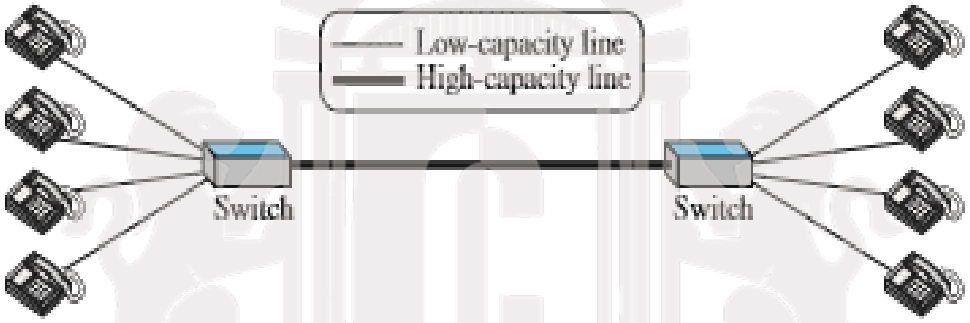
1.3.3 Switching

An internet is a switched network in which a switch connects at least two links together. A switch needs to forward data from a network to another network when required. The two most common types of switched networks are circuit-switched and packet-switched networks.

Circuit-Switched Network:

In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive. Figure 1.13 shows a very simple switched network that connects four telephones to each end. We have used telephone sets instead of computers as an end system because circuit switching was very common in telephone networks in the past, although part of the telephone network today is a packet-switched network.

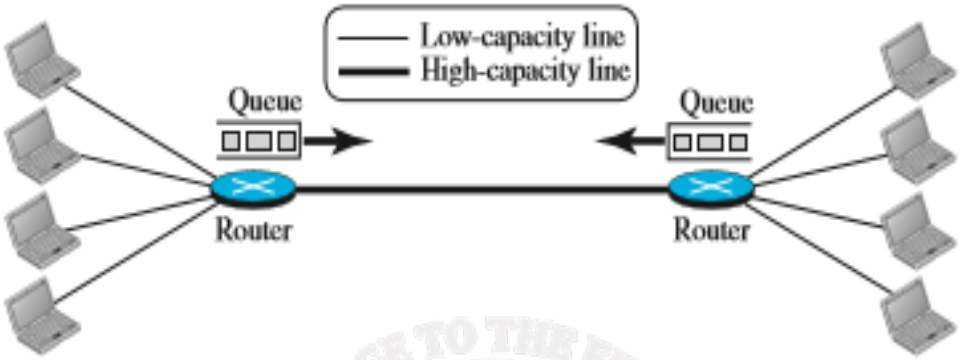
Figure 1.13 *A circuit-switched network*



Packet-Switched Network

In a computer network, the communication between the two ends is done in blocks of data called packets. In other words, instead of the continuous communication we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers. This allows us to make the switches function for both storing and forwarding because a packet is an independent entity that can be stored and sent later. Figure 1.14 shows a small packet-switched network that connects four computers at one site to four computers at the other site.

Figure 1.14 *A packet-switched network*



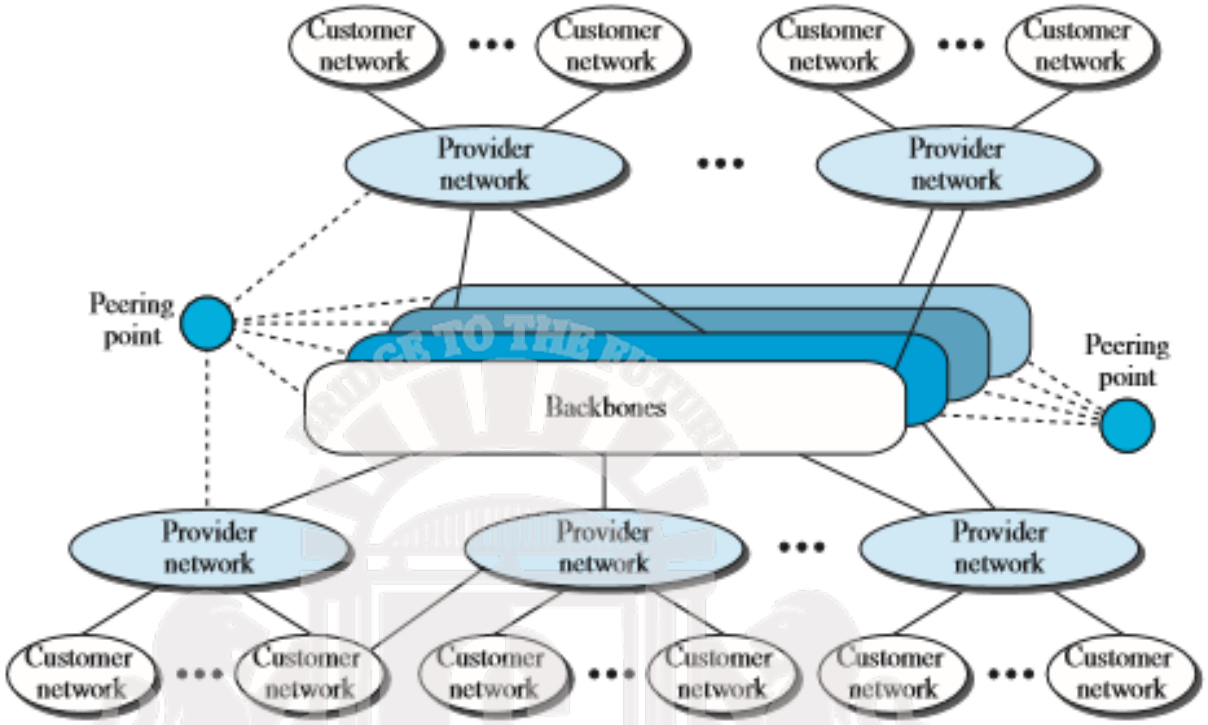
A router in a packet-switched network has a queue that can store and forward the packet. However, if packets arrive at one router when the thick line is already working at its full capacity, the packets should be stored and forwarded in the order they arrived

1.3.4 THE INTERNET

The most notable internet is called the Internet , and is composed of thousands of interconnected networks. Figure 1.15 shows a conceptual (not geographical) view of the Internet. The figure shows the Internet as several backbones, provider networks, and customer networks.

- At the top level, the backbones are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT.
- The backbone networks are connected through some complex switching systems, called peering points.
- At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee.
- The provider networks are connected to backbones and sometimes to other provider networks.
- The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services.
- Backbones and provider networks are also called Internet Service Providers (ISPs).
- The backbones are often referred to as international ISPs; the provider networks are often referred to as national or regional ISPs.

Figure 1.15 *The Internet today*



1.3.5 Accessing the Internet

The Internet today is an internetwork that allows any user to become part of it. The user, however, needs to be physically connected to an ISP. The physical connection is normally done through a point-to-point WAN.

- **Using Telephone Networks**: Today most residences and small businesses have telephone service, which means they are connected to a telephone network. Since most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN. This can be done in two ways.

  ❑ Dial-up service. The first solution is to add to the telephone line a modem that converts data to voice. The software installed on the computer dials the ISP and imitates making a telephone connection. Unfortunately, the dial-up service is very slow, and when the line is used for Internet connection, it cannot be used for telephone (voice) connection. It is only useful for small residences.

  ❑ DSL Service. Since the advent of the Internet, some telephone companies have upgraded their telephone lines to provide higher speed Internet services to residences or small businesses. The DSL service also allows the line to be used simultaneously for voice and data communication..

- **Using Cable Networks:** More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting. The cable companies have been upgrading their cable networks and connecting to the Internet. A

residence or a small business can be connected to the Internet by using this service. It provides a higher speed connection, but the speed varies depending on the number of neighbors that use the same cable.

- **Using Wireless Networks**:Wireless connectivity has recently become increasingly popular. A household or a small business can use a combination of wireless and wired connections to access the Internet. With the growing wireless WAN access, a household or a small business can be connected to the Internet through a wireless WAN.
- **Direct Connection to the Internet**: A large organization or a large corporation can itself become a local ISP and be connected to the Internet. This can be done if the organization or the corporation leases a high-speed WAN from a carrier provider and connects itself to a regional ISP. For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

1.4 INTERNET HISTORY

1.4.1 Early History

- There were some communication networks, such as telegraph and telephone networks, before 1960. These networks were suitable for constant-rate communication at that time, which means that after a connection was made between two users, the encoded message (telegraphy) or voice (telephony) could be exchanged.
- A computer network, on the other hand, should be able to handle bursty data, which means data received at variable rates at different times. The world needed to wait for the packet-switched network to be invented.

Birth of Packet-Switched Networks: The theory of packet switching for bursty traffic was first presented by Leonard Kleinrock in 1961 at MIT. At the same time, two other researchers, Paul Baran at Rand Institute and Donald Davies at National Physical Laboratory in England, published some papers about packet-switched networks.

ARPANET: In the mid-1960s, mainframe computers in research organizations were stand-alone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DOD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for the Advanced Research Projects Agency Network (ARPANET), a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP). The IMPs, in turn, would be connected to each other. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.

1.4.2 Birth of the Internet: In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Project. They wanted to link dissimilar networks so that a host on one network could communicate with a host on another. Cerf and Kahn devised the idea of a device called a gateway to serve as the intermediary hardware to transfer data from one network to another.

- **TCP/IP**: Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of data. This was a new version of NCP. This paper on transmission control protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway. A radical idea was the transfer of responsibility for error correction from the IMP to the host machine. This ARPA Internet now became the focus of the communication effort. Around this time, responsibility for the ARPANET was handed over to the Defense Communication Agency (DCA).
  In October 1977, an internet consisting of three different networks (ARPANET, packet radio, and packet satellite) was successfully demonstrated. Communication between networks was now possible.
  Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection. The new combination became known as TCP/IP.
  In 1981, under a Defence Department contract, UC Berkeley modified the UNIX operating system to include TCP/IP. This inclusion of network software along with a popular operating system did much for the popularity of internetworking. The open (non-manufacturer-specific) implementation of the Berkeley UNIX gave every manufacturer a working code base on which they could build their products.
  In 1983, authorities abolished the original ARPANET protocols, and TCP/IP became the official protocol for the ARPANET. Those who wanted to use the Internet to access a computer on a different network had to be running TCP/IP.

- **MILNET:** In 1983, ARPANET split into two networks: Military Network (MILNET) for military users and ARPANET for nonmilitary users.
- **CSNET:** Another milestone in Internet history was the creation of CSNET in 1981. Computer Science Network (CSNET) was a network sponsored by the National Science Foundation (NSF). The network was conceived by universities that were ineligible to join ARPANET due to an absence of ties to the Department of Defense. CSNET was a less expensive network; there were no redundant links and the transmission rate was slower. By the mid-1980s, most U.S. universities with computer science departments were part of CSNET. Other institutions and companies were also forming their own networks and using TCP/IP to interconnect. The term Internet, originally associated with government-funded connected networks, now referred to the connected networks using TCP/IP protocols.
- **NSFNET**: With the success of CSNET, the NSF in 1986 sponsored the National Science Foundation Network (NSFNET), a backbone that connected five supercomputer centers located throughout the United States. In 1990, ARPANET was officially retired and replaced by NSFNET. In 1995, NSFNET reverted back to its original concept of a research network.

- **ANSNET**:In 1991, the U.S. government decided that NSFNET was not capable of supporting the rapidly increasing Internet traffic. Three companies, IBM, Merit, and Verizon, filled the void by forming a nonprofit organization called Advanced Network & Services (ANS) to build a new, high-speed Internet backbone called Advanced Network Services Network (ANSNET).

1.4.3 Internet Today Today, we witness a rapid growth both in the infrastructure and new applications. The Internet today is a set of pier networks that provide services to the whole world. What has made the Internet so popular is the invention of new applications.

- **World Wide Web** The 1990s saw the explosion of Internet applications due to the emergence of the World Wide Web (WWW). The Web was invented at CERN by Tim Berners-Lee. This invention has added the commercial applications to the Internet.
- **Multimedia** Recent developments in the multimedia applications such as voice over IP (telephony), video over IP (Skype), view sharing (YouTube), and television over IP (PPLive) has increased the number of users and the amount of time each user spends on the network.
- **Peer-to-Peer Applications** Peer-to-peer networking is also a new area of communication with a lot of potential.

1.5 STANDARDS AND ADMINISTRATION

1.5.1 Internet Standards: An Internet standard is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft.

An Internet draft is a working document (a work in progress) with no official status and a six-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment (RFC).**

Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.

Maturity Levels: An RFC, during its lifetime, falls into one of six maturity levels: proposed standard, draft standard, Internet standard, historic, experimental, and informational (see Figure 1.16).

❑ Proposed Standard: A proposed standard is a specification that is stable, well understood, and of sufficient interest to the Internet community. At this level, the specification is usually tested and implemented by several different groups.

Draft Standard. A proposed standard is elevated to draft standard status after at least two successful independent and interoperable implementations. Barring difficulties, a draft standard, with modifications if specific problems are encountered, normally becomes an Internet standard.

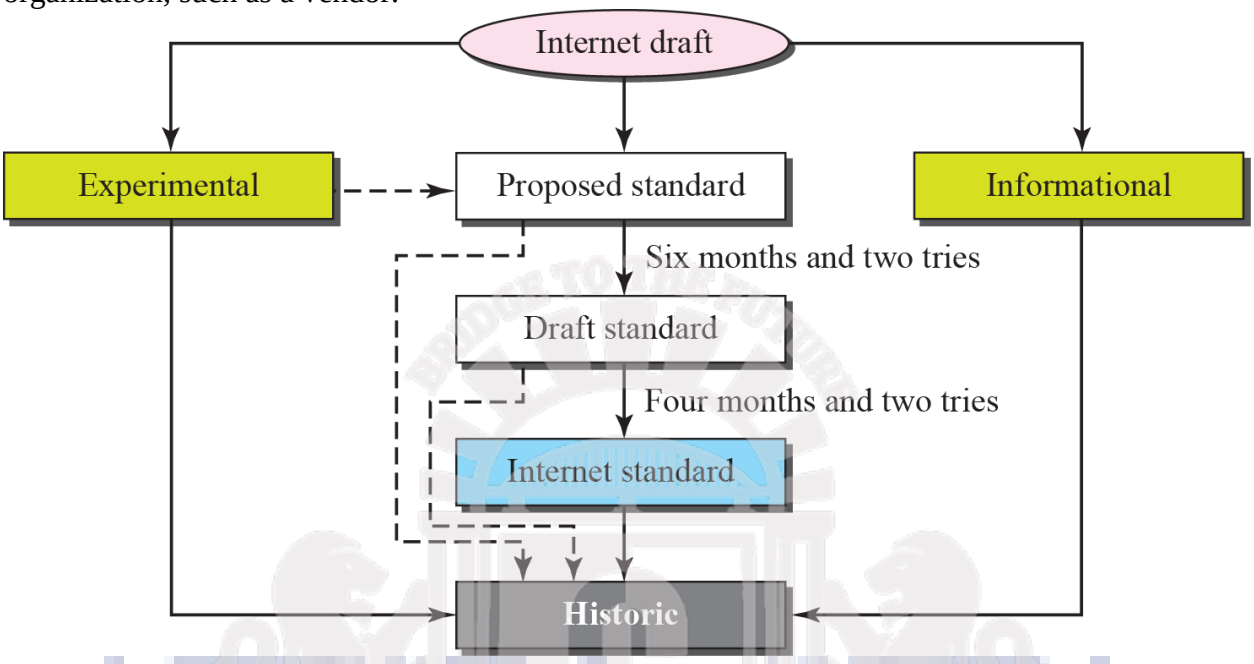
❑ Internet Standard:A draft standard reaches Internet standard status after demonstrations of successful implementation.

❑ Historic: The historic RFCs are significant from a historical perspective. They either have been superseded by later specifications or have never passed the necessary maturity levels to become an Internet standard.

❑ Experimental: An RFC classified as experimental describes work related to an experimental

situation that does not affect the operation of the Internet. Such an RFC should not be implemented in any functional Internet service.

❑ Informational: An RFC classified as informational contains general, historical, or tutorial information related to the Internet. It is usually written by someone in a non-Internet organization, such as a vendor.



Requirement Levels: RFCs are classified into five requirement levels: required, recommended, elective, limited use, and not recommended.

❑ **Required**. An RFC is labeled required if it must be implemented by all Internet systems to achieve minimum conformance. For example, IP and ICMP are required protocols.

❑ **Recommended**. An RFC labeled recommended is not required for minimum conformance; it is recommended because of its usefulness. For example, FTP and TELNET) are recommended protocols.

❑ **Elective**. An RFC labeled elective is not required and not recommended. However, a system can use it for its own benefit.

❑ **Limited Use**. An RFC labeled limited use should be used only in limited situations. Most of the experimental RFCs fall under this category.

❑ **Not Recommended**. An RFC labeled not recommended is inappropriate for general use. Normally a historic (deprecated) RFC may fall under this category

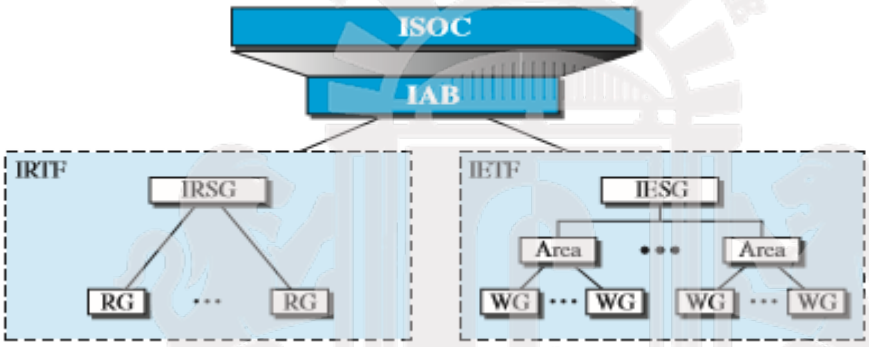
1.5.2 Internet Administration

The Internet, with its roots primarily in the research domain, has evolved and gained a broader user base with significant commercial activity. Various groups that coordinate Internet issues have guided this growth and development. Figure 1.17 shows the general organization of Internet administration.

ISOC: The Internet Society (ISOC) is an international, nonprofit organization formed in 1992 to provide support for the Internet standards process. ISOC accomplishes this through maintaining and supporting other Internet administrative bodies such as IAB, IETF, IRTF, and IANA. ISOC also promotes research and other scholarly activities relating to the Internet.

IAB The Internet Architecture Board (IAB) is the technical advisor to the ISOC. The main purposes of the IAB are to oversee the continuing development of the TCP/IP Protocol Suite and to serve in a technical advisory capacity to research members of the Internet community. IAB accomplishes this through its two primary components, the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). Another responsibility of the IAB is the editorial management of the RFCs, described earlier. IAB is also the external liaison between the Internet and other standards organizations and forums.

Figure 1.17 *Internet administration*



IETF The Internet Engineering Task Force (IETF) is a forum of working groups managed by the Internet Engineering Steering Group (IESG). IETF is responsible for identifying operational problems and proposing solutions to these problems. IETF also develops and reviews specifications intended as Internet standards. The working groups are collected into areas, and each area concentrates on a specific topic. Currently nine areas have been defined. The areas include applications, protocols, routing and security.

IRTF The Internet Research Task Force (IRTF) is a forum of working groups managed by the Internet Research Steering Group (IRSG). IRTF focuses on long-term research topics related to Internet protocols, applications, architecture, and technology

Chapter 2: Network Models

2.1 PROTOCOL LAYERING

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or protocol layering.

2.1.1 Scenarios Let us develop two simple scenarios to better understand the need for protocol layering.

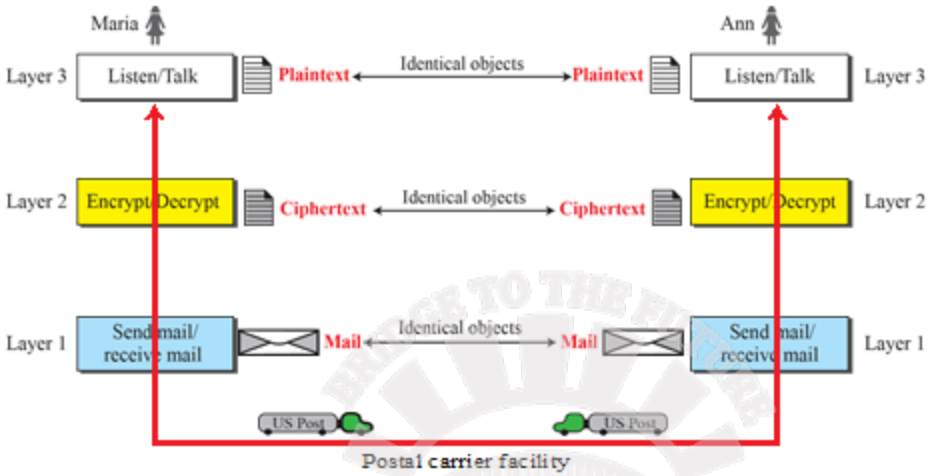
First Scenario: In the first scenario, communication is so simple that it can occur in only one layer. Assume Maria and Ann are neighbors with a lot of common ideas. Communication between Maria and Ann takes place in one layer, face to face, in the same language, as shown in Figure 2.1.

Figure 2.1: A single-layer protocol

Even in this simple scenario, we can see that a set of rules needs to be followed. First, Maria and Ann know that they should greet each other when they meet. Second, they know that they should confine their vocabulary to the level of their friendship. Third, each party knows that she should refrain from speaking when the other party is speaking. Fourth, each party knows that the conversation should be a dialog, not a monolog: both should have the opportunity to talk about the issue. Fifth, they should exchange some nice words when they leave.

Second Scenario: In the second scenario, we assume that Ann is offered a higher-level position in her company, but needs to move to another branch located in a city very far from Maria. The two friends still want to continue their communication and exchange ideas because they have come up with an innovative project to start a new business when they both retire. They decide to continue their conversation using regular mail through the post office. However, they do not want their ideas to be revealed by other people if the letters are intercepted. They agree on an encryption/decryption technique. The sender of the letter encrypts it to make it unreadable by an intruder; the receiver of the letter decrypts it to get the original letter. Now we can say that the communication between Maria and Ann takes place in three layers, as shown in Figure 2.2

Figure 2.2: A three-layer protocol



28

Let us assume that Maria sends the first letter to Ann. Maria talks to the machine at the third layer as though the machine is Ann and is listening to her. The third layer machine listens to what Maria says and creates the plaintext (a letter in English), which is passed to the second layer machine. The second layer machine takes the plaintext, encrypts it, and creates the ciphertext, which is passed to the first layer machine. The first layer machine, presumably a robot, takes the ciphertext, puts it in an envelope, adds the sender and receiver addresses, and mails it.

At Ann's side, the first layer machine picks up the letter from Ann's mail box, recognizing the letter from Maria by the sender address. The machine takes out the ciphertext from the envelope and delivers it to the second layer machine. The second layer machine decrypts the message, creates the plaintext, and passes the plaintext to the third-layer machine. The third layer machine takes the plaintext and reads it as though Maria is speaking.

Protocol layering enables us to divide a complex task into several smaller and simpler tasks. For example, in Figure 2.2, we could have used only one machine to do the job of all three machines. However, if Maria and Ann decide that the encryption/ decryption done by the machine is not enough to protect their secrecy, they would have to change the whole machine. In the present situation, they need to change only the second layer machine; the other two can remain the same. This is referred to as modularity. Modularity in this case means independent layers.

One of **the advantages** of protocol layering is that it allows us to separate the services from the implementation. A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer; we don't care about how the layer is implemented. For example, Maria may decide not to buy the machine (robot) for the first layer; she can do the job herself. As long as Maria can do the tasks provided by the first layer, in both directions, the communication system works.

Another **advantage** of protocol layering, which cannot be seen in our simple examples but reveals itself when we discuss protocol layering in the Internet, is that communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers. If we did not use protocol layering, we would have to make each intermediate system as complex as the end systems, which makes the whole system more expensive.

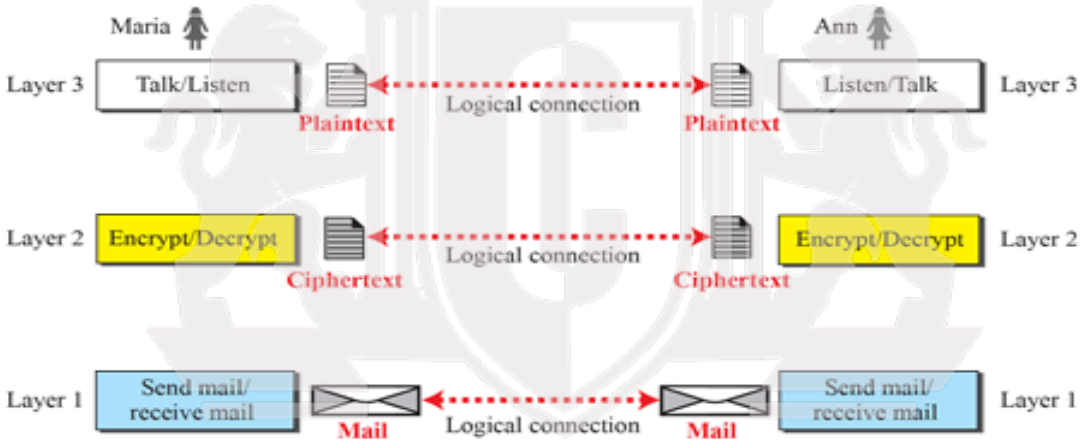
2.1.2 Principles of Protocol Layering

First Principle The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction. For example, the third layer task is to listen (in one direction) and talk (in the other direction). The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail.

Second Principle The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical. For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at both sites should be a ciphertext letter. The object under layer 1 at both sites should be a piece of mail.

2.1.3 Logical Connections: After following the above two principles, we can think about logical connection between each layer as shown in Figure 2.3. This means that we have layer-to-layer communication. Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer.

Figure 2.3: Logical connection between peer layers

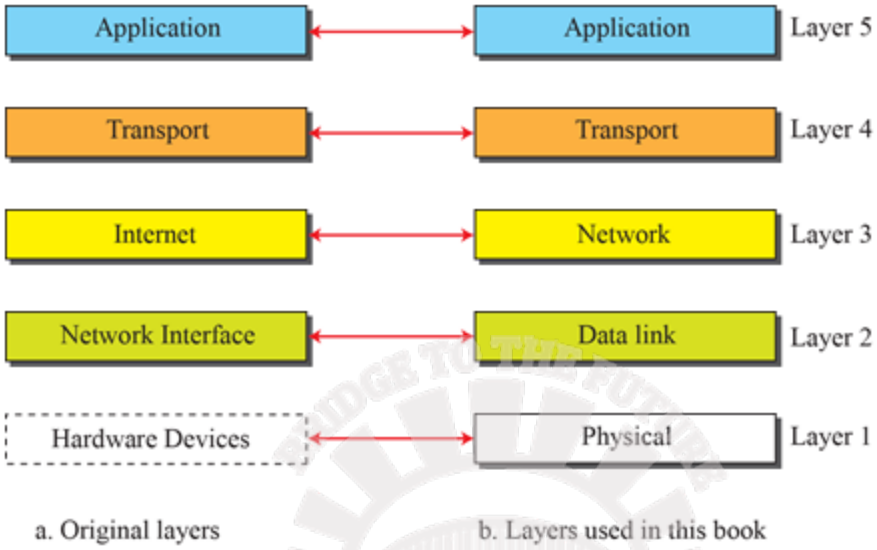


2.11

2.2 TCP/IP PROTOCOL SUITE

TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model. Figure 2.4 shows both configurations.

Figure 2.4: Layers in the TCP/IP protocol suite

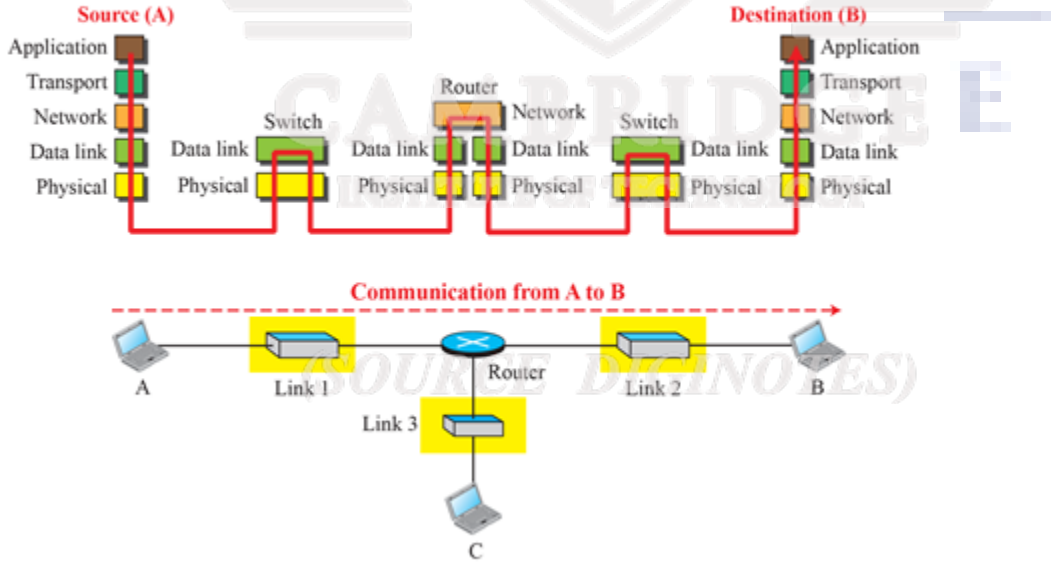


2.13

2.2.1 Layered Architecture

To show how the layers in the TCP/IP protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch. We also assume that the links are connected by one router, as shown in Figure 2.5.

Figure 2.5: Communication through an internet



2.15

Let us assume that computer A communicates with computer B. As the figure shows, we have five communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B). Each device is involved with a set of layers depending on the role of the device in the internet. The two hosts are involved in all five layers; the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host. The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

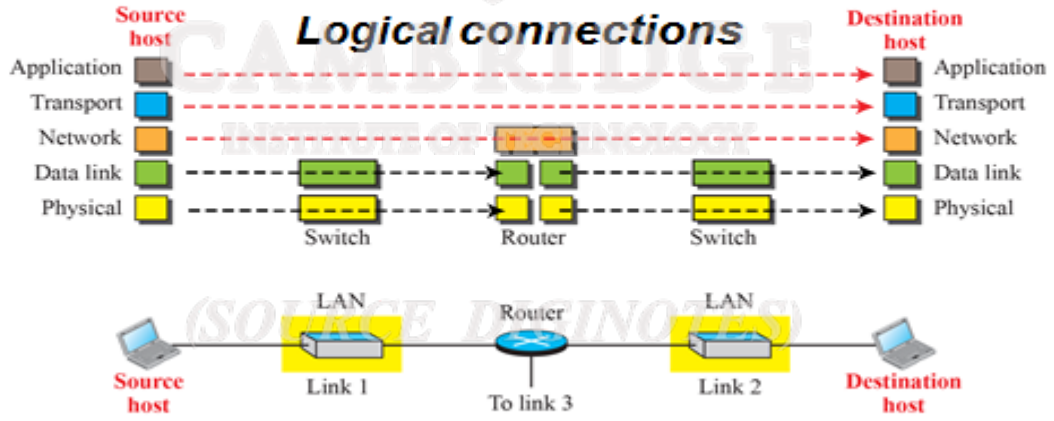
The router is involved in only three layers. Although a router is always involved in one network layer, it is involved in n combinations of link and physical layers in which n is the number of links the router is connected to. The reason is that each link may use its own data-link or physical protocol. For example, in the above figure, the router is involved in three links, but the message sent from source A to destination B is involved in two links. Each link may be using different link-layer and physical-layer protocols; the router needs to receive a packet from link 1 based on one pair of protocols and deliver it to link 2 based on another pair of protocols.

A link-layer switch in a link, however, is involved only in two layers, data-link and physical. Although each switch in the above figure has two different connections, the connections are in the same link, which uses only one set of protocols. This means that, unlike a router, a link-layer switch is involved only in one data-link and one physical layer.

2.2.2 Layers in the TCP/IP Protocol Suite

To better understand the duties of each layer, we need to think about the logical connections between layers. Figure 2.6 shows logical connections in our simple internet.

Figure 2.6: Logical connections between layers in TCP/IP

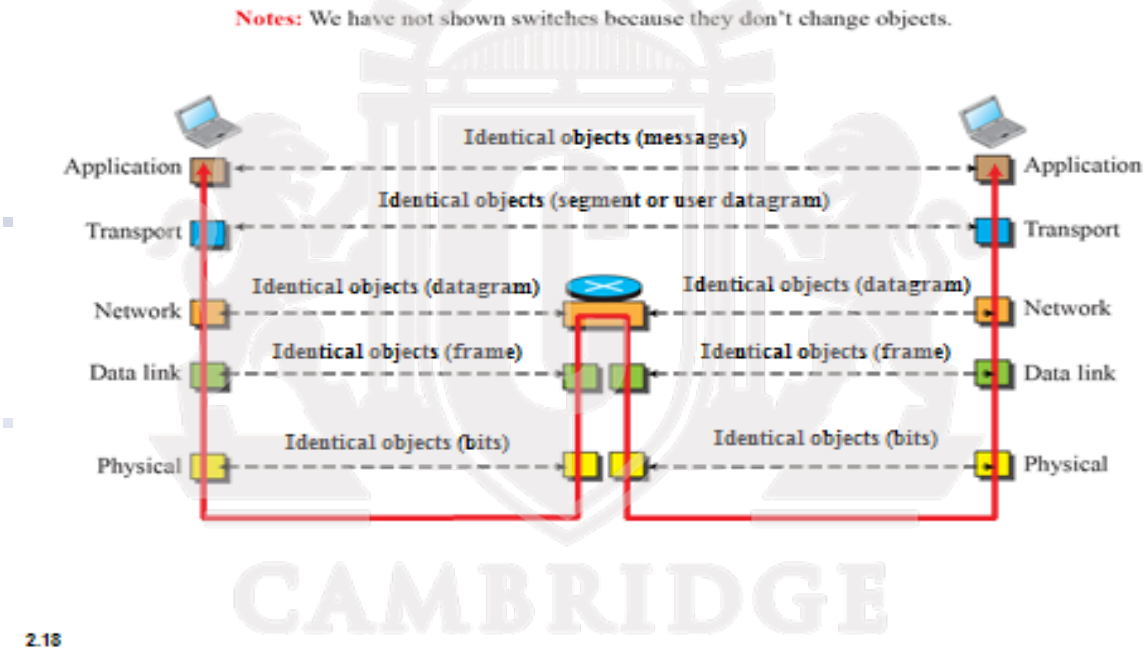


2.17

Using logical connections makes it easier for us to think about the duty of each layer. As the figure shows, the duty of the application, transport, and network layers is end-to-end. However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router. In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link. Another way of thinking of the logical connections is to think about the data unit created from each layer. In the top three layers, the data unit (packets) should not be changed by any router or link-layer switch. In the bottom two layers, the packet created by the host is changed only by the routers, not by the link-layer switches.

Figure 2.7 shows the second principle discussed previously for protocol layering. We show the identical objects below each layer related to each device.

Figure 2.7: Identical objects in the TCP/IP protocol suite



2.18

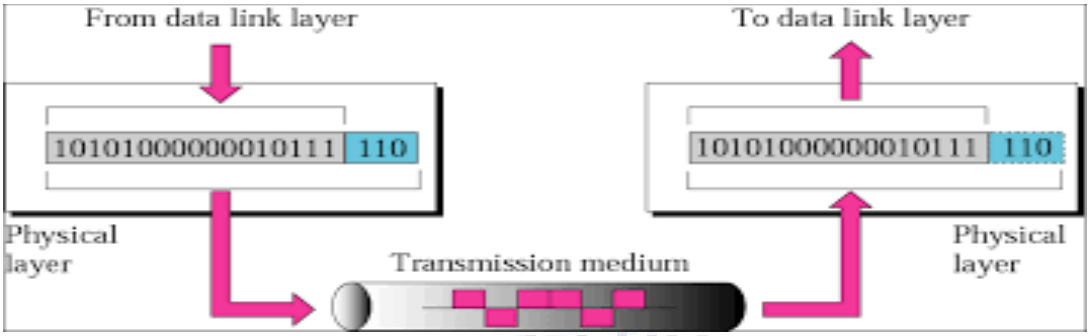
Note that, although the logical connection at the network layer is between the two hosts, we can only say that identical objects exist between two hops in this case because a router may fragment the packet at the network layer and send more packets than received .Note that the link between two hops does not change the object.

2.2.3 Description of Each Layer

Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. The following figure shows the position of

the physical layer with respect to the transmission medium and the data link layer.

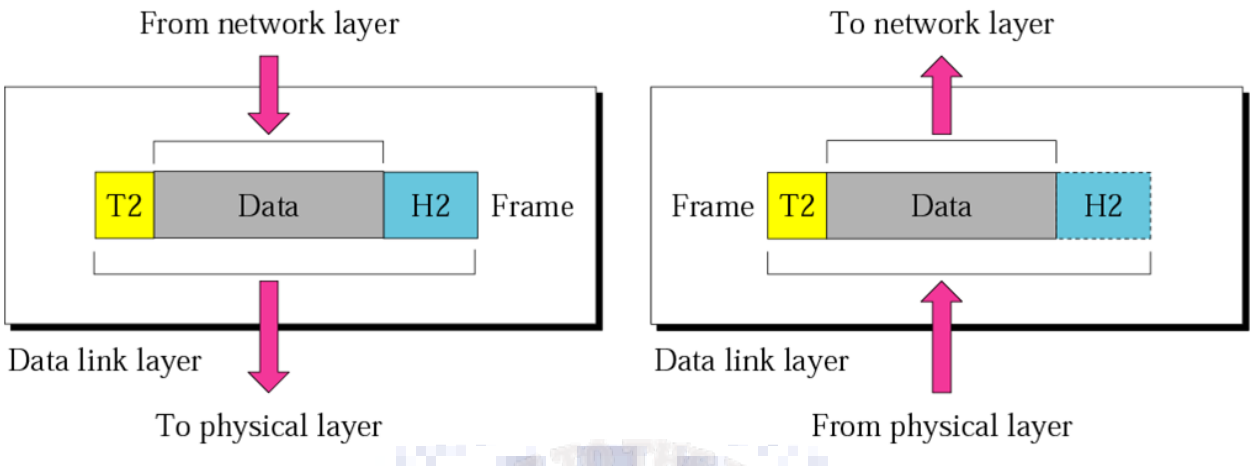


The physical layer is also concerned with the following:

- **Physical characteristics of interfaces and medium.** The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- **Representation of bits.** The physical layer data consists of a stream of bits (sequence of 0s or ls) with no interpretation. To be transmitted, bits must be encoded into signals-electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).
- **Data rate.** The transmission rate--the number of bits sent each second--is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
- **Synchronization of bits.**The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
- **Line configuration.** The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- **Physical topology.** The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology(every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).
- **Transmission mode.** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive.The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

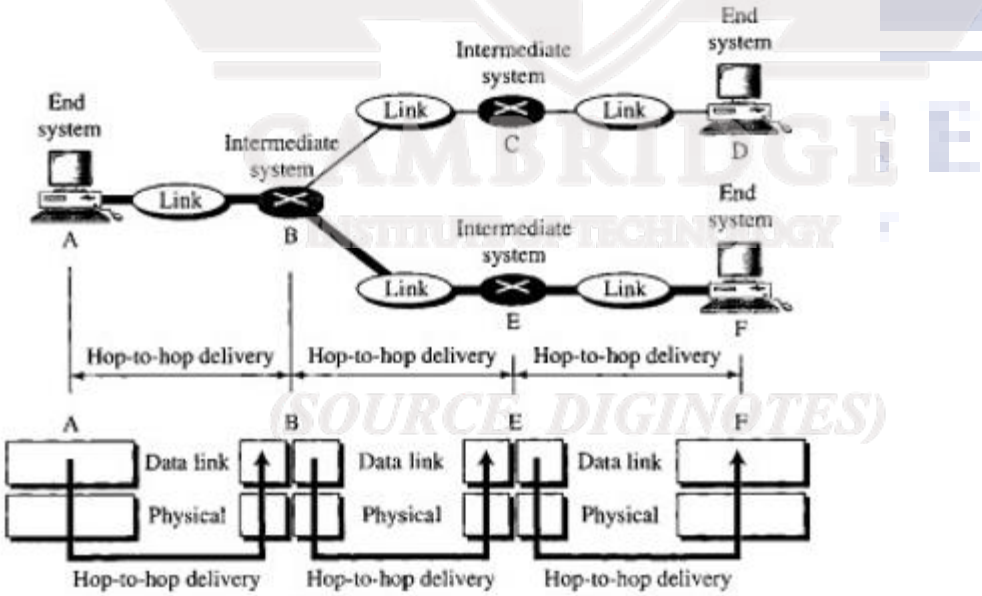
Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). The figure shows the relationship of the data link layer to the network and physical layers.



Other responsibilities of the data link layer include the following:

- **Framing.** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing.** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control.** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access control.** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.



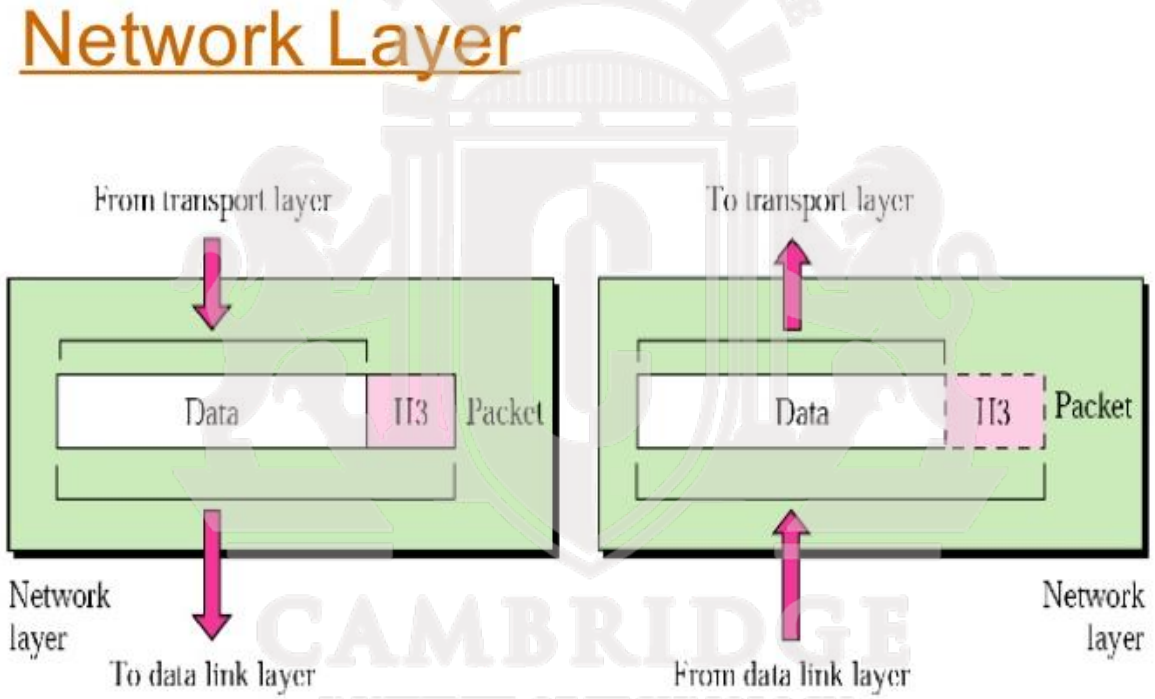
The figure illustrates hop-to-hop (node-to-node) delivery by the data link layer.

Communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made. First, the data link layer at A sends a frame to the data link layer at B (a router). Second, the data link layer at B sends a new frame to the data link layer at E. Finally, the data link layer at E sends a new frame to the data link layer at F.

Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. The figure shows the relationship of the network layer to the data link and transport layers.

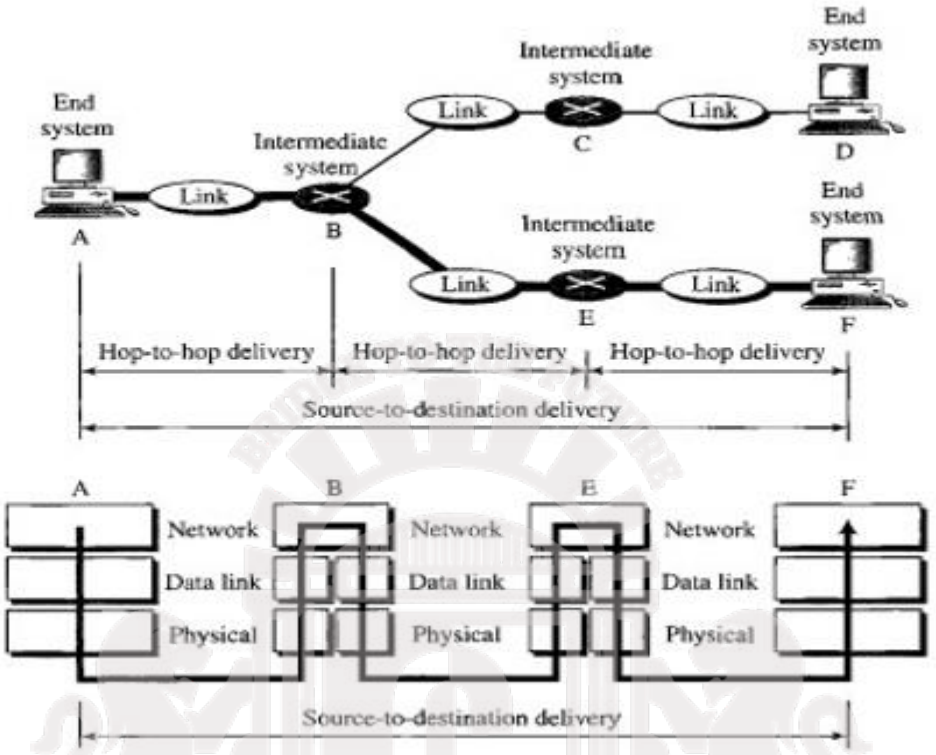


Other responsibilities of the network layer include the following:

- **Logical addressing**.The physical addressing implemented by the data link layer handles the addressing problem locally.If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things includes the logical addresses of the sender and receiver.

- **Routing.** When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

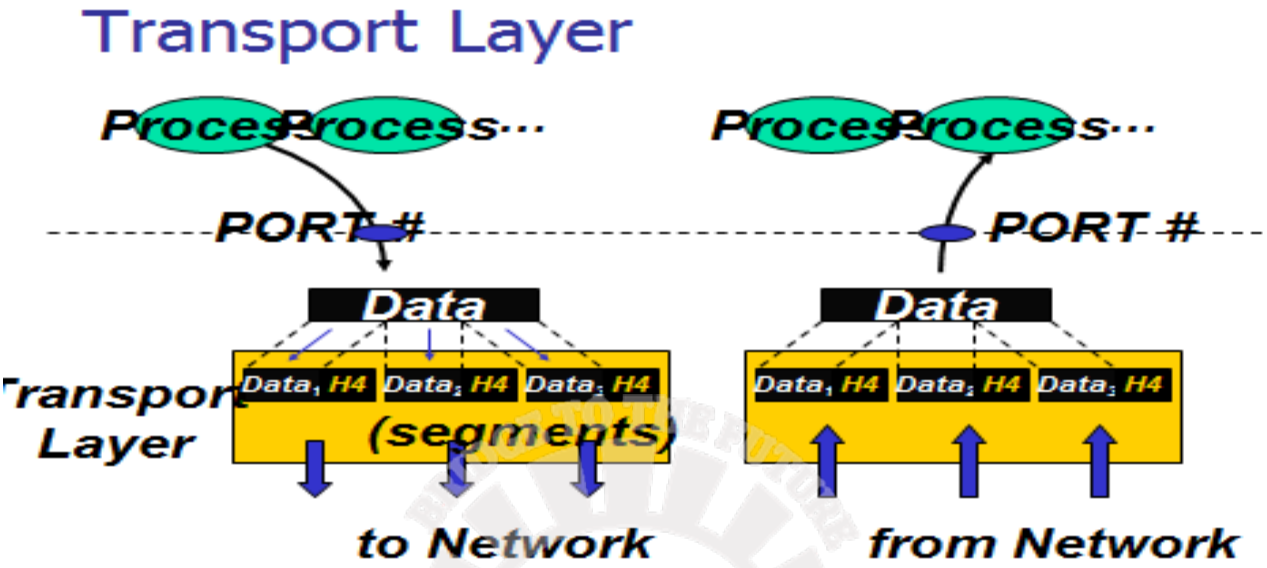
The figure illustrates end-to-end delivery by the network layer.



The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet. As we will see in later chapters, router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in turn, sends the packet to the network layer at F.

Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message.A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. The figure shows the relationship of the transport layer to the network layer.



28

Other responsibilities of the transport layer include the following:

- **Service-point addressing.** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

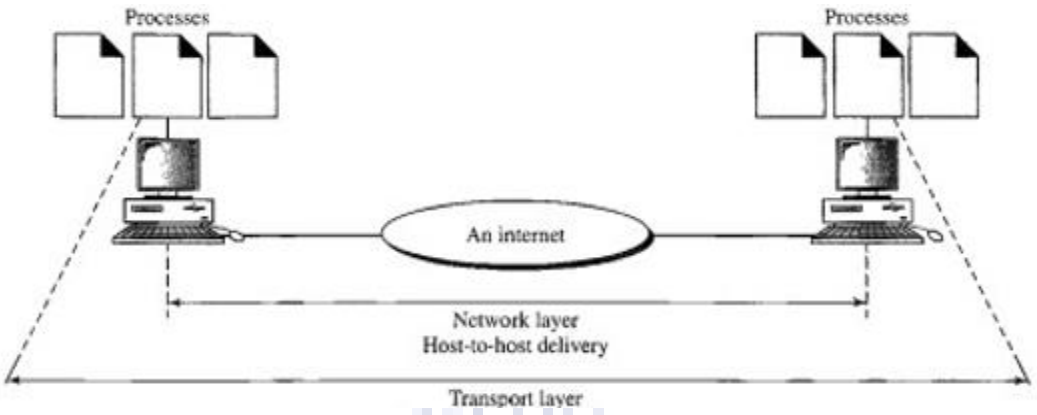
- **Segmentation and reassembly.** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

- **Connection control.** The transport layer can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

- **Flow control.** Like the data link layer, the transport layer is responsible for flow control.However, flow control at this layer is performed end to end rather than across a single link.

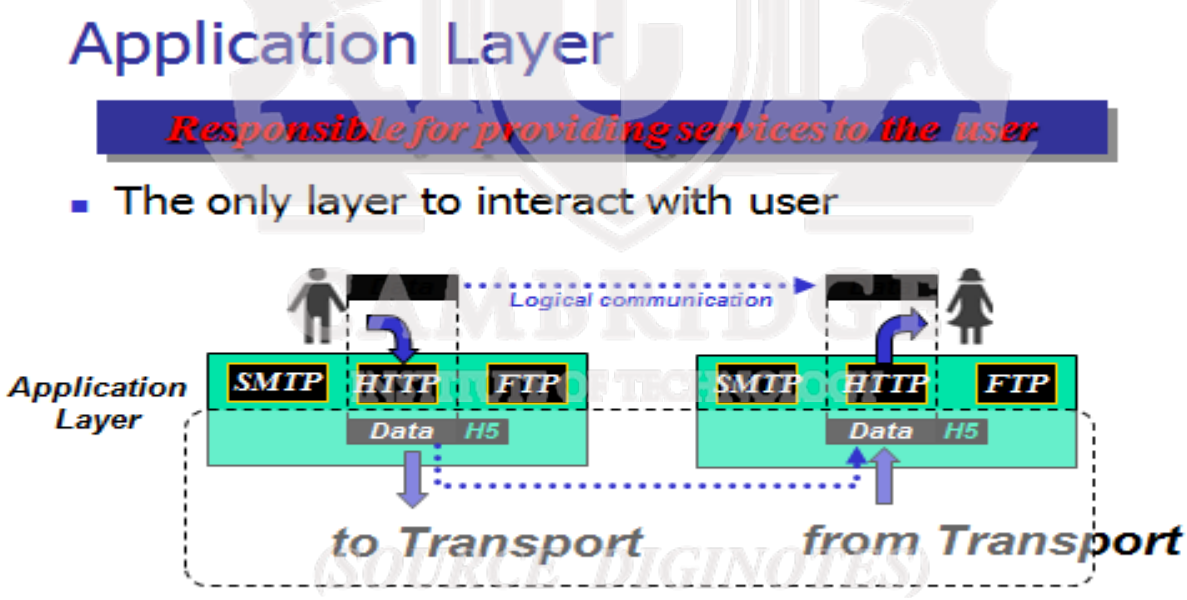
- **Error control.** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

The figure illustrates process-to-process delivery by the transport layer.



Application Layer

The application layer enables the user, whether human or software, to access the network. The two application layers exchange messages between each other as though there were a bridge between the two layers. However, we should know that the communication is done through all the layers. Communication at the application layer is between two processes (two programs running at this layer). To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer. The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.



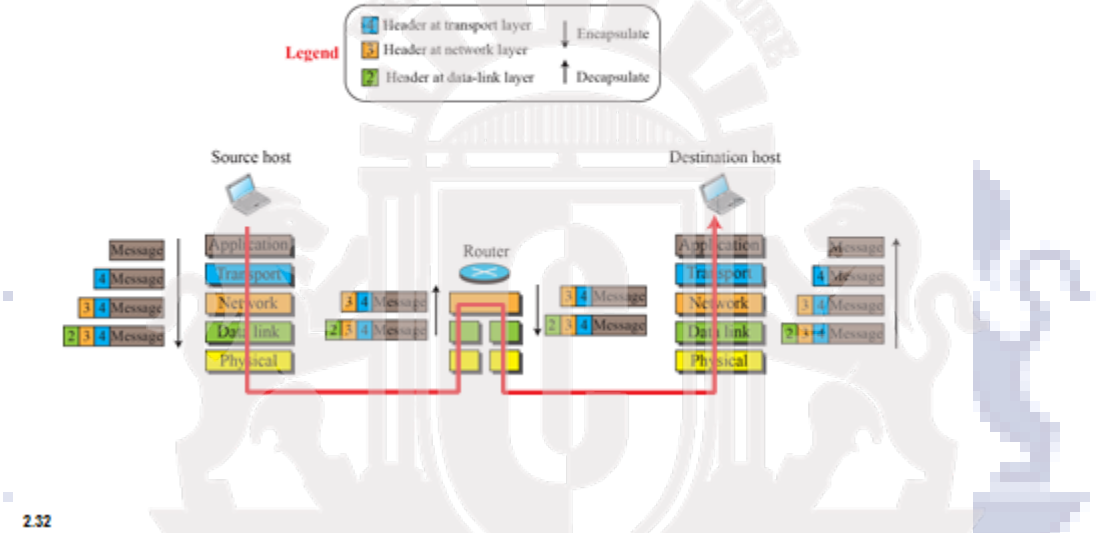
- The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW).
- The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service.
- The File Transfer Protocol (FTP) is used for transferring files from one host to another.

- The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely.
- The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels.
- The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer.

2.2.4 Encapsulation and Decapsulation

One of the important concepts in protocol layering in the Internet is encapsulation/ decapsulation. Figure 2.8 shows this concept for the small internet in Figure 2.5.

Figure 2.8: *Encapsulation / Decapsulation*



2.32

In Figure 2.8, we show the encapsulation in the source host, decapsulation in the destination host, and encapsulation and decapsulation in the router.

Encapsulation at the Source Host: At the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a message. A message normally does not contain any header or trailer, but if it does, we refer to the whole as the message. The message is passed to the transport layer.
2. The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to-end delivery of the message, such as information needed for flow, error control, or congestion control. The result is the transport-layer packet, which is called the segment (in TCP) and the user datagram (in UDP). The transport layer then passes the packet to the network layer.
3. The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation

information, and so on. The result is the network-layer packet, called a datagram. The network layer then passes the packet to the data-link layer.

4. The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router, we have both decapsulation and encapsulation because the router is connected to two or more links.

1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.
2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layer of the next link.
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

Decapsulation at the Destination Host

At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer. It is necessary to say that decapsulation in the host involves error checking.

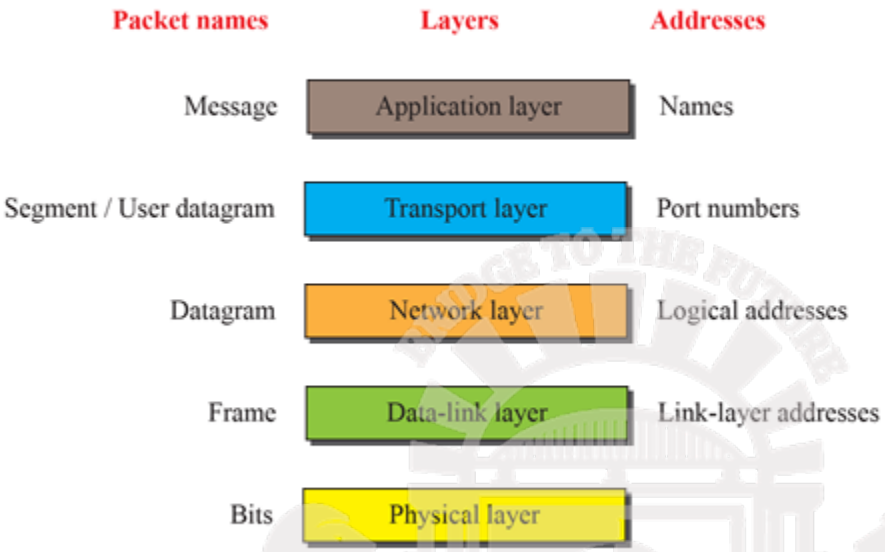
2.2.5 Addressing

Any communication that involves two parties needs two addresses: source address and destination address. Although it looks as if we need five pairs of addresses, one pair per layer, we normally have only four because the physical layer does not need addresses; the unit of data exchange at the physical layer is a bit, which definitely cannot have an address. Figure 2.9 shows the addressing at each layer.

As the figure shows, there is a relationship between the layer, the address used in that layer, and the packet name at that layer.

- At the application layer, we normally use names to define the site that provides services, such as someorg.com, or the e-mail address, such as somebody@coldmail.com.
- At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination. Port numbers are local addresses that distinguish between several programs running at the same time.
- At the network-layer, the addresses are global, with the whole Internet as the scope. A network-layer address uniquely defines the connection of a device to the Internet.
- The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN).

Figure 2.9: Addressing in the TCP/IP protocol suite



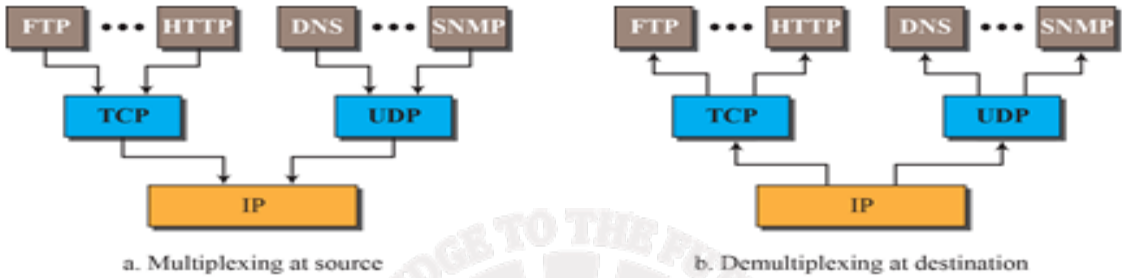
2.34

2.2.6 Multiplexing and Demultiplexing

Since the TCP/IP protocol suite uses several protocols at some layers, we can say that we have multiplexing at the source and demultiplexing at the destination. Multiplexing in this case means that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time); demultiplexing means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time). Figure 2.10 shows the concept of multiplexing and demultiplexing at the three upper layers.

To be able to multiplex and demultiplex, a protocol needs to have a field in its header to identify to which protocol the encapsulated packets belong. At the transport layer, either UDP or TCP can accept a message from several application-layer protocols. At the network layer, IP can accept a segment from TCP or a user datagram from UDP. IP can also accept a packet from other protocols such as ICMP, IGMP, and so on. At the data-link layer, a frame may carry the payload coming from IP or other protocols such as ARP

Figure 2.10: Multiplexing and demultiplexing



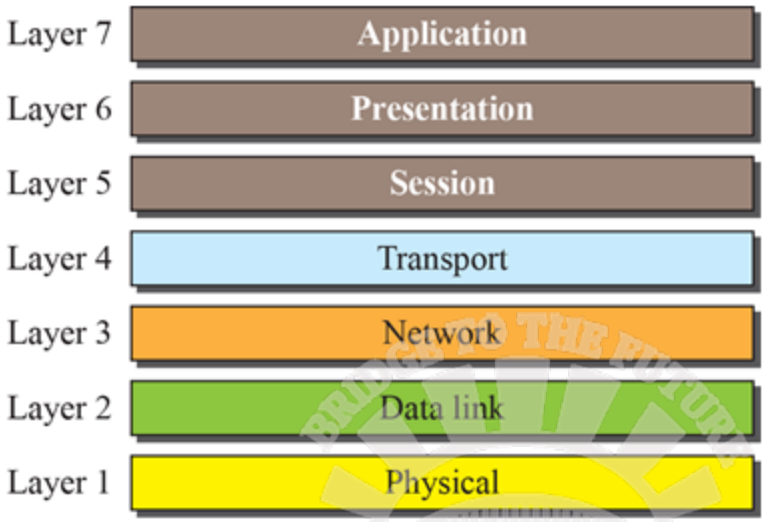
2.36

2.3 THE OSI MODEL

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.
Established in 1947, the International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards. Almost three-fourths of the countries in the world are represented in the ISO. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. The OSI model was intended to be the basis for the creation of the protocols in the OSI stack. The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

Figure 2.11: The OSI model

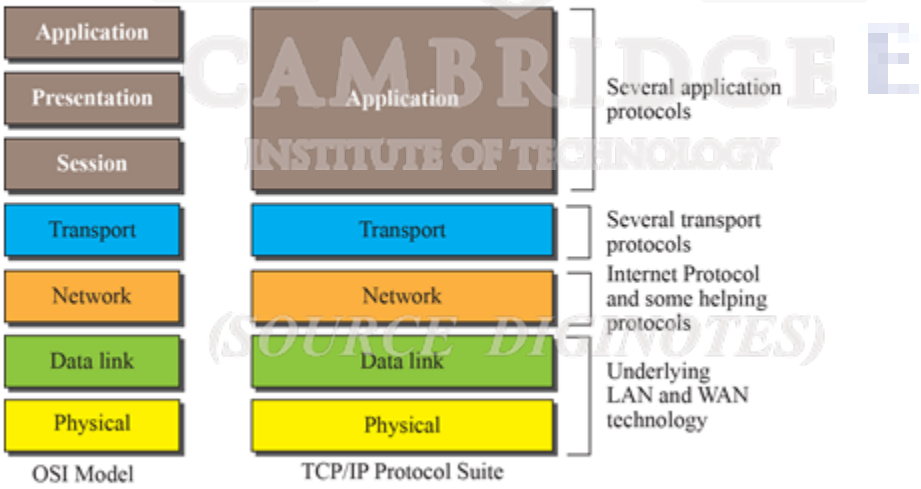


2.39

2.3.1 OSI versus TCP/IP

When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model, as shown in Figure 2.12.

Figure 2.12: TCP/IP and OSI model



2.41

Two reasons were mentioned for this decision. First, TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport-layer protocols. Second, the application layer is not only one piece of software. Many applications can be developed at this layer. If some of the functionalities mentioned in the session and presentation layers are needed for a particular application, they can be included in the development of that piece of software.

Sl.No.	OSI	TCP/IP
1.	It expands to Open System Interconnection	It expands to Transmission control protocol/Internet Protocol
2.	It is a theoretical model which is used for computing system.	It is a client server model used for transmission of data over the internet.
3.	It is developed by International Standard Organisation(ISO)	It is developed by Department of Defence(DoD).
4.	This model is never used	This model is mostly used.
5.	OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
6.	OSI model has a separate Presentation layer and Session layer	TCP/IP does not have a separate Presentation layer or Session layer
7.	OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	TCP/IP model is, in a way implementation of the OSI model.
8.	Network layer of OSI model provides both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
9.	Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
10.	OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
11.	It has 7 layers	It has 5 layers

2.3.2 Lack of OSI Model's Success

The OSI model appeared after the TCP/IP protocol suite. Most experts were at first excited and thought that the TCP/IP protocol would be fully replaced by the OSI model. This did not happen for several reasons, but we describe only three, which are agreed upon by all experts in the field.

- First, OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite; changing it would cost a lot.
- Second, some layers in the OSI model were never fully defined. For example, although

the services provided by the presentation and the session layers were listed in the document, actual protocols for these two layers were not fully defined, nor were they fully described, and the corresponding software was not fully developed.

- Third, when OSI was implemented by an organization in a different application, it did not show a high enough level of performance to entice the Internet authority to switch from the TCP/IP protocol suite to the OSI model.

CAMBRIDGE INSTITUTE OF TECHNOLOGY
Department of CSE and ISE

DATA COMMUNICATIONS (15CS46)
QUESTION BANK

Module 1: CO-1,2,3

1. What is data communication? What are its characteristics and components? Explain
2. Explain data representation.
3. What are the modes of transfer of data? Explain
4. What is the difference between half-duplex and full-duplex transmission modes?
5. What are the three criteria necessary for an effective and efficient network?
6. Explain the types of connections. What are the advantages of a multipoint connection over a point-to-point Connection?
7. When a party makes a local telephone call to another party, is this a point-to-point or multipoint connection? Explain your answer.
8. Name the four basic network topologies, and cite an advantage of each type.
9. Explain with a neat diagram mesh topology and star topology with the application for each.
10. Assume that fifty devices are arranged in a mesh topology. How many links are needed? How many ports are needed for each device?
11. In bus topology, what happens if one of the stations is unplugged?
12. Give the comparison between LAN,WAN & MAN with an example.
    Or
    What are the different types of networks.Explain
13. What are some of the factors that determine whether a communication system is a LAN or WAN?
14. What is switching? Explain two types of switched networks.
15. Explain the conceptual view of internet
16. How do you access the internet?Explain
17. Explain internet history.
18. Distinguish between Internet standard and Internet draft.
19. Why are standards needed?
20. What is an RFC ?Explain the different maturity levels and Requirement Levels
    Or
    What is an internet standard? Explain.
21. Explain the general organization of Internet administration.
22. Discuss Protocol layering with example?
23. What is a protocol?
24. Write the two principles of protocol layering. Discuss with the help of TCP/IP protocol suite.
25. Describe with a neat diagram, the functionalaties of each layer in the TCP/IP model

26. What are the responsibilities of the network layer in the Internet model?
27. What are the responsibilities of the transport layer in the Internet model?
28. Name some of the services provided by the application layer in the Internet model.
29. List responsibilities of DLL.
30. What are the concerns of the physical layer?
31. Explain Encapsulation and Decapsulation in protocol layering with an example.
32. Explain the concept of multiplexing and demultiplexing in TCP/IP Protocol suite
33. Discuss briefly about OSI model.
34. How do the layers of the Internet model correlate to the layers of the OSI model?
35. List out the differences between TCP/IP model and OSI model.
36. Discuss addressing in TCP/IP protocol suite.

MODULE 2: TABLE OF CONTENTS

- Quadrature Amplitude Modulation (QAM)
  - Bandwidth for QAM

MULTIPLEXING

- Frequency Division Multiplexing (FDM)
  - Multiplexing Process
  - Demultiplexing Process
  - Applications of FDM
  - The Analog Carrier System
- Wavelength-Division Multiplexing (WDM)
- Time Division Multiplexing (TDM)
  - Synchronous TDM
    - Time Slots and Frames
    - Interleaving
    - Empty Slots
    - Data Rate Management
    - Frame Synchronizing
  - Statistical TDM

SPREAD-SPECTRUM

- Frequency Hopping Spread Spectrum (FHSS)
  - Bandwidth Sharing
- Direct Sequence Spread Spectrum (DSSS)
  - Bandwidth Sharing

SWITCHING

- Three Methods of Switching
- Switching and TCP/IP Layers

CIRCUIT SWITCHED NETWORK

- Three Phases
- Efficiency
- Delay

PACKET SWITCHED NETWORK

- Datagram Networks
  - Routing Table
    - Destination Address
    - Efficiency
    - Delay

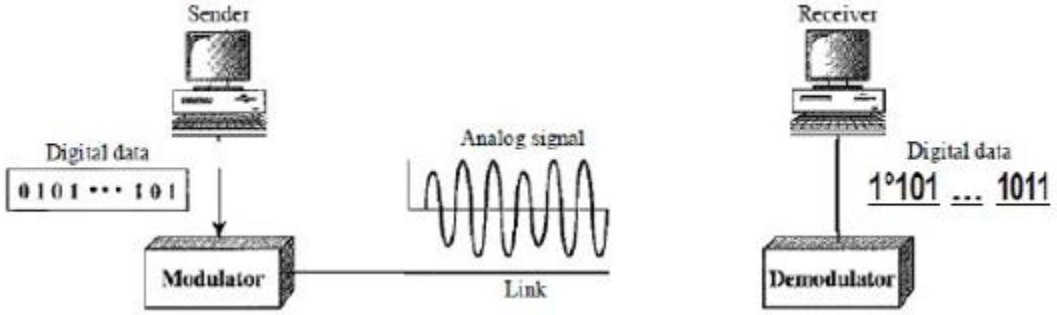
Virtual Circuit Network
- Addressing
- Three Phases
  - Data Transfer Phase
  - Setup Phase
    - Setup Request
  - Teardown Phase
- Efficiency
- Delay in Virtual Circuit Networks

CHAPTER 5

5.1 DIGITAL-TO-ANALOG CONVERSION

Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data. Figure 5.1 shows the relationship between the digital information, the digital-to-analog modulating process, and the resultant analog signal.

FIGURE *Digital-to-analog conversion*



A sine wave is defined by three characteristics: **amplitude, frequency,and phase**. When we vary anyone of these characteristics, we create a different version of that wave. So, by changing one characteristic of a simple electric signal, we can use it to represent digital data. Any of the three characteristics can be altered in this way, giving us at least **three mechanisms** for modulating digital data into an analog signal: amplitude shift keying (ASK),frequency shift keying (FSK), and phase shift keying (PSK). In addition, there is a fourth (and better) mechanism that combines changing both the amplitude and phase, called quadrature amplitude modulation (QAM). QAM is the most efficient of these options and is the mechanism commonly used today.

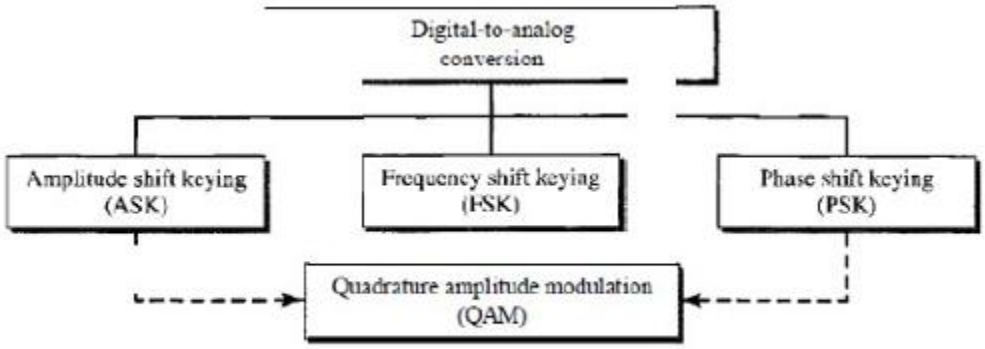


Figure *Types of digital-to-analog conversion*

5.1.1 Aspects of Digital-to-Analog Conversion

Before we discuss specific methods of digital-to-analog modulation, two basic issues must be reviewed: bit and baud rates and the carrier signal.

Data Element Versus Signal Element We defined a data element as the smallest piece of information to be exchanged, the bit. We also defined a signal element as the smallest unit of a signal that is constant.The nature of the signal element is a little bit different in analog transmission.

Data Rate Versus Signal Rate

We can define the data rate (bit rate) and the signal rate (baud rate) as we did for digital transmission. The relationship between them is

$S=Nx1/r$ baud

where N is the data rate (bps) and r is the number of data elements carried in one signal element.The value of r in analog transmission is r =log2 L, where L is the type of signal element, not the level. The same nomenclature is used to simplify the comparisons.

Bit rate is the number of bits per second. Baud rate is the number of signal elements per second. In the analog transmission of digital data, the baud rate is less than or equal to the bit rate.

Example 5.1
An analog signal carries 4 bits per signal element. If 1000 signal elements are sent per second, find the bit rate.

Solution
In this case, r = 4, S = 1000, and N is unknown. We can find the value ofN from
$S=Nx1/r$
or $N=Sxr=$ 1000 x 4 =4000 bps

Example 5.2
An analog signal has a bit rate of 8000 bps and a baud rate of 1000 baud. How many data elements are carried by each signal element? How many signal elements do we need?
Solution
In this example, S = 1000, N =8000, and rand L are unknown. We find first the value of rand then the value of L.
$S=Nx1/r \rightarrow r=N/S=8000/1000=8$ bits/baud
$r= log2L \rightarrow L= 2^r = 2^8 =256$

Bandwidth
The required bandwidth for analog transmission of digital data is proportional to the signal rate except for FSK, in which the difference between the carrier signals needs to be added. We discuss the bandwidth for each technique.

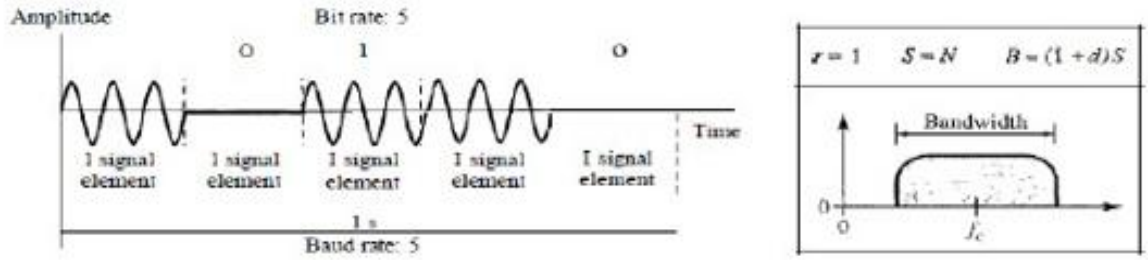
Carrier Signal
In analog transmission, the sending device produces a high-frequency signal that acts as a base for the information signal. This base signal is called the carrier signal or carrier frequency. The receiving device is tuned to the frequency of the carrier signal that it expects from the sender.Digital information then changes the carrier signal by modifying one or more of its characteristics (amplitude, frequency, or phase). This kind of modification is called modulation (shift keying).

5.1.2Amplitude Shift Keying

In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes.

Binary ASK (BASK)
ASK is normally implemented using only two levels. This is referred to as binary amplitude shift keying or *on-off keying* (OOK). The peak amplitude of one signal level is 0; the other is the same as the amplitude of the carrier frequency. Figure 5.3 gives a conceptual view of binary ASK.

Figure 5.3 *Binary amplitude shift keying*



Bandwidth for ASK Figure 5.3 also shows the bandwidth for ASK. Although the carrier signal is only one simple sine wave, the process of modulation produces a nonperiodic composite signal.As we expect, the bandwidth is proportional to the signal rate (baud rate). However, there is normally another factor involved, called *d,* which depends on the modulation and filtering process. The value of *d* is between 0 and 1. This means that the bandwidth can be expressed as shown, where 5 is the signal rate and the *B* is the bandwidth.

$B = (1 + d) \times S$

The formula shows that the required bandwidth has a minimum value of S and a maximum value of 2S. The most important point here is the location of the bandwidth.

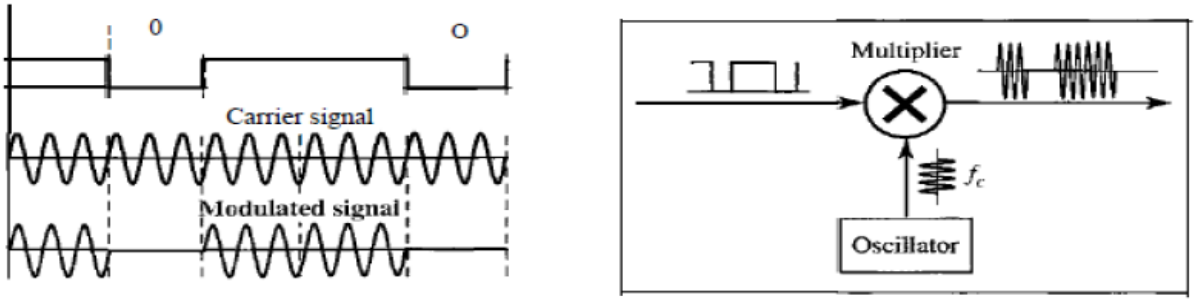
The middle of the bandwidth is where f_c, the carrier frequency, is located. This means if we have a bandpass channel available, we can choose our f_c so that the modulated signal occupies that bandwidth.

This is in fact the most important advantage of digital to- analog conversion. We can shift the resulting bandwidth to match what is available.

Figure 5.4 shows how we can simply implement binary ASK.

If digital data are presented as a unipolar NRZ digital signal with a high voltage of 1 V and a low voltage of 0 V, the implementation can achieved by multiplying the NRZ digital signal by the carrier signal coming from an oscillator. When the amplitude of the NRZ signal is 1, the amplitude of the carrier frequency is held; when the amplitude of the NRZ signal is 0, the amplitude of the carrier frequency is zero.

Figure 5.4 *Implementation of binary ASK*



Example 5.3

We have an available bandwidth of 100 kHz which spans from 200 to 300 kHz. What are the carrier frequency and the bit rate if we modulated our data by using ASK with *d* =1?

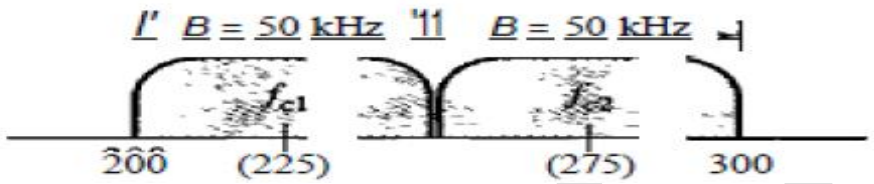
Solution

The middle of the bandwidth is located at 250 kHz. This means that our carrier frequency can be *at* f_c =250 kHz. We can use the formula for bandwidth to find the bit rate (with *d* =1 and *r* =1). *B* =(l +*d)* x S=2 x *N* x1/r=2 x*N* =100 kHz ..... *N* =50 kbps

Example 5.4

In data communications, we normally use full-duplex links with communication in both directions. We need to divide the bandwidth into two with two carrier frequencies, as shown in Figure 5.5. The figure shows the positions of two carrier frequencies and the bandwidths.The available bandwidth for each direction is now 50 kHz, which leaves us with a data rate of 25 kbps in each direction.

Figure 5.5 *Bandwidth of full-duplex ASK used in Example 5.4*



Multilevel ASK

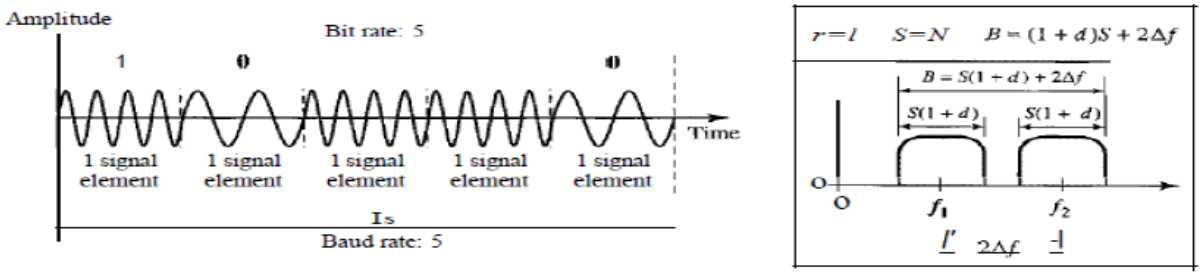
The above discussion uses only two amplitude levels. We can have multilevel ASK in which there are more than two levels. We can use 4,8, 16, or more different amplitudes for the signal and modulate the data using 2, 3, 4, or more bits at a time. In these cases, *r* = 2, *r* = 3, *r* =4, and so on. Although this is not implemented with pure ASK, it is implemented with QAM (as we will see later).

Frequency Shift Keying

In frequency shift keying, the frequency of the carrier signal is varied to represent data. The frequency of the modulated signal is constant for the duration of one signal element, but changes for the next signal element if the data element changes. Both peak amplitude and phase remain constant for all signal elements

Binary FSK (BFSK) One way to think about binary FSK (or BFSK) is to consider two carrier frequencies. In Figure 5.6, we have selected two carrier frequencies,f1 and f2. We use the first carrier if the data element is 0; we use the second if the data element is 1.

Figure 5.6 *Binary frequency shift keying*



As Figure 5.6 shows, the middle of one bandwidth is f1 and the middle of the other is *f2*. Both f1 and *f2* are Δf apart from the midpoint between the two bands. The difference between the two frequencies is *2*Δf.

Bandwidth for BFSK Figure 5.6 also shows the bandwidth of FSK. Again the carrier signals are only simple sine waves, but the modulation creates a nonperiodic composite signal with continuous frequencies. We can think of FSK as two ASK signals, each with its own carrier frequency f1 and f2*).* If the difference between the two frequencies is *2*Δf, then the required bandwidth is

B=(l+d) x S+2Δf.

What should be the minimum value of *2*Δf.*?* In Figure 5.6, we have chosen a value greater than (l + *d)S.* It can be shown that the minimum value should be at least S for the proper operation of modulation and demodulation.

Example 5.5

We have an available bandwidth of 100 kHz which spans from 200 to 300 kHz. What should be the carrier frequency and the bit rate if we modulated our data by using FSK with *d* =1?

Solution

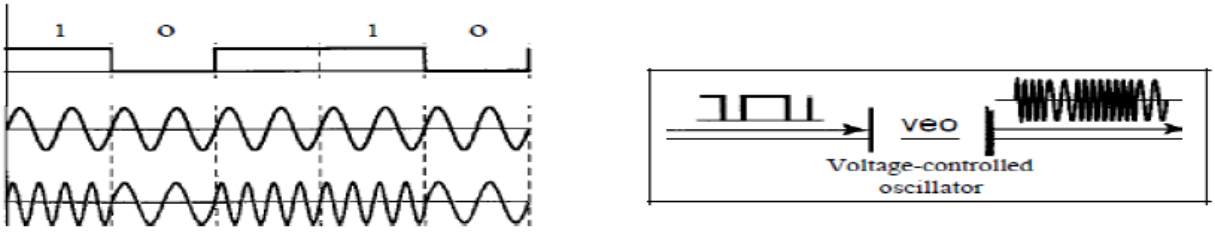
This problem is similar to Example 5.3, but we are modulating by using FSK. The midpoint of the band is at 250 kHz. We choose *2*Δf to be 50 kHz; this means

B =(1 + *d)* x S + *2*Δf =100 →. 2S =50 kHz S = 25 kbaud *N*= 25 kbps

Compared to Example 5.3, we can see the bit rate for ASK is 50 kbps while the bit rate for FSK is 25 kbps.

Implementation There are two implementations of BFSK: **noncoherent and coherent**. In noncoherent BFSK, there may be discontinuity in the phase when one signal element ends and the next begins. In coherent BFSK, the phase continues through the boundary of two signal elements. Noncoherent BFSK can be implemented by treating BFSK as two ASK modulations and using two carrier frequencies. Coherent BFSK can be implemented by using one *voltage-controlled oscillator* (VeO) that changes its frequency according to the input voltage. Figure 5.7 shows the simplified idea behind the second implementation. The input to the oscillator is the unipolar NRZ signal. When the amplitude of NRZ is zero, the oscillator keeps its regular frequency; when the amplitude is positive, the frequency is increased.

Figure 5.7 *Implementation ofBFSK*



Multilevel FSK

Multilevel modulation (MFSK) is not uncommon with the FSK method. We can use more than two frequencies. For example, we can use four different frequencies f1,f2,f3, and f4 to send 2 bits at a time. To send 3 bits at a time, we can use eight frequencies. However, we need to remember that the

frequencies need to be *2*Δf apart. For the proper operation of the modulator and demodulator, it can be shown that the minimum value of *2*Δf needs to be S. We can show that the bandwidth with *d* =0 is

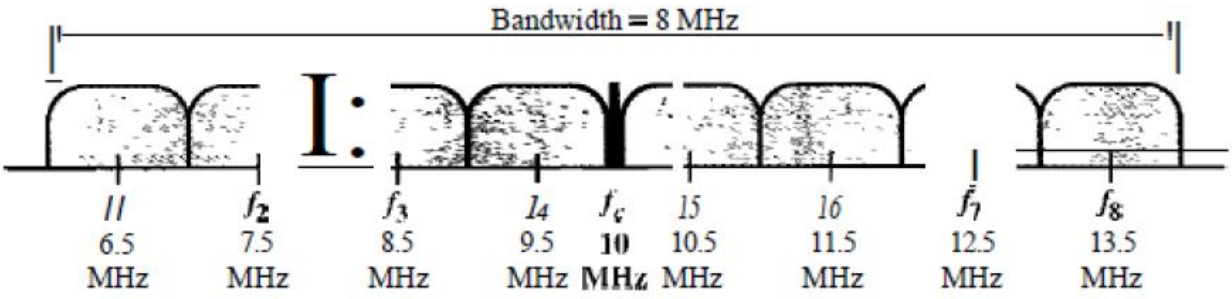
B= (l +*d)* x S + *(L* - 1) *2*Δf → *B* =Lx S

Example 5.6

We need to send data 3 bits at a time at a bit rate of 3 Mbps. The carrier frequency is 10 MHz. Calculate the number of levels (different frequencies), the baud rate, and the bandwidth.

Solution We can have *L* =2^3 =8. The baud rate is S =3 MHz/3 =1000 Mbaud. This means that the carrier frequencies must be 1MHz apart *(2*Δf =1 MHz). The bandwidth is *B*=8 x 1000 =8000. Figure 5.8 shows the allocation of frequencies and bandwidth.

Figure 5.8 *Bandwidth ofMFSK used in Example 5.6*

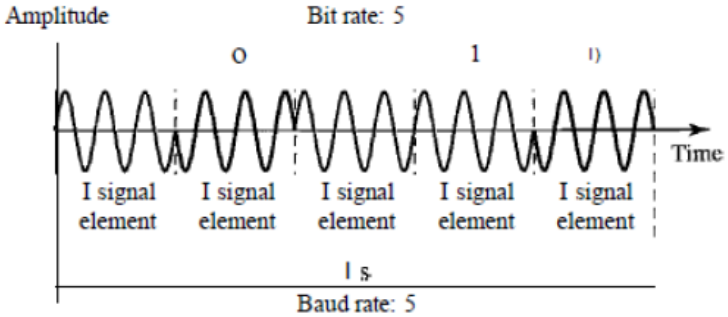


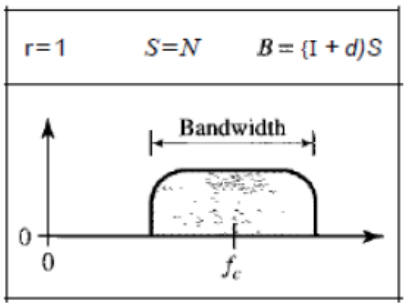
Phase Shift Keying

In phase shift keying, the phase of the carrier is varied to represent .two or more different signal elements. Both peak amplitude and frequency remain constant as the phase changes. Today, PSK is more common than ASK or FSK. QAM, which combines ASK and PSK, is the dominant method of digital-to- analog modulation.

Binary PSK (BPSK)

The simplest PSK is binary PSK, in which we have only two signal elements, one with a phase of 0°, and the other with a phase of 180°. Figure 5.9 gives a conceptual view of PSK. Binary PSK is as simple as binary ASK with one big advantage-it is less susceptible to noise.





In ASK, the criterion for bit detection is the amplitude of the signal; in PSK, it is the phase. Noise can change the amplitude easier than it can change the phase. In other words, PSK is less susceptible to noise than ASK.PSK is superior to FSK because we do not need two carrier signals.

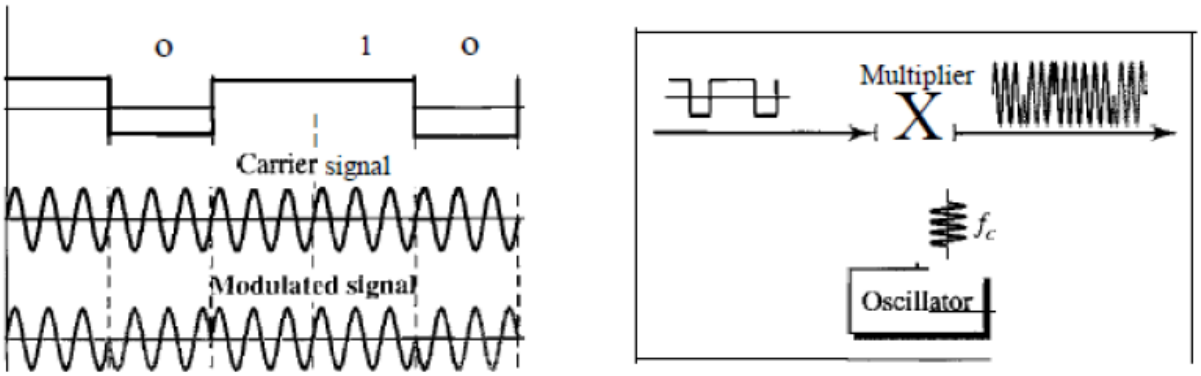
Bandwidth

Figure 5.9 also shows the bandwidth for BPSK. The bandwidth is the same as that for binary ASK, but less than that for BFSK. No bandwidth is wasted for separating two carrier signals.

Implementation

The implementation of BPSK is as simple as that for ASK. The reason is that the signal element with phase 180° can be seen as the complement of the signal element with phase 0°. This gives us a clue on how to implement BPSK. We use the same idea we used for ASK but with a polar NRZ signal instead of a unipolar NRZ signal, as shown in Figure 5.10. The polar NRZ signal is multiplied by the carrier frequency; the 1 bit (positive voltage) is represented by a phase starting at 0°; the 0 bit (negative voltage) is represented by a phase starting at 180°.

Figure 5.10 *Implementation ofBASK*



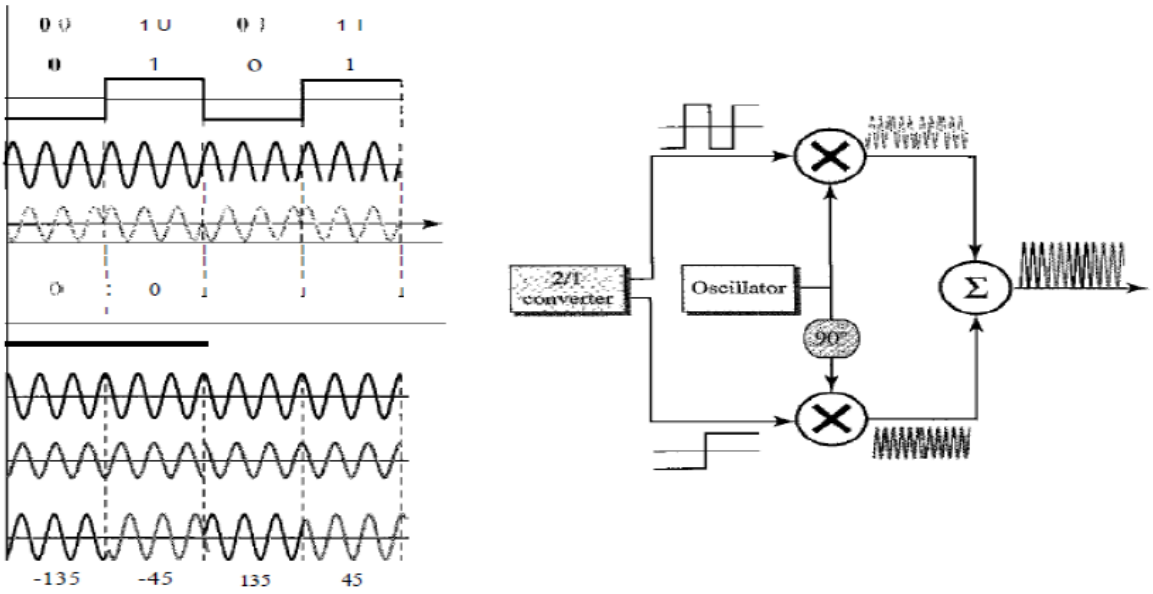
Quadrature PSK (QPSK)

The simplicity of BPSK enticed designers to use 2 bits at a time in each signal element, thereby decreasing the baud rate and eventually the required bandwidth. The scheme is called quadrature PSK or QPSK because it uses two separate BPSK modulations; one is in-phase, the other quadrature (out-of-phase).

The incoming bits are first passed through a serial-to-parallel conversion that sends one bit to one modulator and the next bit to the other modulator. If the duration of each bit in the incoming signal is *T*, the duration of each bit sent to the corresponding BPSK signal is *2T*. This means that the bit to each BPSK signal has one-half the frequency of the original signal. Figure 5.11 shows the idea.

The two composite signals created by each multiplier are sine waves with the same frequency, but different phases. When they are added, the result is another sine wave, with one of four possible phases: *45°*, *-45°*, *135°*, and *-135°*. There are four kinds of signal elements in the output signal *(L* = 4), so we can send 2 bits per signal element *(r* =2).

Figure 5.11 *QPSK and its implementation*



Example 5.7 Find the bandwidth for a signal transmitting at 12 Mbps for QPSK. The value of *d* =O.

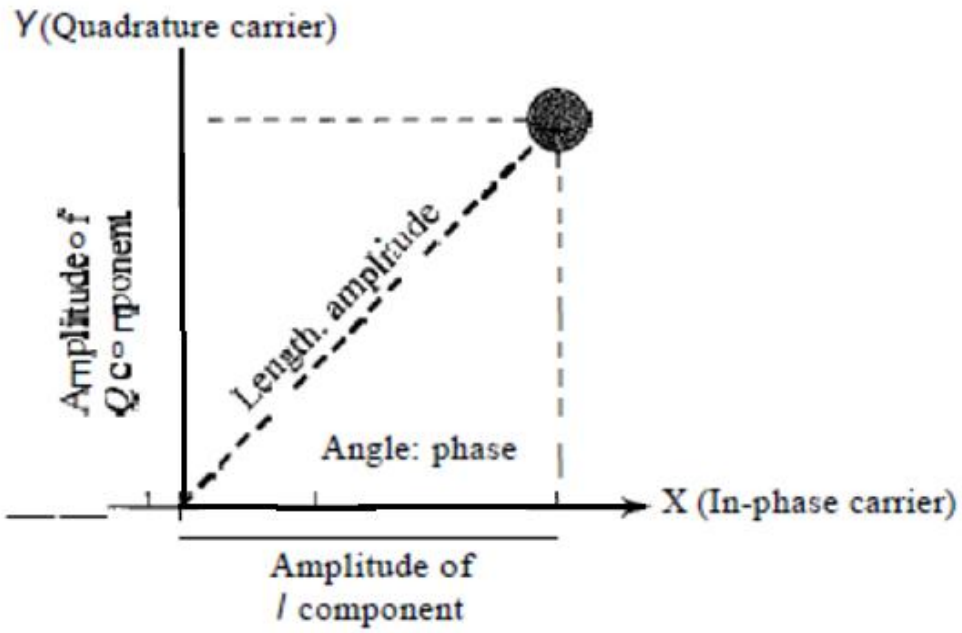
Solution
For QPSK, 2 bits is carried by one signal element. This means that *r* =2. So the signal rate (baud rate) is S =*N* x *(1/r)* =6 Mbaud. With a value of *d* =0, we have *B* =S =6 MHz.

Constellation Diagram

A **constellation diagram** can help us define the amplitude and phase of a signal element, particularly when we are using two carriers (one in-phase and one quadrature), The diagram is useful when we are dealing with multilevel ASK, PSK, or QAM. In a constellation diagram, a signal element type is represented as a dot. The bit or combination of bits it can carry is often written next to it.

The diagram has two axes. The horizontal X axis is related to the in-phase carrier; the vertical *Y* axis is related to the quadrature carrier. For each point on the diagram, four pieces of information can be deduced. The projection of the point on the X axis defines the peak amplitude of the in-phase component; the projection of the point on the *Y* axis defines the peak amplitude of the quadrature component. The length of the line (vector) that connects the point to the origin is the peak amplitude of the signal element (combination of the X and *Y* components); the angle the line makes with the X axis is the phase of the signal element. All the information we need, can easily be found on a constellation diagram. Figure 5.12 shows a constellation diagram.

Figure 5.12 *Concept of a constellation diagram*

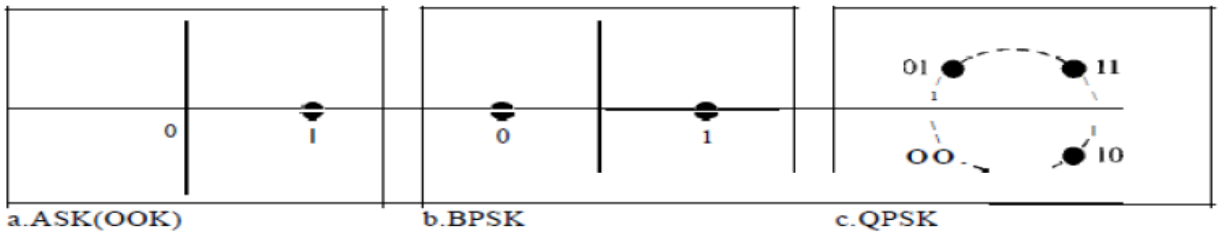


Example 5.8

Show the constellation diagrams for an ASK (OOK), BPSK, and QPSK signals.

Solution Figure 5.13 shows the three constellation diagrams

Figure 5.13 *Three constellation diagrams.*



Let us analyze each case separately:

a. For ASK, we are using only an in-phase carrier. Therefore, the two points should be on the X axis. Binary 0 has an amplitude of 0 V; binary 1 has an amplitude of 1V (for example). The points are located at the origin and at 1 unit.

b. BPSK also uses only an in-phase carrier. However, we use a polar NRZ signal for modulation. It creates two types of signal elements, one with amplitude 1 and the other with amplitude -1. This can be stated in other words: BPSK creates two different signal elements, one with amplitude I V and in phase and the other with amplitude 1V and 180^0 out of phase.

c. QPSK uses two carriers, one in-phase and the other quadrature. The point representing 11 is made of two combined signal elements, both with an amplitude of 1V. One element is represented by an in-phase carrier, the other element by a quadrature carrier. The amplitude of the final signal element sent for this 2-bit data element is $2^{1/2}$, and the phase is *45°*. The argument is similar for the other three points. All signal

elements have an amplitude of $2^{1/2}$, but their phases are different *(45°*, 135°, -135°, and -45°). Of course, we could have chosen the amplitude of the carrier to be $1/(2^{1/2})$ to make the final amplitudes 1 V.

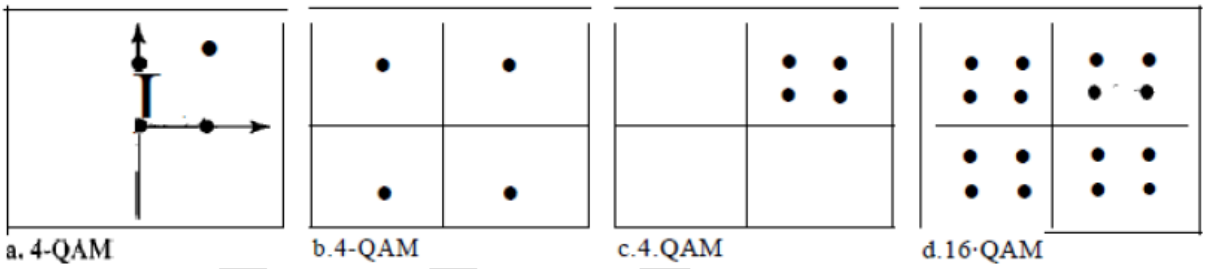
Quadrature Amplitude Modulation

PSK is limited by the ability of the equipment to distinguish small differences in phase. This factor limits its potential bit rate. So far, we have been altering only one of the three characteristics of a sine wave at a time; but what if we alter two? Why not combine ASK and PSK? The idea of using two carriers, one in-phase and the other quadrature, with different amplitude levels for each carrier is the concept behind quadrature amplitude modulation (QAM).

Quadrature amplitude modulation is a combination of ASK and PSK.

The possible variations of QAM are numerous. Figure 5.14 shows some of these schemes. Figure 5.14a shows the simplest 4-QAM scheme (four different signal element types) using a unipolar NRZ signal to modulate each carrier. This is the same mechanism we used for ASK (OOK). Part b shows another 4-QAM using polar NRZ, but this is exactly the same as QPSK. Part c shows another QAM-4 in which we used a signal with two positive levels to modulate each of the two carriers. Finally, Figure 5.14d shows a 16-QAM constellation of a signal with eight levels, four positive and four negative.

Figure 5.14 *Constellation diagrams for some QAMs*



Bandwidth for QAM

The minimum bandwidth required for QAM transmission is the same as that required for ASK and PSK transmission. QAM has the same advantages as PSK over ASK.

CHAPTER 6
BANDWIDTH UTILIZATION : MULTIPLEXING AND SPREAD SPECTRUM

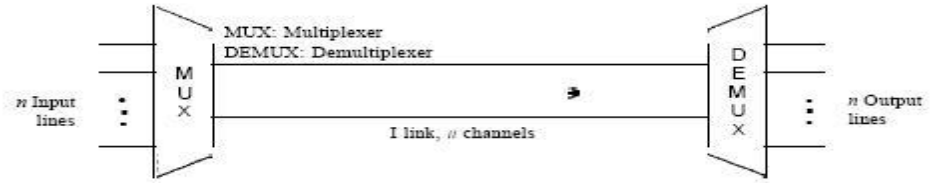
6.1 MULTIPLEXING

Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. As data and telecommunications use increases, so does traffic. We can accommodate this increase by continuing to add individual links each time a new channel is needed; or we can install higher-bandwidth links and use each to carry multiple signals.Today's technology includes high-bandwidth media such as optical fiber and terrestrial and satellite microwaves. Each has a

bandwidth far in excess of that needed for the average transmission signal. If the bandwidth of a link is greater than the bandwidth needs of the devices connected to it, the bandwidth is wasted. An efficient system maximizes the utilization of all resources;bandwidth is one of the most precious resources we have in data communications.

In a multiplexed system, n lines share the bandwidth of one link. Figure 6.1 shows the basic format of a multiplexed system. The lines on the left direct their transmission streams to a multiplexer(MUX), which combines them into a single stream (many-toone). At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines. In the figure, the word link refers to the physical path. The word channel refers to the portion of a link that carries a transmission between a given pair of lines. One link can have many (n) channels.

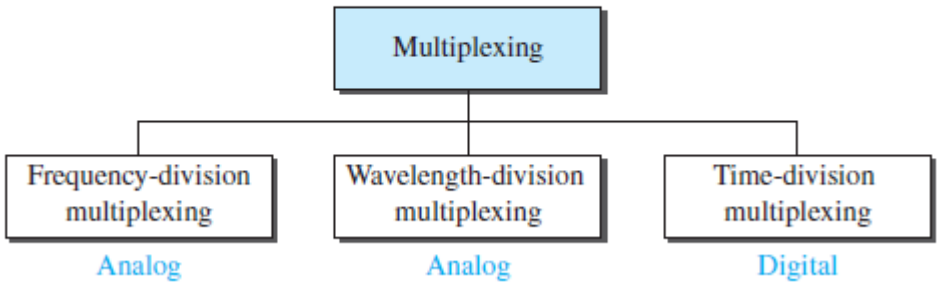
Figure 6.1 *Dividing a link into channels*



There are three basic multiplexing techniques: frequency-division multiplexing, wavelength-division multiplexing, and time-division multiplexing. The first two are techniques designed for analog signals, the third, for digital signals (see Figure 6.2).

Figure 6.2 *Categories of multiplexing*

Figure 6.2 *Categories of multiplexing*

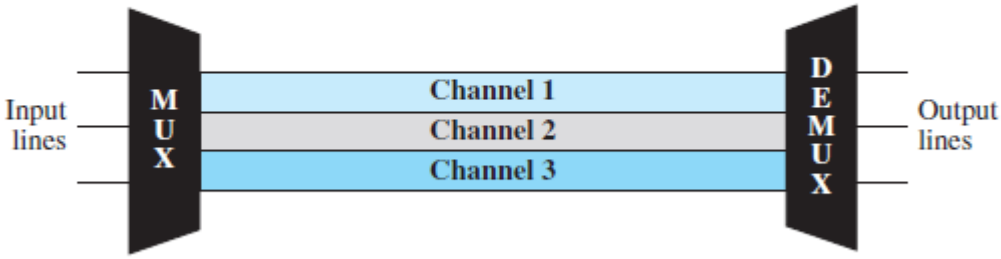


Frequency-Division Multiplexing

Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to

accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-guard bands-to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original data frequencies. Figure 6.3 gives a conceptual view of FDM. In this illustration, the transmission path is divided into three parts, each representing a channel that carries one transmission.

Figure 6.3 *Frequency-division multiplexing*



We consider FDM to be an analog multiplexing technique; however, this does not mean that FDM cannot be used to combine sources sending digital signals. A digital signal can be converted to an analog signal before FDM is used to multiplex them.

FDM is an analog multiplexing technique that combines analog signals.

Multiplexing Process

Figure 6.4 is a conceptual illustration of the multiplexing process. Each source generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulates different carrier frequencies *(/1,12,* and *h).* The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

Demultiplexing Process

The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines. Figure 6.5 is a conceptual illustration of demultiplexing process.

Figure 6.4 *FDM process*

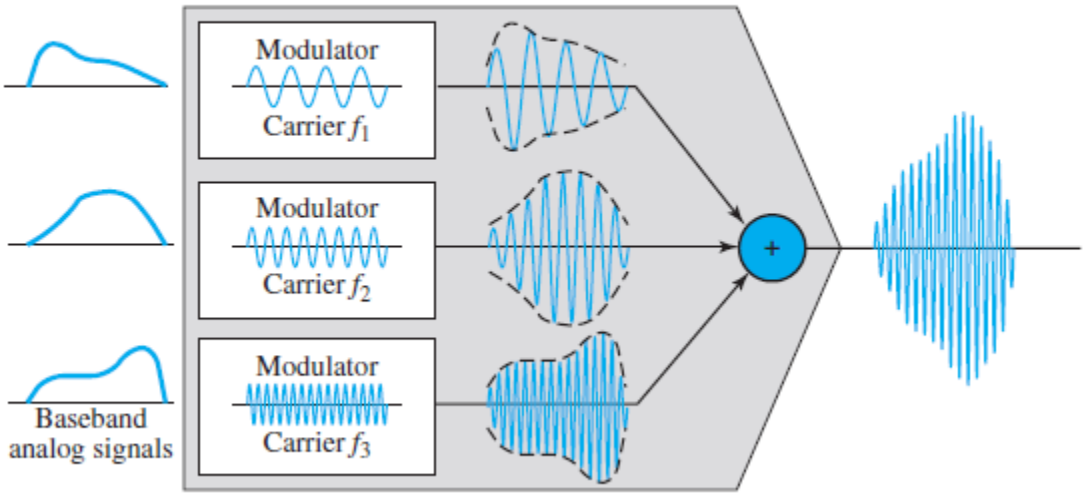
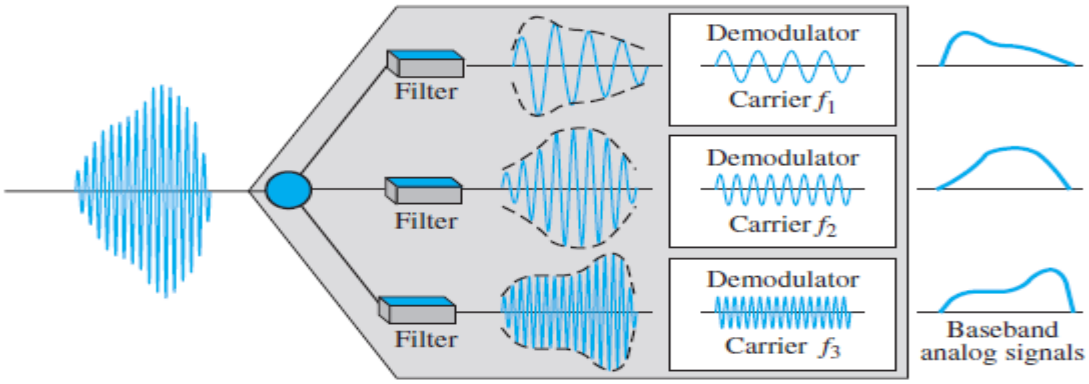


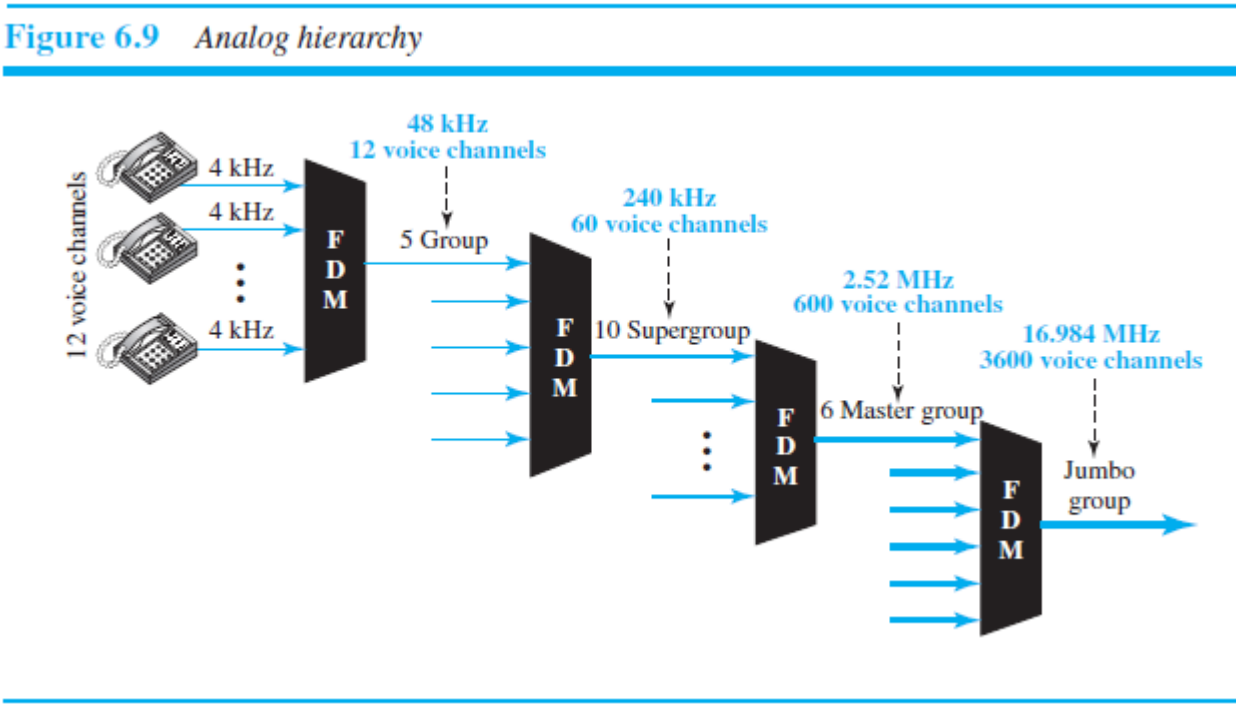
Figure 6.5 *FDM demultiplexing example*



The Analog Carrier System

To maximize the efficiency of their infrastructure, telephone companies have traditionally multiplexed signals from lower-bandwidth lines onto higher-bandwidth lines. In this way, many switched or leased lines can be combined into fewer but bigger channels. For analog lines, FDM is used. One of these hierarchical systems used by AT&T is made up of groups, super groups, master groups, and jumbo groups

Figure 6.9 *Analog hierarchy*



In this analog hierarchy, 12 voice channels are multiplexed onto a higher-bandwidth line to create a group. A group has 48 kHz of bandwidth and supports 12 voice channels. At the next level, up to five groups can be multiplexed to create a composite signal called a supergroup. A supergroup has a bandwidth of 240 kHz and supports up to 60 voice channels. Supergroups can be made up of either five groups or 60 independent voice channels. At the next level, 10 supergroups are multiplexed to create a master group. A master group must have 2.40 MHz of bandwidth, but the need for guard bands between the supergroups increases the necessary bandwidth to 2.52 MHz. Master groups support up to 600 voice channels. Finally, six master groups can be combined into a jumbo group. A jumbo group must have 15.12 MHz (6 x 2.52 MHz) but is augmented to 16.984 MHz to allow for guard bands between the master groups.

Wavelength-Division Multiplexing

Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber-optic cable.

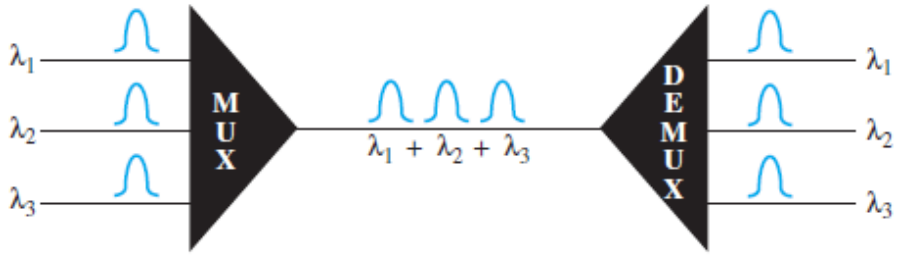
The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.

WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high.

Figure 6.10 gives a conceptual view of a WDM multiplexer and demultiplexer. Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer

Figure 6.10 ***Wavelength-division multiplexing***

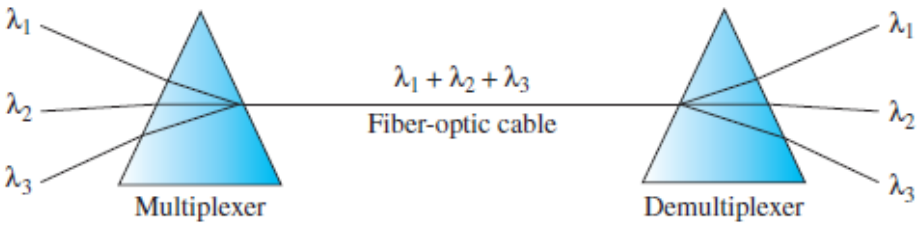
Figure 6.10 *Wavelength-division multiplexing*



WDM is an analog multiplexing technique to combine optical signals.

Although WDM technology is very complex, the basic idea is very simple. We want to combine multiple light sources into one single light at the multiplexer and do the reverse at the demultiplexer. The combining and splitting of light sources are easily handled by a prism. A prism bends a beam of light based on the angle of incidence and the frequency. Using this technique, a multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies. A demultiplexer can also be made to reverse the process. Figure 6.11 shows the concept.

Figure 6.11 *Prisms in wavelength-division multiplexing and demultiplexing*

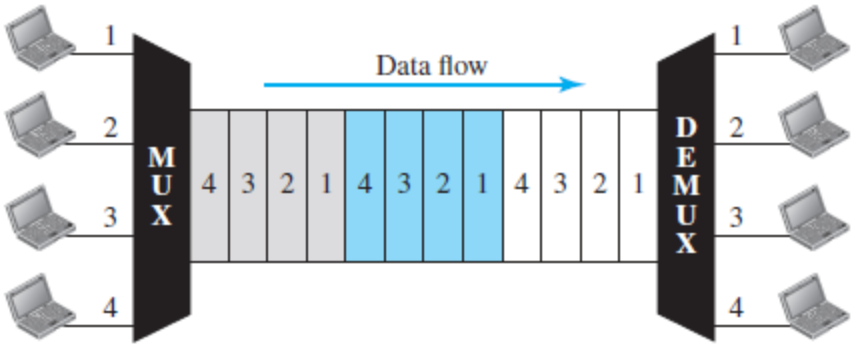


Time-Division Multiplexing

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a link. Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link.

Figure 6.12 gives a conceptual view of TDM. Note that the same link is used as in FDM; here, however,the link is shown sectioned by time rather than by frequency. In the figure, portions of signals 1, 2, 3, and 4 occupy the link sequentially.

Figure 6.12 *TDM*



All the data in a message from source 1 always go to one specific destination, be it 1, 2, 3, or 4. The delivery is fixed and unvarying, unlike switching. We also need to remember that TDM is, in principle, a digital multiplexing technique.

Digital data from different sources are combined into one timeshared link. However, this does not mean that the sources cannot produce analog data; analog data can be sampled,changed to digital data, and then multiplexed by using TDM. We can divide TDM into two different schemes: synchronous and statistical

In synchronous TDM, the data flow of each input connection is divided into units, where each input occupies one input time slot. A unit can be 1 bit, one character, or one block of data. Each input unit becomes one output unit and occupies one output time slot.

The duration of an output time slot is *n* times shorter than the duration of an input time slot. If an input time slot is *T* s, the output time slot is *Tin* s where *n* is the number of connections. In other words, a unit in the output connection has a shorter duration; it travels faster. Figure 6.13 shows an example of synchronous TDM where *n* is 3.

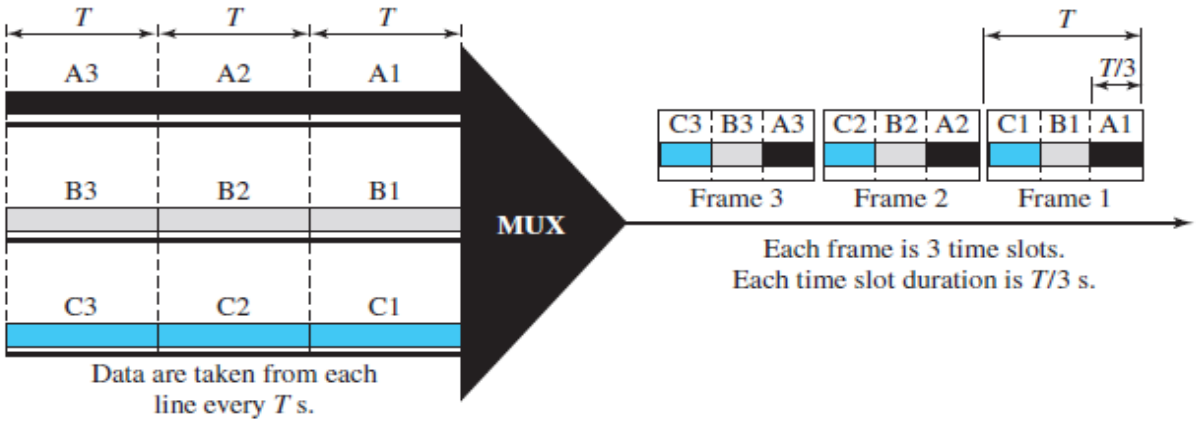
In synchronous TDM, a round of data units from each input connection is collected into a frame . If we have *n* connections, frames divided into *n* time slots and one slot is allocated for each unit, one for each input line.

If the duration of the input unit is *T*, the duration of each slot is *Tin* and the duration of each frame is *T*. The data rate of the output link must be *n* times the data rate of a connection to guarantee the flow of data. In Figure 6.13, the data rate of the link is 3 times the data rate of a connection; likewise, the duration of a unit on a connection is 3 times that of the time slot (duration of a unit on the link). In the figure we represent the data prior to multiplexing as 3 times the size of the data after multiplexing. This is just to convey the idea that each unit is 3 times longer in duration before multiplexing than after.

In synchronous TDM, the data rate of the link is *n* times faster, and the unit duration is *n* times shorter.

Time slots are grouped into frames. A frame consists of one complete cycle of time slots, with one slot dedicated to each sending device. In a system with *n* input lines, each frame has *n* slots, with each slot allocated to carrying data from a specific input line.

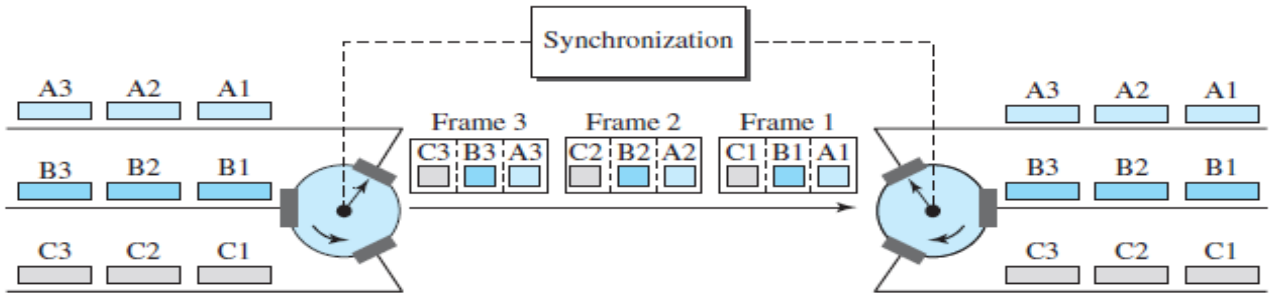
Figure 6.13 *Synchronous time-division multiplexing*



Interleaving

TDM can be visualized as two fast-rotating switches, one on the multiplexing side and the other on the demultiplexing side. The switches are synchronized and rotate at the same speed, but in opposite directions. On the multiplexing side, as the switch opens in front of a connection, that connection has the opportunity to send a unit onto the path. This process is called interleaving. On the demultiplexing side, as the switch opens in front of a connection, that connection has the opportunity to receive a unit from the path. Figure 6.15 shows the interleaving process for the connection shown in Figure 6.13.In this figure, we assume that no switching is involved and that the data from the first connection at the multiplexer site go to the first connection at the demultiplexer.

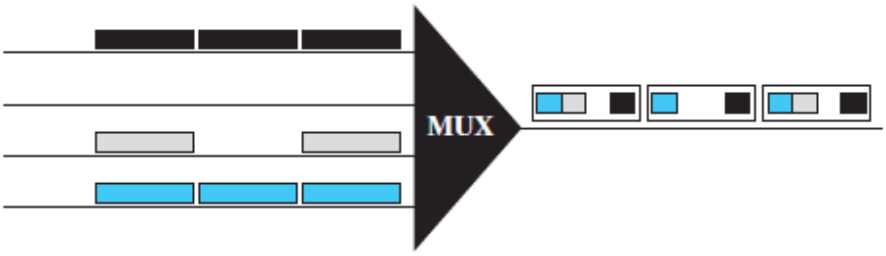
Figure 6.15 *Interleaving*



Empty Slots

Synchronous TDM is not as efficient as it could be. If a source does not have data to send, the corresponding slot in the output frame is empty. Figure 6.18 shows a case in which one of the input lines has no data to send and one slot in another input line has discontinuous data.

Figure 6.18 *Empty slots*



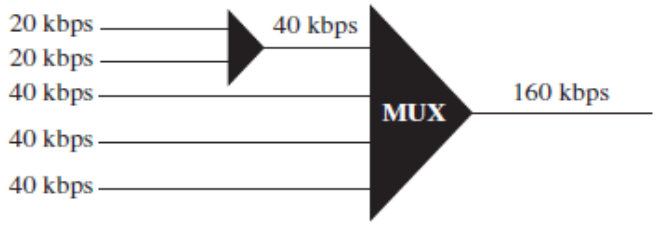
The first output frame has three slots filled, the second frame has two slots filled, and the third frame has three slots filled. No frame is full. We learn in the next section that statistical TDM can improve the efficiency by removing the empty slots from the frame.

Data Rate Management

One problem with TDM is how to handle a disparity in the input data rates. In all our discussion so far, we assumed that the data rates of all input lines were the same. However, if data rates are not the same, three strategies, or a combination of them, can be used. **We call these three strategies multilevel multiplexing, multiple-slot allocation, and pulse stuffing.**

Multilevel Multiplexing Multilevel multiplexing is a technique used when the data rate of an input line is a multiple of others. For example, in Figure 6.19, we have two inputs of 20 kbps and three inputs of 40 kbps. The first two input lines can be multiplexed together to provide a data rate equal to the last three. A second level of multiplexing can create an output of 160 kbps.

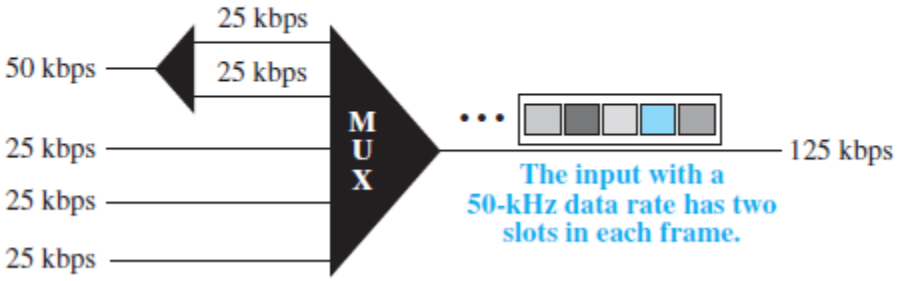
Figure 6.19 *Multilevel multiplexing*



Multiple-Slot Allocation Sometimes it is more efficient to allot more than one slot in a frame to a single input line. For example, we might have an input line that has a data rate that is a multiple

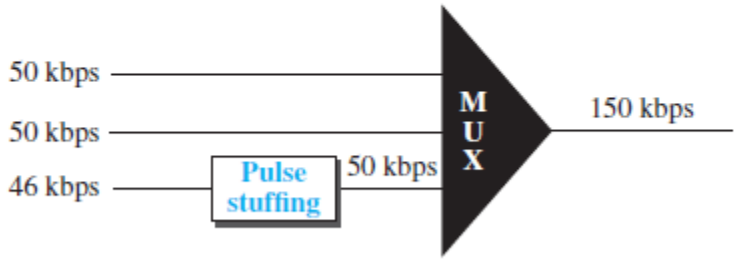
of another input. In Figure 6.20, the input line with a SO-kbps data rate can be given two slots in the output. We insert a serial-to-parallel converter in the line to make two inputs out of one.

Figure 6.20 *Multiple-slot multiplexing*



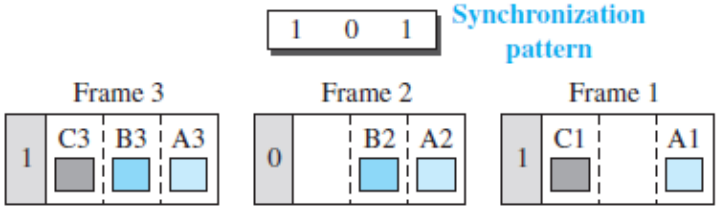
Pulse Stuffing Sometimes the bit rates of sources are not multiple integers of each other. Therefore, neither of the above two techniques can be applied. One solution is to make the highest input data rate the dominant data rate and then add dummy bits to the input lines with lower rates. This will increase their rates. This technique is called pulse stuffing, bit padding, or bit stuffing. The idea is shown in Figure 6.21. The input with a data rate of 46 is pulse-stuffed to increase the rate to 50 kbps. Now multiplexing can take place.

Figure 6.21 *Pulse stuffing*



The implementation of TDM is not as simple as that of FDM. Synchronization between the multiplexer and demultiplexer is a major issue. If the multiplexer and the demultiplexer are not synchronized, a bit belonging to one channel may be received by the wrong channel. For this reason, one or more synchronization bits are usually added to the beginning of each frame. These bits, called framing bits, follow a pattern, frame to frame, that allows the demultiplexer to synchronize with the incoming stream so that it can separate the time slots accurately. In most cases, this synchronization information consists of 1 bit per frame, alternating between 0 and I, as shown in Figure 6.22.

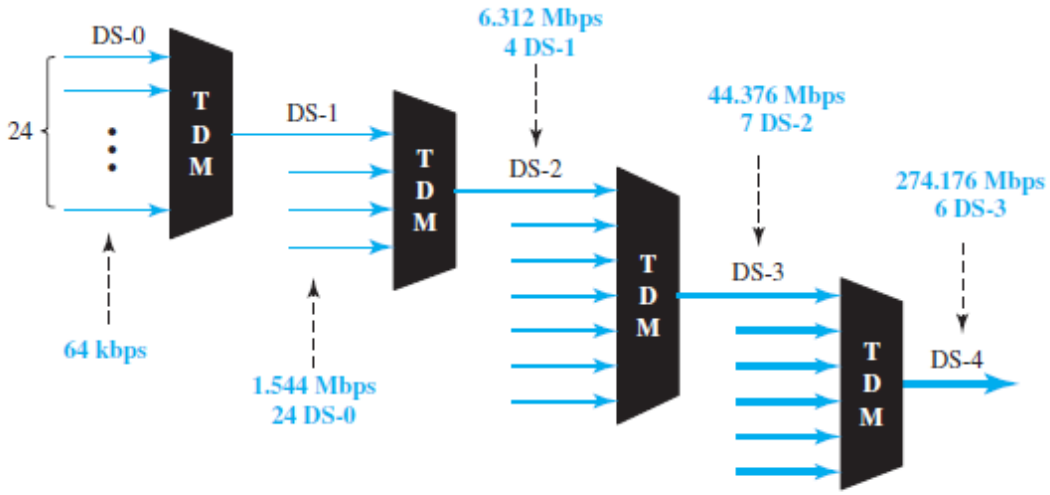
Figure 6.22 *Framing bits*



Digital Signal Service

Telephone companies implement TDM through a hierarchy of digital signals, called digital signal (DS) service or digital hierarchy. Figure 6.23 shows the data rates supported by each level

Figure 6.23 *Digital hierarchy*



- **DS-0** is a single digital channel of 64 kbps.
- **DS-1** is a 1.544-Mbps service; 1.544 Mbps is 24 times 64 kbps plus 8 kbps of overhead. It can be used as a single service for 1.544-Mbps transmissions, or it can be used to multiplex 24 DS-0 channels or to carry any other combination desired by the user that can fit within its 1.544-Mbps capacity.
- **DS-2** is a 6.312-Mbps service; 6.312 Mbps is 96 times 64 kbps plus 168 kbps of overhead. It can be used as a single service for 6.312-Mbps transmissions; or it can be used to multiplex 4 DS-1 channels, 96 DS-0 channels, or a combination of these service types.
- **DS-3** is a 44.376-Mbps service; 44.376 Mbps is 672 times 64 kbps plus 1.368 Mbps of overhead. It can be used as a single service for 44.376-Mbps transmissions; or it can be used to multiplex 7 DS-2 channels, 28 DS-1 channels, 672 DS-0 channels, or a combination of these service types.
- **DS-4** is a 274.176-Mbps service; 274.176 is 4032 times 64 kbps plus 16.128 Mbps of overhead. It can be used to multiplex 6 DS-3 channels, 42 DS-2 channels, 168 DS-1 channels, 4032 DS-0 channels, or a combination of these service types.

T Lines

DS-0, DS-1, and so on are the names of services. To implement those services, the telephone companies use **T lines** (T-1 to T-4). These are lines with capacities precisely matched to the data rates of the DS-1 to DS-4 services (see Table 6.1). So far only T-1 and T-3 lines are commercially available.

Table 6.1 *DS and T line rates*

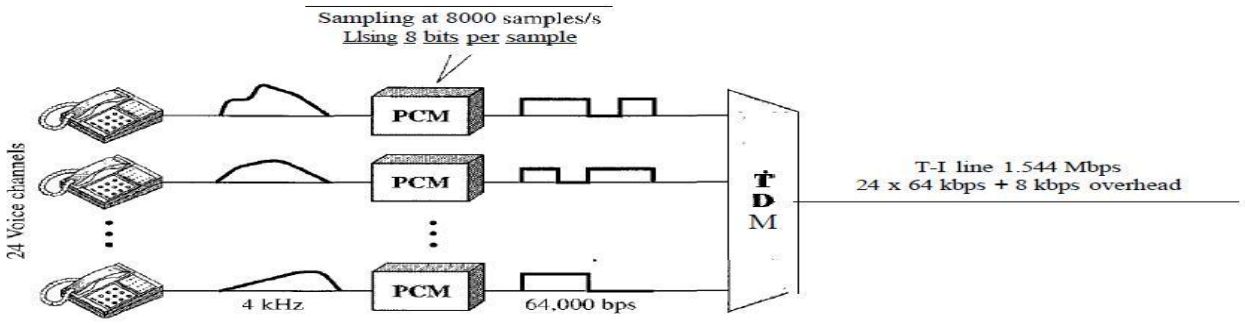
Sen/ice	*Line*	*Rate (Mbps)*	*Voice Channels*
DS-1	T-1	1.544	24
DS-2	T-2	6.312	96
DS-3	T-3	44.736	672
DS-4	T-4	274.176	4032

The T-l line is used to implement DS-l; T-2 is used to implement DS-2; and so on. As you can see from Table 6.1, DS-O is not actually offered as a service, but it has been defined as a basis for reference purposes.

T Lines for Analog Transmission

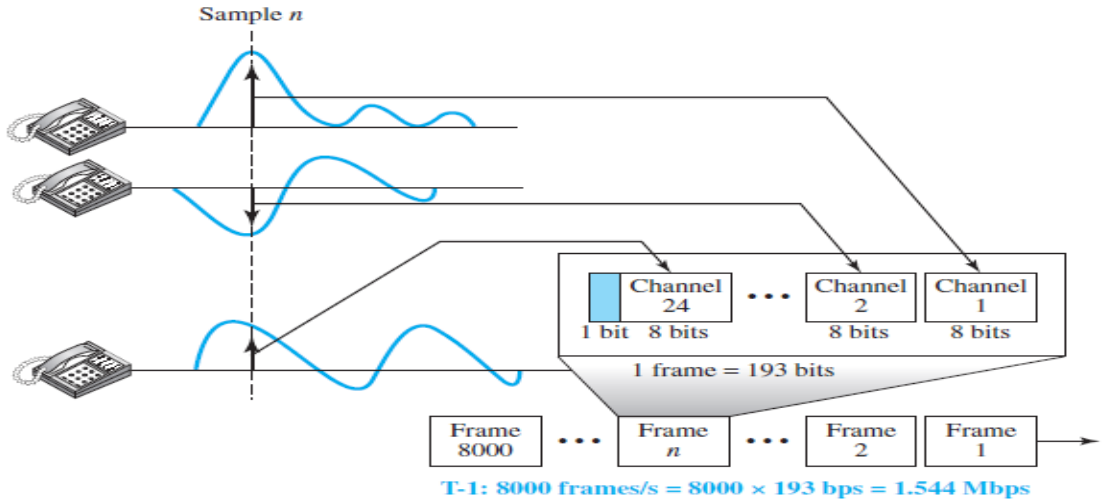
T lines are digital lines designed for the transmission of digital data, audio, or video. However, they also can be used for analog transmission (regular telephone connections), provided the analog signals are first sampled, then time-division multiplexed. The possibility of using T lines as analog carriers opened up a new generation of services for the telephone companies. Earlier, when an organization wanted 24 separate telephone lines, it needed to run 24 twisted-pair cables from the company to the central exchange.

Figure 6.24 *T-l line for multiplexing telephone lines*



The T-1 Frame As noted above, DS-l requires 8 kbps of overhead. To understand how this overhead is calculated, we must examine the format of a 24-voice-channel frame. The frame used on a T-l line is usually 193 bits divided into 24 slots of 8 bits each plus 1 extra bit for synchronization (24 x 8 + 1 = 193); see Figure 6.25. In other words, each slot contains one signal segment from each channel; 24 segments are interleaved in one frame. If a T-1 line carries 8000 frames, the data rate is 1.544 Mbps (193 × 8000 =1.544 Mbps)—the capacity of the line.

Figure 6.25 *T-1 frame structure*



E Lines Europeans use a version of T lines called E lines. The two systems are conceptually identical, but their capacities differ. Table 6.2 shows the E lines and their capacities.

Table 6.2 *E line rates*

Line	*Rate (Mbps)*	*Voice Channels*
E-1	2.048	30
E-2	8.448	120
E-3	34.368	480
E-4	139.264	1920

Statistical Time-Division Multiplexing

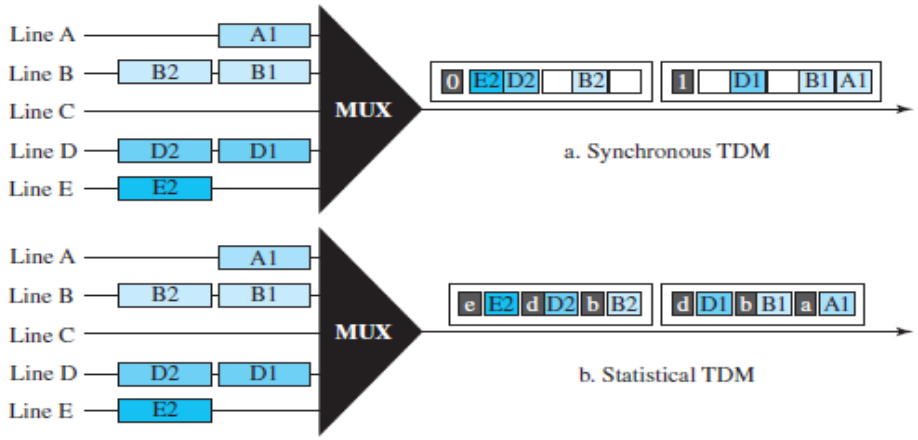
In synchronous TDM, each input has a reserved slot in the output frame. This can be inefficient if some input lines have no data to send.In statistical time-division multiplexing, slots are dynamically allocated to improve bandwidth efficiency. Only when an input line has a slot's worth of data to send is it given a slot in the output frame. In statistical multiplexing, the number of slots in each frame is less than the number of input lines. The multiplexer checks each input line in round robin fashion; it allocates a slot for an input line if the line has data to send; otherwise, it skips the line and checks the next line. Figure 6.26 shows a synchronous and a statistical TDM example. In the former, some slots are empty because the corresponding line does not have data to send. In the latter, however, no slot is left empty as long as there are data to be sent by any input line.

Addressing

Figure 6.26 also shows a major difference between slots in synchronous TDM and statistical TDM.

- An output slot in synchronous TDM is totally occupied by data; in statistical TDM, a slot needs to carry data as well as the address of the destination.
- In synchronous TDM, there is no need for addressing; synchronization and preassigned relationships between the inputs and outputs serve as an address. We know, for example, that input 1 always goes to input 2. If the multiplexer and the demultiplexer are synchronized, this is guaranteed. In statistical multiplexing, there is no fixed relationship between the inputs and outputs because there are no preassigned or reserved slots. We need to include the address of the receiver inside each slot to show where it is to be delivered. The addressing in its simplest form can be *n* bits to define *N* different output lines with *n* =10g2 *N*. For example, for eight different output lines, we need a 3-bit address.

Figure 6.26 *TDM slot comparison*



Slot Size

Since a slot carries both data and an address in statistical TDM, the ratio of the data size to address size must be reasonable to make transmission efficient. For example, it would be inefficient to send 1 bit per slot as data when the address is 3 bits. This would mean an overhead of 300 percent. In statistical TDM, a block of data is usually many bytes while the address is just a few bytes.

No Synchronization Bit

There is another difference between synchronous and statistical TDM, but this time it is at the frame level. The frames in statistical TDM need not be synchronized, so we do not need synchronization bits.

Bandwidth

In statistical TDM, the capacity of the link is normally less than the sum of the capacities of each channel. The designers of statistical TDM define the capacity of the link based on the statistics of the load for each channel.

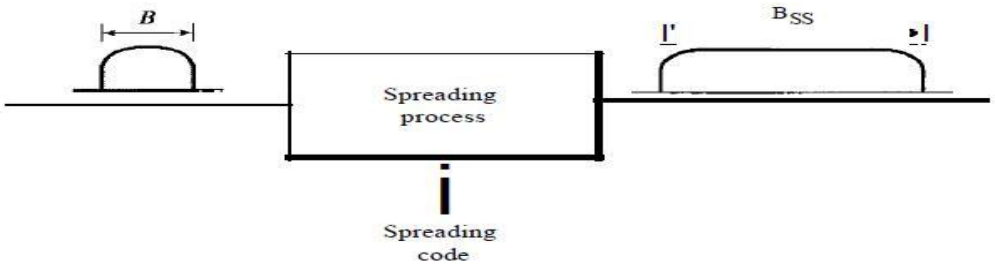
6.2 SPREAD SPECTRUM

Multiplexing combines signals from several sources to achieve bandwidth efficiency; the available bandwidth of a link is divided between the sources. In spread spectrum, we also combine signals from different sources to fit into a larger bandwidth, but our goals are somewhat different. Spread spectrum is designed to be used in wireless applications(LANs and WANs). Figure 6.27 shows the idea of spread spectrum. Spread spectrum achieves its goals through two principles:

1. The bandwidth allocated to each station needs to be, by far, larger than what is needed. This allows redundancy.

2. The expanding of the original bandwidth *B* to the bandwidth Bss must be done by a process that is independent of the original signal. In other words, the spreading process occurs after the signal is created by the source.

Figure 6.27 *Spread spectrum*



After the signal is created by the source, the spreading process uses a spreading code and spreads the bandwidth. The figure shows the original bandwidth *B* and the spreaded bandwidth *Bss*. The spreading code is a series of numbers that look random, but are actually a pattern. There are two

techniques to spread the bandwidth: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS).

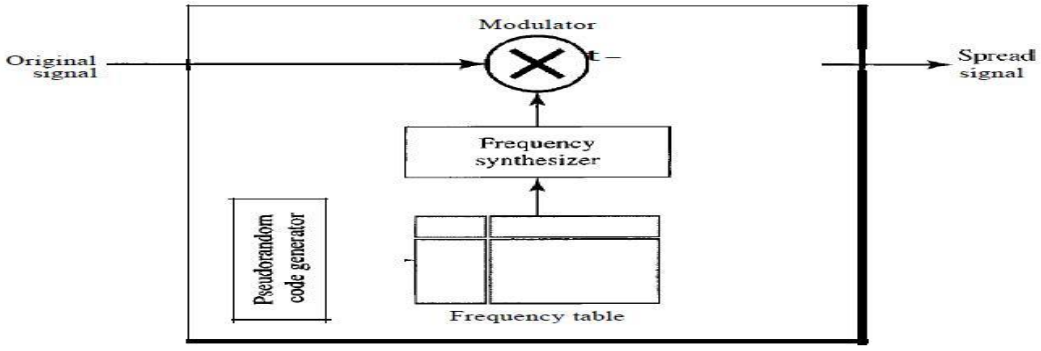
Frequency Hopping Spread Spectrum (FHSS)

The frequency hopping spread spectrum (FHSS) technique uses *M* different carrier frequencies that are modulated by the source signal.At one moment, the signal modulates one carrier frequency; at the next moment, the signal modulates another carrier frequency. Although the modulation is done using one carrier frequency at a time, *M* frequencies are used in the long run. The bandwidth occupied by a source after spreading is *BpHSS »B.*

Figure 6.28 shows the general layout for FHSS. A pseudorandom code generator, called pseudorandom noise (PN), creates a k-bit pattern for every hopping period *Th•* The frequency table uses the pattern to find the frequency to be used for this hopping period and passes it to the frequency synthesizer. The

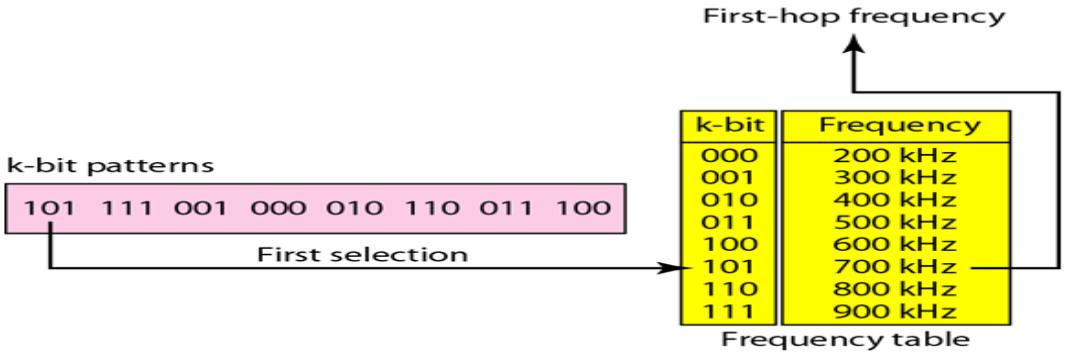
frequency synthesizer creates a carrier signal of that frequency, and the source signal modulates the carrier signal.

Figure 6.28 *Frequency hopping spread spectrum (FHSS)*



Suppose we have decided to have eight hopping frequencies. This is extremely low for real applications and is just for illustration. In this case, *M is* 8 and *k* is 3. The pseudorandom code generator will create eight different 3-bit patterns. These are mapped to eight different frequencies in the frequency table (see Figure 6.29).

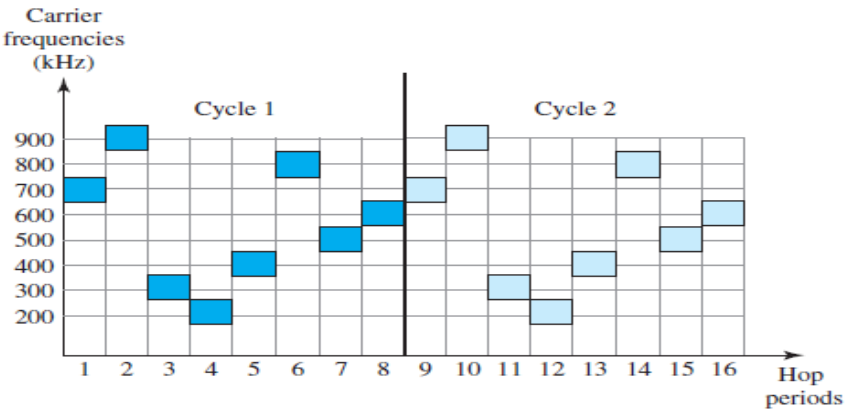
Figure 6.29 *Frequency selection in FHSS*



The pattern for this station is 101, 111, 001, 000, 010, all, 100. Note that the pattern is pseudorandom it is repeated after eight hoppings. This means that at hopping period 1, the pattern is 101. The frequency selected is 700 kHz; the source signal modulates this carrier frequency. The second k-bit pattern selected is 111, which selects the 900-kHz carrier; the eighth pattern is 100, the frequency is 600 kHz. After eight hoppings, the pattern repeats, starting from 101 again. Figure 6.30 shows how the signal hops around from carrier to carrier. We assume the required bandwidth of the original signal is 100 kHz.

It can be shown that this scheme can accomplish the previously mentioned goals. If there are many k-bit patterns and the hopping period is short, a sender and receiver can have **privacy**. If an intruder tries to intercept the transmitted signal, she can only access a small piece of data because she does not know the spreading sequence to quickly adapt herself to the next hop. The scheme has also an **antijamming** effect. A malicious sender may be able to send noise to jam the signal for one hopping period (randomly), but not for the whole period.

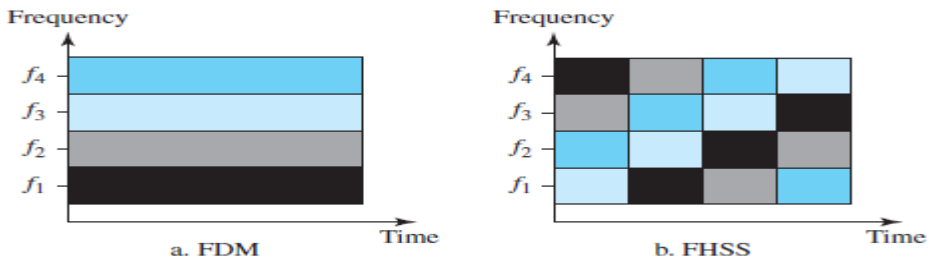
Figure 6.30 *FHSS cycles*



Bandwidth Sharing

If the number of hopping frequencies is *M*, we can multiplex *M* channels into one by using the same Bss bandwidth. This is possible because a station uses just one frequency in each hopping period; *M* - 1 other frequencies can be used by other *M* - 1 stations. In other words, *M* different stations can use the same Bss if an appropriate modulation technique such as multiple FSK (MFSK) is used. FHSS is similar to FDM, as shown in Figure 6.31.Figure 6.31 shows an example of four channels using FDM and four channels using FHSS.

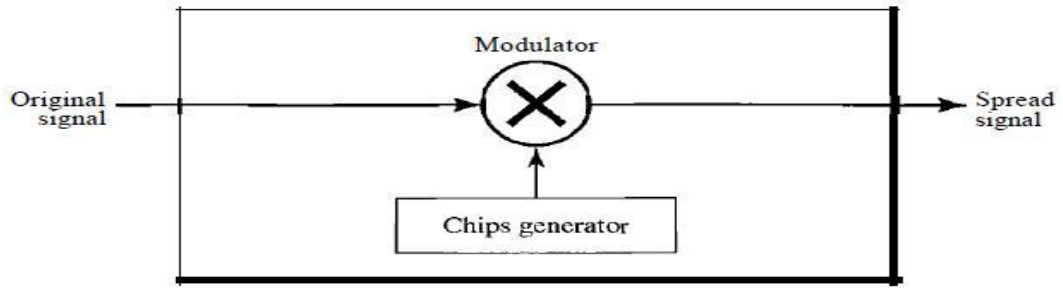
Figure 6.31 *Bandwidth sharing*



Direct Sequence Spread Spectrum

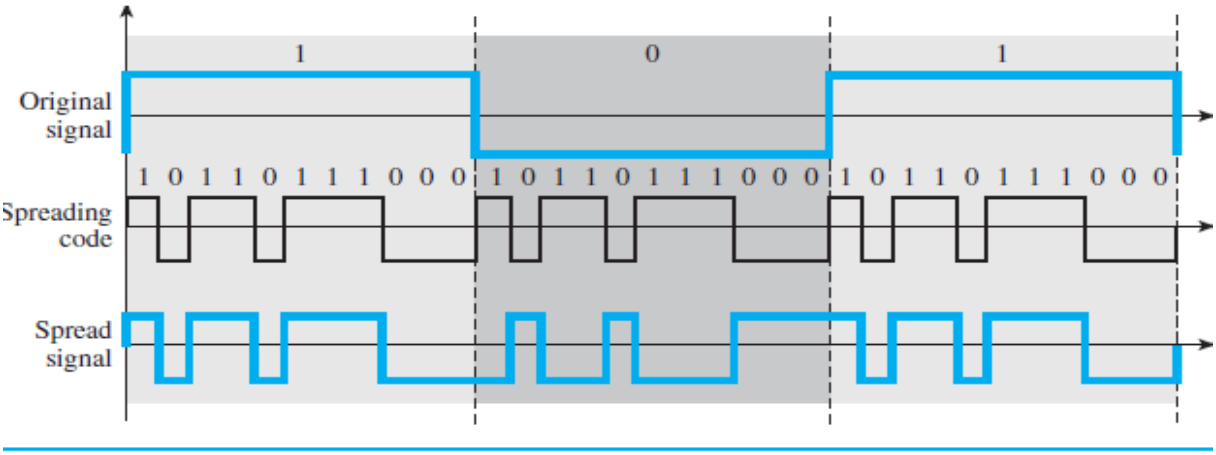
The direct sequence spread spectrum (nSSS) technique also expands the bandwidth of the original signal, but the process is different. In DSSS, we replace each data bit with 11 bits using a spreading code. In other words, each bit is assigned a code of 11 bits, called chips, where the chip rate is 11 times that of the data bit. Figure 6.32 shows the concept of DSSS.

Figure 6.32 *DSSS*



As an example, let us consider the sequence used in a wireless LAN, the famous **Barker sequence** where n is 11. We assume that the original signal and the chips in the chip generator use polar NRZ encoding. Figure 6.33 shows the chips and the result of multiplying the original data by the chips to get the spread signal. In Figure 6.33, the spreading code is 11 chips having the pattern 10110111000 (in this case). If the original signal rate is *N*, the rate of the spread signal is *lIN*. This means that the required bandwidth for the spread signal is 11 times larger than the bandwidth of the original signal. The spread signal can provide **privacy** if the intruder does not know the code. It can also provide immunity against interference if each station uses a different code.

Figure 6.33 *DSSS example*



Bandwidth Sharing

Can we share a bandwidth in DSSS as we did in FHSS? The answer is no and yes. If we use a spreading code that spreads signals (from different stations) that cannot be combined and separated, we cannot share a bandwidth.

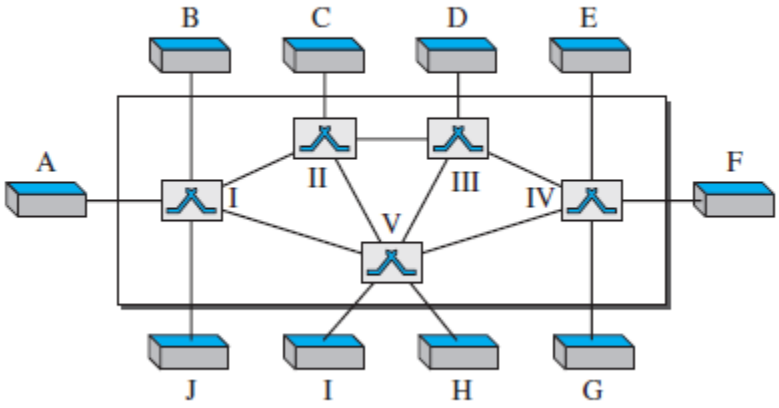
CHAPTER 8
Switching

8.1 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, however, are impractical and wasteful when applied to very large networks.The number and length of the links require too much infrastructure to be cost-efficient,and the majority of those links would be idle most of the time. 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 the 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 (computers or telephones, for example). Others are used only for routing. Figure 8.1 shows a switched network.

Figure 8.1 *Switched network*

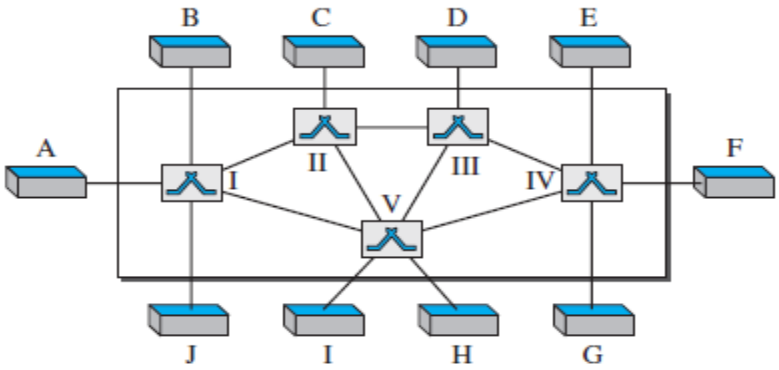


The **end systems** (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

8.1.1 Three Methods of Switching

Traditionally, three methods of switching have been discussed: **circuit switching**, **packet switching**, and **message switching**. The first two are commonly used today.The third has been phased out in general communications but still has networking applications. Packet switching can further be divided into two subcategories—virtual circuit approach and datagram approach—as shown in Figure 8.2.

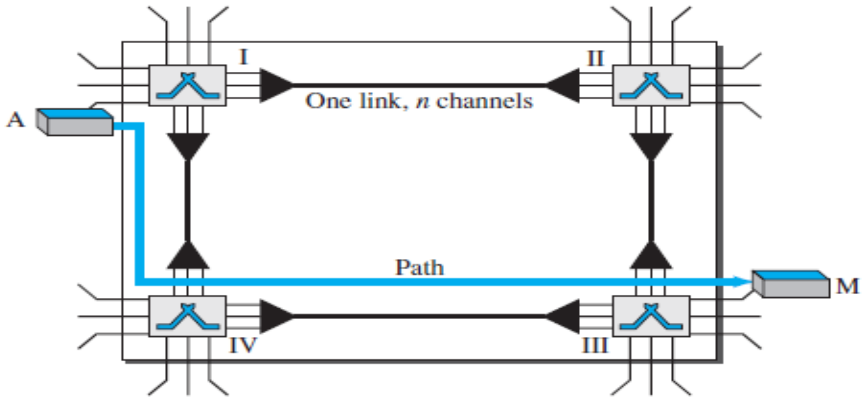
Figure 8.1 *Switched network*



8.2 CIRCUIT-SWITCHED NETWORKS

Circuit-switched network consists of a set of switches connected by physical links.A connection between two stations is a **dedicated path** made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into *n* channels by using FDM or TDM.

Figure 8.3 *A trivial circuit-switched network*



We have explicitly shown the multiplexing symbols to emphasize the division of the link into channels even though multiplexing can be implicitly included in the switch fabric. The end systems, such as computers or telephones, are directly connected to a switch. We have shown only two end systems for simplicity. When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the **setup phase;** a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels) is established, the **data-transfer phase** can take place. After all data have been transferred,the circuits are torn down.

We need to emphasize several points here:

- Circuit switching takes place at the physical layer.
- Before starting communication, the stations must make a reservation for the resources

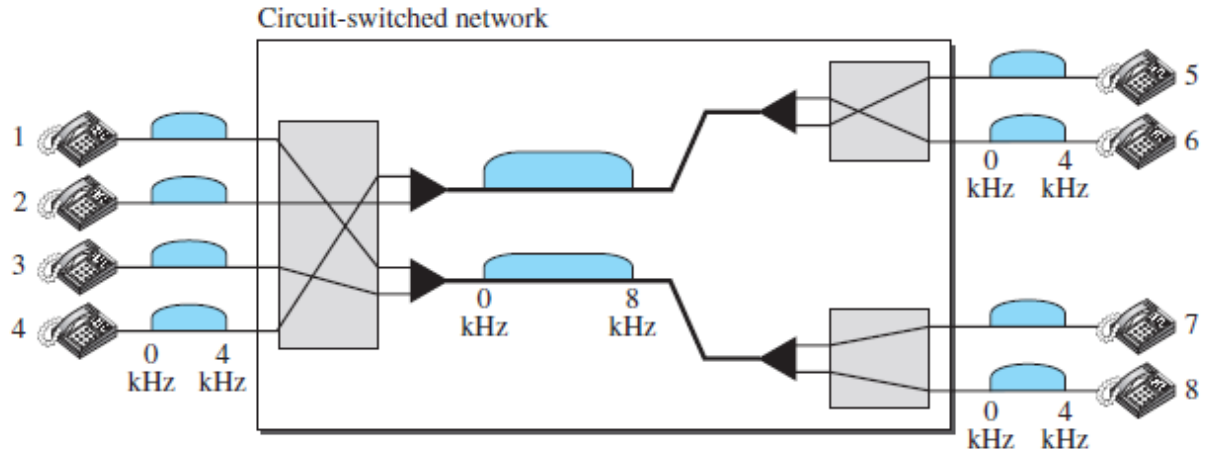
to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the **teardown phase.**

- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.
- There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to-end addressing used during the setup phase.

Example 8.1

As a trivial example, let us use a circuit-switched network to connect eight telephones in a small area. Communication is through 4-kHz voice channels. We assume that each link uses FDM to connect a maximum of two voice channels. The bandwidth of each link is then 8 kHz. Figure 8.4 shows the situation. Telephone 1 is connected to telephone 7; 2 to 5; 3 to 8; and 4 to 6. Of course the situation may change when new connections are made. The switch controls the connections.

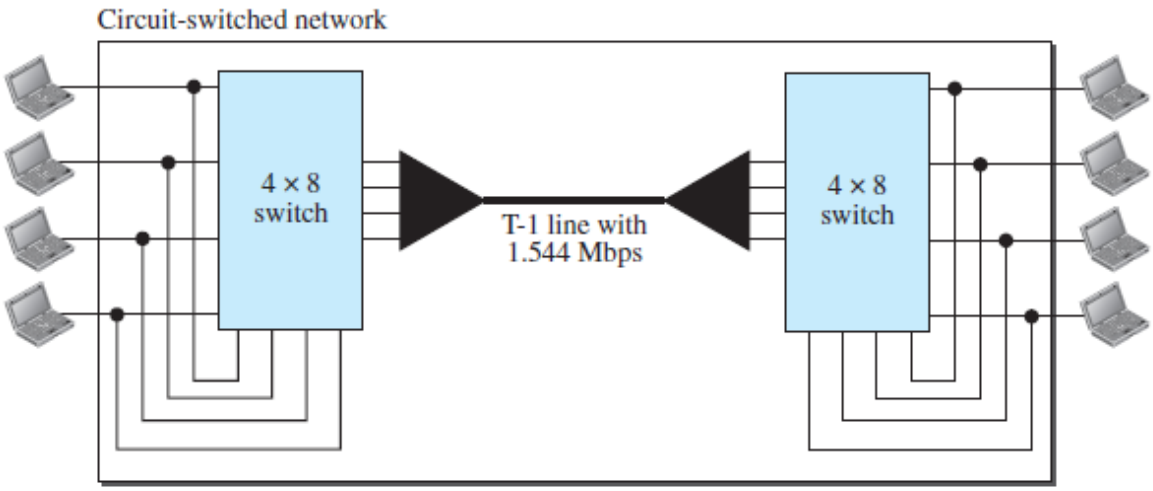
Figure 8.4 *Circuit-switched network used in Example 8.1*



Example 8.2

As another example, consider a circuit-switched network that connects computers in two remote offices of a private company. The offices are connected using a T-1 line leased from a communication service provider. There are two $4 \cdot 8$ (4 inputs and 8 outputs) switches in this network. For each switch, four output ports are folded into the input ports to allow communication between computers in the same office. Four other output ports allow communication between the two offices. Figure 8.5 shows the situation.

Figure 8.5 *Circuit-switched network used in Example 8.2*



8.2.1 Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. For example, in Figure 8.3,when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time. In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established. Note that **end-to-end addressing** is required for creating a connection between the two end systems. These can be, for example, the addresses of the computers assigned by the administrator in a TDM network, or telephone numbers in an FDM network.

Data-Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

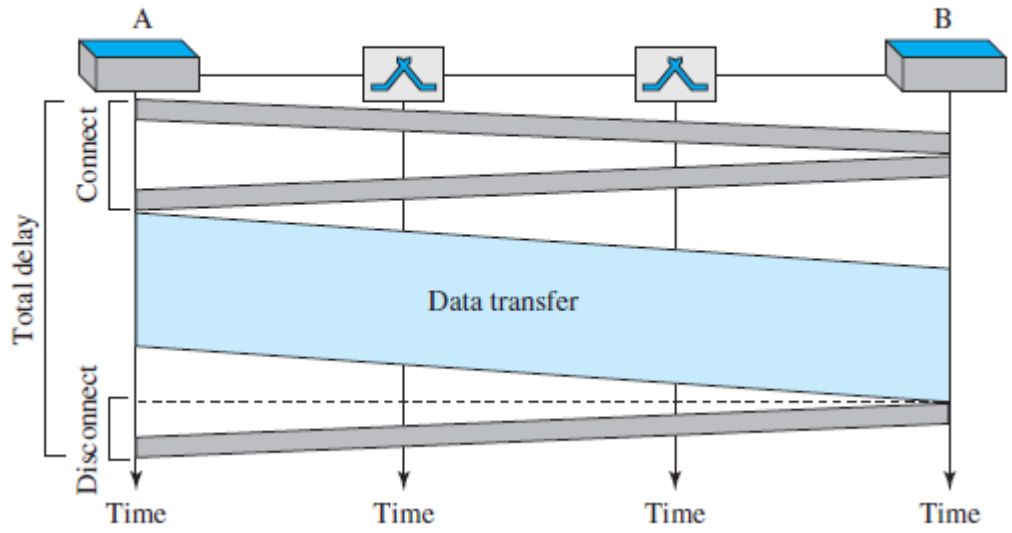
8.2.2 Efficiency

It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation. However, in computer networks, a computer can be connected to another computer even if there is no activity for a long time. In this case, allowing resources to be dedicated means that other connections are deprived.

8.2.3 Delay

Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection. Figure 8.6 shows the idea of delay in a circuit-switched network when only two switches are involved.

Figure 8.6 *Delay in a circuit-switched network*



The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit. The delay caused by the setup is the sum of four parts: the propagation time of the source computer request (slope of the first gray box), the request signal transfer time (height of the first gray box), the propagation time of the acknowledgment from the destination computer (slope of the second gray box), and the signal transfer time of the acknowledgment(height of the second gray box). The delay due to data transfer is the sum of two parts: the propagation time (slope of the colored box) and data transfer time (height of the colored box), which can be very long. The third box shows the time needed to tear down the circuit. We have shown the case in which the receiver requests disconnection, which creates the maximum delay.

8.3 PACKET SWITCHING

In data communications, we need to send messages from one end system to another. If the message is going to pass through a **packet-switched network**, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol.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. The allocation is done on a first come, first-served basis. When a switch receives a packet, no matter what the source or destination is, the packet must wait if there are other packets being processed.

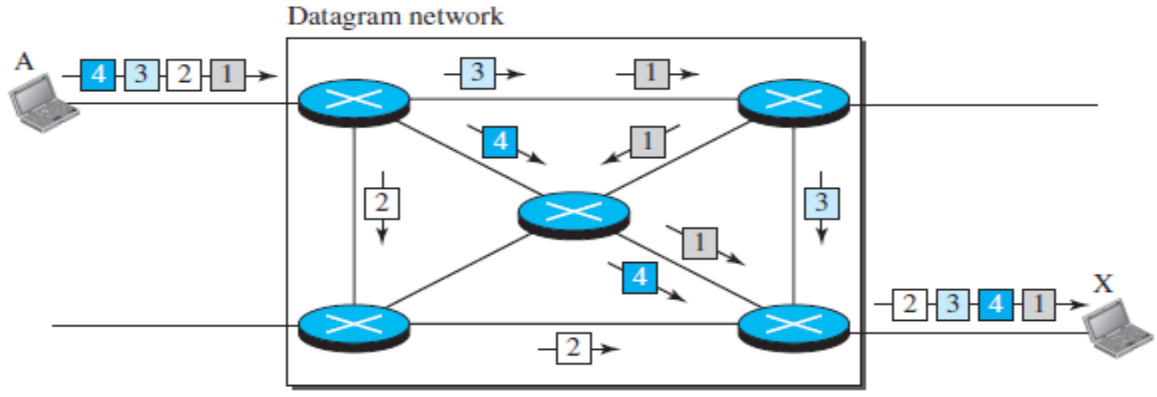
We can have two types of packet-switched networks: datagram networks and virtual circuit networks.

8.3.1 Datagram Networks

In a **datagram network**, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as ***datagrams***. Datagram switching is normally done at the network layer.

Figure 8.7 shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers. That is why we use a different symbol for the switches in the figure.

Figure 8.7 *A datagram network with four switches (routers)*



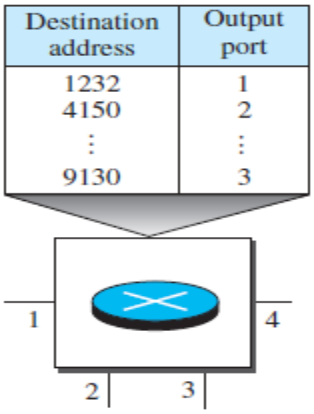
In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.The datagram networks are sometimes referred to as *connectionless networks*. The

term *connectionless* here means that the switch does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

Routing Table

If there are no setup or teardown phases, how are the packets routed to their destinations in a datagram network? In this type of network, each switch has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. Figure 8.8 shows the routing table for a switch.

Figure 8.8 *Routing table in a datagram network*



Destination Address

Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet,this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded. This address, unlike the address in a virtual-circuit network, remains the same during the entire journey of the packet.

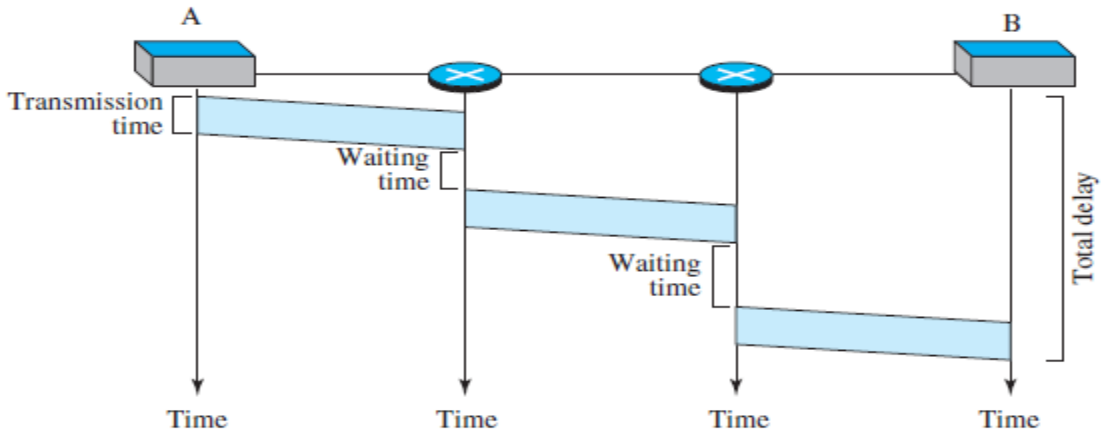
Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

Delay

There may be greater delay in a datagram network than in a virtual-circuit network.Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message. Figure 8.9 gives an example of delay in a datagram network for one packet.

Figure 8.9 *Delay in a datagram network*



The packet travels through two switches. There are three transmission times (3*T*), three propagation delays (slopes 3 | of the lines), and two waiting times ($w1 + w2$). We ignore the processing time in each switch. The total delay is

$$\text{Total delay} = 3T + 3\tau + w_1 + w_2$$

8.3.2 Virtual-Circuit Networks

A **virtual-circuit network** is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

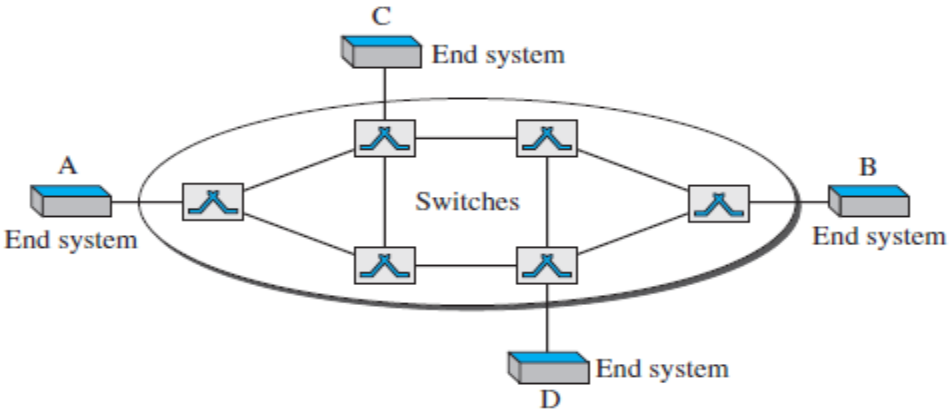
3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what the next switch should be and the channel on which the packet is being carried), not end-to-end jurisdiction.

4. As in a circuit-switched network, all packets follow the same path established during the connection.

5. A virtual-circuit network is normally implemented in the data-link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future.

Figure 8.10 is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

Figure 8.10 *Virtual-circuit network*



Addressing

In a virtual-circuit network, two types of addressing are involved: global and local(virtual-circuit identifier).

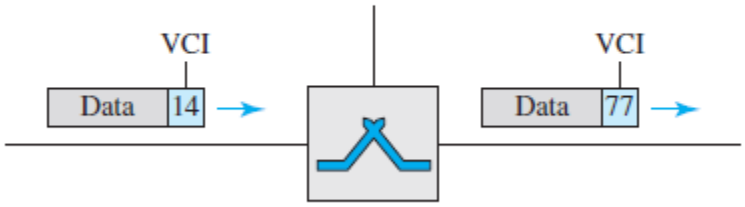
Global Addressing

A source or a destination needs to have a global address—an address that can be unique in the scope of the network or internationally if the network is part of an international network.

Virtual-Circuit Identifier

The identifier that is actually used for data transfer is called the ***virtual-circuit identifier*(VCI)** or the ***label*.** A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI. Figure 8.11 shows how the VCI in a data frame changes from one switch to another. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCIs.

Figure 8.11 *Virtual-circuit identifier*



Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown. In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection. In

the teardown phase, the source and destination inform the switches to delete the corresponding entry. Data transfer occurs between these two phases.

.

Data-Transfer Phase

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up.

Figure 8.12 shows such a switch and its corresponding table.

Figure 8.12 *Switch and tables in a virtual-circuit network*

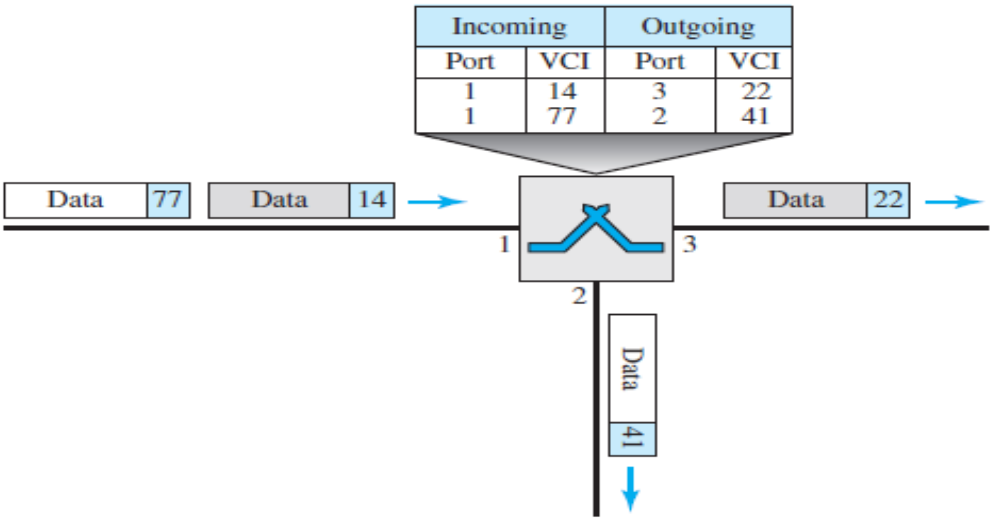
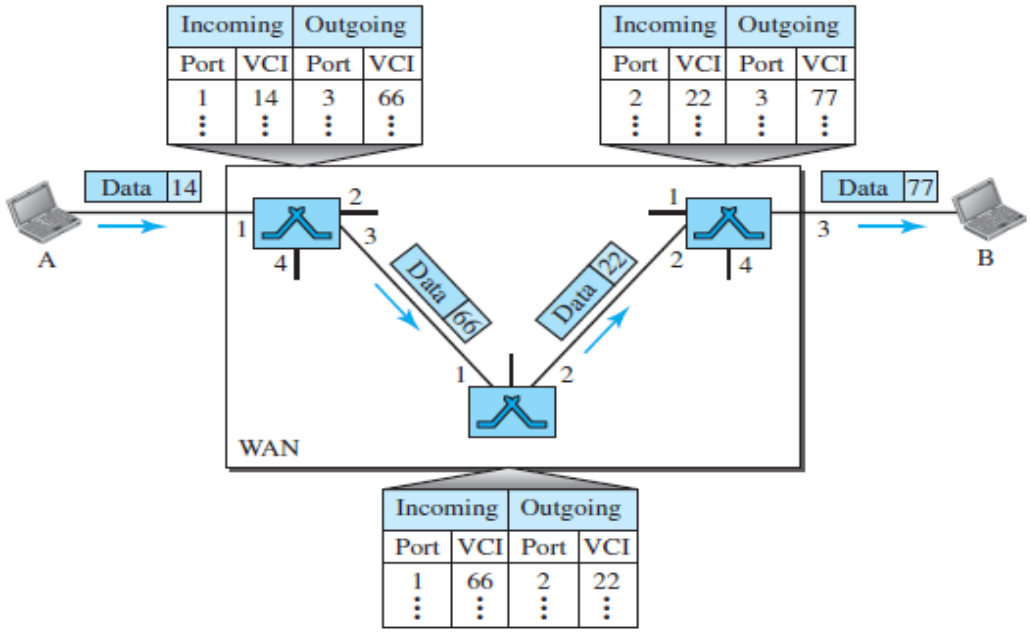


Figure 8.12 shows a frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3.

Figure 8.13 shows how a frame from source A reaches destination B and how its VCI changes during the trip. Each switch changes the VCI and routes the frame. The data-transfer phase is active until the source sends all its frames to the destination. The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.

Figure 8.13 *Source-to-destination data transfer in a virtual-circuit network*



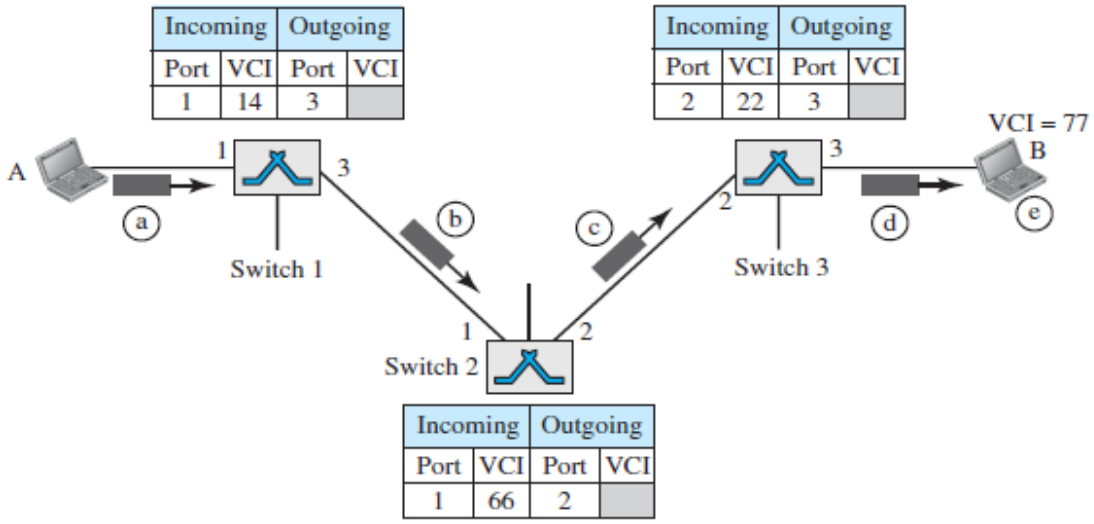
Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment.

Setup Request

A setup request frame is sent from the source to the destination. Figure 8.14 shows the process.

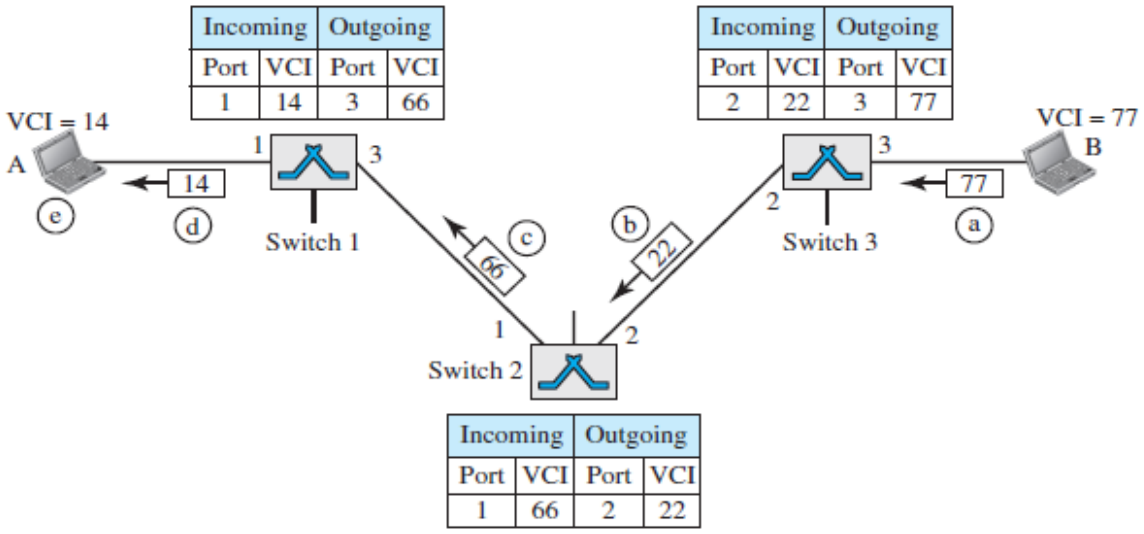
Figure 8.14 *Setup request in a virtual-circuit network*



a. Source A sends a setup frame to switch 1.
b. Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port 3. The switch, in the setup phase, acts as a packet switch; it has a routing table which is different from the switching table. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.
c. Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are completed: in this case, incoming port (1),incoming VCI (66), and outgoing port (2).
d. Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).
e. Destination B receives the setup frame, and if it is ready to receive frames from A,it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not other sources.

Acknowledgment
A special frame, called the *acknowledgment frame*, completes the entries in the switching tables. Figure 8.15 shows the process.

Figure 8.15 *Setup acknowledgment in a virtual-circuit network*



a. The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.
b. Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.

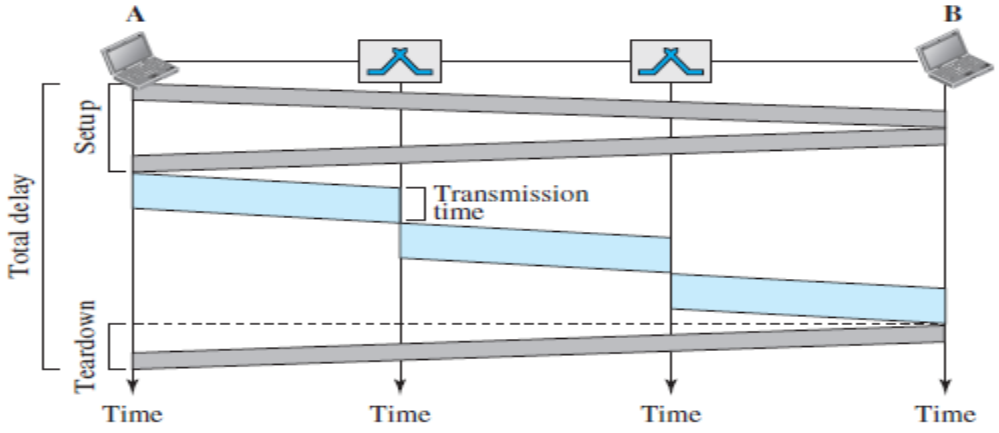
c. Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.
d. Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.
e. The source uses this as the outgoing VCI for the data frames to be sent to destination B

Teardown Phase
In this phase, source A, after sending all frames to B, sends a special frame called a *teardown request*. Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Efficiency
Resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data-transfer phase. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays. There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it.

Delay in Virtual-Circuit Networks
In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Figure 8.16 shows the delay for a packet traveling through two switches in a virtual-circuit network.

Figure 8.16 *Delay in a virtual-circuit network*



The packet is traveling through two switches (routers). There are three transmission times ($3T$), three propagation times (3τ), data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction).The total delay time is

$$\text{Total delay} = 3T + 3\tau + \text{setup delay} + \text{teardown delay}$$

Circuit Switching	Datagram Packet Switching	Virtual circuit Packet switching
Dedicate transmission path	No dedicate path	No dedicate path
Continuous transmission of data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Message are not stored	Packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Packet transmission delay	Call setup delay; Packet transmission delay
Busy signal if called party busy	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases packet delay	Overload may block call setup; increases packet delay
Electromechanical or computerized switching nodes	Small switching nodes	Small switching nodes
User responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each packet	Overhead bits in each packet

MODULE 2: DIGITAL TRANSMISSION

1.Explain the PCM encoder with neat diagram. (8*)
2.What do you mean by Sampling? Explain three sampling methods with a neat diagram. (4)
3.Explain non-uniform quantization and how to recover original signal using PCM decoder. (4)
4.Explain different types of transmission modes. (8*)
5.What is sampling and quantization? Explain briefly. (6)

ANALOG TRANSMISSION

1.Define digital to analog conversion? List different types of digital to analog conversion. (2)

2.Describe ASK, FSK and PSK mechanisms and apply them over the digital data 101101. (4)

3.Discuss the bandwidth requirement for ASK, FSK and PSK. (4*)
4.Explain different aspects of digital-to-analog conversion? (6*)
5.Define ASK. Explain BASK. (6*)

6.Define FSK. Explain BFSK. (6*)

7.Define PSK. Explain BPSK. (6*)
8.Explain QPSK (QPSK). (6)

9.Explain the concept of constellation diagram. (6)

10.Explain QAM. (6)

BANDWIDTH UTILIZATION -- MULTIPLEXING AND SPREADING

1.Explain the concepts of multiplexing and list the categories of multiplexing? (4)

2.Define FDM? Explain the FDM multiplexing and demultiplexing process with neat diagrams. (6*)

3.Define and explain the concept of WDM. (6*)

4.Explain in detail synchronous TDM. (6*)
5.What do you mean by interleaving? Explain (4)
6.Explain Data Rate Management in Multi-level Multiplexing. (4*)

7.Explain the concept of empty-slots and frame-synchronizing in Multi-level Multiplexing. (6)

8.Explain in detail Statistical TDM. (6*)
9.Define FHSS and explain how it achieves bandwidth multiplexing. (8*)
10.Define DSSS and explain how it achieves bandwidth multiplexing. (8*)

11.Explain the analog hierarchy used by the telephone companies. (6)

SWITCHING

1.Explain in detail circuit-switched-network. (6*)

2.Explain switching with reference to TCP/IP Layers. (4)
3.Explain in detail datagram networks (8*)

4.What is Virtual-circuit Network? List five characteristics of VCN. (6*)

5.With relevant diagrams, explain the data transfer phase in a virtual circuit network. (8*)
6.Explain in detail setup Phase in VCN. (6)

7.Explain in detail acknowledgment Phase in VCN. (6)

8.Compare circuit-switched-network, Datagram & Virtual-circuit. (5*)

MODULE 3: TABLE OF CONTENTS

Flow and Error Control

Flow-control

Buffers

Error-control

Combination of Flow and Error Control

Connectionless and Connection-Oriented

DATA-LINK LAYER PROTOCOLS

Simple Protocol

Design

FSMs

Stop-and-Wait Protocol

Design

FSMs

Sequence and Acknowledgment Numbers

Piggybacking

High-level Data Link Control (HDLC)

Configurations and Transfer Modes

Framing

Frame Format

Control Fields of HDLC Frames

POINT-TO-POINT PROTOCOL (PPP)

Framing

Byte Stuffing

Transition Phases

Chapter 10

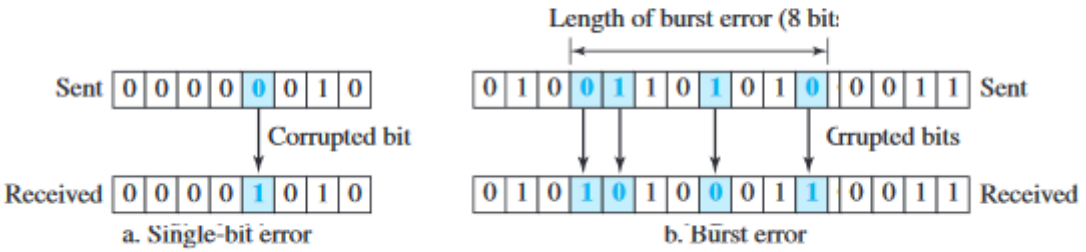
Error Detection and Correction

INTRODUCTION

Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. In a single-bit error, a 0 is changed to a 1 or a 1 to a 0. In a burst error, multiple bits are changed. For example, a 11100 s burst of impulse noise on a transmission with a data rate of 1200 bps might change all or some of the12 bits of information.

Figure 10.1 *Single-bit and burst error*



The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1. The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Redundancy

The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.

Detection Versus Correction

The correction of errors is more difficult than the detection. In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of errors. A single-bit error is the same for us as a burst error.

In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message. The number of the errors and the size of the message are important factors. If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in a data unit of the same size, we need to consider 28 possibilities. You can imagine the receiver's difficulty in finding 10 errors in a data unit of 1000 bits.

Forward Error Correction Versus Retransmission

There are two main methods of error correction. Forward error correction is the process in which the receiver tries to guess the message by using redundant bits. This is possible, as we see later, if the number of errors is small. Correction by retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free.

Coding

Redundancy is achieved through various coding schemes. The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits. The receiver checks the relationships between the two sets of bits to detect or correct the errors. The ratio of redundant bits to the data bits and the robustness of the process are important factors in any coding scheme. Figure 10.3 shows the general idea of coding.

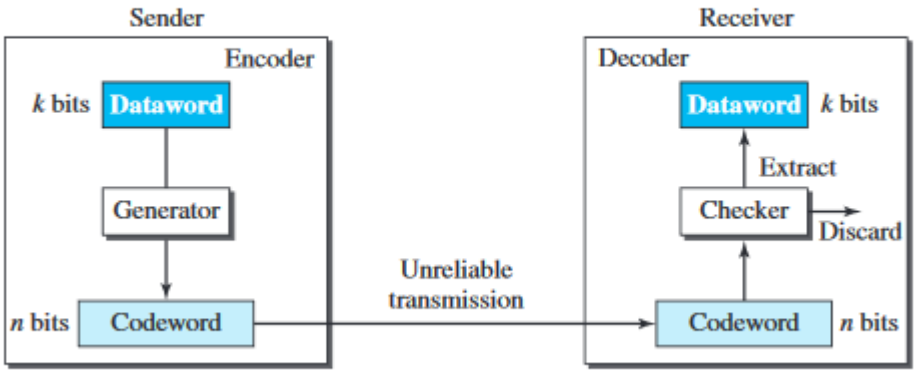
We can divide coding schemes into two broad.

Categories: block coding and convolution coding.

BLOCK CODING

Figure 10.2 shows the role of block coding in error detection. The sender creates code word out of data words by using a generator that applies the rules and procedures of encoding. Each codeword sent to the receiver may change during transmission. If the received codeword is the same as one of the valid code words, the
word is accepted; the corresponding data word is extracted for use. If the received code-word is not valid, it is discarded. However, if the codeword is corrupted during trans-mission but the received word still matches a valid codeword, the error remains undetected.

Figure 10.2 *Process of error detection in block coding*



In block coding, we divide our message into blocks, each of *k* bits, called data words. We add *r* redundant bits to each block to make the length $n = k + r$. The resulting *n-bit* blocks are called code words. How the extra *r* bits is chosen or calculated is something we will discuss later. For the moment, it is important to know that we have a set of data words, each of size *k,*

and a set of code words, each of size of *n*. With *k* bits, we can create a combination of *2k* data words; with *n* bits, we can create a combination of *2n* code words. Since *n > k*, the number of possible code words is larger than the number of possible data words.

The block coding process is one-to-one; the same data word is always encoded as the same codeword. This means that we have *2n - 2k* code words that are not used. We call these code words invalid or illegal.

Example

Let us assume that k=2 and n=3. Table 10.1 shows the list of data words and code words. Later, we will see how to derive a codeword from a data word.

Table 10.1 *A code for error detection in Example 10.1*

Dataword	*Codeword*	*Dataword*	*Codeword*
00	000	10	101
01	011	11	110

Assume the sender encodes the data word 01 as 011 and sends it to the receiver. Consider the following cases:

1. The receiver receives 011. It is a valid codeword. The receiver extracts the dataword 01 from it.
2. The codeword is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is discarded.
3. The codeword is corrupted during transmission, and 000 is received (the right two bits are corrupted). This is a valid codeword. The receiver incorrectly extracts the data word 00. Two corrupted bits have made the error undetectable.

Hamming Distance

One of the central concepts in coding for error control is the idea of the Hamming distance. The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. We show the Hamming distance between two words *x* and *y* as *d(x, y)*. The Hamming distance can easily be found if we apply the XOR operation on the two words and count the number of Is in the result. Note that the Hamming distance is a value greater than zero.

Minimum Hamming Distance

Although the concept of the Hamming distance is the central point in dealing with error detection and correction codes, the measurement that is used for designing a code is the minimum Hamming distance. In a set of words, the minimum Hamming distance is the smallest Hamming distance between all possible pairs. We use dmin to define the minimum Hamming distance in a coding scheme. To find this value, we find the Hamming distances between all words and select the smallest one.

Before we continue with our discussion, we need to mention that any coding scheme needs to have at least three parameters: the codeword size *n*, the data word size *k*, and the minimum Hamming distance *dmin*. A coding scheme C is written as *C(n, k)* with a separate expression

for *dmin*- For example, we can call our first coding scheme *C(3, 2)* with dmin =2 and our second coding scheme *C(5,* 2) with dmin ::= 3.

Hamming Distance and Error

Before we explore the criteria for error detection or correction, let us discuss the relationship between the Hamming distance and errors occurring during transmission. When a codeword is corrupted during transmission, the Hamming distance between the sent and received code words is the number of bits affected by the error. In other words, the Hamming distance between the received codeword and the sent codeword is the number of bits that are corrupted during transmission. For example, if the codeword 00000 is sent and 01101 is received, 3 bits are in error and the Hamming distance between the two is *d(OOOOO,* 01101) =3.

Minimum Distance for Error Detection

Now let us find the minimum Hamming distance in a code if we want to be able to detect up to s errors. If s errors occur during transmission, the Hamming distance between the sent codeword and received codeword is s. If our code is to detect up to s errors, the minimum distance between the valid codes must be s + 1, so that the received codeword does not match a valid codeword. In other words, if the minimum distance between all valid codewords is s + 1, the received codeword cannot be erroneously mistaken for another codeword. The distances are not enough (s + 1) for the receiver to accept it as valid. The error will be detected. We need to clarify a point here: Although a code with *dmin* =s + 1

Minimum Distance for Error Correction

Error correction is more complex than error detection; a decision is involved. When a received codeword is not a valid codeword, the receiver needs to decide which valid codeword was actually sent. The decision is based on the concept of territory, an exclusive area surrounding the codeword. Each valid codeword has its own territory. We use a geometric approach to define each territory. We assume that each valid codeword has a circular territory with a radius of *t* and that the valid codeword is at the center. For example, suppose a codeword *x* is corrupted by *t* bits or less. Then this corrupted codeword is located either inside or on the perimeter of this circle. If the receiver receives a codeword that belongs to this territory, it decides that the original codeword is the one at the center. Note that we assume that only up to *t* errors have occurred; otherwise, the decision is wrong. Figure 10.9 shows this geometric interpretation. Some texts use a sphere to show the distance between all valid block codes.

LINEAR BLOCK CODES

Almost all block codes used today belong to a subset called linear block codes. The use of nonlinear block codes for error detection and correction is not as widespread because their

structure makes theoretical analysis and implementation difficult. We therefore concentrate on linear block codes. The formal definition of linear block codes requires the knowledge of abstract algebra (particularly Galois fields), which is beyond the scope of this book. We therefore give an informal definition. For our purposes, a linear block code is a code in which the exclusive OR (addition modulo-2) of two valid codewords creates another valid codeword.

Minimum Distance for Linear Block Codes

It is simple to find the minimum Hamming distance for a linear block code. The minimum Hamming distance is the number of Is in the nonzero valid codeword with the smallest number of 1s.

Some Linear Block Codes

Let us now show some linear block codes. These codes are trivial because we can easily find the encoding and decoding algorithms and check their performances.

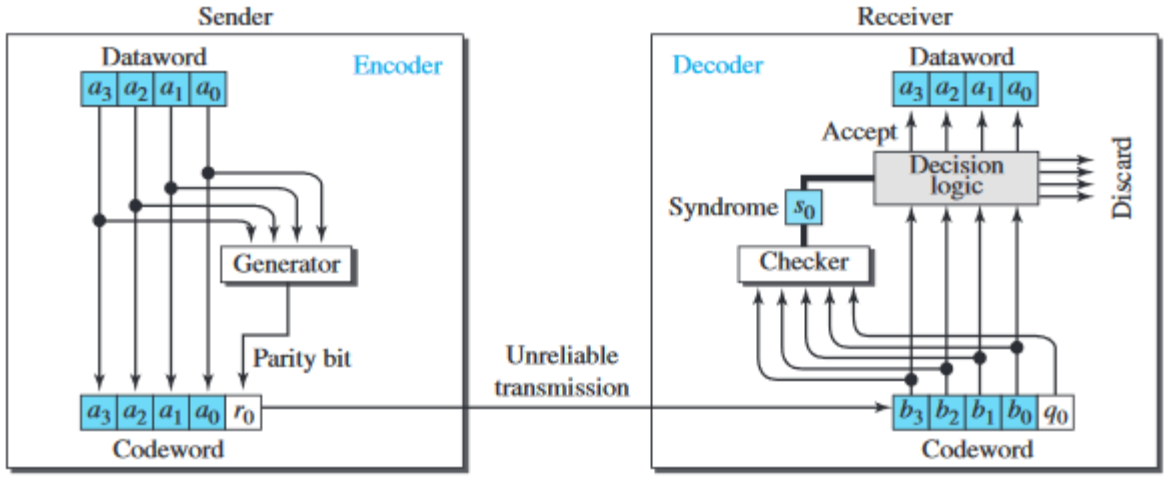
Simple Parity-Check Code

Perhaps the most familiar error-detecting code is the simple parity-check code. In this code, a *k-bit* data word is changed to an n-bit codeword where $n = k + 1$. The extra bit, called the parity bit, is selected to make the total number of Is in the codeword even. Although some implementations specify an odd number of Is, we discuss the even case. The minimum Hamming distance for this category is dmin =2, which means that the code is a single-bit error-detecting code; it cannot correct any error.

Table 10.2 *Simple parity-check code C(5, 4)*

Dataword	Codeword	Dataword	Codeword
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
0101	01010	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110

Figure 10.4 *Encoder and decoder for simple parity-check code*



This is normally done by adding the 4 bits of the dataword (modulo-2); the result is the parity bit. In other words,

$$r_0 = a_3 + a_2 + a_1 + a_0 \quad \text{(modulo-2)}$$

If the number of 1s is even, the result is 0; if the number of 1s is odd, the result is 1. In both cases, the total number of 1s in the codeword is even. The sender sends the codeword which may be corrupted during transmission. The receiver receives a 5-bit word. The checker at the receiver does the same thing as the generator in the sender with one exception: The addition is done over all 5 bits. The result, which is called the syndrome, is just 1 bit. The syndrome is 0 when the number of 1s in the received codeword is even; otherwise, it is 1.

$$s_0 = b_3 + b_2 + b_1 + b_0 + q_0 \quad \text{(modulo-2)}$$

The syndrome is passed to the decision logic analyzer. If the syndrome is 0, there is no error in the received codeword; the data portion of the received codeword is accepted as the data word; if the syndrome is 1, the data portion of the received codeword is discarded. The data word is not created.

Example

Let us look at some transmission scenarios. Assume the sender sends the data word 1011. The codeword created from this dataword is 10111, which is sent to the receiver. We examine five cases:

1. No error occurs; the received codeword is 10111. The syndrome is 0. The data word 1011 is created.

2. One single-bit error changes a1, the received codeword is 10011. The syndrome is 1. No data word is created.

3. One single-bit error changes r0, the received codeword is 10110. The syndrome is 1. No data word is created. Note that although none of the data word bits are corrupted, no data word is created because the code is not sophisticated enough to show the position of the corrupted bit.

4. An error changes *ro* and a second error changes *a3*,the received codeword is 00110. The syndrome is 0. The data word 0011 is created at the receiver. Note that here the data word is wrongly created due to the syndrome value. The simple parity-check decoder cannot detect an even number of errors. The errors cancel each other out and give the syndrome a value of 0.

5. Three bits-a3, a2, and a1- are changed by errors. The received codeword is 01011. The syndrome is 1. The data word is not created. This shows that the simple parity check, guaranteed to detect one single error, can also find any odd number of errors.

A parity-check code can detect an odd number of errors.

CYCLIC CODES

Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword. For example, if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword.

In this case, if we call the bits in the first word *ao* to *a6'* and the bits in the second word *B0* to *b6,* we can shift the bits by using the following:

$$b_1 = a_0 \quad b_2 = a_1 \quad b_3 = a_2 \quad b_4 = a_3 \quad b_5 = a_4 \quad b_6 = a_5 \quad b_0 = a_6$$

In the rightmost equation, the last bit of the first word is wrapped around and becomes the first bit of the second word.

Cyclic Redundancy Check

We can create cyclic codes to correct errors. However, the theoretical background required is beyond the scope of this book. In this section, we simply discuss a category of cyclic codes called the cyclic redundancy check (CRC) that is used in networks such as LANs and WANs.

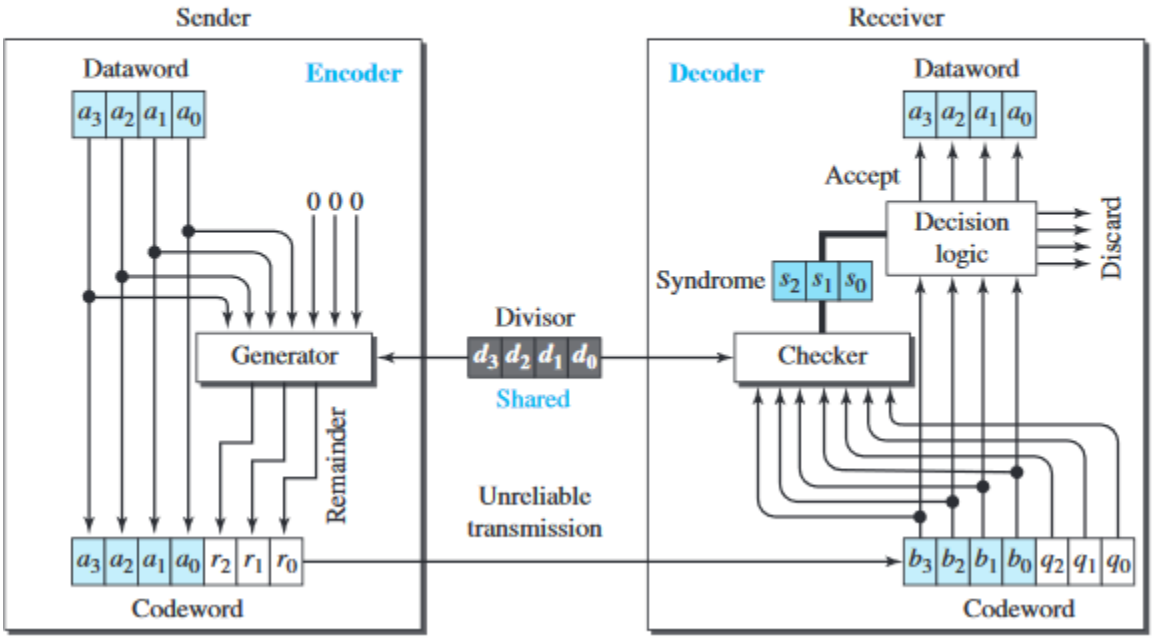
Table shows an example of a CRC code.

Table 10.3 *A CRC code with C(7, 4)*

Dataword	*Codeword*	*Dataword*	*Codeword*
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

Figure 10.5 shows one possible design for the encoder and decoder.

Figure 10.5 *CRC encoder and decoder*

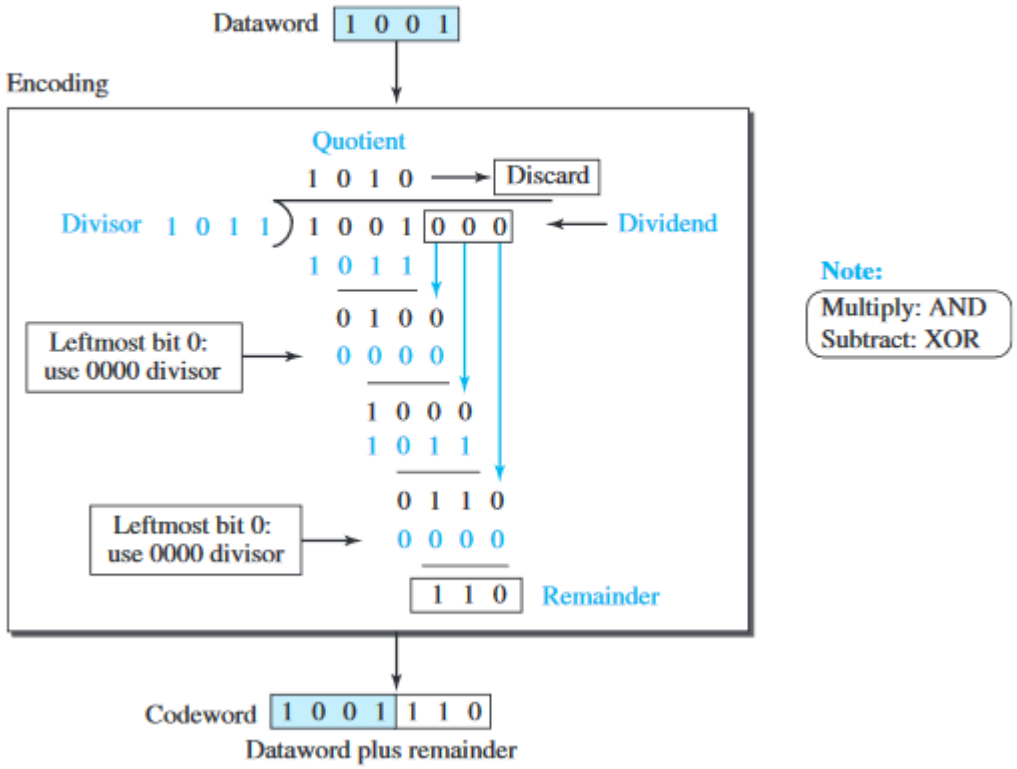


In the encoder, the data word has *k* bits (4 here); the codeword has *n* bits. The size of the data word is augmented by adding *n* - *k* (3 here) Os to the right-hand side of the word. The n-bit result is fed into the generator. The generator uses a divisor of size *n* - *k* + I (4 here), predefined and agreed upon. The generator divides the augmented data word by the divisor (modulo-2 division). The quotient of the division is discarded; the remainder *(r2 r1 r0)* is appended to the data word to create the codeword. The decoder receives the possibly corrupted codeword. A copy of all *n* bits is fed to the checker which is a replica of the generator. The remainder produced by the checker is a syndrome of *n* - *k* (3 here) bits, which is fed to the decision logic analyzer. The analyzer has a simple function. If the syndrome bits are all as, the 4 leftmost bits of the codeword are accepted as the data word (interpreted as no error); otherwise, the 4 bits are discarded (error).

Encoder

Let us take a closer look at the encoder. The encoder takes the data word and augments it with *n* - *k* number of as. It then divides the augmented data word by the divisor, as shown in Figure.

Figure 10.6 *Division in CRC encoder*



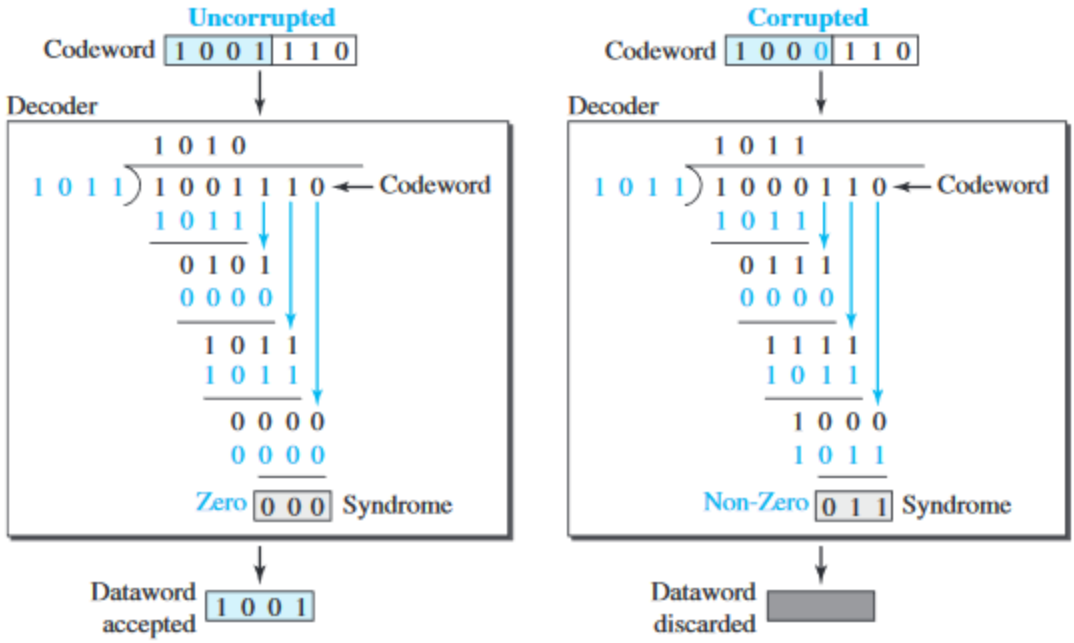
The process of modulo-2 binary division is the same as the familiar division process we use for decimal numbers. However, as mentioned at the beginning of the chapter, in this case addition and subtraction are the same. We use the XOR operation to do both. As in decimal division, the process is done step by step. In each step, a copy of the divisor is XORed with the 4 bits of the dividend. The result of the XOR operation (remainder) is 3 bits (in this case), which is used for the next step after 1 extra bit is pulled down to make it 4 bits long. There is one important point we need to remember in this type of division. If the leftmost bit of the dividend (or the part used in each step) is 0, the step cannot use the regular divisor; we need to use an all-0s divisor. When there are no bits left to pull down, we have a result. The 3-bit remainder forms the check bits *(r2 r1* and *r0).* They are appended to the data word to create the codeword.

Decoder

The codeword can change during transmission. The decoder does the same division process as the encoder. The remainder of the division is the syndrome. If the syndrome is all 0s, there is no error; the data word is separated from the received codeword and accepted. Otherwise, everything is discarded. Figure 10.16 shows two cases: The left hand figure shows the value

of syndrome when no error has occurred; the syndrome is 000. The right-hand part of the figure shows the case in which there is one single error. The syndrome is not all 0s (it is 011).

Figure 10.7 *Division in the CRC decoder for two cases*



Polynomials

A better way to understand cyclic codes and how they can be analyzed is to represent them as polynomials. Again, this section is optional. A pattern of Os and 1s can be represented as a **polynomial** with coefficients of 0 and 1. The power of each term shows the position of the bit; the coefficient shows the value of the bit. Figure shows a binary pattern and its polynomial representation. In Figure 10.21a we show how to translate a binary pattern to a polynomial; in Figure we show how the polynomial can be shortened by removing all terms with zero coefficients and replacing x^1 by x and x^0 by 1.

Figure 10.8 *A polynomial to represent a binary word*

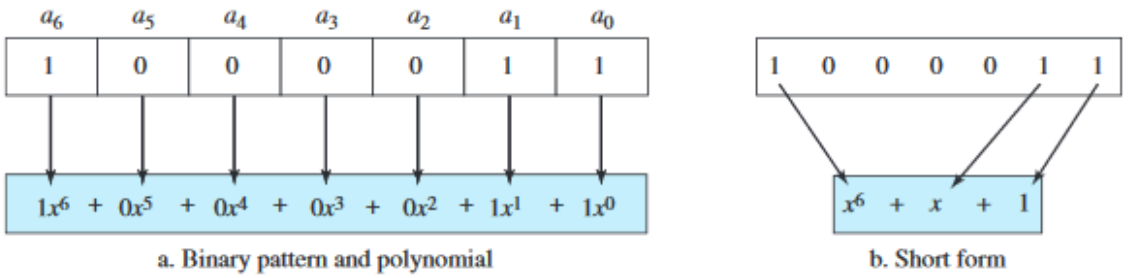


Figure shows one immediate benefit; a 7-bit pattern can be replaced by three terms. The benefit is even more conspicuous when we have a polynomial such as *x23 + X3 + 1*. Here the bit pattern is 24 bits in length (three Is and twenty-one Os) while the polynomial is just three terms.

Degree of a Polynomial

The degree of a polynomial is the highest power in the polynomial. For example, the degree of the polynomial *x6 + x + 1* is 6. Note that the degree of a polynomial is 1 less that the number of bits in the pattern. The bit pattern in this case has 7 bits.

Adding and Subtracting Polynomials

Adding and subtracting polynomials in mathematics are done by adding or subtracting the coefficients of terms with the same power. In our case, the coefficients are only 0 and 1, and adding is in modulo-2. This has two consequences. First, addition and subtraction are the same. Second, adding or subtracting is done by combining terms and deleting pairs of identical terms. For example, adding $x^5 + x^4 + x^2$ and $x^6 + x^4 + x^2$ gives just $x^6 + x^5$. The terms x^4 and x^2 are deleted. However, note that if we add, for example, three polynomials and we get x^2 three times, we delete a pair of them and keep the third.

Multiplying or Dividing Terms

In this arithmetic, multiplying a term by another term is very simple; we just add the powers. For example, $x^3 * x^4$ is x^7, For dividing, we just subtract the power of the second term from the power of the first. For example, x^5 / x^2 is x^3.

Multiplying Two Polynomials

Multiplying a polynomial by another is done term by term. Each term of the first polynomial must be multiplied by all terms of the second. The result, of course, is then simplified, and pairs of equal terms are deleted. The following is an example:

$$(x^5 + x^3 + x^2 + x)(x^2 + x + 1)$$
$$= x^7 + x^6 + x^5 + x^5 + x^4 + x^3 + x^4 + x^3 + x^2 + x^3 + x^2 + x$$
$$= x^7 + x^6 + x^3 + x$$

Dividing One Polynomial by Another

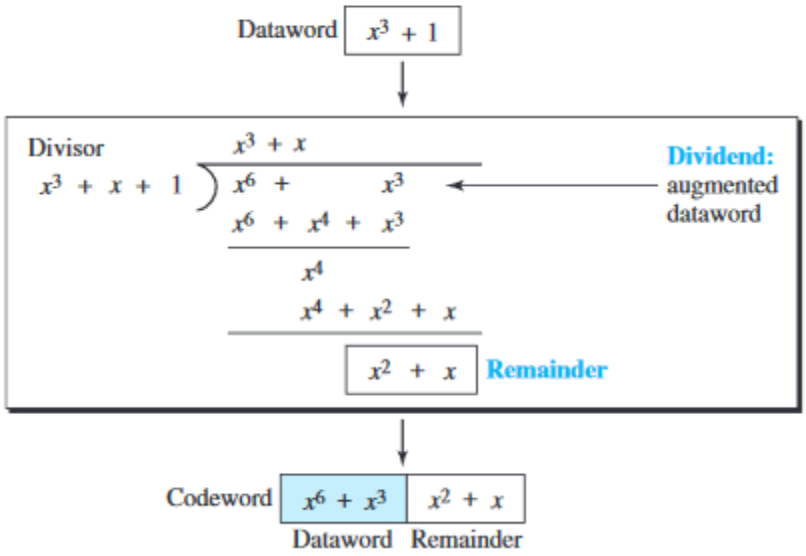
Division of polynomials is conceptually the same as the binary division we discussed for an encoder. We divide the first term of the dividend by the first term of the divisor to get the first term of the quotient. We multiply the term in the quotient by the divisor and subtract the result from the dividend. We repeat the process until the dividend degree is less than the divisor degree. We will show an example of division later in this chapter.

Cyclic Code Encoder Using Polynomials

Now that we have discussed operations on polynomials, we show the creation of a codeword from a data word. Figure 10.22 is the polynomial version of Figure 10.15. We can see that the process is shorter. The data word 1001 is represented as *x3 + 1*. The divisor 1011 is represented as $x^3 + x + 1$. To find the augmented data word, we have left-shifted the data word 3 bits (multiplying by *x*\ The result is $x^6 + x^3$. Division is straightforward. We divide the first term of the dividend, *x6*, by the first term of the divisor, x^3. The first term of the quotient

is then x^6/x^3, or x^3. Then we multiply x^3 by the divisor and subtract (according to our previous definition of subtraction) the result from the dividend. The result is x^4, with a degree greater than the divisor's degree; we continue to divide until the degree of the remainder is less than the degree of the divisor.

Figure 10.9 *CRC division using polynomials*



It can be seen that the polynomial representation can easily simplify the operation of division in this case, because the two steps involving all-Os divisors are not needed here. (Of course, one could argue that the all-Os divisor step can also be eliminated in binary division.) In a polynomial representation, the divisor is normally referred to as the generator polynomial *t(x)*.

Cyclic Code Analysis

We can analyze a cyclic code to find its capabilities by using polynomials. We define the following, *where f(x)* is a polynomial with binary coefficients.

Dataword:
d(x)
Syndrome:
s(x)
Codeword:
c(x)

Error: *e(x)*

Generator: *g(x)*

If *s(x)* is not zero, then one or more bits is corrupted. However, if *s(x)* is zero, either no bit is corrupted or the decoder failed to detect any errors.

In a cyclic code,

1. If $s(x) \neq 0$, one or more bits is corrupted.
2. If $s(x) = 0$, either
   a. No bit is corrupted, or
   b. Some bits are corrupted, but the decoder failed to detect them.

In our analysis we want to find the criteria that must be imposed on the generator, *g(x)* to detect the type of error we especially want to be detected. Let us first find the relationship among the sent codeword, error, received codeword, and the generator. We can say

Received codeword =c(x) +e(x)

In other words, the received codeword is the sum of the sent codeword and the error. The receiver divides the received codeword by *g(x)* to get the syndrome. We can write this as

$$\frac{\text{Received codeword}}{g(x)} = \frac{c(x)}{g(x)} + \frac{e(x)}{g(x)}$$

The first term at the right-hand side of the equality does not have a remainder (according to the definition of codeword). So the syndrome is actually the remainder of the second term on the right-hand side. If this term does not have a remainder (syndrome =0), either *e(x)* is 0 or *e(x)* is divisible by *g(x).* We do not have to worry about the first case (there is no error); the second case is very important. Those errors that are divisible by *g(x)* are not caught. Let us show some specific errors and see how they can be caught by a well designed *g(x).*

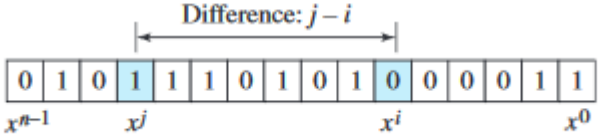
Single-Bit Error

What should be the structure of *g(x)* to guarantee the detection of a single-bit error? A single-bit error is *e(x) =xi,* where *i* is the position of the bit. If a single-bit error is caught, then *xi* is not divisible by *g(x).* (Note that when we say *not divisible,* we mean that there is a remainder.) If *g(x)* ha~ at least two terms (which is normally the case) and the coefficient of *x0* is not zero (the rightmost bit is 1), then *e(x)* cannot be divided by *g(x).*

Two Isolated Single-Bit Errors

Now imagine there are two single-bit isolated errors. Under what conditions can this type of error be caught? We can show this type of error as *e(x) =: xl + xi.* The values of *I* and *j* define the positions of the errors, and the difference *j - i* defines the distance between the two errors, as shown in Figure.

Figure 10.10 *Representation of two isolated single-bit errors using polynomials*



Odd Numbers of Errors

A generator with a factor of $x + 1$ can catch all odd numbers of errors. This means that we need to make $x + 1$ a factor of any generator. Note that we are not saying that the generator itself should be $x + 1$; we are saying that it should have a factor of $x + 1$. If it is only $x + 1$, it cannot catch the two adjacent isolated errors (see the previous section). For example, $x4 + x2 + X + 1$ can catch all odd-numbered errors since it can be written as a product of the two polynomials $x + 1$ and $x3 + x2 + 1$.

Burst Errors

Now let us extend our analysis to the burst error, which is the most important of all. A burst error is of the form $e(x) = eJ + \ldots + xi)$. Note the difference between a burst error and two isolated single-bit errors. The first can have two terms or more; the second can only have two terms. We can factor out xi and write the error as $xi(xJ-i + \ldots + 1)$. If our generator can detect a single error (minimum condition for a generator), then it cannot divide xi. What we should worry about are those generators that divide $xJ-i + \ldots + 1$. In other words, the remainder of $(xJ-i + \ldots + 1)/(xr + \ldots + 1)$ must not be zero. Note that the denominator is the generator polynomial.

We can have three cases:

1. If $j - i < r$, the remainder can never be zero. We can write $j - i = L - 1$, where L is the length of the error. So $L - 1 < r$ or $L < r + 1$ or L :::;: r. This means all burst errors with length smaller than or equal to the number of check bits r will be detected.

2. In some rare cases, if $j - i = r$, or $L = r + 1$, the syndrome is 0 and the error is undetected. It can be proved that in these cases, the probability of undetected burst error of length $r + 1$ is (ll2r-l. For example, if our generator is $x\ l4 + \sim + 1$, in which r =14, aburst error of length L =15 can slip by undetected with the probability of (1/2)14-1 or almost 1 in 10,000.

3. In some rare cases, if $j - i > r$, or $L > r + 1$, the syndrome is 0 and the error is undetected. It can be proved that in these cases, the probability of undetected burst error of length greater than $r + 1$ is (112t For example, if our generator is $x14 + x3 + 1$, in which r =14, a burst error of length greater than 15 can slip by undetected with the probability of (112)14 or almost 1 in 16,000 cases.

Summary

We can summarize the criteria for a good polynomial generator:

A good polynomial generator needs to have the following characteristics:

1. **It should have at least two terms.**
2. **The coefficient of the term x^0 should be 1.**
3. **It should not divide $x^t + 1$, for t between 2 and $n - 1$.**
4. **It should have the factor $x + 1$.**

Standard Polynomials

Some standard polynomials used by popular protocols for Regeneration are shown in Table

Table 10.4 *Standard polynomials*

Name	*Polynomial*	*Used in*
CRC-8	x^8+x^2+x+1 **100000111**	ATM header
CRC-10	$x^{10}+x^9+x^5+x^4+x^2+1$ **11000110101**	ATM AAL
CRC-16	$x^{16}+x^{12}+x^5+1$ **10001000000100001**	HDLC
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$ **10000010011000001000111011011011 1**	LANs

Example 10.8

Which of the following $g(x)$ values guarantees that a single-bit error is caught? For each case, what is the error that cannot be caught?

a. $x+1$
b. x^3
c. 1

Solution

a. No x^i can be divisible by $x+1$. In other words, $x^i/(x+1)$ always has a remainder. So the syndrome is nonzero. Any single-bit error can be caught.
b. If i is equal to or greater than 3, x^i is divisible by $g(x)$. The remainder of x^i/x^3 is zero, and the receiver is fooled into believing that there is no error, although there might be one. Note that in this case, the corrupted bit must be in position 4 or above. All single-bit errors in positions 1 to 3 are caught.
c. All values of i make x^i divisible by $g(x)$. No single-bit error can be caught. In addition, this $g(x)$ is useless because it means the codeword is just the dataword augmented with $n-k$ zeros.

Example 10.9

Find the status of the following generators related to two isolated, single-bit errors.

a. $x+1$
b. x^4+1
c. x^7+x^6+1
d. $x^{15}+x^{14}+1$

Solution

a. This is a very poor choice for a generator. Any two errors next to each other cannot be detected.
b. This generator cannot detect two errors that are four positions apart. The two errors can be anywhere, but if their distance is 4, they remain undetected.
c. This is a good choice for this purpose.
d. This polynomial cannot divide any error of type x^t+1 if t is less than 32,768. This means that a codeword with two isolated errors that are next to each other or up to 32,768 bits apart can be detected by this generator.

Example 10.10

Find the suitability of the following generators in relation to burst errors of different lengths.

a. x^6+1
b. $x^{18}+x^7+x+1$
c. $x^{32}+x^{23}+x^7+1$

Solution

a. This generator can detect all burst errors with a length less than or equal to 6 bits; 3 out of 100 burst errors with length 7 will slip by; 16 out of 1000 burst errors of length 8 or more will slip by.
b. This generator can detect all burst errors with a length less than or equal to 18 bits; 8 out of 1 million burst errors with length 19 will slip by; 4 out of 1 million burst errors of length 20 or more will slip by.
c. This generator can detect all burst errors with a length less than or equal to 32 bits; 5 out of 10 billion burst errors with length 33 will slip by; 3 out of 10 billion burst errors of length 34 or more will slip by.

Advantages of Cyclic Codes

We have seen that cyclic codes have a very good performance in detecting single-bit errors, double errors, an odd number of errors, and burst errors. They can easily be implemented in hardware and software. They are especially fast when implemented in hardware. This has made cyclic codes a good candidate for many networks.

Other Cyclic Codes

The cyclic codes we have discussed in this section are very simple. The check bits and syndromes can be calculated by simple algebra. There are, however, more powerful polynomials that are based on abstract algebra involving Galois fields. These are beyond the scope of this book. One of the most interesting of these codes is the Reed-Solomon code used today for both detection and correction.

CHECKSUM

The last error detection method we discuss here is called the checksum. The checksum is used in the Internet by several protocols although not at the data link layer. However,we briefly discuss it here to complete our discussion on error checking. Like linear and cyclic codes, the checksum is based on the concept of redundancy. Several protocols still use the checksum for error detection although the tendency is to replace it with a CRC. This means that the CRC is also used in layers other than the data link layer.

Idea

The concept of the checksum is not difficult. Let us illustrate it with a few examples. One's Complement The previous example has one major drawback. All of our data can be written as a 4-bit word (they are less than 15) except for the checksum. One solution is to use one's complement arithmetic. In this arithmetic, we can represent unsigned numbers between 0 and *2n* - 1 using only *n* bits. t If the number has more than *n* bits, the extra leftmost bits need to be added to the *n* rightmost bits (wrapping). In one's complement arithmetic, a negative number can be represented by inverting all bits (changing a 0 to a 1 and a 1 to a 0). This is the same as subtracting the number from *2n* - 1.

Internet Checksum

Traditionally, the Internet has been using a 16-bit checksum. The sender calculates the checksum by following these steps.

Sender site:

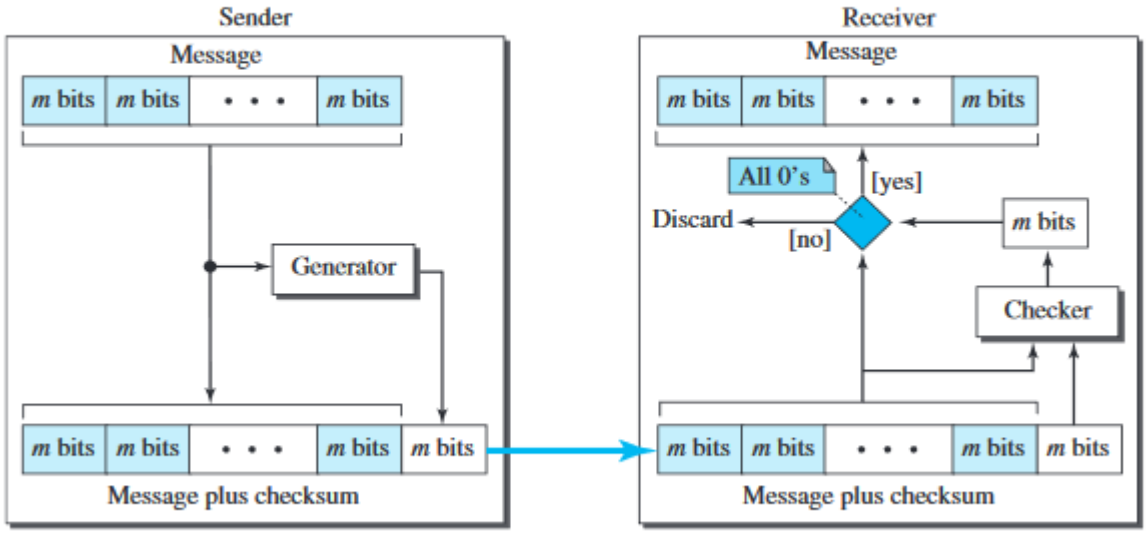
1. The message is divided into 16-bit words.
2. The value of the checksum word is set to O.
3. All words including the checksum are added ushtg one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

Receiver site:

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

At the source, the message is first divided into m-bit units. The generator then creates an extra m-bit unit called the checksum, which is sent with the message. At the destination, the checker creates a new checksum from the combination of the message and sent checksum. If the new checksum is all 0s, the message is accepted; otherwise, the message is discarded (Figure 10.15). Note that in the real implementation, the checksum unit is not necessarily added at the end of the message; it can be inserted in
the middle of the message.

Figure 10.15 *Checksum*



Concept

The idea of the traditional checksum is simple. We show this using a simple example.
Example 10.11 Suppose the message is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers , we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12, 0, 6, 36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise, there is an error somewhere and the message is not accepted. One's Complement Addition The previous example has one major drawback. Each number can be written as a 4-bit word (each is less than 15) except for the sum. One solution is to use one's complement arithmetic. In this arithmetic, we can represent unsigned numbers between 0 and 2^m-1 using only m bits. If the number has more than m bits, the extra leftmost bits need to be added to the m rightmost bits (wrapping).

In the previous example, the decimal number 36 in binary is (100100)2. To change it to a 4-bit number we add the extra leftmost bit to the right four bits as shown below. Instead of sending 36 as the sum, we can send 6 as the sum (7, 11, 12, 0, 6, 6). The receiver can add the first five numbers in one's complement arithmetic. If the result is 6, the numbers are accepted; otherwise, they are rejected.

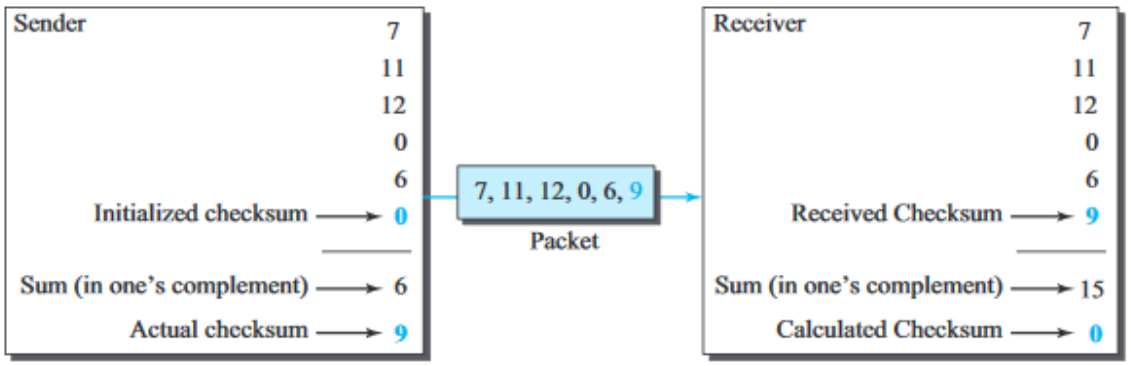
Checksum

We can make the job of the receiver easier if we send the complement of the sum, the checksum. In one's complement arithmetic, the complement of a number is found by completing all bits (changing all 1s to 0s and all 0s to 1s). This is the same as subtracting the number from 2m−1. In one's complement arithmetic, we have two 0s: one positive and one negative, which are complements of each other. The positive zero has all m bits set to 0; the negative zero has all bits set to 1 (it is 2m− 1). If we add a number with its complement, we get a negative zero (a number with all bits set to 1). When the receiver adds all five numbers (including the checksum), it gets a negative zero. The receiver can complement the result again to get a positive zero.

Example

Let us use the idea of the checksum in Example. The sender adds all five numbers in one's complement to get the sum = 6. The sender then complements the result to get the checksum =9, which is 15 −6. Note that 6 =(0110)2 and 9 =(1001)2; they are complements of each other. The sender sends the five data numbers and the checksum (7, 11, 12, 0, 6, 9). If there is no corruption in transmission, the receiver receives (7, 11, 12, 0, 6, 9) and adds them in one's complement to get 15.The sender complements 15 to get 0. This shows that data have not been corrupted. Figure shows the process.

Figure 10.16 *Example 10.13*



Internet Checksum

Traditionally, the Internet has used a 16-bit checksum. The sender and the receiver follow the steps depicted in Table 10.5. The sender or the receiver uses five steps.

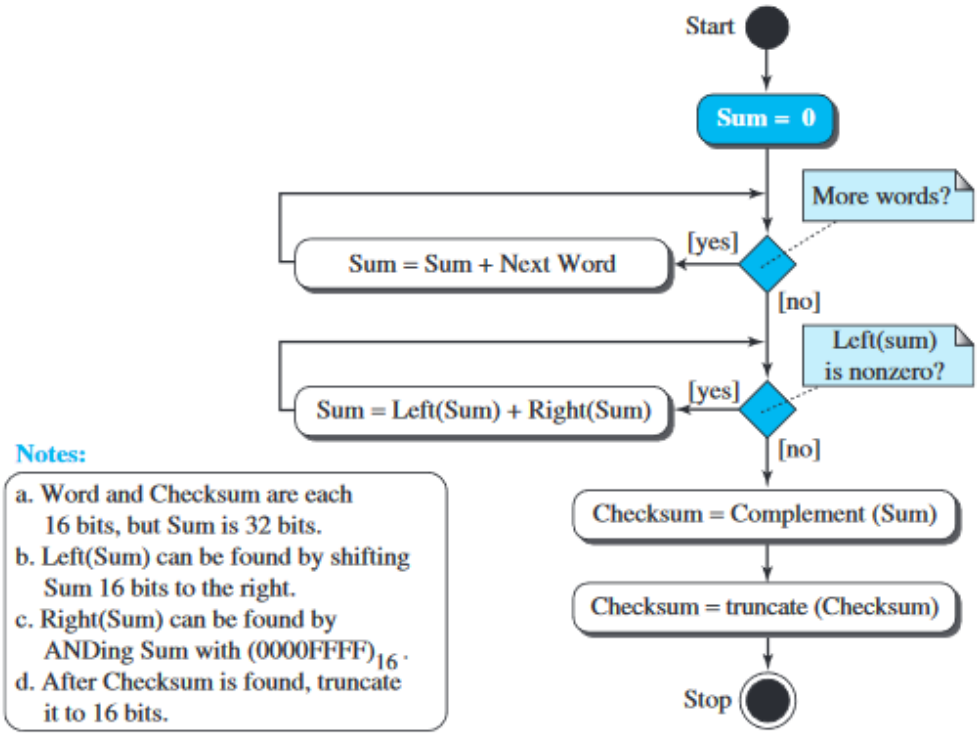
Table 10.5 *Procedure to calculate the traditional checksum*

Sender	*Receiver*
1. The message is divided into 16-bit words.	1. The message and the checksum are received.
2. The value of the checksum word is initially set to zero.	2. The message is divided into 16-bit words.
3. All words including the checksum are added using one's complement addition.	3. All words are added using one's complement addition.
4. The sum is complemented and becomes the checksum.	4. The sum is complemented and becomes the new checksum.
5. The checksum is sent with the data.	5. If the value of the checksum is 0, the message is accepted; otherwise, it is rejected.

Algorithm

We can use the flow diagram of Figure 10.17 to show the algorithm for calculation of the checksum. A program in any language can easily be written based on the algorithm. Note that the first loop just calculates the sum of the data units in two's complement; the second loop wraps the extra bits created from the two's complement calculation to simulate the calculations in one's complement. This is needed because almost all computers today do calculation in two's complement.

Figure 10.17 *Algorithm to calculate a traditional checksum*



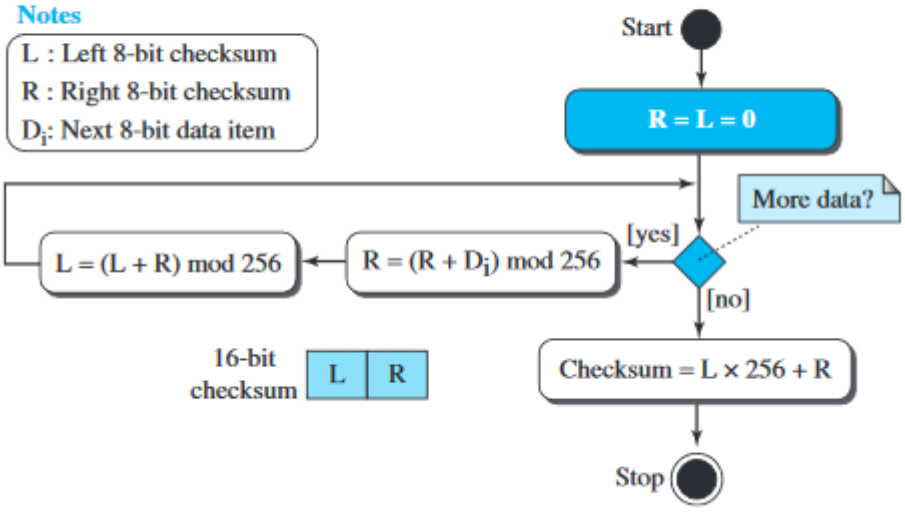
Other Approaches to the Checksum

As mentioned before, there is one major problem with the traditional checksum calculation. If two 16-bit items are transposed in transmission, the checksum cannot catch this error. The reason is that the traditional checksum is not weighted: it treats each data item equally. In other words, the order of data items is immaterial to the calculation. Several approaches have been used to prevent this problem. We mention two of them here: Fletcher and Adler.

Fletcher Checksum

The Fletcher checksum was devised to weight each data item according to its position. Fletcher has proposed two algorithms: 8-bit and 16-bit. The first, 8-bit Fletcher, calculates on 8-bit data items and creates a 16-bit checksum. The second, 16-bit Fletcher, calculates on 16-bit data items and creates a 32-bit checksum. The 8-bit Fletcher is calculated over data octets (bytes) and creates a 16-bit check-sum. The calculation is done modulo 256 (2^8), which means the intermediate results are divided by 256 and the remainder is kept. The algorithm uses two accumulators, L and R. The first simply adds data items together; the second adds a weight to the calculation. There are many variations of the 8-bit Fletcher algorithm; we show a simple one in Figure 10.18. The 16-bit Fletcher checksum is similar to the 8-bit Fletcher checksum, but it is calculated over 16-bit data items and creates a 32-bit checksum. The calculation is done modulo 65,536.

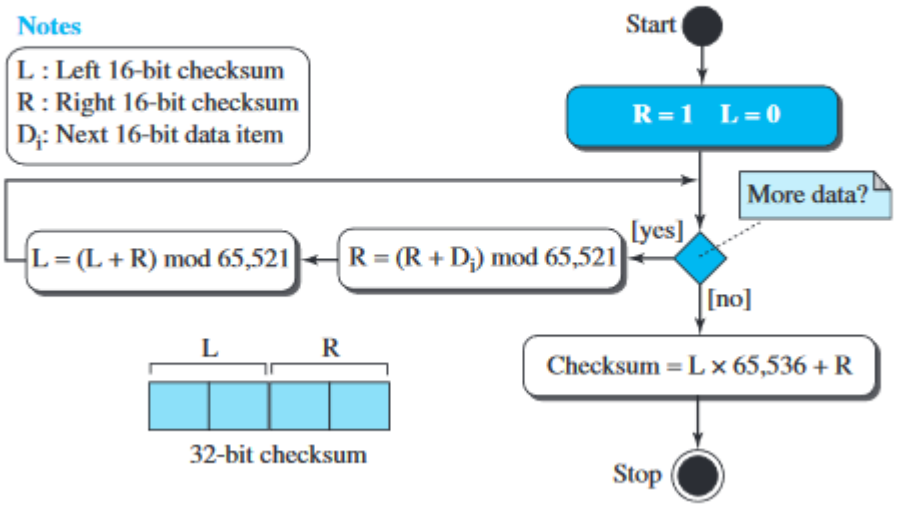
Figure 10.18 *Algorithm to calculate an 8-bit Fletcher checksum*



Adler Checksum

The Adler checksum is a 32-bit checksum. Figure 10.19 shows a simple algorithm in flowchart form. It is similar to the 16-bit Fletcher with three differences. First, calculation is done on single bytes instead of 2 bytes at a time. Second, the modulus is a prime number (65,521) instead of 65,536. Third, L is initialized to 1 instead of 0. It has been proved that a prime modulo has a better detecting capability in some combinations of data.

Figure 10.19 *Algorithm to calculate an Adler checksum*



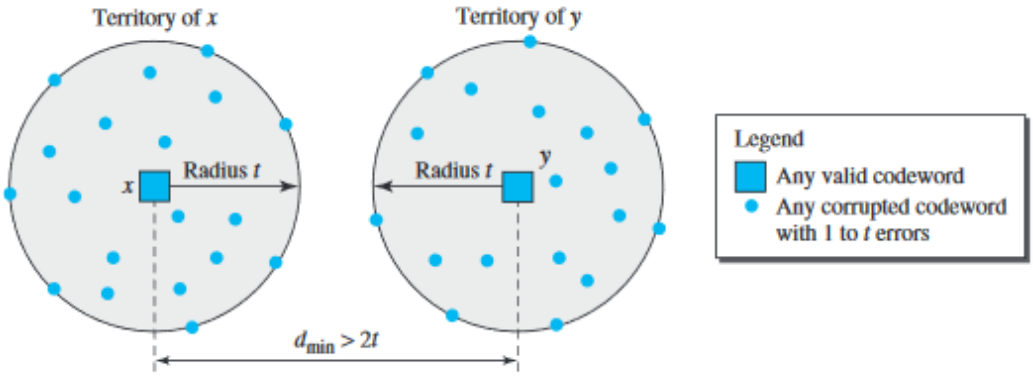
FORWARD ERROR CORRECTION

We discussed error detection and retransmission in the previous sections. However, retransmission of corrupted and lost packets is not useful for real-time multimedia transmission because it creates an unacceptable delay in reproducing: we need to wait until the lost or corrupted packet is resent. We need to correct the error or reproduce the packet immediately. Several schemes have been designed and used in this case that are collectively referred to as forward error correction (FEC) techniques. We briefly discuss some of the common techniques here.

Using Hamming Distance

We earlier discussed the Hamming distance for error detection. We said that to detect s errors, the minimum Hamming distance should be $d_{min}=s+1$. For error detection, we definitely need more distance. It can be shown that to detect t errors, we need to have $d_{min}=2t+1$. In other words, if we want to correct 10 bits in a packet, we need to make the minimum hamming distance 21 bits, which means a lot of redundant bits need to be sent with the data. To give an example, consider the famous BCH code. In this code, if data is 99 bits, we need to send 255 bits (extra 156 bits) to correct just 23 possible bit errors. Most of the time we cannot afford such a redundancy. We give some examples of how to calculate the required bits in the practice set. Figure 10.20 shows the geometrical representation of this concept.

Figure 10.20 *Hamming distance for error correction*



Using XOR

Another recommendation is to use the property of the exclusive OR operation as shown below.

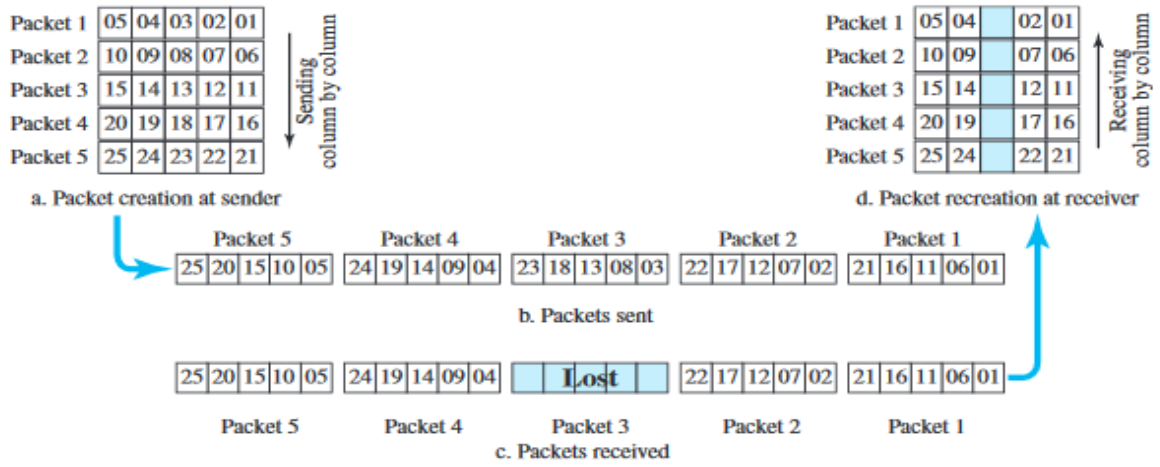
$$R=P_1 \oplus P_2 \oplus \ldots \oplus P_i \oplus \ldots \oplus P_N \rightarrow P_i=P_1 \oplus P_2 \oplus \ldots \oplus R \oplus \ldots \oplus P_N$$

In other words, if we apply the exclusive OR operation on N data items (P1to PN), we can recreate any of the data items by exclusive-ORing all of the items, replacing the one to be created by the result of the previous operation (R). This means that we can divide a packet into N chunks, create the exclusive OR of all the chunks and send N+1 chunks. If any chunk is lost or corrupted, it can be created at the receiver site. Now the question is what should the value of N be. If N= 4, it means that we need to send 25 percent extra data and be able to correct the data if only one out of four chunks is lost.

Chunk Interleaving

Another way to achieve FEC in multimedia is to allow some small chunks to be missing at the receiver. We cannot afford to let all the chunks belonging to the same packet be missing; however, we can afford to let one chunk be missing in each packet. Figure 10.21 shows that we can divide each packet into 5 chunks (normally the number is much larger). We can then create data chunk by chunk (horizontally), but combine the chunks into packets vertically. In this case, each packet sent carries a chunk from several original packets. If the packet is lost, we miss only one chunk in each packet, which is normally acceptable in multimedia communication.

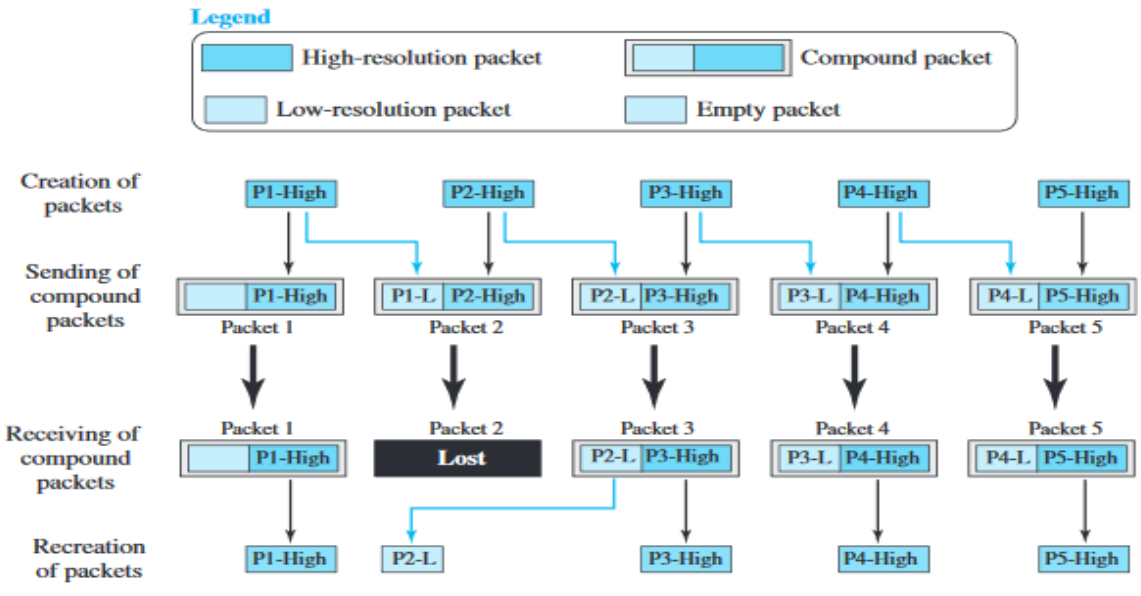
Figure 10.21 *Interleaving*



Compounding High- and Low-Resolution Packets

Still another solution is to create a duplicate of each packet with a low-resolution redundancy and combine the redundant version with the next packet. For example, we can create four low-resolution packets out of five high-resolution packets and send them as shown in Figure 10.22. If a packet is lost, we can use the low-resolution version from the next packet. Note that the low-resolution section in the first packet is empty. In this method, if the last packet is lost, it cannot be recovered, but we use the low-resolution version of a packet if the lost packet is not the last one. The audio and video reproduction does not have the same quality, but the lack of quality is not recognized most of the time.

Figure 10.22 *Compounding high- and low-resolution packets*



CHAPTER 11

DATA LINK CONTROL

DLC Services

- DLC deals with procedures for communication between two adjacent nodes.(dedicated or broadcast).
- DLC functions include framing and flow and error control.

Frames

- The data-link layer needs to pack bits into frames, so that each frame is distinguishable from another.

- Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Frame Size

- Frames can be of fixed or variable size.
- In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.
- An example of this type of framing is the ATM WAN, which uses frames of fixed size called cells.

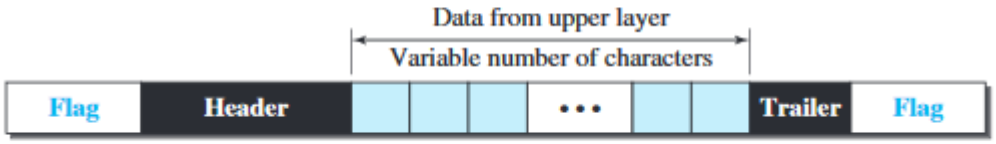
.

- Variable size framing, prevalent in local-area networks. In variable-size framing, we need a way to define the end of one frame and the beginning of the next.
- Historically, two approaches were used for this purpose: a character-oriented approach and a bit oriented approach.

Character-Oriented Framing

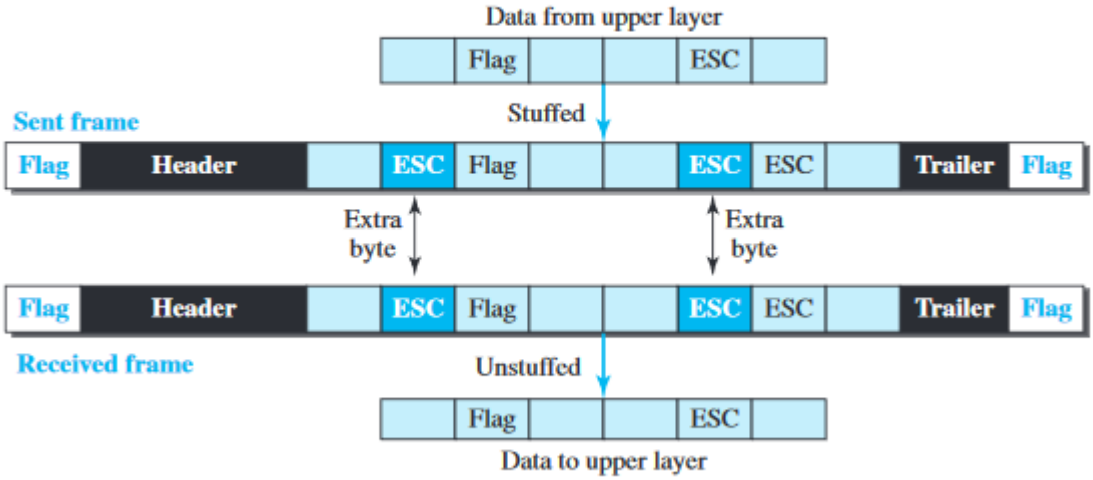
- In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters from a coding system such as ASCII.
- The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection redundant bits, are also multiples of 8 bits.
- To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame.

Figure 11.1 *A frame in a character-oriented protocol*



- Any character used for the flag could also be part of the information.
- If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame.
- To fix this problem, a byte-stuffing strategy was added to character oriented framing.
- In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC) and has a predefined bit pattern.
- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not as a delimiting flag.

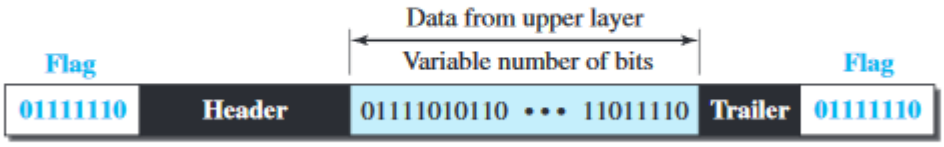
Figure 11.2 *Byte stuffing and unstuffing*



Bit-Oriented Framing

- In bit-oriented framing, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- In addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other.
- Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame.

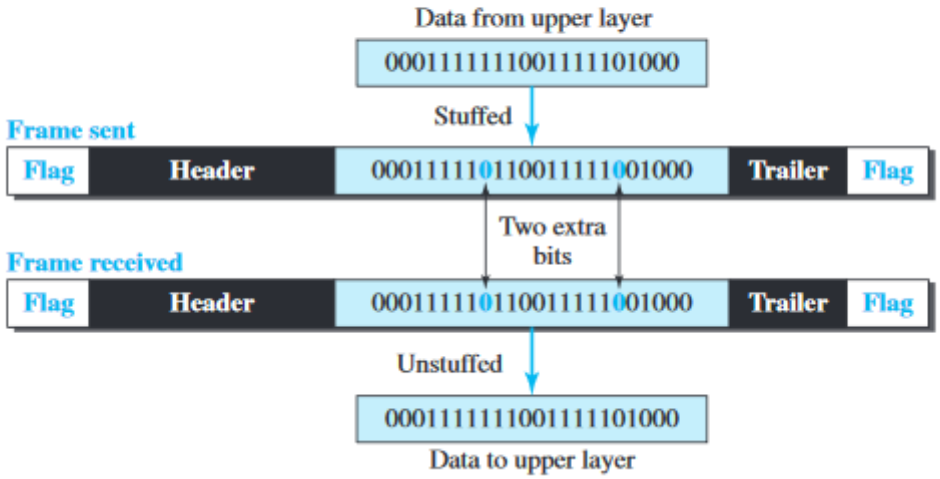
Figure 11.3 *A frame in a bit-oriented protocol*



- If the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end of the frame.
- We do this by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag.
- The strategy is called bit stuffing.
- In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added.
- This extra stuffed bit is eventually removed from the data by the receiver.
- Note that the extra bit is added after one 0 followed by five 1s regardless of the value of the next bit.
- This guarantees that the flag field sequence does not inadvertently appear in the frame.

Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

Figure 11.4 *Bit stuffing and unstuffing*

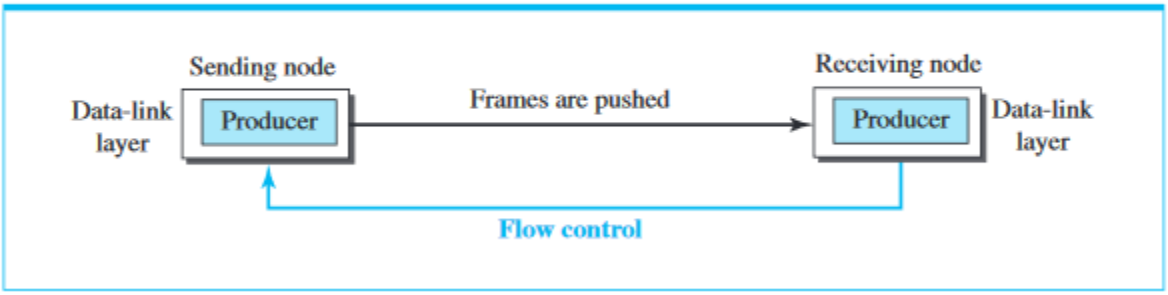


Flow and Error Control

Flow Control

- Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.
- If the items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items.
- If the items are produced more slowly than they can be consumed, the consumer must wait, and the system becomes less efficient.
- Flow control is related to the first issue.
- We need to prevent losing the data items at the consumer site.

Figure 11.5 *Flow control at the data-link layer*



The figure shows that the data-link layer at the sending node tries to push frames toward the data-link layer at the receiving node. If the receiving node cannot process and deliver the packet to its network at the same rate that the frames arrive, it becomes overwhelmed with frames. Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.

Buffers

Although flow control can be implemented in several ways, one of the solutions is normally to use two buffers; one at the sending data-link layer and the other at the receiving data-link layer. A buffer is a set of memory locations that can hold packets at the sender and receiver. The flow control communication can occur by sending signals from the consumer to the producer. When the buffer of the receiving data-link layer is full, it informs the sending data-link layer to stop pushing frames.

Connectionless and Connection-Oriented

Connectionless Protocol

- In a connectionless protocol, frames are sent from one node to the next without any relationship between the frames; each frame is independent.
- Connectionless means that there is no connection between frames.
- The frames are not numbered and there is no sense of ordering.
- Most of the data-link protocols for LANs are connectionless protocols.

Connection oriented Protocol

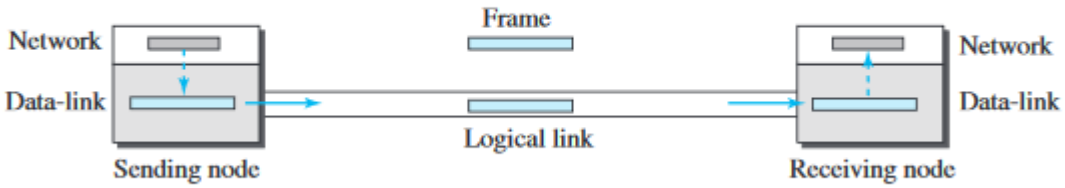
- In a connection-oriented protocol, a logical connection should first be established between the two nodes (setup phase).
- After all frames that are somehow related to each other are transmitted (transfer phase)
- The logical connection is terminated (teardown phase).
- Connection-oriented protocols are rare in wired LANs, but we can see them in some point-to-point protocols, some wireless LANs, and some WANs.

Data Link Layer Protocols

Simple Protocol

- First protocol is a simple protocol with neither flow nor error control.

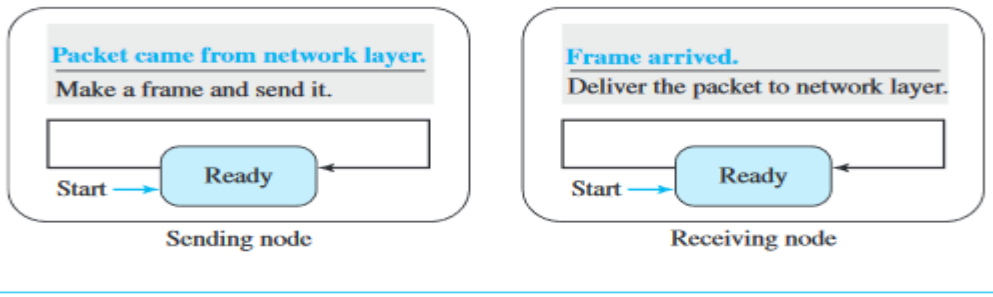
Figure 11.7 *Simple protocol*



- The data-link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame.
- The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer.
- The data-link layers of the sender and receiver provide transmission services for their network layers.

Finite State Machine (FSM)

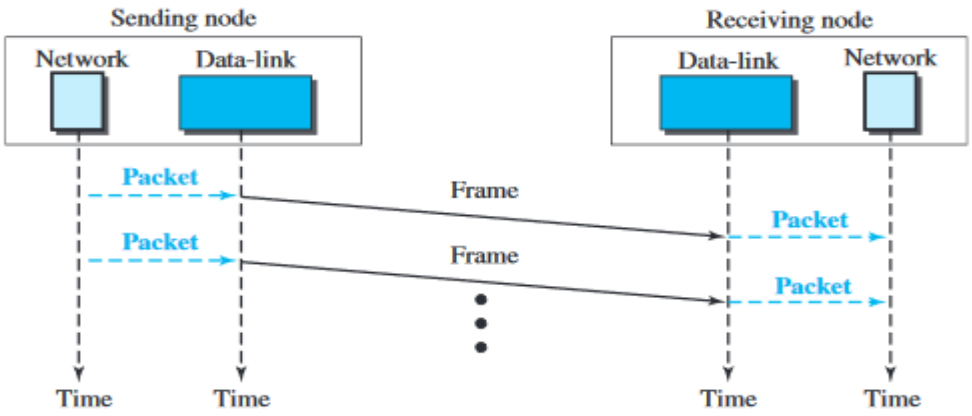
Figure 11.8 *FSMs for the simple protocol*



- The sender site should not send a frame until its network layer has a message to send. The receiver site cannot deliver a message to its network layer until a frame arrives. We can show these requirements using two FSMs.
- Each FSM has only one state, the ready state.
- The sending machine remains in the ready state until a request comes from the process in the network layer.
- When this event occurs, the sending machine encapsulates the message in a frame and sends it to the receiving machine.
- The receiving machine remains in the ready state until a frame arrives from the sending machine.
- When this event occurs, the receiving machine decapsulates the message out of the frame and delivers it to the process at the network layer.

Figure shows an example of communication using this protocol. It is very simple. The sender sends frames one after another without even thinking about the receiver.

Figure 11.9 *Flow diagram for Example 11.2*

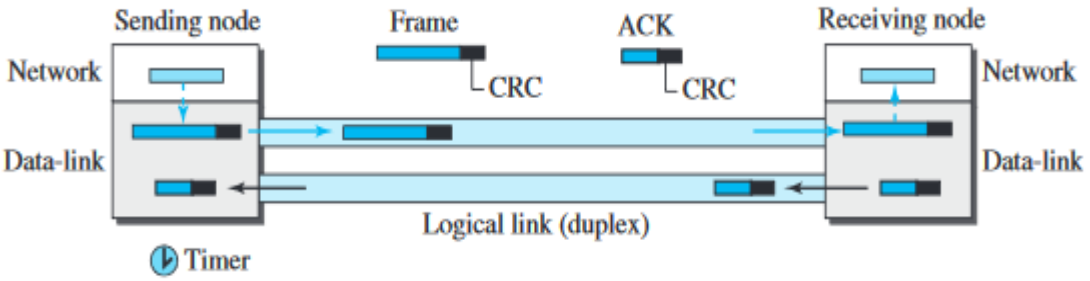


Stop-and-Wait Protocol

- Second protocol is called the Stop-and-Wait protocol, which uses both flow and error control.
- In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one.
- To detect corrupted frames, we need to add a CRC to each data frame.
- When a frame arrives at the receiver site, it is checked.
- If its CRC is incorrect, the frame is corrupted and silently discarded.
- The silence of the receiver is a signal for the sender that a frame was either corrupted or lost.
- Every time the sender sends a frame, it starts a timer.
- If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send).
- If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted.

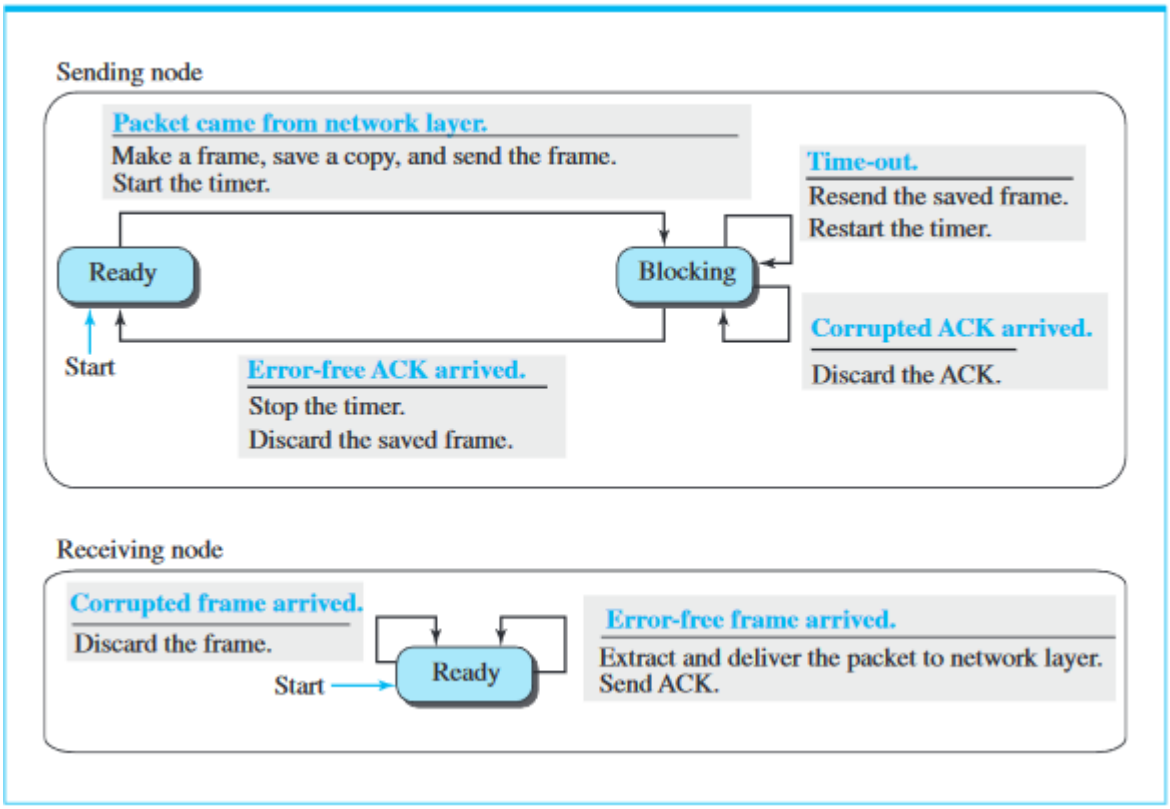
- This means that the sender needs to keep a copy of the frame until its acknowledgment arrives.
- When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.
- Figure shows the outline for the Stop-and-Wait protocol.
- Note that only one frame and one acknowledgment can be in the channels at any time.

Figure 11.10 *Stop-and-Wait protocol*



FSM

Figure 11.11 *FSM for the Stop-and-Wait protocol*



We describe the sender and receiver states below.

Sender States

The sender is initially in the ready state, but it can move between the ready and blocking state.

Ready State

- When the sender is in this state, it is only waiting for a packet from the network layer.
- If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame.
- The sender then moves to the blocking state.

Blocking State: When the sender is in this state, three events can occur

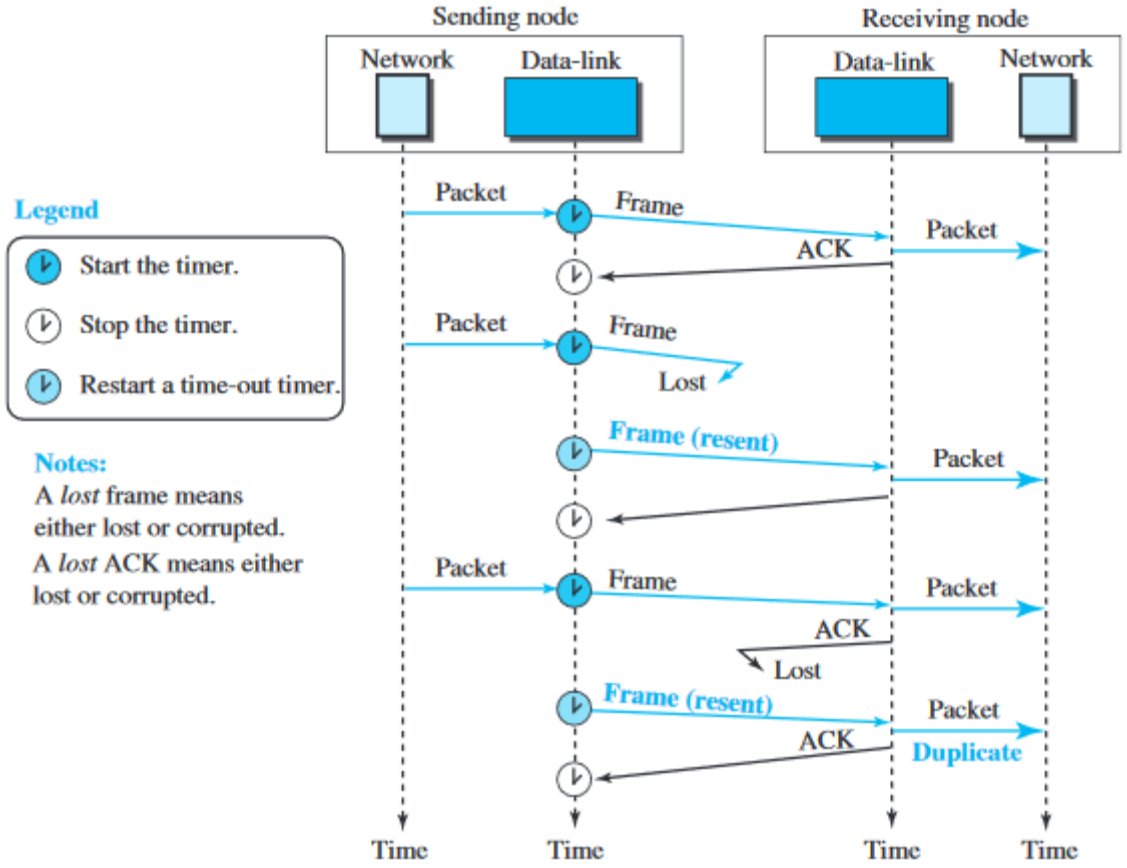
- If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer.
- If a corrupted ACK arrives, it is discarded.
- If an error-free ACK arrives, the sender stops the timer and discards the saved copy of the frame. It then moves to the ready state.

Receiver

The receiver is always in the ready state. Two events may occur:
a. If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent.
b. If a corrupted frame arrives, the frame is discarded.

Figure shows an example. The first frame is sent and acknowledged. The second frame is sent, but lost. After time-out, it is resent. The third frame is sent and acknowledged, but the acknowledgment is lost. The frame is resent. However, there is a problem with this scheme. The network layer at the receiver site receives two copies of the third packet, which is not right.

Figure 11.12 *Flow diagram for Example 11.3*

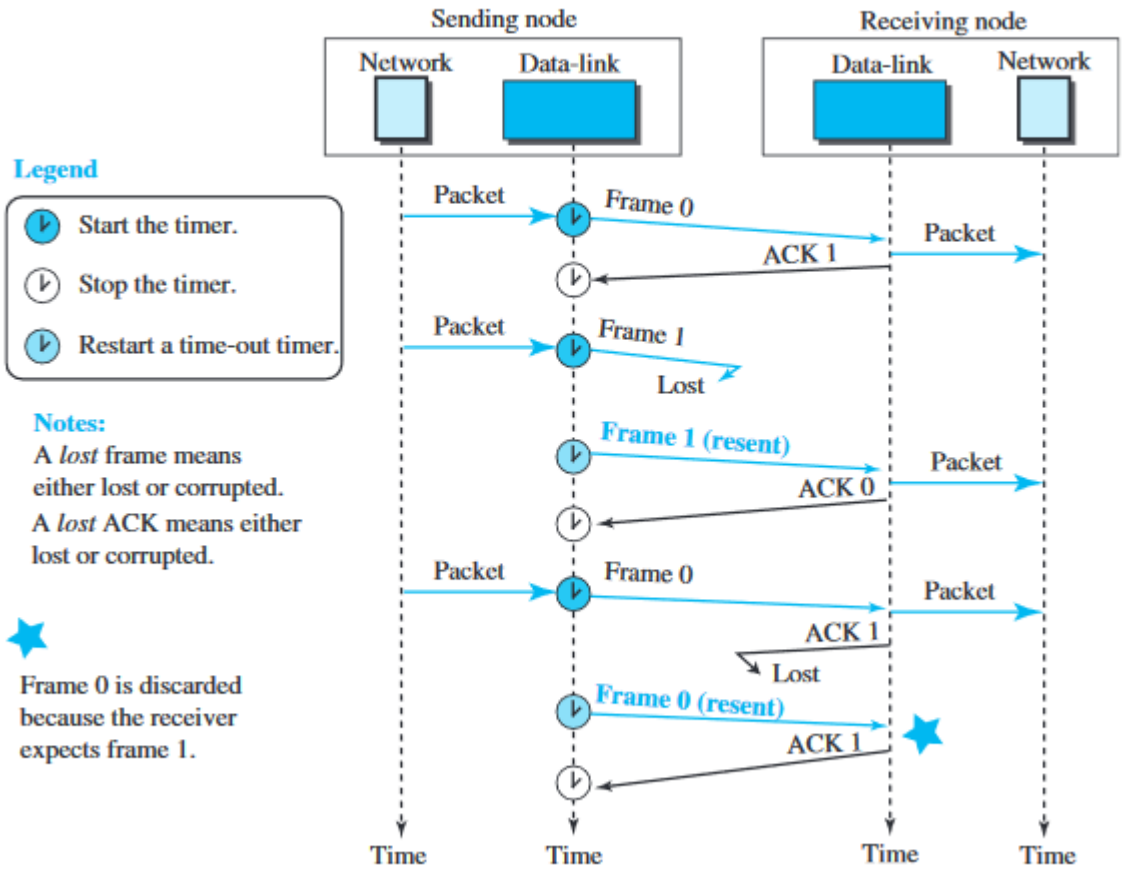


Sequence and Acknowledgment Numbers

- We need to add sequence numbers to the data frames and acknowledgment numbers to the ACK frames.
- Sequence numbers are 0, 1, 0, 1, 0, 1, . . . ; the acknowledgment numbers can also be 1, 0, 1, 0, 1, 0, ...
- In other words, the sequence numbers start with 0, the acknowledgment numbers start with 1. An acknowledgment number always defines the sequence number of the next frame to receive.

Figure shows how adding sequence numbers and acknowledgment numbers can prevent duplicates. The first frame is sent and acknowledged. The second frame is sent, but lost. After time-out, it is resent. The third frame is sent and acknowledged, but the acknowledgment is lost. The frame is resent.

Figure 11.13 *Flow diagram for Example 11.4*



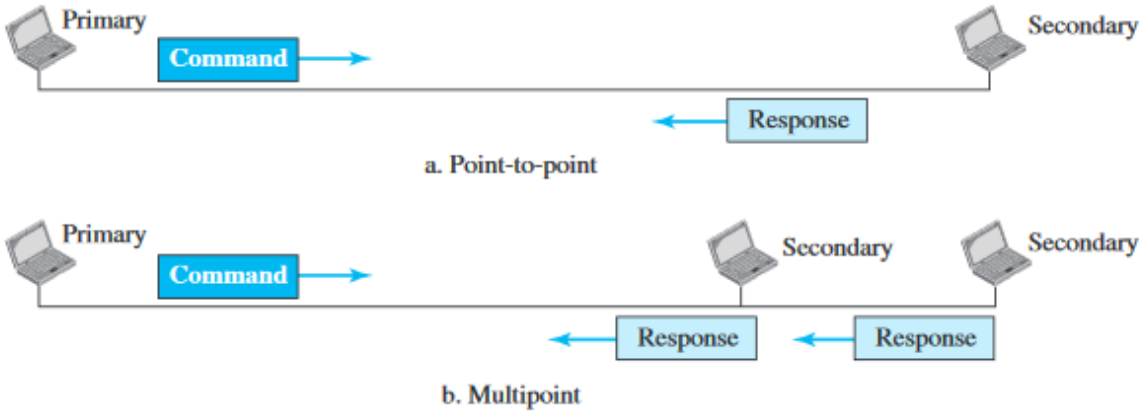
HDLC

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links.

Configurations and Transfer Modes

HDLC provides two common transfer modes that can be used in different configurations: normal response mode (NRM) and asynchronous balanced mode (ABM) .In normal response mode (NRM) , the station configuration is unbalanced. We have one primary station and multiple secondary stations. A primary station can send commands; a secondary station can only respond. The NRM is used for both point-to point and multi point links, as shown in Figure. In ABM, the configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary

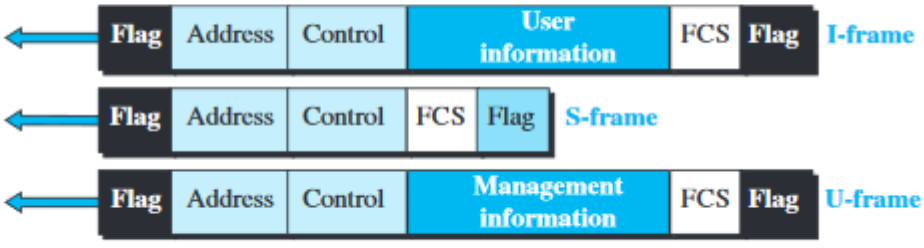
Figure 11.14 *Normal response mode*



Framing

- To provide the flexibility necessary to support all the options possible in the modes and configurations just described, HDLC defines three types of frames:
- Information frames (I-frames) , supervisory frames (S-frames), and unnumbered frames (U frames).
- Each type of frame serves as an envelope for the transmission of a different type of message.
- I-frames are used to data-link user data and control information relating to user data (piggy-backing).
- S-frames are used only to transport control information.
- U frames are reserved for system management.
- Information carried by U-frames is intended for managing the link itself.
- Each frame in HDLC may contain up to six fields, as shown in Figure a beginning flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field.
- In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.

Figure 11.16 *HDLC frames*



Flag field

This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.

Address field

This field contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary station creates the frame, it contains a from address. The address field can be one byte or several bytes long, depending on the needs of the network.

Control field

The control field is one or two bytes used for flow and error control.

Information field

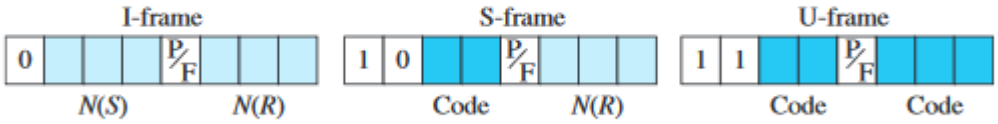
The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.

FCS field

The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte CRC.

The control field determines the type of frame and defines its functionality

Figure 11.17 *Control field format for the different frame types*



Control Field for I-Frames

- I-frames are designed to carry user data from the network layer.
- In addition, they can include flow- and error-control information (piggybacking).
- The subfields in the control field are used to define these functions.
- The first bit defines the type.
- If the first bit of the control field is 0, this means the frame is an I-frame.
- The next 3 bits, called N(S), define the sequence number of the frame.
- Note that with 3 bits, we can define a sequence number between 0 and 7.

- The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used.
- The single bit between N(S) and N(R) is called the P/F bit.
- The P/F field is a single bit with a dual purpose.
- It has meaning only when it is set (bit =1) and can mean poll or final.
- It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver).
- It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

Control Field for S-Frames

- Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate.
- S-frames do not have information fields.
- If the first 2 bits of the control field are 10, this means the frame is an S-frame.
- The last 3 bits, called N(R), correspond to the acknowledgment number (ACK) or negative acknowledgment number (NAK), depending on the type of S-frame.
- The 2 bits called code are used to define the type of S-frame itself.
- With 2 bits, we can have four types of S-frames, as described below:

Receive ready (RR)

- If the value of the code subfield is 00, it is an RR S-frame.
- This kind of frame acknowledges the receipt of a safe and sound frame or group of frames.
- In this case, the value of the N(R) field defines the acknowledgment number.

Receive not ready (RNR)

- If the value of the code subfield is 10, it is an RNR S-frame.
- This kind of frame is an RR frame with additional functions.
- It acknowledges the receipt of a frame or group of frames, and it announces that the receiver is busy and cannot receive more frames. It acts as a kind of congestion control mechanism by asking the sender to slow down. The value of N(R) is the acknowledgment number.

Reject (REJ)

- If the value of the code subfield is 01, it is an REJ S-frame.
- This is a NAK frame, but not like the one used for Selective Repeat ARQ.
- It is a NAK that can be used in Go-Back-N ARQ to improve the efficiency of the process by informing the sender, before the sender timer expires, that the last frame is lost or damaged.
- The value of N(R) is the negative acknowledgment number.

Selective reject (SREJ)

- If the value of the code subfield is 11, it is an SREJ S-frame.
- This is a NAK frame used in Selective Repeat ARQ.
- Note that the HDLC Protocol uses the term selective reject instead of selective repeat.
- The value of N(R) is the negative acknowledgment number.

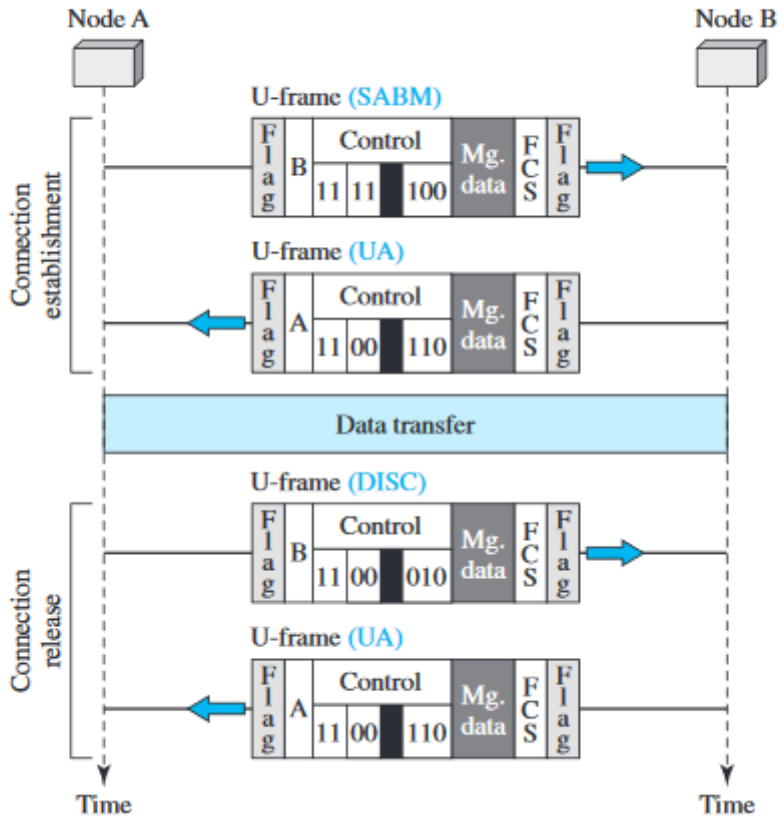
Control Field for U-Frames

- Unnumbered frames are used to exchange session management and control information between connected devices.
- U-frames contain an information field, but one used for system management information, not user data.
- U-frame codes are divided in to two sections: a 2-bit prefix before the P/F bit and a 3 bit suffix after the P/F bit. Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.

Example 11.5

Figure 11.18 shows how U-frames can be used for connection establishment and connection release. Node A asks for a connection with a set asynchronous balanced mode (SABM) frame; node B gives a positive response with an unnumbered acknowledgment (UA) frame. After these two exchanges, data can be transferred between the two nodes (not shown in the figure). After data transfer, node A sends a DISC (disconnect) frame to release the connection; it is confirmed by node B responding with a UA (unnumbered acknowledgment).

Figure 11.18 *Example of connection and disconnection*

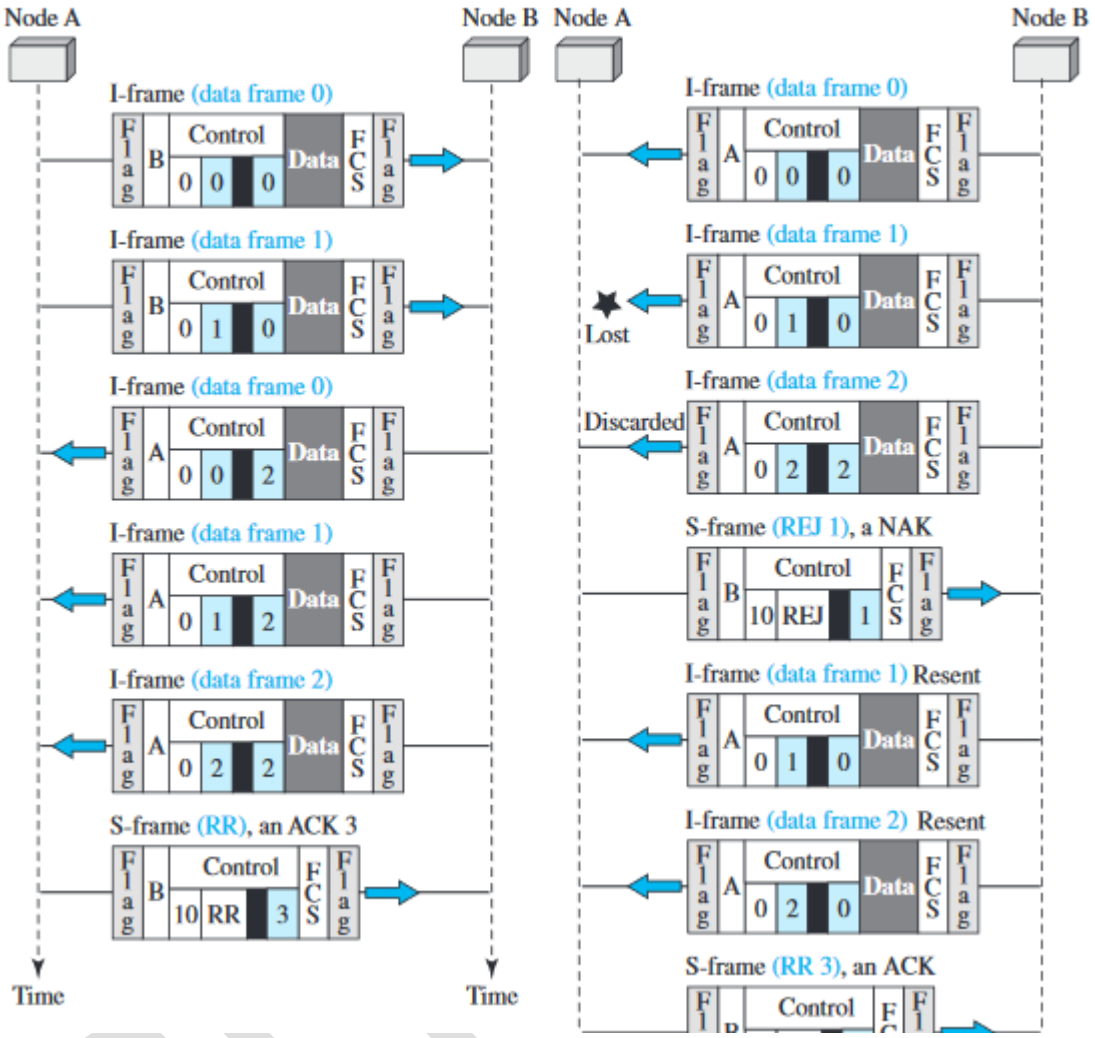


Example

Figure shows two exchanges using piggybacking.

The first is the case where no error has occurred; the second is the case where an error has occurred and some frames are discarded.

Figure 11.19 *Example of piggybacking with and without error*



POINT-TO-POINT PROTOCOL (PPP)

One of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP).

Services

Services Provided by PPP

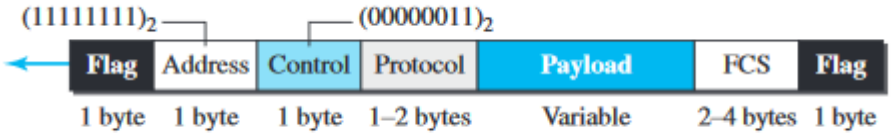
- PPP does not provide flow control.
- A sender can send several frames one after another with no concern about overwhelming the receiver.
- PPP has a very simple mechanism for error control.
- A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs to take care of the problem.
- Lack of error control and sequence numbering may cause a packet to be received out of order.

- PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

Framing

PPP uses a character-oriented (or byte-oriented) frame. Figure shows the format of a PPP frame. The description of each field follows:

Figure 11.20 *PPP frame format*



Address
The address field in this protocol is a constant value and set to 11111111 (broadcast address).

Control
This field is set to the constant value 00000011 (imitating unnumbered frames in HDLC). As we will discuss later, PPP does not provide any flow control. Error control is also limited to error detection.

Protocol
The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

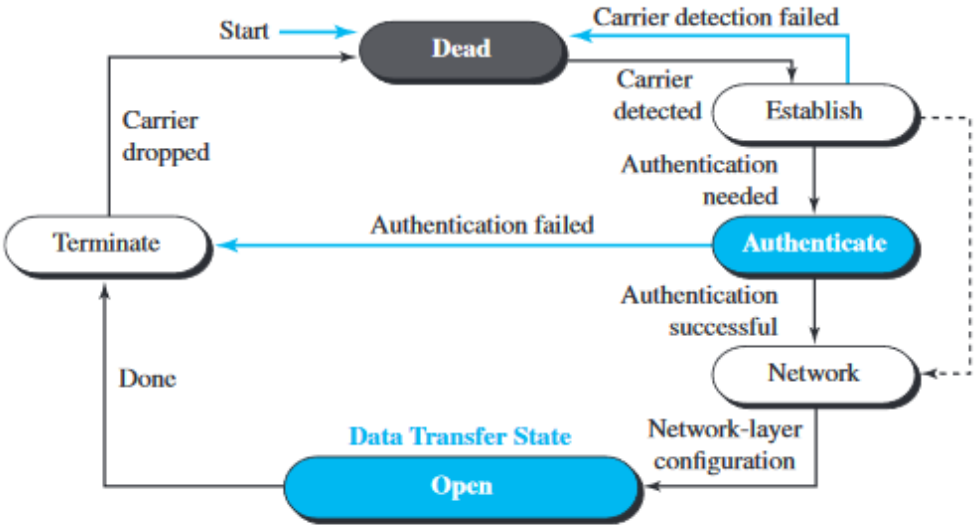
Payload field
This field carries either the user data or other information that we will discuss shortly. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte-stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.

FCS
The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

Transition Phases

- A PPP connection goes through phases which can be shown in a transition phase diagram.
- The transition diagram, which is an FSM, starts with the **dead state**.
- In **dead state**, there is no active carrier (at the physical layer) and the line is quiet. When one of the two nodes starts the communication, the connection goes into the **establish state**.
- In **establish state**, options are negotiated between the two parties.
- If the two parties agree that they need authentication (for example, if they do not know each other), then the system needs to do authentication (an extra step); otherwise, the parties can simply start communication.
- Data transfer takes place in the **open state**.
- When a connection reaches **open state**, the exchange of data packets can be started.
- The connection remains in **open state** until one of the end points wants to terminate the connection.
- In this case, the system goes to the **terminate state**. The system remains in this state until the carrier (physical-layer signal) is dropped, which moves the system to the **dead state** again.

Figure 11.21 *Transition phases*



MODULE 3: ERROR-DETECTION AND CORRECTION

1.Explain two types of errors (4*)

2.Compare error detection vs. error correction (2)
3.Explain error detection using block coding technique. (10*)

4.Explain hamming distance for error detection (6*)

5.Explain parity-check code with block diagram. (6*)
6.Explain CRC with block diagram & an example. (10*)

7.Write short notes on polynomial codes. (5*)

8.Explain internet checksum algorithm along with an example. (6*)
9.Explain the following:
Fletcher checksum and ii) Adler checksum (8)

10.Explain various FEC techniques. (6)

MODULE 3: DATA LINK CONTROL

1.Explain two types of frames. (2)
2.Explain character oriented protocol. (6*)
3.Explain the concept of byte stuffing and unstuffing with example. (6*)

4.Explain bit oriented protocol. (6*)

5.Differentiate between character oriented and bit oriented format for Framing. (6*)
6.Compare flow control and error control. (4)
7.With a neat diagram, explain the design of the simplest protocol with no flow control. (6)

8.Write algorithm for sender site and receiver site for the simplest protocol. (6)

9.Explain Stop-and-Wait protocol (8*)
10.Explain the concept of Piggybacking (2*)

11.Explain in detail HDLC frame format. (8*)

12.Explain 3 type of frame used in HDLC (8*)
13.With a neat schematic, explain the frame structure of PPP protocol. (8*)
14.Explain framing and transition phases in Point-to-Point Protocol. (8*)

MODULE 4: TABLE OF CONTENTS

- Switched Ethernet
- Full-Duplex Ethernet

FAST ETHERNET (100 MBPS)
- Access Method
- Physical Layer
  - Topology
  - Implementation
  - Encoding

GIGABIT ETHERNET
- MAC Sublayer
- Physical Layer
  - Topology
  - Implementation
  - Encoding

TEN GIGABIT ETHERNET
- Implementation

INTRODUCTION OF WIRELESS-LANS
- Architectural Comparison
- Characteristics
- Access Control

IEEE 802.11 PROJECT
- Architecture
  - BSS
  - ESS
  - Station Types
- MAC Sublayer
  - DCF
    - Network Allocation Vector
    - Collision During Handshaking
  - PCF
    - Fragmentation
    - Frame Types
    - Frame Format
- Addressing Mechanism
  - Exposed Station Problem
- Physical Layer
  - IEEE 802.11 FHSS
  - IEEE 802.11 DSSS
  - IEEE 802.11 Infrared
  - IEEE 802.11a OFDM
  - IEEE 802.11b DSSS
  - IEEE 802.11g

BLUETOOTH
- Architecture
  - Piconets
  - Scatternet
  - Bluetooth Devices
- Bluetooth Layers
  - Radio Layer
  - Baseband Layer
    - TDMA
    - Links
    - Frame Types
    - Frame Format
  - L2CAP

MODULE 4: MULTIPLE ACCESS

4.1 Introduction

When nodes use shared-medium, we need multiple-access protocol to coordinate access to medium.
Analogy:
This problem is similar to the rules of speaking in an assembly.
We need to ensure
Each people has right to speak.
Two people do not speak at the same time
Two people do not interrupt each other (i.e. Collision Avoidance)
Many protocols have been designed to handle access to a shared-link (Figure 12.1).
These protocols belong to a sublayer in the data-link layer called Media Access Control (MAC).

1) Four random-access protocols (or Contention Methods):
   i) ALOHA ii) CSMA iii) CSMA/CD iv) CSMA/CA
   These protocols are mostly used in LANs and WANs.
2) Three controlled-access protocols:
   i) Reservation ii) Polling iii) Token-passing
   Some of these protocols are used in LANs.
3) Three channelization protocols:
   i) FDMA ii) TDMA iii) CDMA
   These protocols are used in cellular telephony.

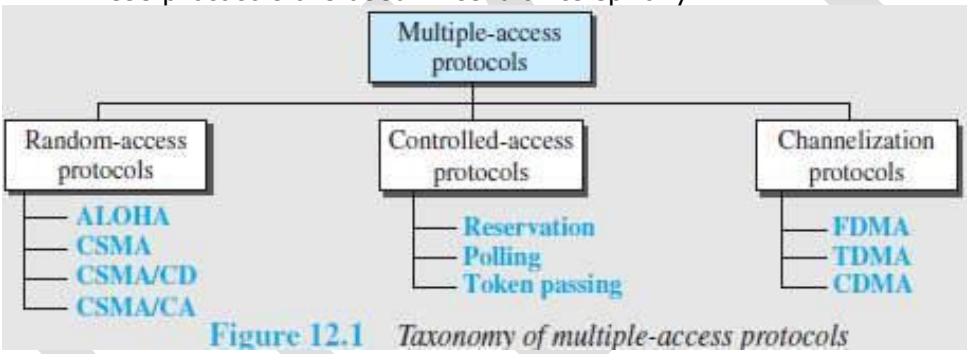


Figure 12.1 *Taxonomy of multiple-access protocols*

4.2 RANDOM ACCESS PROTOCOL

No station is superior to another station.
No station is assigned control over other station.
To send the data, a station uses a procedure to make a decision on whether or not to send.
This decision depends on the state of the medium: idle or busy.
This is called Random Access because
Transmission is random among the stations.
There is no scheduled-time for a station to transmit.
This is called Contention Method because
Stations compete with one another to access the medium.
If more than one station tries to send,
there is an access-conflict (i.e. collision) and the frames will be destroyed.
Each station follows a procedure that answers the following questions:
When can the station access the medium?
What can the station do if the medium is busy?
How can the station determine the success or failure of the transmission?
What can the station do if there is a collision?
Four random-access protocols (or Contention methods):
ALOHA
CSMA (Carrier Sense Multiple Access)
CSMA/CD (Carrier Sense Multiple Access with Collision-detection)
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

4.2.1 ALOHA

ALOHA was designed for a wireless LAN, but it can be used on any shared medium.
Since the medium is shared between the stations, there is possibility of collisions.
When 2 or more stations send the data simultaneously, there is possibility of collision & data loss.

4.2.1.1 Pure ALOHA

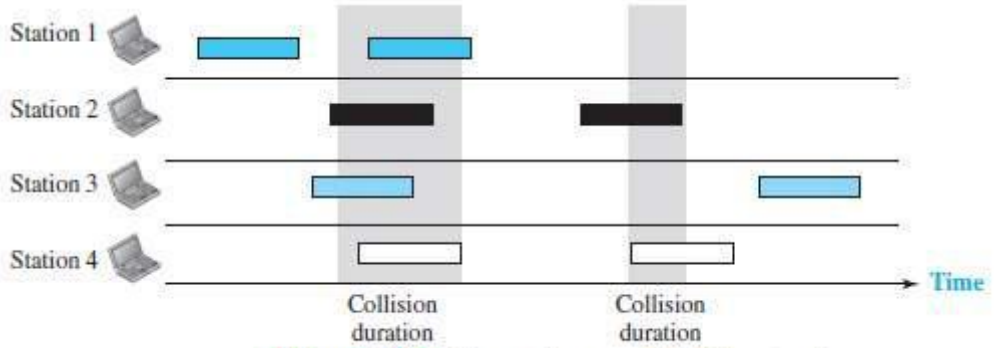


Figure 12.2 *Frames in a pure ALOHA network*

Here is how it works (Figure 12.2):

The sender sends a frame & starts the timer.
The receiver receives the frame and responds with an acknowledgment.
If the acknowledgment does not arrive after a time-out period, the sender resends the frame. The sender assumes that the frame (or the acknowledgment) has been destroyed.
Since the medium is shared between the stations, there is possibility of collisions.
If two stations try to resend the frames after the time-out, the frames will collide again.
Two methods to deal with collision:

Randomness

When the time-out period passes, each station waits a random amount of time before resending the frame. This time is called back-off time T_B.
The randomness will help avoid more collisions.

ii) Limit Maximum Retransmission

This method prevents congestion by reducing the number of retransmitted frames.
After a maximum number of retransmission-attempts K_{max}, a station must give up and try later (Figure 12.3).

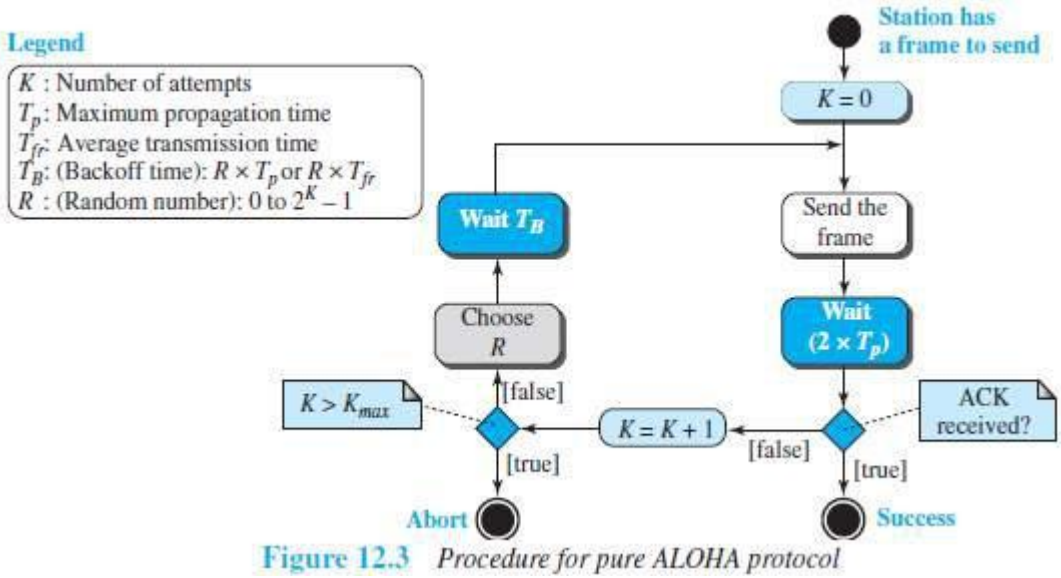


Figure 12.3 *Procedure for pure ALOHA protocol*

4.2.1.1.1 Vulnerable time

- The vulnerable-time is defined as a time during which there is a possibility of collision.

Pure ALOHA vulnerable time = $2 \times T_{fr}$

where T_{fr} = Frame transmission time

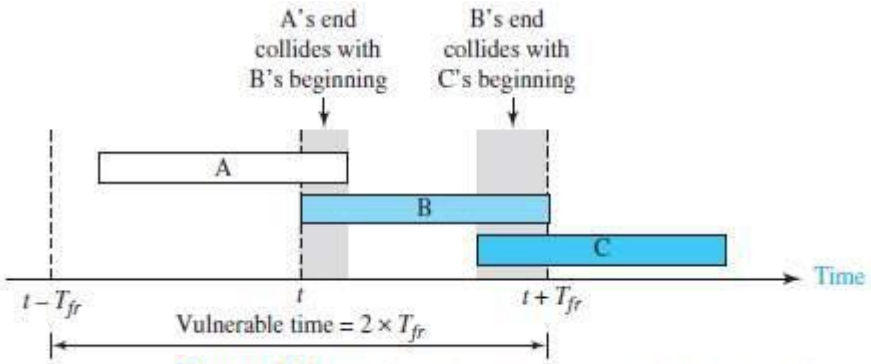


Figure 12.4 *Vulnerable time for pure ALOHA protocol*

In Figure 12.4,

If station B sends a frame between t-T_{fr} and t, this leads to a collision between the frames from station A and station B.

- If station C sends a frame between t and t+T_{fr}, this leads to a collision between the frames from station A and station C.

Example 4.1

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the period (1 ms) that this station is sending.

4.2.1.1.2 Throughput

- The average number of successful transmissions is given by

$$S = G \times e^{-2G}$$

where G = average no. of frames in one frame transmission time (T_{fr})

For G = 1, the maximum throughput S_{max} = 0.184.

In other words, out of 100 frames, 18 frames reach their destination successfully.

Example 4.2

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

a. 1000 frames per second? b. 500 frames per second? c. 250 frames per second?

Solution

The frame transmission time is 200/200 kbps or 1 ms.

a. If the system creates 1000 frames per second, or 1 frame per millisecond, then $G = 1$. In this case $S = G \times e^{-2G} = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

b. If the system creates 500 frames per second, or 1/2 frames per millisecond, then $G = 1/2$. In this case $S = G \times e^{-2G} = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the *maximum* throughput case, percentagewise.

c. If the system creates 250 frames per second, or 1/4 frames per millisecond, then $G = 1/4$. In this case $S = G \times e^{-2G} = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

4.2.1.2 Slotted ALOHA

Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
The time is divided into time-slots of T_{fr} seconds (Figure 12.5).
The stations are allowed to send only at the beginning of the time-slot.

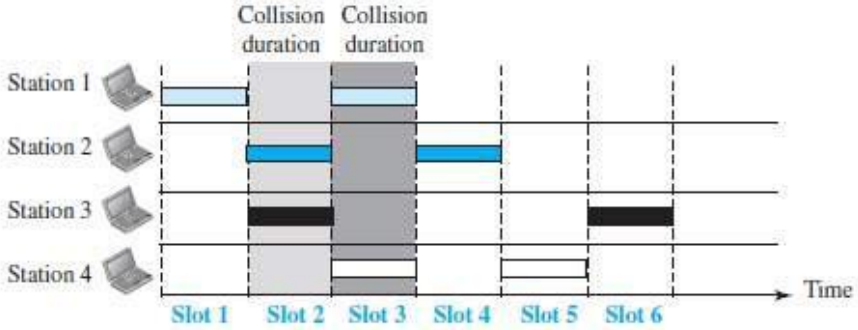


Figure 12.5 *Frames in a slotted ALOHA network*

If a station misses the time-slot, the station must wait until the beginning of the next time-slot.
If 2 stations try to resend at beginning of the same time-slot, the frames will collide again (Fig 12.6).

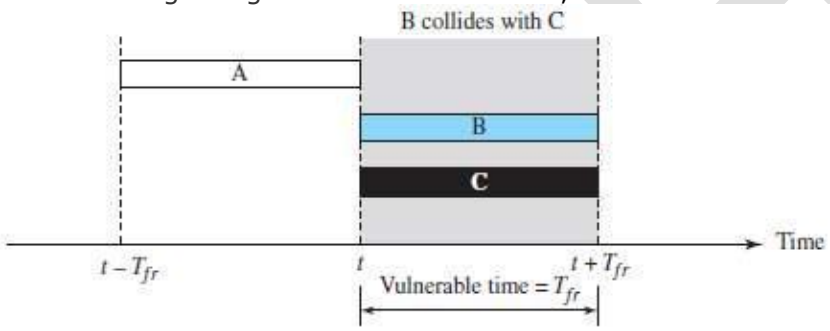


Figure 12.6 *Vulnerable time for slotted ALOHA protocol*

- The vulnerable time is given by:

$$\text{vulnerable time} = T_{fr}$$

4.2.1.2.1 Throughput

The average number of successful transmissions is given by

$$S = G \times e^{-G}$$

For G = 1, the maximum throughput S_{max} = 0.368.
In other words, out of 100 frames, 36 frames reach their destination successfully.

Example 4.3

A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces

a. 1000 frames per second.
b. 500 frames per second.
c. 250 frames per second.

Solution

This situation is similar to the previous exercise except that the network is using slotted ALOHA instead of pure ALOHA. The frame transmission time is 200/200 kbps or 1 ms.

a. In this case G is 1. So $S = G \times e^{-G} = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise.
b. Here G is 1/2. In this case $S = G \times e^{-G} = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.
c. Now G is 1/4. In this case $S = G \times e^{-G} = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.

DATA COMMUNICATION

4.2.2 CSMA

CSMA was developed to minimize the chance of collision and, therefore, increase the performance.
CSMA is based on the principle "sense before transmit" or "listen before talk."
Here is how it works:

Each station checks the state of the medium: idle or busy.
i) If the medium is idle, the station sends the data.
If the medium is busy, the station defers sending.

CSMA can reduce the possibility of collision, but it cannot eliminate it.

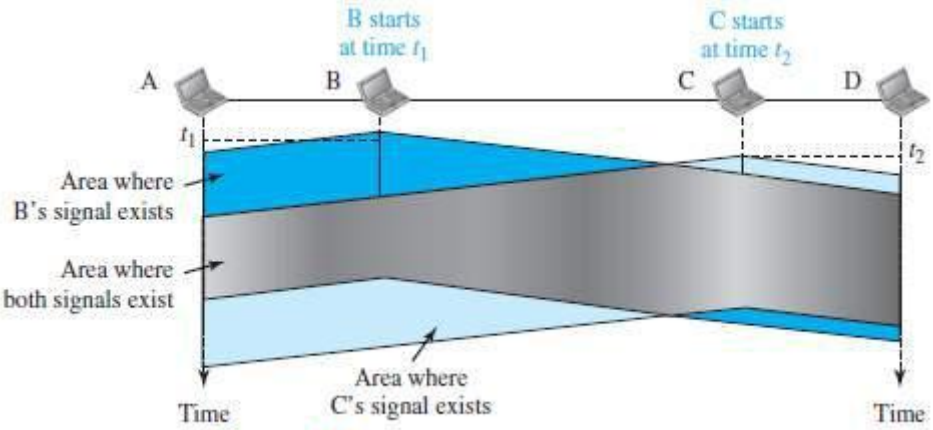


Figure 12.7 *Space/time model of a collision in CSMA*

The possibility of collision still exists. For example:

When a station sends a frame, it still takes time
for the first bit to reach every station and
for every station to sense it.

For example: In Figure 12.7,
At time t1, station B senses & finds the medium idle, so sends a frame.
At time t2, station C senses & finds the medium idle, so sends a frame.
The 2 signals from both stations B & C collide and both frames are destroyed.

4.2.2.1 Vulnerable Time

The vulnerable time is the propagation time T_p (Figure 12.8).
The propagation time is the time needed for a signal to propagate from one end of the medium to the other.
Collision occurs when
a station sends a frame, and
other station also sends a frame during propagation time
If the first bit of the frame reaches the end of the medium, every station will refrain from sending.

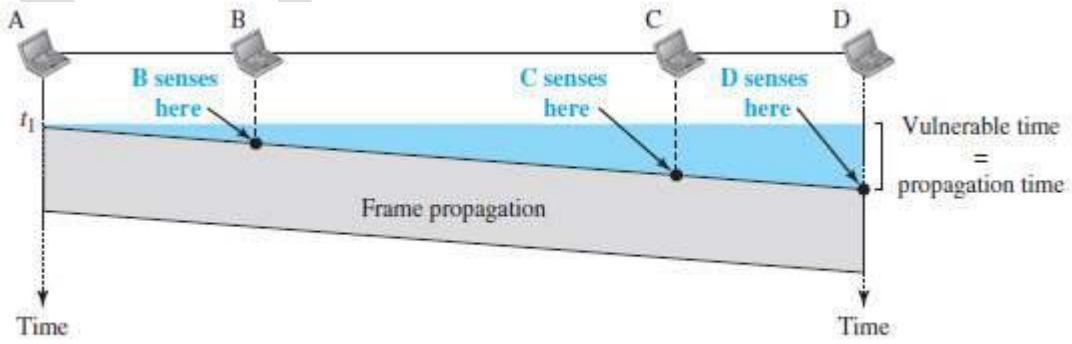


Figure 12.8 *Vulnerable time in CSMA*

4.2.2.2 Persistence Methods

• Q: What should a station do if the channel is busy or idle?

Three methods can be used to answer this question:

1) 1-persistent method 2) Non-persistent method and 3) p-persistent method

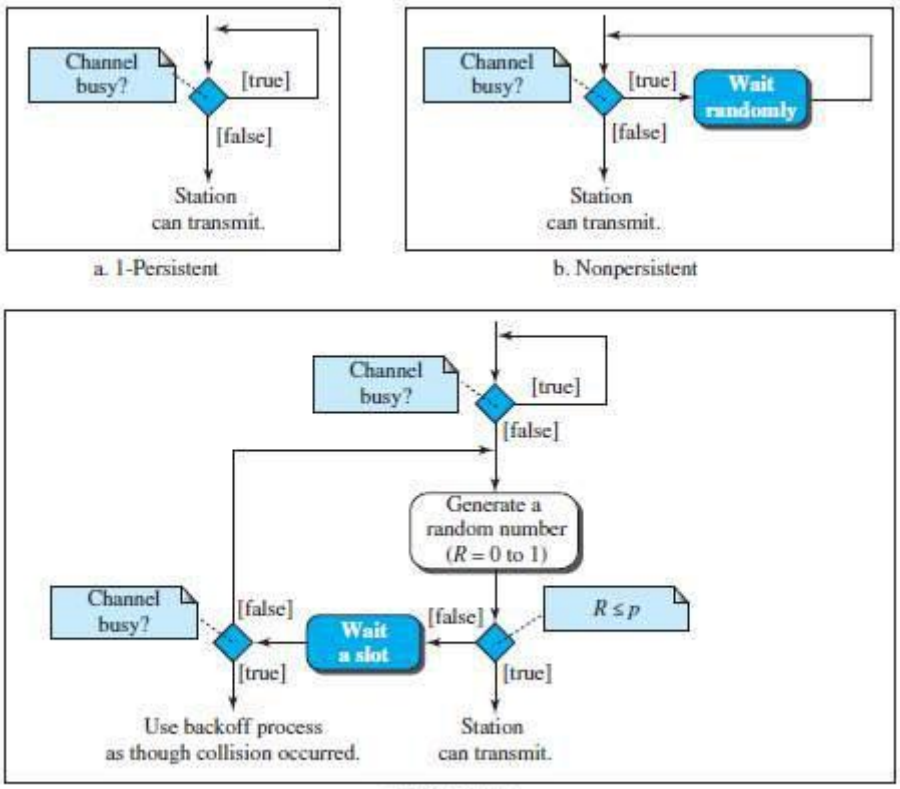


Figure 12.10 *Flow diagram for three persistence methods*

1) 1-Persistent

Before sending a frame, a station senses the line (Figure 12.10a).

If the line is idle, the station sends immediately (with probability = 1).

If the line is busy, the station continues sensing the line.

This method has the highest chance of collision because 2 or more stations:

may find the line idle and

send the frames immediately.

2) Non-persistent

• Before sending a frame, a station senses the line (Figure 12.10b).

i) If the line is idle, the station sends immediately.

ii) If the line is busy, the station waits a random amount of time and then senses the line again.

• This method reduces the chance of collision because 2 or more stations:

→ will not wait for the same amount of time and

→ will not retry to send simultaneously.

3) P-Persistent

This method is used if the channel has time-slots with a slot-duration equal to or greater than the maximum propagation time (Figure 12.10c).

Advantages:

It combines the advantages of the other 2 methods.

It reduces the chance of collision and improves efficiency.

After the station finds the line idle, it follows these steps:

With probability p, the station sends the frame.

With probability q=1-p, the station waits for the beginning of the next time-slot and checks the line again.

If line is idle, it goes to step 1.

If line is busy, it assumes that collision has occurred and uses the back off procedure.

4.2.3 CSMA/CD

Disadvantage of CSMA: CSMA does not specify the procedure after a collision has occurred.

Solution: CSMA/CD enhances the CSMA to handle the collision.

Here is how it works (Figure 12.12):

A station

sends the frame &

then monitors the medium to see if the transmission was successful or not.

If the transmission was unsuccessful (i.e. there is a collision), the frame is sent again.

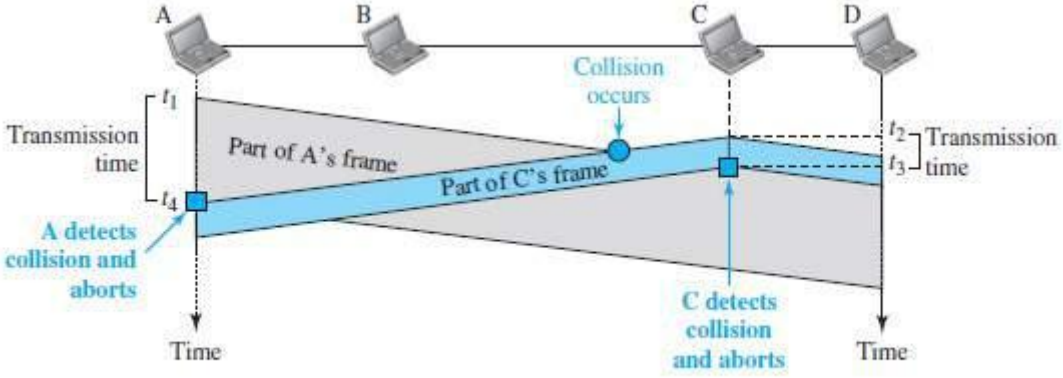


Figure 12.12 *Collision and abortion in CSMA/CD*

In the Figure 12.11,

At time t_1, station A has executed its procedure and starts sending the bits of its frame.
At time t_2, station C has executed its procedure and starts sending the bits of its frame.
The collision occurs sometime after time t_2.
Station C detects a collision at time t_3 when it receives the first bit of A's frame.
Station C immediately aborts transmission.
Station A detects collision at time t_4 when it receives the first bit of C's frame.
Station A also immediately aborts transmission.

Station A transmits for the duration $t_4 - t_1$. Station C transmits for the duration $t_3 - t_2$.

For the protocol to work:

The length of any frame divided by the bit rate must be more than either of these durations.

4.2.3.1 Minimum Frame Size

For CSMA/CD to work, we need to restrict the frame-size.

Before sending the last bit of the frame, the sender must

detect a collision and

abort the transmission.

This is so because the sender

does not keep a copy of the frame and

does not monitor the line for collision-detection.

Frame transmission time T_{fr} is given by

$T_{fr} = 2T_p$ where T_p=maximum propagation time

Example 4.4

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 μs, what is the minimum size of the frame?

Solution

The minimum frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet, as we will see later in the chapter.

4.2.3.2 Procedure

CSMA/CD is similar to ALOHA with 2 differences (Figure 12.13):

Addition of the persistence process.

We need to sense the channel before sending the frame by using non-persistent, 1-persistent or p-persistent.

Frame transmission.

In ALOHA, first the entire frame is transmitted and then acknowledgment is waited for. In CSMA/CD, transmission and collision-detection is a continuous process.

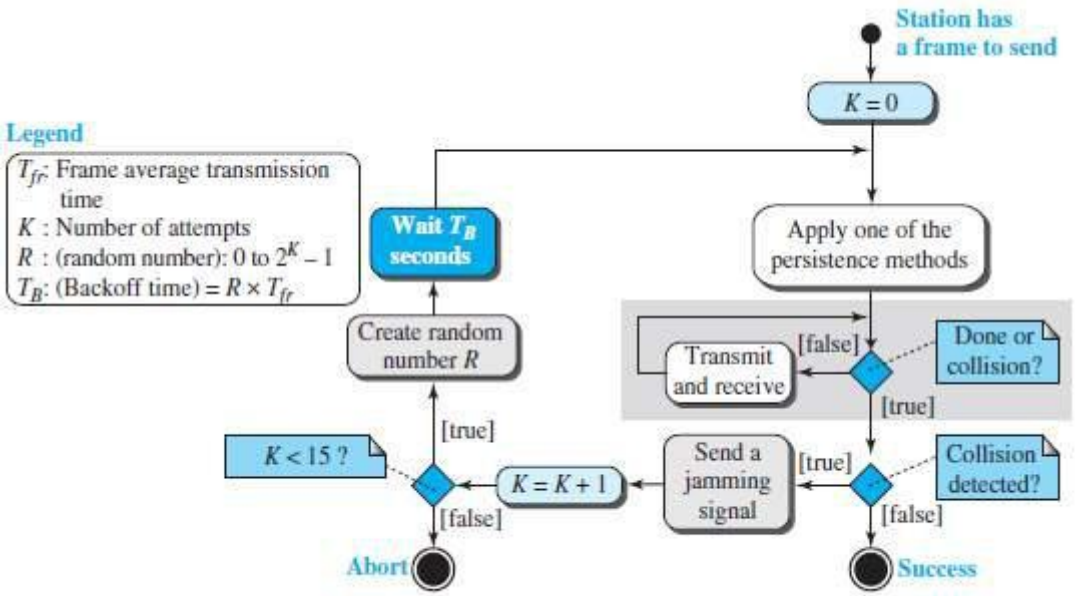


Figure 12.13 *Flow diagram for the CSMA/CD*

4.2.3.3 Energy Level

- In a channel, the energy-level can have 3 values: 1) Zero 2) Normal and 3) Abnormal.
  1) At zero level, the channel is idle (Figure 12.14).
  2) At normal level, a station has successfully captured the channel and is sending its frame. 3) At abnormal level, there is a collision and the level of the energy is twice the normal level.
- A sender needs to monitor the energy-level to determine if the channel
  is → Idle
  → Busy or
  → Collision mode

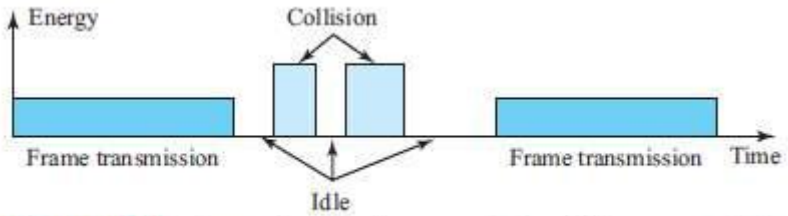


Figure 12.14 *Energy level during transmission, idleness, or collision*

4.2.3.4 Throughput

The throughput of CSMA/CD is greater than pure or slotted ALOHA.

The maximum throughput is based on

different value of G

persistence method used (non-persistent, 1-persistent, or p-persistent) and

'p" value in the p-persistent method.

For 1-persistent method, the maximum throughput is 50% when G =1.

For non-persistent method, the maximum throughput is 90% when G is between 3 and 8.

4.2.4 CSMA/CA

Here is how it works (Figure 12.15):

A station needs to be able to receive while transmitting to detect a collision.

When there is no collision, the station receives one signal: its own signal.

When there is a collision, the station receives 2 signals:

Its own signal and

Signal transmitted by a second station.

To distinguish b/w these 2 cases, the received signals in these 2 cases must be different.

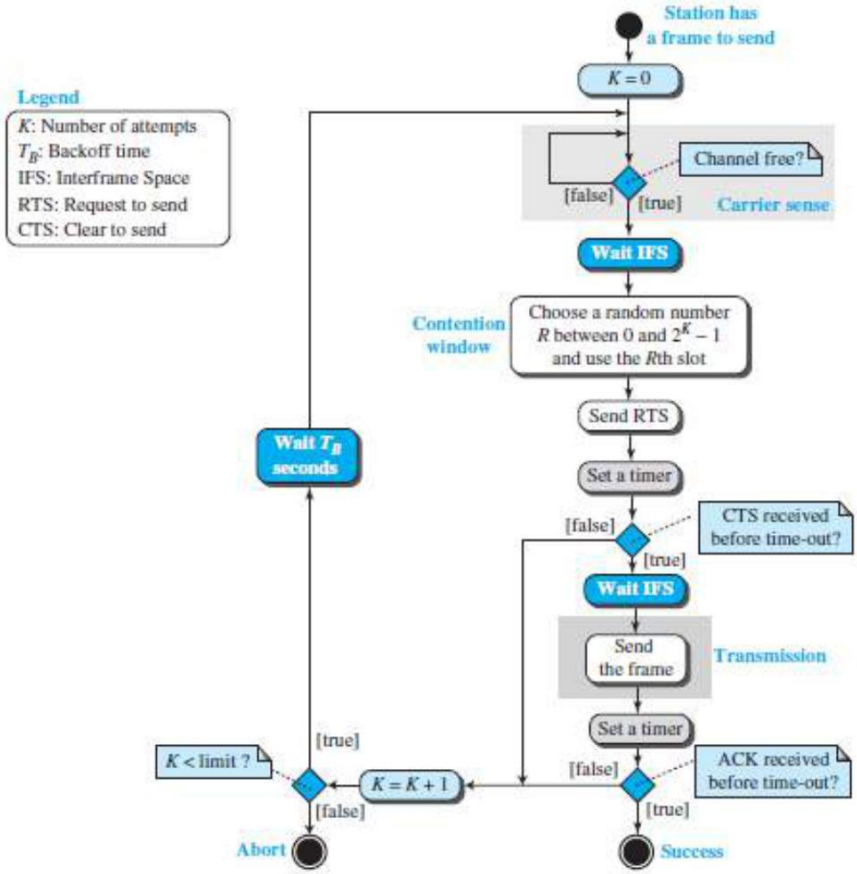


Figure 12.15 *Flow diagram of CSMA/CA*

CSMA/CA was invented to avoid collisions on wireless networks.

Three methods to avoid collisions (Figure 12.16):

Interframe space 2) Contention window and 3) Acknowledgments

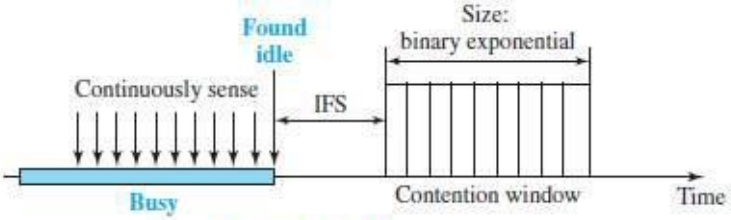


Figure 12.16 *Contention window*

1) Interframe Space (IFS)

Collisions are avoided by deferring transmission even if the channel is found idle.

When the channel is idle, the station does not send immediately.

Rather, the station waits for a period of time called the inter-frame space or IFS.

- After the IFS time,

if the channel is still idle,

then, the station waits for the contention-time &

finally, the station sends the frame.

- IFS variable can also be used to prioritize stations or frame types.

For example, a station that is assigned a shorter IFS has a higher priority.

2) Contention Window

The contention-window is an amount of time divided into time-slots.
A ready-station chooses a random-number of slots as its wait time.
In the window, the number of slots changes according to the binary exponential back-off strategy.
For example:
At first time, number of slots is set to one slot and
Then, number of slots is doubled each time if the station cannot detect an idle channel.

3) Acknowledgment

There may be a collision resulting in destroyed-data.
In addition, the data may be corrupted during the transmission.
To help guarantee that the receiver has received the frame, we can use
Positive acknowledgment and
Time-out timer

Frame Exchange Time Line

- Two control frames are used: 1)
  Request to send (RTS) 2)
  Clear to send (CTS)
- The procedure for exchange of data and control frames in time (Figure 12.17):
  1) The source senses the medium by checking the energy level at the carrier frequency.
  If the medium is idle,
  then the source waits for a period of time called the DCF interframe space (DIFS); finally, the source sends a RTS.
  The destination
  receives the RTS
  waits a period of time called the short interframe space (SIFS)
  sends a control frame CTS to the source.
  CTS indicates that the destination station is ready to receive data.
  The source
  receives the CTS
  waits a period of time SIFS
  sends a data to the destination
  The destination
  receives the data
  waits a period of time SIFS
  sends a acknowledgment ACK to the source.
  ACK indicates that the destination has been received the frame.

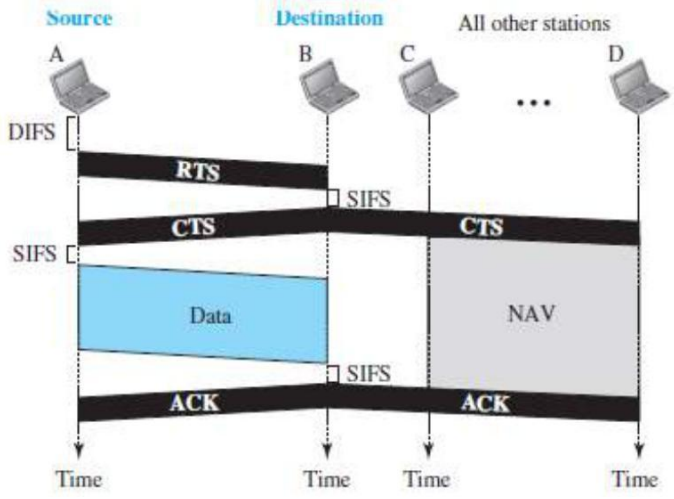


Figure 12.17 *CSMA/CA and NAV*

4.2.4.2 Network Allocation Vector

• When a source-station sends an RTS, it includes the duration of time that it needs to occupy the channel.
• The remaining stations create a timer called a network allocation vector (NAV).
• NAV indicates waiting time to check the channel for idleness.
• Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

4.2.4.3 Collision During Handshaking

• Two or more stations may try to send RTS at the same time.
• These RTS may collide.
• The source assumes there has been a collision if it has not received CTS from the destination.
• The backoff strategy is employed, and the source tries again.

4.2.4.4 Hidden-Station Problem

• Figure 12.17 also shows that the RTS from B reaches A, but not C.
• However, because both B and C are within the range of A, the CTS reaches C.
• Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

4.2.4.5 CSMA/CA and Wireless Networks

CSMA/CA was mostly intended for use in wireless networks.

However, it is not sophisticated enough to handle some particular issues related to wireless networks, such as hidden terminals or exposed terminals.

4.3 CONTROLLED ACCESS PROTOCOLS

Here, the stations consult one another to find which station has the right to send.
A station cannot send unless it has been authorized by other stations.
Three popular controlled-access methods are: 1) Reservation 2) Polling 3) Token Passing

4.3.1 Reservation

Before sending data, each station needs to make a reservation of the medium.
Time is divided into intervals.
In each interval, a reservation-frame precedes the data-frames.
If no. of stations = N, then there are N reservation mini-slots in the reservation-frame.
Each mini-slot belongs to a station.
When a station wants to send a data-frame, it makes a reservation in its own minislot.
The stations that have made reservations can send their data-frames.

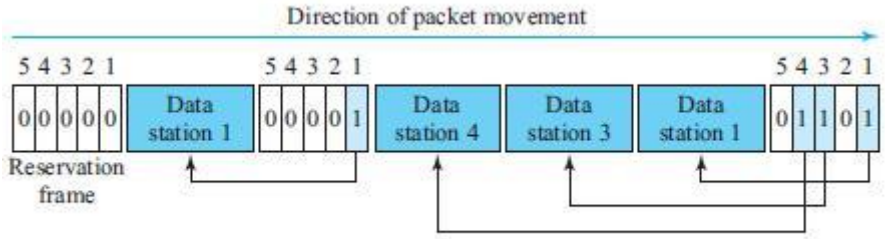


Figure 12.18 *Reservation access method*

For example (Figure 12.18):
5 stations have a 5-minislot reservation-frame.
In the first interval, only stations 1, 3, and 4 have made reservations.
In the second interval, only station-1 has made a reservation.

4.3.2 Polling

- In a network,
  - One device is designated as a primary station and
  - Other devices are designated as secondary stations.

Functions of primary-device:
- The primary-device controls the link.
- The primary-device is always the initiator of a session.
- The primary-device is determines which device is allowed to use the channel at a given time.
- All data exchanges must be made through the primary-device.

The secondary devices follow instructions of primary-device.

Disadvantage: If the primary station fails, the system goes down.

Poll and select functions are used to prevent collisions (Figure 12.19).

Select

If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

The primary
- alerts the secondary about upcoming transmission by sending select frame (SEL)
- then waits for an acknowledgment (ACK) from secondary
- then sends the data frame and
- finally waits for an acknowledgment (ACK) from the secondary.

2) Poll

If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function.

When the first secondary is approached, it responds either
- with a NAK frame if it has no data to send or
- with data-frame if it has data to send.

If the response is negative (NAK frame), then the primary polls the next secondary in the same manner.

When the response is positive (a data-frame), the primary
- reads the frame and
- returns an acknowledgment (ACK frame).

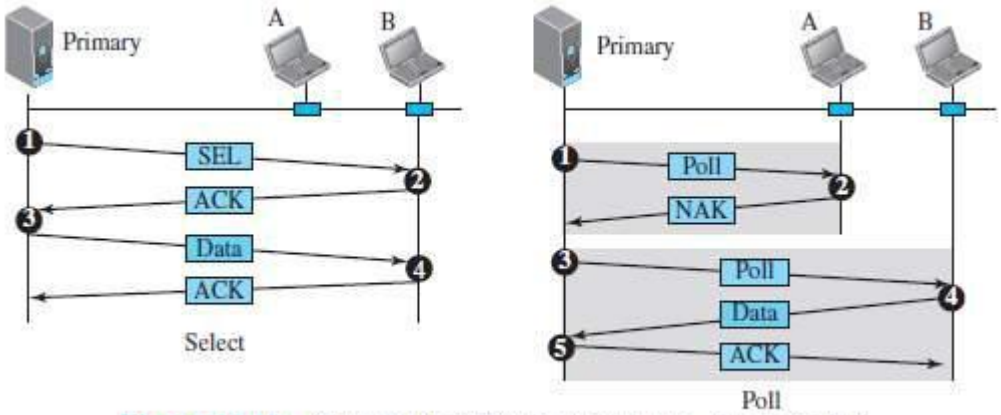


Figure 12.19 *Select and poll functions in polling-access method*

4.3.3 Token Passing

In a network, the stations are organized in a ring fashion i.e. for each station; there is a predecessor and a successor.

The predecessor is the station which is logically before the station in the ring.
The successor is the station which is after the station in the ring.

The current station is the one that is accessing the channel now.
A token is a special packet that circulates through the ring.
Here is how it works:

A station can send the data only if it has the token.
When a station wants to send the data, it waits until it receives the token from its predecessor.
Then, the station holds the token and sends its data.
When the station finishes sending the data, the station
releases the token
passes the token to the successor.

Main functions of token management:

Stations must be limited in the time they can hold the token.
The token must be monitored to ensure it has not been lost or destroyed.
For ex: if a station that is holding the token fails, the token will disappear from the network
Assign priorities
to the stations and
to the types of data being transmitted.
Make low-priority stations release the token to high priority stations.

Logical Ring

In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one.

Four physical topologies to create a logical ring (Figure 12.20):

Physical ring
Dual ring
Bus ring
Star ring

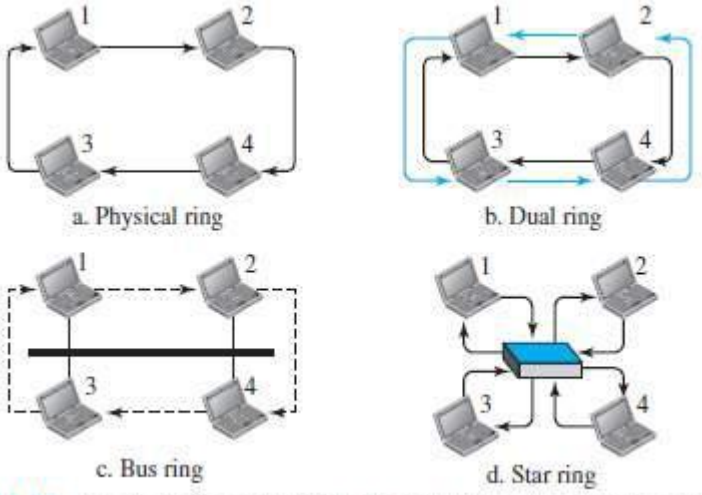


Figure 12.20 *Logical ring and physical topology in token-passing access method*

1) Physical Ring Topology

When a station sends token to its successor, token cannot be seen by other stations. (Figure 12.20a)
This means that the token does not have the address of the next successor.
Disadvantage: If one of the links fails, the whole system fails.

2) Dual Ring Topology

- A second (auxiliary) ring
  - → is used along with the main ring (Figure 12.20b).
  - → operates in the reverse direction compared with the main ring.
  - → is used for emergencies only (such as a spare tire for a car).
- If the main ring fails, the system automatically combines the 2 rings to form a temporary ring.
- After the failed link is restored, the second ring becomes idle again.
- Each station needs to have 2 transmitter-ports and 2 receiver-ports.
- This topology is used in
  - i) FDDI (Fiber Distributed Data Interface) and
  - ii) CDDI (Copper Distributed Data Interface).

3) Bus Ring Topology

- The stations are connected to a single cable called a bus (Figure 12.20c).
- This makes a logical ring, because each station knows the address of its successor and predecessor.
- When a station has finished sending its data, the
  - station → releases the token and
  - → inserts the address of its successor in the token.
- Only the station gets the token to access the shared media.
- This topology is used in the Token Bus LAN.

4) Star Ring Topology

The physical topology is a star (Figure 12.20d).

There is a hub that acts as the connector.

The wiring inside the hub makes the ring i.e. the stations are connected to the ring through the 2 wire connections.

Disadvantages:

This topology is less prone to failure because

If a link goes down,

then the link will be bypassed by the hub and

the rest of the stations can operate.

Also adding and removing stations from the ring is easier.

This topology is used in the Token Ring LAN.

4.4 CHANNELIZATION PROTOCOLS

Channelization is a multiple-access method.
The available bandwidth of a link is shared b/w different stations in time, frequency, or through code.
Three channelization protocols:

FDMA (Frequency Division Multiple Access)
TDMA (Time Division Multiple Access) and
CDMA (Code Division Multiple Access)

4.4.1 FDMA

The available bandwidth is divided into frequency-bands (Figure 12.21).
Each band is reserved for a specific station.
Each station can send the data in the allocated band.
Each station also uses a bandpass filter to confine the transmitter frequencies.
To prevent interferences, small guard bands are used to separate the allocated bands from one another.

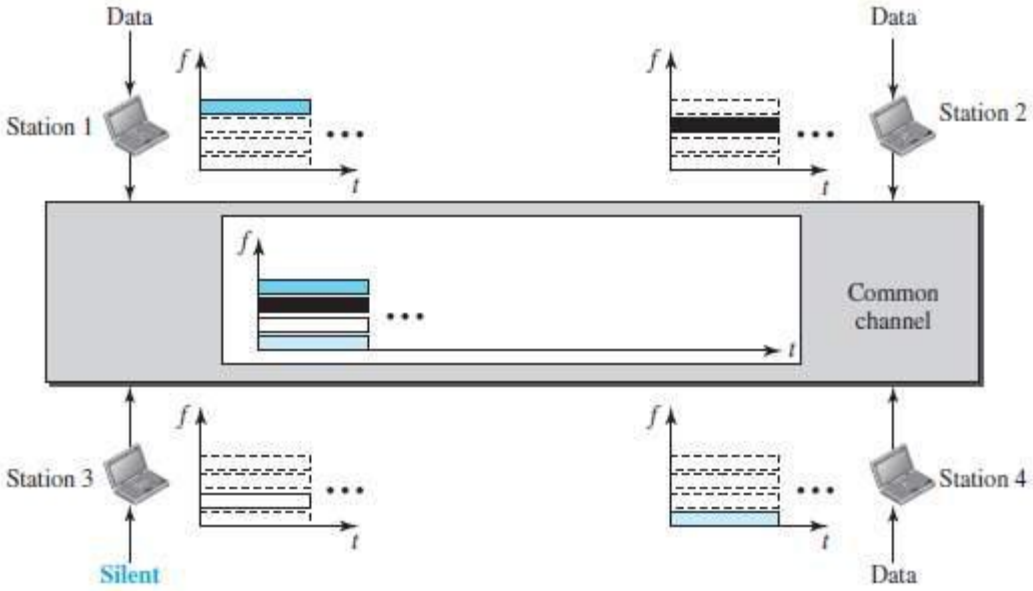


Figure 12.21 *Frequency-division multiple access (FDMA)*

- FDM vs. FDMA

1) FDM

FDM is a multiplexing method in the physical layer.
FDM

combines individual-loads from low-bandwidth channels and
transmits aggregated-load by using a high-bandwidth channel.

The channels that are combined are low-pass.
The multiplexer

modulates & combines the signals and
creates a bandpass signal.

The bandwidth of each channel is shifted by the multiplexer.

2) FDMA

FDMA is an access method in the data link layer.
In each station, the data link layer tells the physical layer to make a bandpass signal from the data passed to it.
The signal must be created in the allocated band.
There is no physical multiplexer at the physical layer.
The signals created at each station are automatically bandpass-filtered.

➢ They are mixed when they are sent to the common channel.

4.4.2 TDMA

The stations share the bandwidth of the channel in time (Figure 12.22).
Each time-slot is reserved for a specific station.
Each station can send the data in the allocated time-slot.

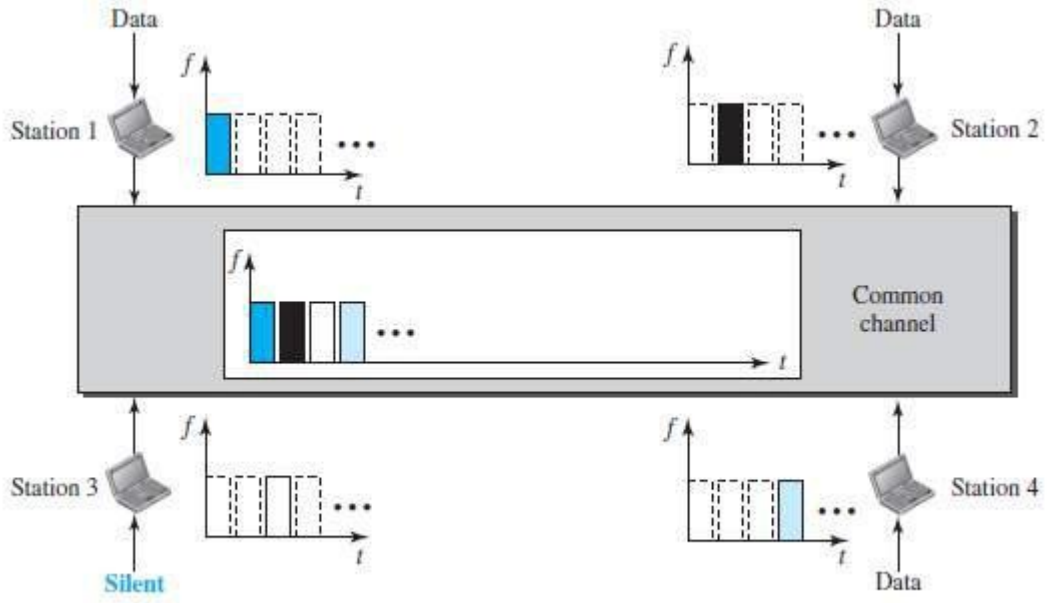


Figure 12.22 *Time-division multiple access (TDMA)*

• Main problem: Achieving synchronization between the different stations.
i.e. each station needs to know the beginning of its slot and the location of its slot. This may be difficult because of propagation delays introduced in the system.

To compensate for the delays, we can insert guard-times.

Normally, synchronization is accomplished by having some synchronization bits at the beginning of each slot.

TDMA vs. TDM

1) TDM

TDM is a multiplexing method in the physical layer.
TDM

combines the individual-data from slower channels and
transmits the aggregated- data by using a faster channel.

The multiplexer interleaves data units from each channel.

2) TDMA

TDMA is an access method in the data link layer.
In each station, the data link layer tells the physical layer to use the allocated time-slot.
There is no physical multiplexer at the physical layer.

4.4.3 CDMA

CDMA simply means communication with different codes.
CDMA differs from FDMA because
only one channel occupies the entire bandwidth of the link.
CDMA differs from TDMA because
all stations can send data simultaneously; there is no timesharing.

(Analogy: CDMA simply means communication with different codes.
For example, in a large room with many people, 2 people can talk privately in English if nobody else understands English. Another 2 people can talk in Chinese if they are the only ones who understand Chinese, and so on).

4.4.3.1 Implementation

Let us assume we have four stations 1, 2, 3, and 4 connected to the same channel.
The data from station-1 are d_1, from station-2 are d_2, and so on.
The code assigned to the first station is c_1, to the second is c_2, and so on.
We assume that the assigned codes have 2 properties.
If we multiply each code by another, we get 0.
If we multiply each code by itself, we get 4 (the number of stations).

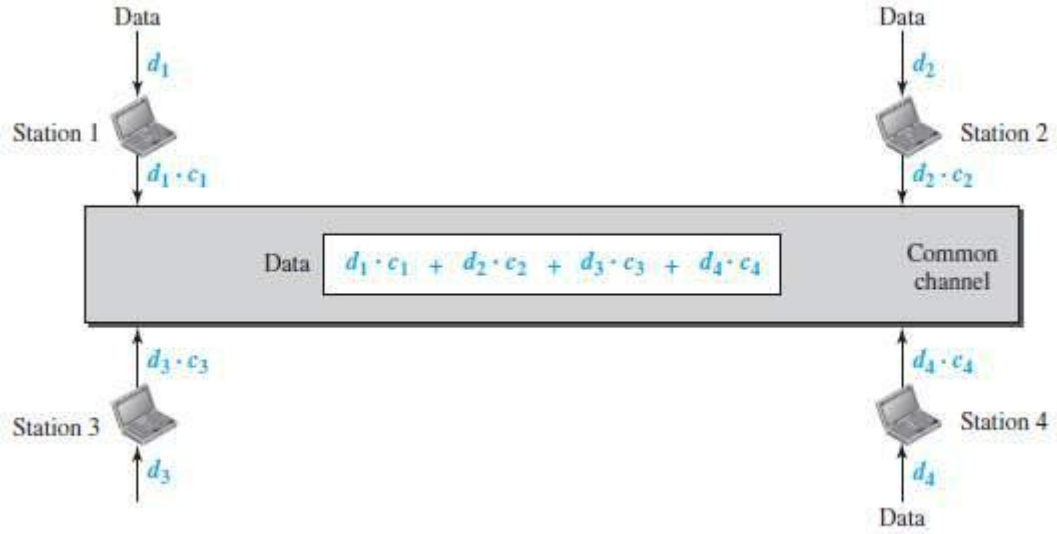


Figure 12.23 *Simple idea of communication with code*

Here is how it works (Figure 12.23):
Station-1 multiplies the data by the code to get $d_1.c_1$.
Station-2 multiplies the data by the code to get $d_2.c_2$. And so on.
The data that go on the channel are the sum of all these terms.

The receiver multiplies the data on the channel by the code of the sender.
For example, suppose stations 1 and 2 are talking to each other.
Station-2 wants to hear what station-1 is saying.
Station-2 multiplies the data on the channel by c_1 the code of station-1.
$(c_1.c_1)=4$, $(c_2.c_1)=0$, $(c_3.c_1)=0$, and $(c_4.c_1)=0$,
Therefore, station-2 divides the result by 4 to get the data from station-1.

$$\text{data} = (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \cdot c_1$$
$$= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 = 4 \times d_1$$

4.4.3.2 Chips

CDMA is based on coding theory.

Each station is assigned a code, which is a sequence of numbers called chips (Figure 12.24).

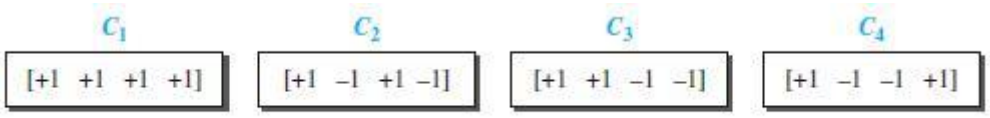


Figure 12.24 *Chip sequences*

These sequences were carefully selected & are called orthogonal sequences

These sequences have the following properties:

Each sequence is made of N elements, where N is the number of stations.

Multiplication of a sequence by a scalar:

If we multiply a sequence by a number i.e. every element in the sequence is multiplied by that element.

For example,

$$2 \cdot [+1 +1 -1 -1] = [+2 +2 -2 -2]$$

3) Inner product of 2 equal sequences:

If we multiply 2 equal sequences, element by element, and add the results, we get N, where N is the number of elements in the each sequence.

For example,

$$[+1 +1 -1 -1] \cdot [+1 +1 -1 -1] = 1 + 1 + 1 + 1 = 4$$

4) Inner product of 2 different sequences:

If we multiply 2 different sequences, element by element, and add the results, we get 0. For example,

$$[+1 +1 -1 -1] \cdot [+1 +1 +1 +1] = 1 + 1 - 1 - 1 = 0$$

5) Adding 2 sequences means adding the corresponding elements. The result is another sequence.

For example,

$$[+1 +1 -1 -1] + [+1 +1 +1 +1] = [+2 +2 \ 0 \ 0]$$

4.4.3.3 Data Representation

We follow the following rules for encoding:

To send a 0 bit, a station encodes the bit as -1

To send a 1 bit, a station encodes the bit as +1

When a station is idle, it sends no signal, which is interpreted as a 0.

4.4.3.4 Encoding and Decoding

We assume that

Stations 1 and 2 are sending a 0 bit.
Station-4 is sending a 1 bit.
Station-3 is silent.

Here is how it works (Figure 12.26):

At the sender-site, the data are translated to -1, -1, 0, and +1.
Each station multiplies the corresponding number by its chip (its orthogonal sequence).
The result is a new sequence which is sent to the channel.
The sequence on the channel is the sum of all 4 sequences.
Now imagine station-3, which is silent, is listening to station-2.

Station-3 multiplies the total data on the channel by the code for station-2, which is [+1 -1 +1-1], to get

$$[-1\ -1\ -3\ +1] \cdot [+1\ -1\ +1\ -1] = -4/4 = -1 \rightarrow \text{bit 1}$$

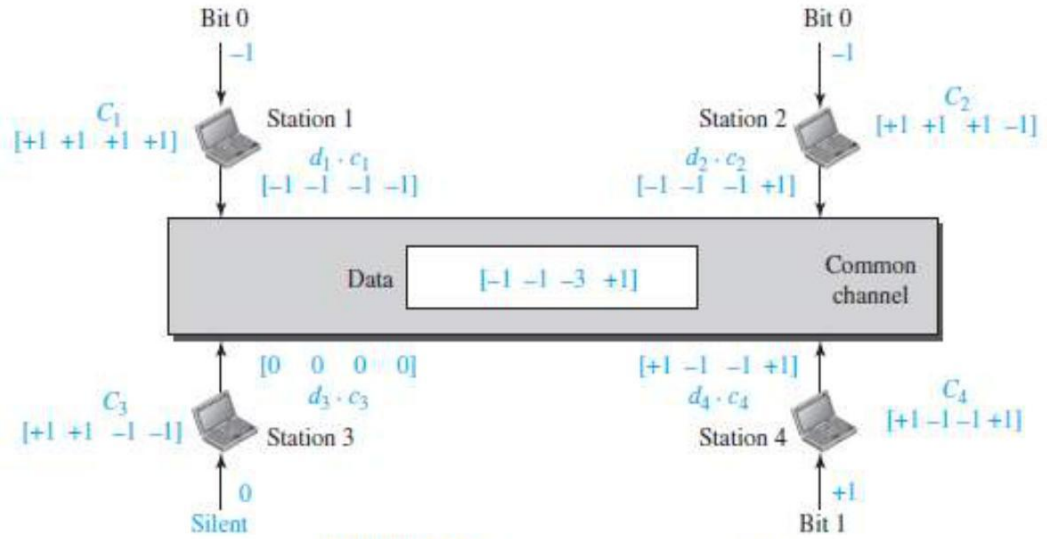
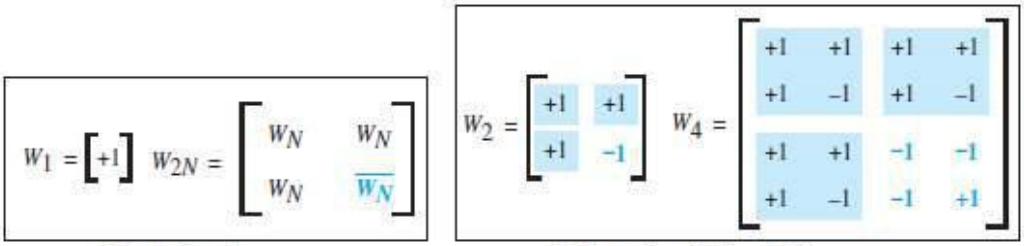


Figure 12.26 *Sharing channel in CDMA*

4.4.3.5 Sequence Generation

To generate chip sequences, we use a Walsh table (Figure 12.29).

Walsh table is a 2-dimensional table with an equal number of rows and columns.



a. Two basic rules b. Generation of W_2 and W_4

Figure 12.29 *General rule and examples of creating Walsh tables*

In the Walsh table, each row is a sequence of chips.

W_1 for a one-chip sequence has one row and one column. We can choose –1 or +1 for the chip for this trivial table (we chose +1).

According to Walsh, if we know the table for N sequences W_N, we can create the table for 2N sequences W_{2N} (Figure 12.29).

The W_N with the overbar W_N stands for the complement of W_N where each +1 is changed to -1 and vice versa.

After we select W_1, W_2 can be made from four W_1's, with the last one the complement of W_1

After W_2 is generated, W_4 can be made of four W_2's, with the last one the complement of W_2.

The number of sequences in a Walsh table needs to be $N = 2^m$.

Example 4.5

Find the chips for a network with

a. Two stations
b. Four stations

Solution

We can use the rows of W_2 and W_4 in Figure 12.29:

a. For a two-station network, we have [+1 +1] and [+1 –1].
b. For a four-station network we have [+1 +1 +1 +1], [+1 –1 +1 –1], [+1 +1 –1 –1], and [+1 –1 –1 +1].

Example 4.6

What is the number of sequences if we have 90 stations in our network?

Solution

The number of sequences needs to be 2^m. We need to choose $m = 7$ and $N = 2^7$ or 128. We can then use 90 of the sequences as the chips.

Example 4.7

Prove that a receiving station can get the data sent by a specific sender if it multiplies the entire data on the channel by the sender's chip code and then divides it by the number of stations.

Solution

Let us prove this for the first station, using our previous four-station example. We can say that the data on the channel $D = (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4)$. The receiver that wants to get the data sent by station 1 multiplies these data by c_1.

$$
\begin{aligned}
D \cdot c_1 &= (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \quad c_1 \\
&= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 \\
&= d_1 \times N + d_2 \times 0 + d_3 \times 0 + d_4 \times 0 \\
&= d_1 \times N
\end{aligned}
$$

When we divide the result by N, we get d_1.

MODULE 4(CONT.): WIRED LANS -- ETHERNET

4.5 ETHERNET PROTOCOL

4.5.1 IEEE Project 802

• The data-link-layer is divided into 2 sublayers (Figure 13.1):

1) LLC

- Flow-control, error-control, and framing duties are grouped into one sublayer called LLC. Framing is handled in both the LLC and the MAC.
- LLC vs. MAC
  - i) LLC provides one single data-link-control protocol for all IEEE LANs. ii) MAC provides different protocols for different LANs.
- A single LLC protocol can provide interconnectivity between different LANs because → it makes the MAC sublayer transparent.

2) MAC

This defines the specific access-method for each LAN.
For example:

CSMA/CD is used for Ethernet LANs.
Token-passing method is used for Token Ring and Token Bus LANs.

The framing function is also handled by the MAC layer.
The MAC contains a number of distinct modules.
Each module defines the access-method and the framing-format specific to the corresponding LAN protocol.

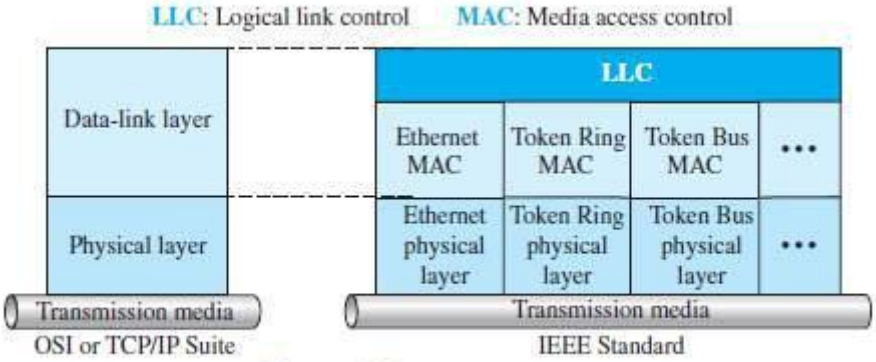


Figure 13.1 *IEEE standard for LANs*

4.5.2 Ethernet Evolution

Four generations of Ethernet (Figure 13.2):
Standard-Ethernet (10 Mbps)
Fast-Ethernet (100 Mbps)
Gigabit-Ethernet (1 Gbps) and
Ten-Gigabit-Ethernet (10 Gbps)

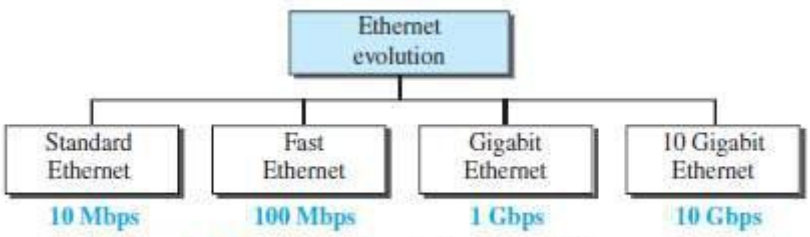


Figure 13.2 *Ethernet evolution through four generations*

4.6 STANDARD-ETHERNET

The original Ethernet technology with data-rate of 10 Mbps are referred to as the Standard Ethernet.

4.6.1 Characteristics

4.6.1.1 Connectionless and Unreliable Service

Ethernet provides a connectionless service. Thus, each frame sent is independent of another frame.
Ethernet has no connection establishment or connection termination phases.
The sender sends a frame whenever it has it.
The receiver may or may not be ready for receiving the frame.
The sender may overload the receiver with frames, which may result in dropping frames.
If a frame drops, the sender will not know about it.
If a frame is corrupted during transmission, the receiver drops the frame.
Since IP is also connectionless, it will also not know about frame drops.
If the transport layer is UDP (connectionless protocol), the frame is lost.
If the transport layer is TCP, the sender-TCP does not receive acknowledgment for its segment and sends it again.
Ethernet is also unreliable like IP and UDP.

4.6.1.2 Frame Format

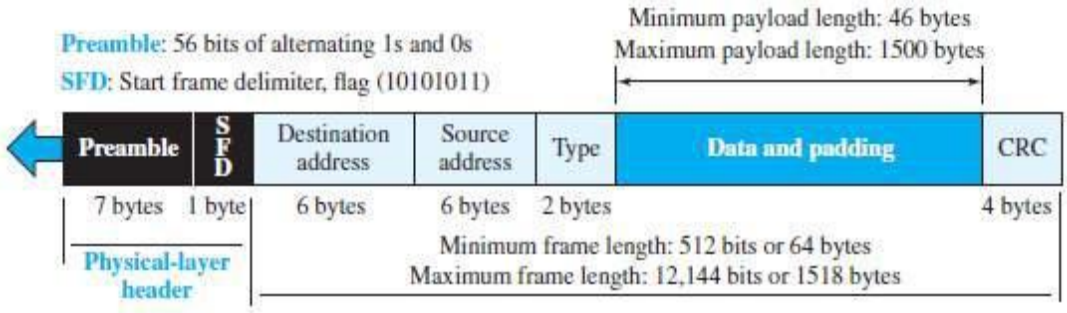


Figure 13.3 *Ethernet frame*

- The Ethernet frame contains 7 fields (Figure 13.3):

1) Preamble

- This field contains 7 bytes (56 bits) of alternating 0s and 1s.

This field
→ alerts the receiving-system to the coming frame and
→ enables the receiving-system to synchronize its input timing.

- The preamble is actually added at the physical-layer and is not (formally) part of the frame.

2) Start frame delimiter (SFD)

This field signals the beginning of the frame.
The SFD warns the stations that this is the last chance for synchronization.
This field contains the value: 10101011.
The last 2 bits (11) alerts the receiver that the next field is the destination-address.

3) Destination-address (DA)

This field contains the physical-address of the destination-station.

4) Source-address (SA)

This field contains the physical-address of the sender-station.

5) Length or type

This field is defined as a i) type field or ii) length field.
In original Ethernet, this field is used as the type field.
Type field defines the upper-layer protocol using the MAC frame.
In IEEE standard, this field is used as the length field.
Length field defines the number of bytes in the data-field.

6) Data

- This field carries data encapsulated from the upper-layer protocols.
- Minimum data size = 46 bytes. Maximum data size = 1500 bytes.

7) CRC

- This field contains error detection information such as a CRC-32.

4.6.1.3 Frame Length

• Ethernet has imposed restrictions on both minimum & maximum lengths of a frame (Figure 13.5).

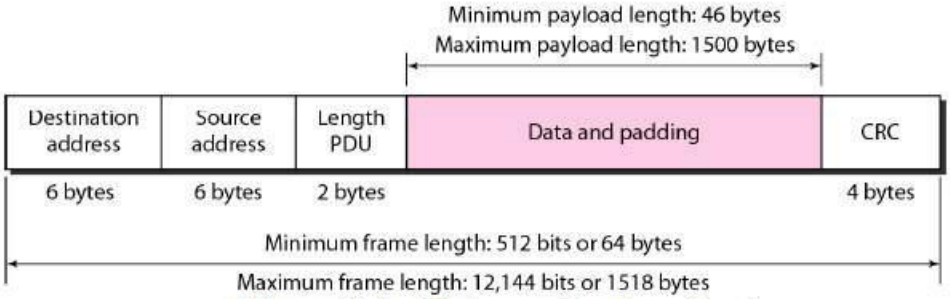


Figure 13.5 *Minimum and maximum lengths*

The minimum length restriction is required for the correct operation of CSMA/CD.
Minimum length of frame = 64 bytes.

Minimum data size = 46 bytes.

Header size + Trailer size = 14 + 4 = 18 bytes.

(i.e. 18 bytes ➔ 6 bytes source-address + 6 bytes dest-address + 2 bytes length + 4 bytes CRC).

The minimum length of data from the upper layer = 46 bytes.
If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.
Maximum length of frame =1518 bytes.

Maximum data size = 1500 bytes.

Header size + trailer size = 14 + 4 = 18 bytes.

The maximum length restriction has 2 reasons:

Memory was very expensive when Ethernet was designed.

A maximum length restriction helped to reduce the size of the buffer.

This restriction prevents one station from

monopolizing the shared medium

blocking other stations that have data to send.

4.6.2 Addressing

In an Ethernet-network, each station has its own NIC (6-byte → 48 bits).

The NIC provides the station with a 6-byte physical-address (or Ethernet-address).

For example, the following shows an Ethernet MAC address:

06:01 :02:01:2C:4B

6 bytes = 12 hex digits = 48 bits

(NIC → network interface card)

Example 4.8

Show how the address 47:20:1B:2E:08:EE is sent out online.

Solution

The address is sent left to right, byte by byte; for each byte, it is sent right to left, bit by bit, as shown below

Hexadecimal	47	20	1B	2E	08	EE
Binary	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

4.6.2.1 Unicast, Multicast, and Broadcast Addresses

A source-address is always a unicast address i.e. the frame comes from only one station.

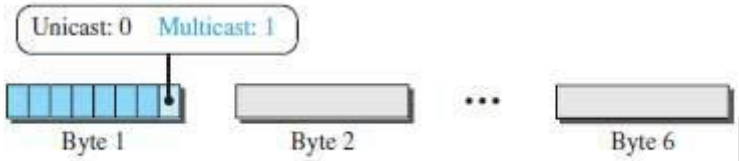


Figure 13.4 *Unicast and multicast addresses*

However, the destination-address can be 1) Unicast 2) Multicast or 3) Broadcast.

As shown in Figure 13.4,

If LSB of first byte in a destination-address is 0,

Then, the address is unicast;

Otherwise, the address is multicast.

A unicast destination-address defines only one recipient.

The relationship between the sender and the receiver is one-to-one.

A multicast destination-address defines a group of addresses.

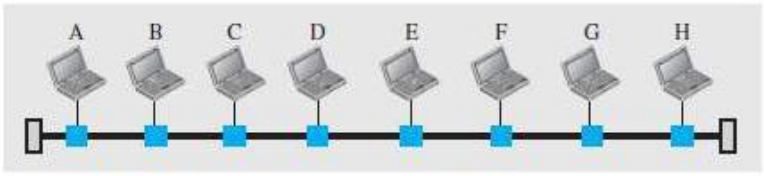
The relationship between the sender and the receivers is one-to-many.

The broadcast address is a special case of the multicast address.

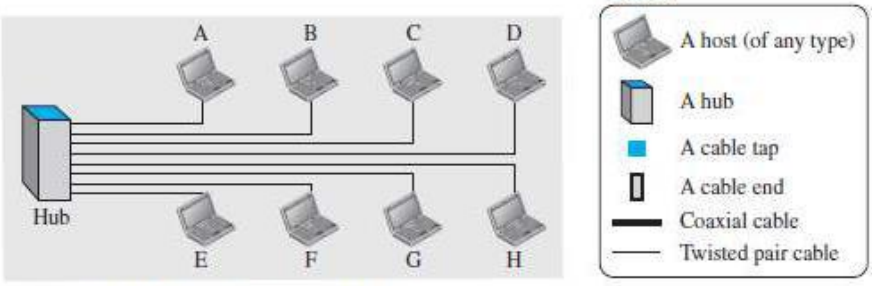
The recipients are all the stations on the LAN.

A broadcast destination-address is 48 1s (6-byte → 48 bits).

Standard Ethernet uses a coaxial cable (bus topology) or a set of twisted-pair cables with a hub (star topology) (Figure 13.5).



a. A LAN with a bus topology using a coaxial cable



b. A LAN with a star topology using a hub

Figure 13.5 *Implementation of standard Ethernet*

• Question: How actual unicast, multicast & broadcast transmissions are distinguished from each other?

Answer: The way the frames are kept or dropped.

In a unicast transmission, all stations will receive the frame, the intended recipient keeps and handles the frame; the rest discard it.

In a multicast transmission, all stations will receive the frame, the stations that are members of the group keep and handle it; the rest discard it.

In a broadcast transmission, all stations (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

Example 4.9

Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are Fs, the address is broadcast. Therefore, we have the following:

a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are Fs in hexadecimal.

4.6.3 Access-method

Standard-Ethernet uses 1-persistent CSMA/CD.

1) Slot Time

Slot time = round-trip time + time required to send the jam sequence.

The RTT means time required for a frame to travel from one end of a maximum-length network to the other end (RTT → round-trip time).

The slot time is defined in bits.

The slot time is the time required for a station to send 512 bits.

The actual slot time depends on the data-rate.

For example: 10-Mbps Ethernet has slot time of 51.2 μs.

2) Slot Time and Collision

The choice of a 512-bit slot time was not accidental.

It was chosen to allow the proper functioning of CSMA/CD.

3) Slot Time and Maximum Network Length

There is a relationship between
slot time and
maximum length of the network (collision domain).

This relationship is dependent on the propagation-speed of the signal in the particular medium.

In most transmission media, the signal propagates at $2x10^8$ m/s (two-thirds of the rate for propagation in air).

For traditional Ethernet, we calculate

$$\text{MaxLength} = \text{PropagationSpeed} \times \frac{\text{SlotTime}}{2}$$

$$\text{MaxLength} = (2 \times 10^8) \times (51.2 \times 10^{-6})/2 = 5120\text{m}$$

4.6.4 Efficiency of Standard Ethernet

The efficiency is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station.

The practical efficiency of standard Ethernet has been measured to be

$$\text{Efficiency} = 1 / (1 + 6.4 \times a)$$

where a = number of frames that can fit on the medium.

a = (propagation delay)/(transmission delay)

As the value of parameter a decreases, the efficiency increases.

If the length of the media is shorter or the frame size longer, the efficiency increases.

In the ideal case, a = 0 and the efficiency is 1.

Example 4.10

In the Standard Ethernet with the transmission rate of 10 Mbps, we assume that the length of the medium is 2500 m and the size of the frame is 512 bits. The propagation speed of a signal in a cable is normally 2×10^8 m/s.

Propagation delay = $2500/(2 \times 10^8) = 12.5\ \mu s$	Transmission delay = $512/(10^7) = 51.2\ \mu s$
$a = 12.5/51.2 = 0.24$	Efficiency = 39%

4.6.5 Implementation

• The Standard-Ethernet defines several physical-layer implementations (Table 13.1).

Table 13.1 *Summary of Standard Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000 m	Manchester

4.6.5.1 Encoding and Decoding

All standard implementations use digital-signaling (baseband) at 10 Mbps (Figure 13.6).

At the sender, data are converted to a digital-signal using the Manchester scheme.

At the receiver, the received-signal is interpreted as Manchester and decoded into data.

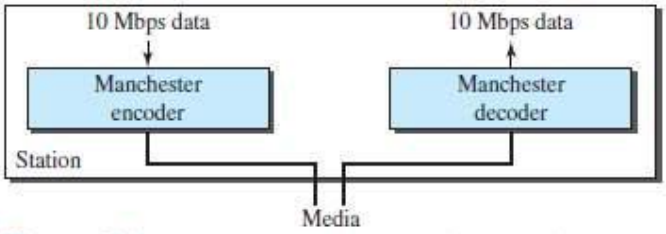


Figure 13.6 *Encoding in a Standard Ethernet implementation*

1) 10Base5: Thick Ethernet

10Base5 uses a bus topology (Figure 13.7).

A external transceiver is connected to a thick coaxial-cable. (transceiver → transmitter/receiver)

The transceiver is responsible for
- transmitting
- receiving and
- detecting collisions.

The transceiver is connected to the station via a coaxial-cable. The cable provides separate paths for sending and receiving.

The collision can only happen in the coaxial cable.

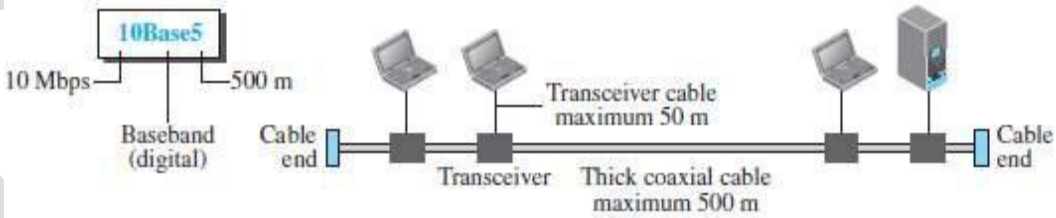


Figure 13.7 *10Base5 implementation*

➢ The maximum-length of the cable must not exceed 500m.

If maximum-length is exceeded, then there will be excessive degradation of the signal.

If a cable-length of more than 500 m is needed, the total cable-length can be divided into up to 5 segments.

Each segment of maximum length 500-meter, can be connected using repeaters.

2) 10Base2: Thin Ethernet

10Base2 uses a bus topology (Figure 13.8).

The cable is much thinner and more flexible than 10Base5.

Flexible means the cable can be bent to pass very close to the stations.

The transceiver is part of the NIC, which is installed inside the station.

The collision can only happen in the coaxial cable.

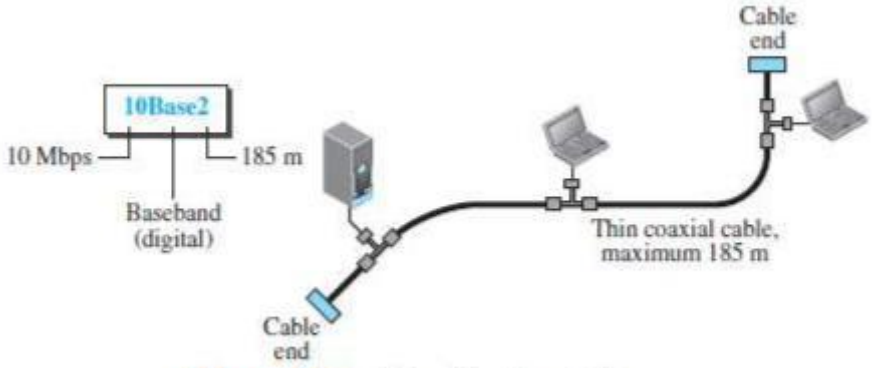


Figure 13.8 *10Base2 implementation*

Advantages:

Thin coaxial-cable is less expensive than thick coaxial-cable.
Tee connections are much cheaper than taps.
Installation is simpler because the thin coaxial cable is very flexible.

Disadvantage:

Length of each segment cannot exceed 185m due to the high attenuation in the cable.

3)10Base- T: Twisted-Pair Ethernet

10Base-T uses a star topology to connect stations to a hub (Figure 13.9).
The stations are connected to a hub using two pairs of twisted-cable.

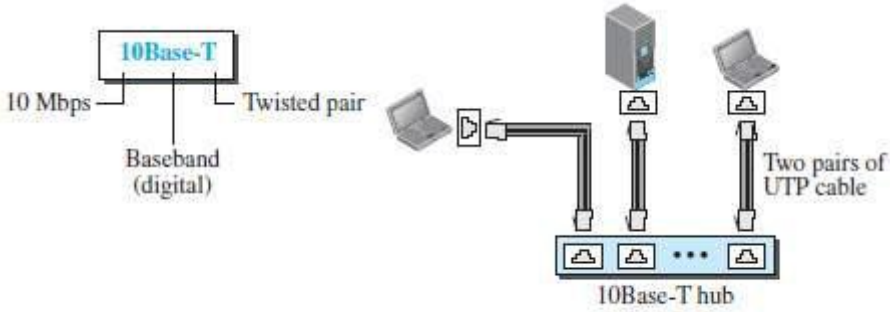


Figure 13.9 *10Base-T implementation*

Two pairs of twisted cable create two paths between the station and the hub.

First path for sending.
Second path for receiving.

The collision can happen in the hub.
The maximum length of the cable is 100 m. This minimizes the effect of attenuation in the cable.

4) 10Base-F: Fiber Ethernet

10Base-F uses a star topology to connect stations to a hub (Figure 13.10).
The stations are connected to the hub using two fiber-optic cables.

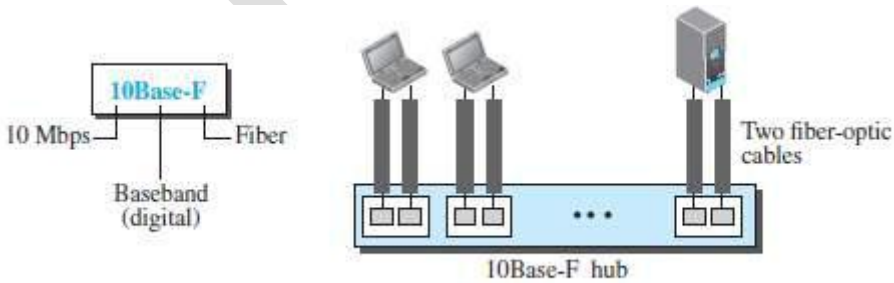


Figure 13.10 *10Base-F implementation*

4.6.6 Changes in the Standard

4.6.6.1 Bridged Ethernet

Bridges have two effects on an Ethernet LAN:

They raise the bandwidth &

They separate collision domains.

1) Raising the Bandwidth

A bridge divides the network into two or more networks.

Bandwidth-wise, each network is independent.

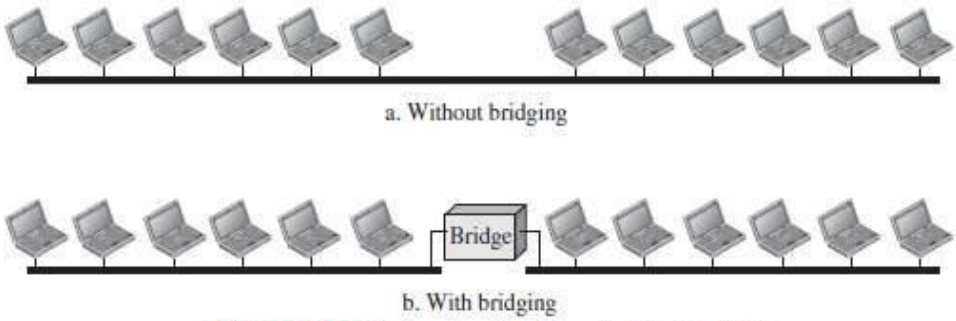


Figure 13.12 *A network with and without a bridge*

For example (Figure 13.12):

A network with 12 stations is divided into two networks, each with 6 stations.
Now each network has a capacity of 10 Mbps.
The 10-Mbps capacity in each segment is now shared between 6 stations (actually 7 because the bridge acts as a station in each segment), not 12 stations.

- In a network with a heavy load, each station theoretically is offered 10/7 Mbps instead of 10/12 Mbps.

2) Separating Collision Domains

Another advantage of a bridge is the separation of the collision domain.

Figure 13.13 shows the collision domains for an un-bridged and a bridged network.

You can see that the collision domain becomes much smaller and the probability of collision is reduced tremendously.

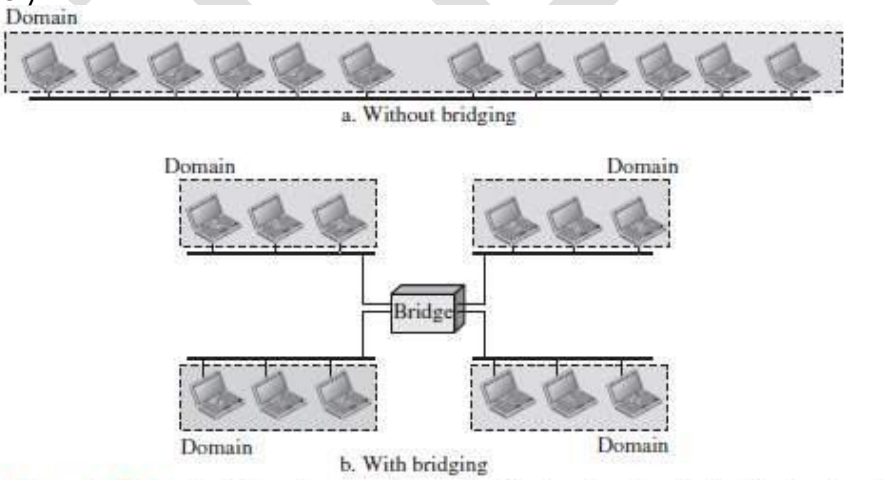


Figure 13.13 *Collision domains in an unbridged network and a bridged network*

4.6.6.2 Switched Ethernet

The idea of a bridged LAN can be extended to a switched LAN (Figure 13.14).

If we can have a multiple-port bridge, we can have an N-port switch.

In this way, the bandwidth is shared only between the station and the switch.

A layer-2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets.

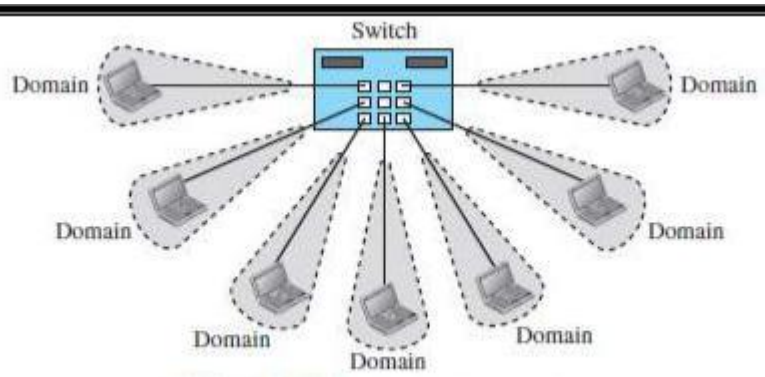


Figure 13.14 *Switched Ethernet*

4.6.6.3 Full-Duplex Ethernet

The full-duplex mode increases the capacity of each domain from 10 to 20 Mbps.

Instead of using one link between the station and the switch, the configuration uses two links: one to transmit and one to receive.

1) No Need for CSMA/CD

In full-duplex switched Ethernet,

There is no need for the CSMA/CD method.

Each station is connected to the switch via two separate links.

Each station or switch can send and receive independently without worrying about collision.

Each link is a point-to-point dedicated path between the station and the switch.

There is no longer a need for carrier sensing; there is no longer a need for collision-detection.

The job of the MAC layer becomes much easier.

Carrier sensing and collision-detection functionalities of the MAC sublayer can be turned off.

MAC Control Layer

To provide for flow and error control in full-duplex switched Ethernet, a new sublayer, called the MAC control, is added between the LLC sublayer and the MAC sublayer.

4.7 FAST ETHERNET (100 MBPS)

IEEE created Fast-Ethernet under the name 802.3u.
Fast-Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel.
Goals of Fast-Ethernet:

- Upgrade the data-rate to 100 Mbps.
- Make it compatible with Standard-Ethernet.
- Keep the same 48-bit address.
- Keep the same frame format.
- Keep the same minimum and maximum frame-lengths.

4.7.1 Access Method

Access method is same in Standard-Ethernet.
Only the star topology is used.
For the star topology, there are 2 choices:

- In the half-duplex approach, the stations are connected via a hub. CSMA/CD was used as access-method.
- In the full-duplex approach, the connection is made via a switch with buffers at each port. There is no need for CSMA/CD.

Autonegotiation

A new feature added to Fast-Ethernet is called autonegotiation.
It provides a station/hub with a range of capabilities.
It was used for the following purposes:

- To allow 2 devices to negotiate the mode or data-rate of operation.
- To allow incompatible devices to connect to one another.
  - For example: a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity.
- To allow one device to have multiple capabilities.
- To allow a station to check a hub's capabilities.

4.7.2 Physical-layer

The physical-layer in Fast-Ethernet is more complicated than the one in Standard-Ethernet. Some of the features of this layer are as follows. 1) Topology 2) Implementation and 3) Encoding.

4.7.2.1 Topology

Fast-Ethernet is used to connect two or more stations together (Figure 13.19).

If there are only 2 stations, they can be connected in point-to-point.

If there are 3 or more stations, they can be connected in star topology with a hub at the center.

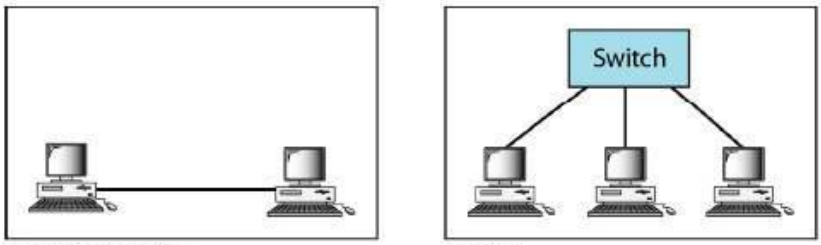


Figure 13.19 *Fast Ethernet topology*

4.7.2.2 Implementation

Fast-Ethernet can be classified as either a two-wire or a four-wire implementation (Table 13.2).

The 2-wire implementations use

Category 5 UTP (100Base-TX) or

Fiber-optic cable (100Base-FX)

The 4-wire implementations use category 3 UTP (100Base-T4).

Table 13.2 *Summary of Fast Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	UTP or STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

4.7.2.3 Encoding

There are 3 different encoding schemes.

100Base-TX

This uses 2 pairs of twisted-pair cable (either category 5 UTP or STP) (Figure 13.16a).
The MLT-3 encoding scheme is used for implementation.

➢ This is because MLT -3 has good bandwidth performance.

However, 4B/5B block-coding is used to provide bit synchronization.

This is because MLT-3 is not a self-synchronous line coding scheme.

4B/5B coding creates a data-rate of 125 Mbps, which is fed into MLT-3 for encoding.

2) 100Base-FX

This uses 2 pairs of fiber-optic cables (Figure 13.16b).
Optical fiber can easily handle high bandwidth requirements.
The NRZ-I encoding scheme is used for implementation.
However, 4B/5B block-coding is used to provide bit synchronization.

This is because NRZ-I is not a self-synchronous line coding scheme.

4B/5B encoding increases the bit rate from 100 to 125 Mbps, which can easily be handled by fiber-optic cable.

3) 100Base-T4

This uses 4 pairs of UTP for transmitting 100 Mbps (Figure 13.16c).
Each UTP cannot easily handle more than 25 Mbaud.
One pair switches between sending and receiving.
Three pairs of UTP can handle only 75 Mbaud (25 Mbaud) each.
Encoding/decoding is more complicated.

We need an encoding scheme that converts 100 Mbps to a 75 Mbaud signal. This requirement is satisfied by 8B/6T.

The 8B/6T encoding scheme is used for implementation.

8 data elements are encoded as 6 signal elements.

This means that 100 Mbps uses only (6/8) x 100 Mbps, or 75 Mbaud.

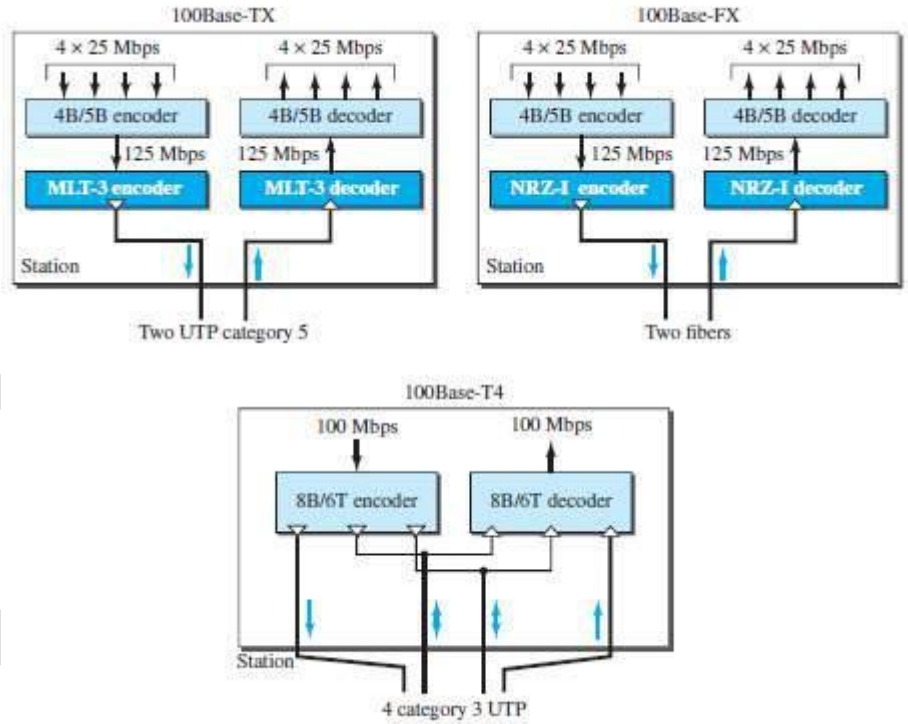


Figure 13.16 *Encoding for Fast Ethernet implementation*

4.8 GIGABIT ETHERNET

IEEE created Gigabit-Ethernet under the name 802.3z.

Goals of Gigabit-Ethernet:

Upgrade the data-rate to 1 Gbps.
Make it compatible with Standard or Fast-Ethernet.
Use the same 48-bit address.
Use the same frame format.
Keep the same minimum and maximum frame-lengths.
To support auto-negotiation as defined in Fast-Ethernet.

4.8.1 MAC Sublayer

Gigabit-Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex.
Almost all implementations of Gigabit-Ethernet follow the full-duplex approach.

1) Full-Duplex Mode

There is a central switch connected to all computers or other switches.
Each switch has buffers for each input-port in which data are stored until they are transmitted.
There is no collision. This means that CSMA/CD is not used.
Lack of collision implies that
the maximum length of the cable is determined
→ by the signal attenuation in the cable &
→ not by the collision-detection process.

2) Half-Duplex Mode

- A switch is replaced by a hub, which acts as the common cable in which a collision might occur.
- CSMA/CD is used.
- The maximum length of the network is totally dependent on the minimum frame size.
- Three methods have been defined: traditional, carder extension, and frame bursting. **i) Traditional**

➢ Like traditional Ethernet, the minimum length of a frame is 512 bits. ➢
However, because the length of a bit is 1/100 shorter,
Slot time is 512 bits x 1/1000 gs which is equal to 0.512 gs. ➢
The reduced slot time means that collision is detected 100 times earlier.
The maximum length of the network is 25 m.
This length may be suitable if all the stations are in one room. **ii) Carrier Extension**
To allow for a longer network, we increase the minimum frame-length.
Minimum length of frame is 512 bytes (4096 bits). Thus, minimum length is 8 times longer.
A station adds extension bits (padding) to any frame that is less than 4096 bits.
The maximum length of the network is 200 m.
A length from the hub to the station is 100 m.

iii) Frame Bursting

Carrier extension is very inefficient if
we have a series of short frames to send
each frame carries redundant data.
To improve efficiency, frame bursting was proposed.
Instead of adding an extension to each frame, multiple frames are sent.
However, to make these multiple frames look like one frame, padding is added between the frames. Thus, the channel is not idle.

4.8.2 Physical-layer

The physical-layer in Gigabit-Ethernet is more complicated than that in Standard or Fast-Ethernet. Some of the features of this layer are as follows. 1) Topology 2) Implementation and 3) Encoding.

4.8.2.1 Topology

Gigabit-Ethernet is used to connect two or more stations together.

If there are only 2 stations, they can be connected in point-to-point.

If there are 3 or more stations, they can be connected in star topology with a hub at center.

4.8.2.2 Implementation

Gigabit-Ethernet can be classified as either a two-wire or a four-wire implementation (Table 13.3).

The 2-wire implementations use

Fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave) or STP (1000Base-CX)

The 4-wire implementations use category 5 twisted-pair cable (1000Base-T).

Table 13.3 *Summary of Gigabit Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

4.8.2.3 Encoding

1) Two-wire Implementation

The NRZ encoding scheme is used for two-wire implementation (Figure 13.17a).

However, 8B/10B block-coding is used to provide bit synchronization.

This is because NRZ is not a self-synchronous line coding scheme.

8B/10B coding creates a data-rate of 1.25 Gbps.

One wire (fiber or STP) is used for sending.

Another wire is used for receiving.

2) Four-wire Implementation

In this, it is not possible to have 2 wires for input and 2 for output (Figure 13.17b).

This is „." each wire would need to carry 500 Mbps, which exceeds the capacity for category 5 UTP.

As a solution, 4D-PAM5 encoding is used to reduce the bandwidth.

Thus, all four wires are involved in both input and output.

Each wire carries 250 Mbps, which is in the range for category 5 UTP cable.

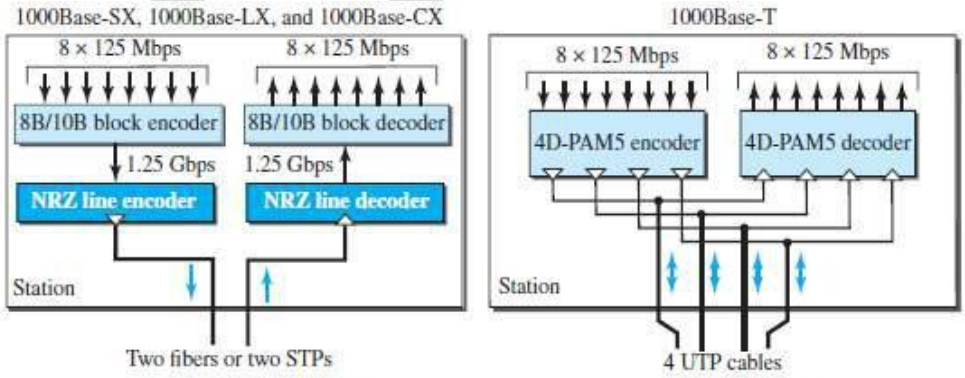


Figure 13.17 *Encoding in Gigabit Ethernet implementations*

4.9 TEN GIGABIT ETHERNET

IEEE created Ten-Gigabit-Ethernet under the name 802.3ae.

Goals of the Gigabit-Ethernet:

- Upgrade the data-rate to 10 Gbps.
- Make it compatible with Standard, Fast, and Gigabit-Ethernet.
- Use the same 48-bit address.
- Use the same frame format.
- Keep the same minimum and maximum frame-lengths.
- Allow the interconnection of existing LANs into a MAN or a WAN .
- Make Ethernet compatible with technologies such as Frame Relay and ATM.

4.9.1 Implementation

Ten-Gigabit-Ethernet operates only in full duplex mode.

This means there is no need for contention; CSMA/CD is not used.

Four implementations are the most common (Table 13.4):

- 10GBase-SR
- 10GBase-LR
- 10GBase-EW and
- 10GBase-X4

Table 13.4 *Summary of 10 Gigabit Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Number of wires*	*Encoding*
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

MODULE 4(CONT.): WIRELESS-LANS

4.10 INTRODUCTION OF WIRELESS-LANS

4.10.1 Architectural Comparison

1) Medium

In a wired LAN, we use wires to connect hosts.

In a switched LAN, with a link-layer switch, the communication between the hosts is point-to-point and full-duplex (bidirectional).

In a wireless LAN, the medium is air, the signal is generally broadcast.

When hosts in a wireless LAN communicate with each other, they are sharing the same medium (multiple access).

2) Hosts

In a wired LAN, a host is always connected to its network at a point with a fixed link layer address related to its network interface card (NIC).

Of course, a host can move from one point in the Internet to another point.

In this case, its link-layer address remains the same, but its network-layer address will change.

In a wireless LAN, a host is not physically connected to the network; it can move freely and can use the services provided by the network.

Therefore, mobility in a wired network and wireless network are totally different issues.

3) Isolated LANs

A wired isolated LAN is a set of hosts connected via a link-layer switch (Figure 15.1).

A wireless isolated LAN, called an ad hoc network in wireless LAN terminology, is a set of hosts that communicate freely with each other.

The concept of a link-layer switch does not exist in wireless LANs.

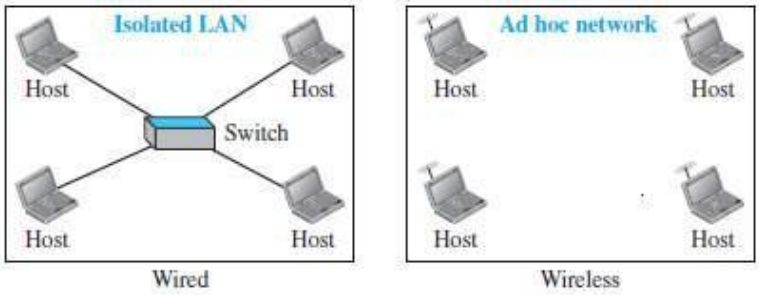


Figure 15.1 *Isolated LANs: wired versus wireless*

4) Connection to Other Networks

A wired LAN can be connected to another network or the Internet using a router.

A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN (Figure 15.2).

In this case, the wireless LAN is referred to as an infrastructure network, and the connection to the wired infrastructure, such as the Internet, is done via a device called an access point (AP).

An access point is gluing two different environments together: one wired and one wireless.

Communication between the AP and the wireless host occurs in a wireless environment.

Communication between the AP and the infrastructure occurs in a wired environment.

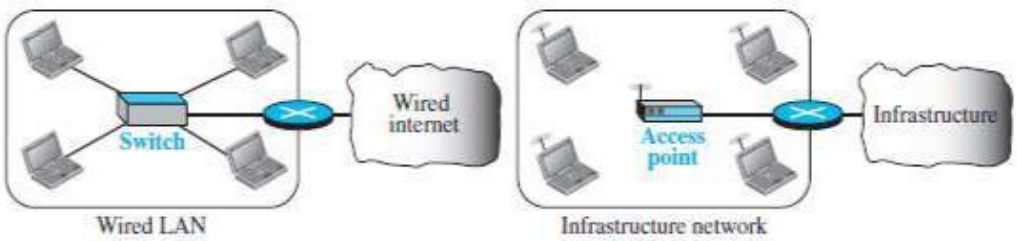


Figure 15.2 *Connection of a wired LAN and a wireless LAN to other networks*

Characteristics

1) Attenuation

• The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver.

• The situation becomes worse with mobile senders that operate on batteries and normally have small power supplies.

2) Interference

• Another issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.

3) Multipath Propagation

• A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects.

• The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.

4) Error

• Error detection is more serious issues in a wireless network than in a wired network.

If SNR is high, it means that the signal is stronger than the noise (unwanted signal), so we may be able to convert the signal to actual data.

When SNR is low, it means that the signal is corrupted by the noise and the data cannot be recovered.

Access Control

The CSMA/CD algorithm does not work in wireless LANs for three reasons:

To detect a collision, a host needs to send and receive at the same time which means the host needs to work in a duplex mode. Wireless hosts do not have enough power to do so (the power is supplied by batteries).

They can only send or receive at one time.

The distance between stations can be great.

Signal fading could prevent a station at one end from hearing a collision at other end.

Because of the hidden station problem, in which a station may not be aware of another station"s transmission due to some obstacles or range problems, collision may occur but not be detected.

Hidden station problem

Figure 15.3 shows an example of the hidden station problem.

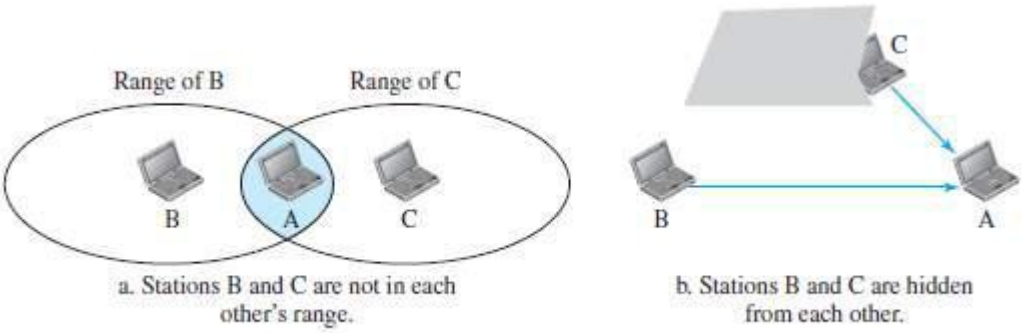
Every station in transmission range of Station B can hear any signal transmitted by station B.

Every station in transmission range of Station C can hear any signal transmitted by station C.

Station C is outside the transmission range of B;

Likewise, station B is outside the transmission range of C. ¤ However, Station A is in the area covered by both B and C;

Therefore, Station A can hear any signal transmitted by B or C.



a. Stations B and C are not in each other's range.

b. Stations B and C are hidden from each other.

Figure 15.3 *Hidden station problem*

4.11 IEEE 802.11

4.11.1 Architecture

• The standard defines 2 kinds of services: 1) Basic service set (BSS) and
2) Extended service set (ESS).

4.11.1.1 BSS

• IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless-LAN.
• A basic service set is made of (Figure 15.4):
→ stationary or mobile wireless stations and
→ optional central base station, known as the access point (AP).
• There are 2 types of architecture:

1) Ad hoc Architecture

- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. Stations can form a network without the need of an AP.
- Stations can locate one another and agree to be part of a BSS.

2) Infrastructure Network

- A BSS with an AP is referred to as an infrastructure network.

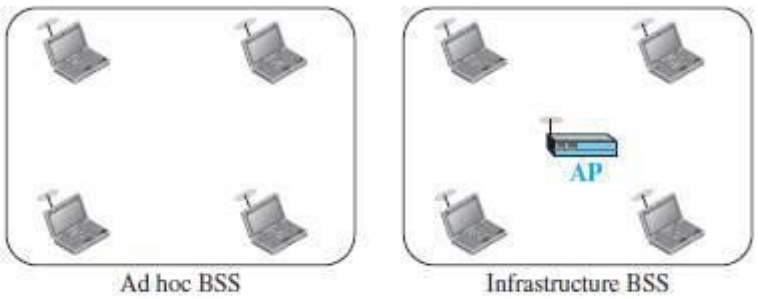


Figure 15.4 *Basic service sets (BSSs)*

4.11.1.2 ESS

The ESS is made up of 2 or more BSSs with APs (Figure 15.5).
The BSSs are connected through a distribution-system, which is usually a wired LAN.
The distribution-system connects the APs in the BSSs.
IEEE 802.11 does not restrict the distribution-system;
The distribution-system can be any IEEE LAN such as an Ethernet.
The ESS uses 2 types of stations:
Mobile stations are normal stations inside a BSS.
Stationary stations are AP stations that are part of a wired LAN.

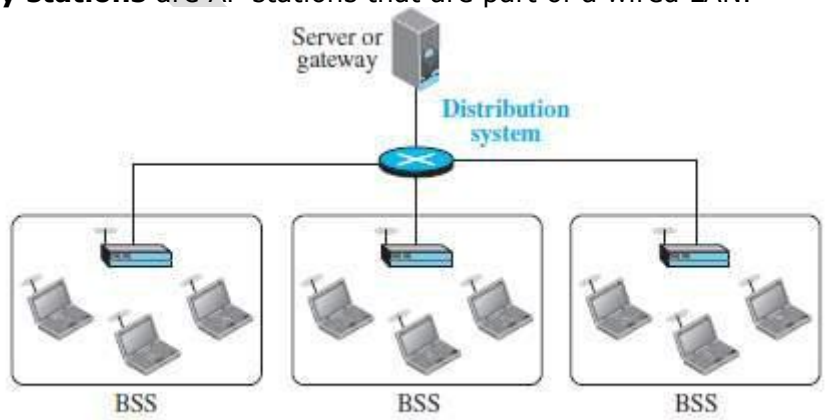


Figure 15.5 *Extended service set (ESS)*

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.
However, communication between two stations in two different BSSs usually occurs via two APs.

4.11.1.3 Station Types

• IEEE 802.11 defines three types of stations based on their mobility in a wireless-LAN:
1) No-transition 2) BSS-transition 3) ESS-transition mobility

A station with no-transition mobility is either
stationary (not moving) or
moving only inside a BSS.

A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.

A station with ESS-transition mobility can move from one ESS to another.
However, IEEE 802.11 does not guarantee that communication is continuous during the move.

4.11.2 MAC Sublayer

IEEE 802.11 defines 2 MAC sublayers:
Distributed coordination function (DCF) &
Point coordination function (PCF).

The figure 15.6 shows the relationship between
Two MAC sublayers
LLC sublayer &
Physical layer.

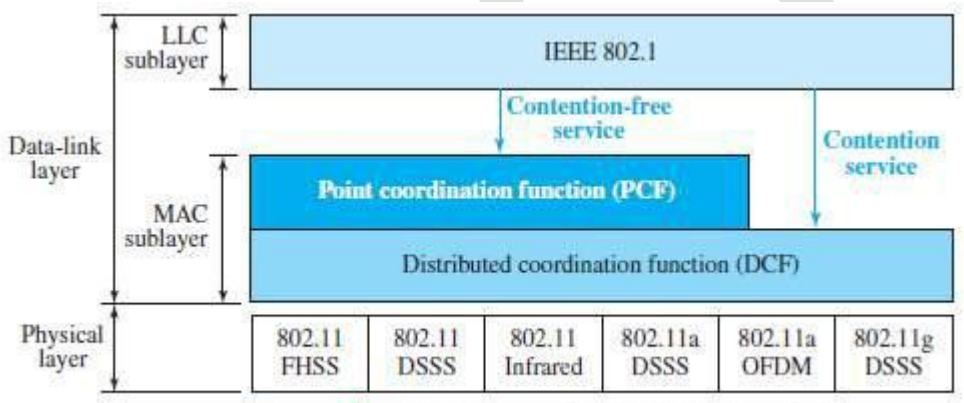


Figure 15.6 *MAC layers in IEEE 802.11 standard*

4.11.2.1 DCF

One of the 2 protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF).

DCF uses CSMA/CA as the access method.

Wireless-LANs cannot implement CSMA/CD for 3 reasons:

For collision-detection, a station must be able to send data & receive collision-signals at the same time. This can mean costly stations and increased bandwidth requirements.

Collision may not be detected because of the hidden station problem.

The distance between stations can be great.

Signal fading could prevent a station at one end from hearing a collision at the other end.

• Process Flowchart: Figure 15.7 shows the process flowchart for CSMA/CA as used in wireless-LANs.

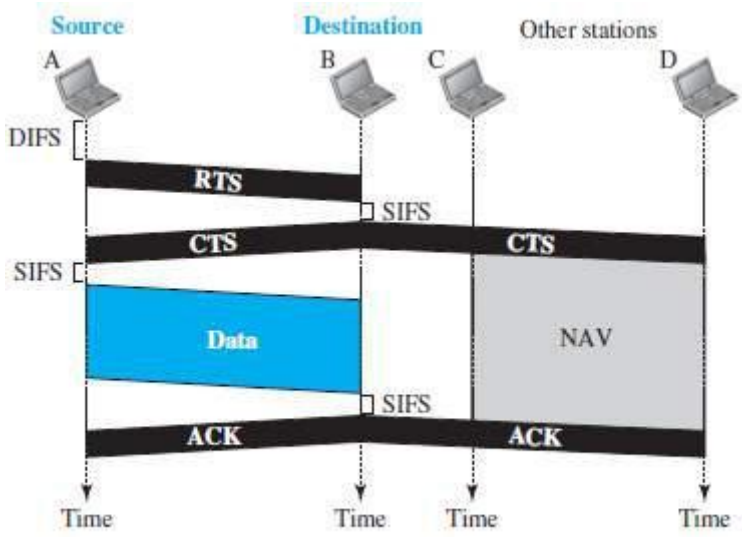


Figure 15.7 *CSMA/CA and NAV*

Before sending a frame, the source-station senses the medium by checking the energy-level at the carrier-frequency.

The channel uses a persistence strategy with back-off until the channel is idle.

After the station is found to be idle,

the station waits for a period of time called the DIFS.

then the station sends a control frame called the RTS.

After receiving the RTS and waiting a period of time called the SIFS, the destination-station sends a control frame, called the CTS, to the source-station.

CTS frame indicate that the destination-station is ready to receive data.

The source-station sends data after waiting an amount of time equal to SIFS.

The destination-station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.

Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination.

On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

(DIFS → distributed inter frame space

(RTS → request to send

SIFS → short inter frame space)

CTS → clear to send)

4.11.2.1.1 Network Allocation Vector

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel (NAV Network Allocation Vector). →

The stations that are affected by this transmission create a timer called a NAV.

NAV shows how much time must pass before these stations are allowed to check the channel for idleness.

Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

In other words, each station, before sensing the medium to see if it is idle, first checks its NAV to see if it has expired.

4.11.2.1.2 Collision During Handshaking

Two or more stations may try to send RTS frames at the same time.

These control frames may collide.

However, because there is no mechanism for collision-detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver.

The back-off strategy is employed, and the sender tries again.

4.11.2.2 PCF

The PCF is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network) (PCF → Point Coordination Function).

The PCF is implemented on top of the DCF.

The PCF is used mostly for time-sensitive transmission.

PCF has a centralized, contention-free polling access method.

The AP performs polling for stations that are capable of being polled.

The stations are polled one after another, sending any data they have to the AP.

To give priority to PCF over DCF, another set of inter-frame spaces has been defined: PIFS and SIFS.

The SIFS is the same as that in DCF &

PIFS (PCF IFS) is shorter than the DIFS.

This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.

Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium.

To prevent this, a repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF) traffic.

The repetition interval, which is repeated continuously, starts with a special control frame, called a beacon frame.

When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval.

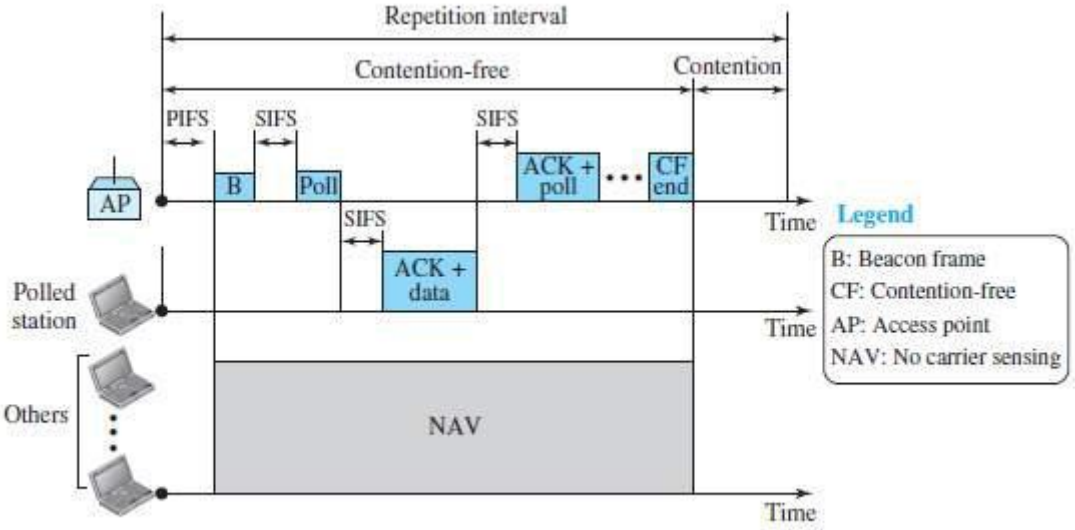


Figure 15.8 *Example of repetition interval*

During the repetition interval, the PC (point controller) can send a poll frame, receive data, send an ACK, receive an ACK, or do any combination of these (802.11 uses piggybacking).

At the end of the contention-free period, the PC sends a CF end (contention-free end) frame to allow the contention-based stations to use the medium.

4.11.2.2.1 Fragmentation

The wireless environment is very noisy; a corrupt frame has to be retransmitted.

The protocol, therefore, recommends fragmentation--the division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.

4.11.2.2.2 Frame Format

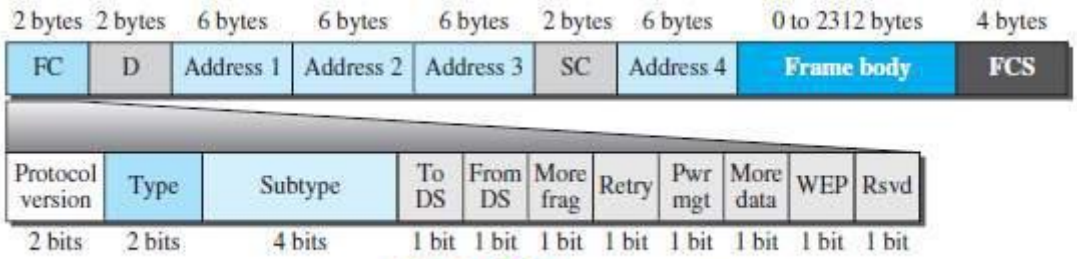


Figure 15.9 *Frame format*

- The MAC layer frame consists of nine fields (Figure 15.9):

1) Frame control (FC)

➢ The FC field is 2 bytes long and defines the type of frame and some control information. The table describes the subfields.

Table 15.1 *Subfields in FC field*

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 15.2)
To DS	Defined later
From DS	Defined later
More frag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

2) D

➢ In all frame types except one, this field defines the duration of the transmission that is used to set the value of NAV.

➢ In one control frame, this field defines the ID of the frame.

3) Addresses

There are four address fields, each 6 bytes long.
The meaning of each address field depends on the value of the ToDS and FromDS subfields.

4) Sequence control

This field defines the sequence number of the frame to be used in flow control.

5) Frame body

➢ This field contains information based on the type and the subtype defined in the FC field. ➢ This field can be between 0 and 2312 bytes,

6) FCS

➢ The FCS contains a CRC-32 error detection sequence.

2.2.3 Frame Types

• A wireless-LAN defined by IEEE 802.11 has three categories of frames: 1.management frames, 2.control frames, and 3.data-frames.

1) Management Frames

Management frames are used for the initial communication between stations and access points.

2) Control Frames

Control frames are used for accessing the channel and acknowledging frames (Figure 15.10).

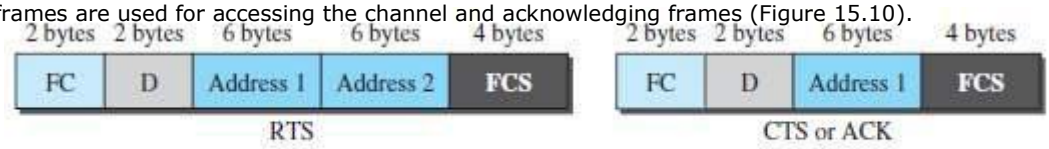


Figure 15.10 *Control frames*

For control frames the value of the type field is 01; the values of the subtype fields for frames are shown in the table 14.2.

Table 15.2 *Values of subtype fields in control frames*

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

3) Data-frames

➢ Data-frames are used for carrying data and control information.

4.11.3 Addressing Mechanism

The IEEE 802.11 addressing mechanism specifies 4 cases, defined by the value of the 2 flags in the FC field, To DS and From DS.

Each flag can be either 0 or 1, resulting in 4 different situations.

The interpretation of the 4 addresses (address 1 to address 4) in the MAC frame depends on the value of these flags, as shown in the Table 15.3.

Table 15.3 *Addresses*

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Address 1 is always the address of the next device.
Address 2 is always the address of the previous device.
Address 3 is the address of the final destination-station if it is not defined by address 1.
Address 4 is the address of the original source-station if it is not the same as address 2.

Case-1:00

In this case, To DS = 0 and From DS = 0 (Figure 15.11a).
This means that the frame is

not going to a distribution-system (To DS = 0) and i
not coming from a distribution-system (From DS = 0).

The frame is going from one station in a BSS to another without passing through the distribution-system.

- The ACK frame should be sent to the original sender.

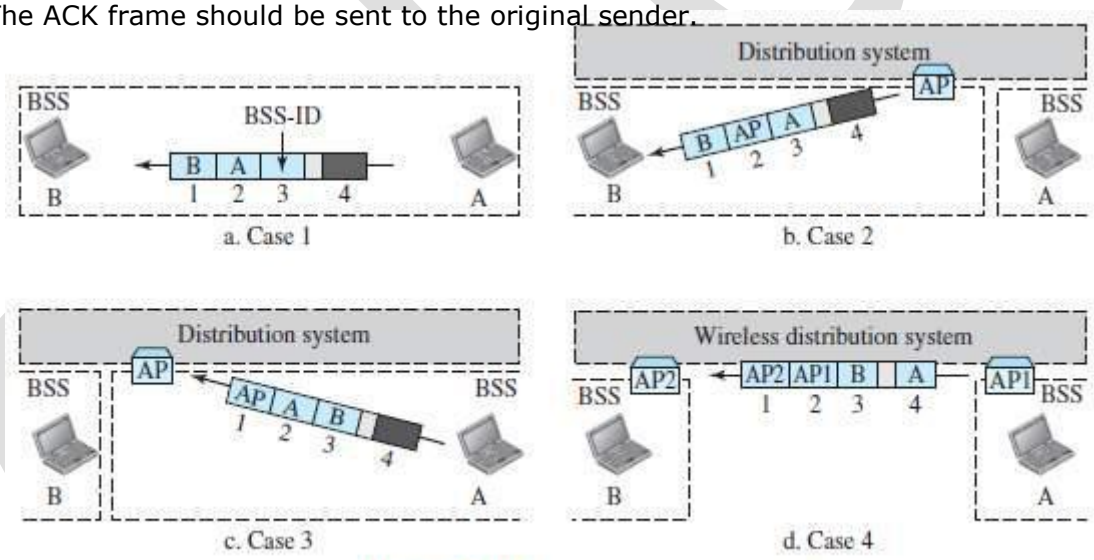


Figure 15.11 *Addressing mechanisms*

Case-2:01

In this case, To DS = 0 and From DS = 1 (Figure 15.11b).
This means that the frame is coming from a distribution-system (From DS = 1).
The frame is coming from an AP and going to a station.
The ACK should be sent to the AP.
The address 3 contains the original sender of the frame (in another BSS).

Case-3:10

In this case, To DS = 1 and From DS = 0 (Figure 15.11c).
This means that the frame is going to a distribution-system (To DS = 1).
The frame is going from a station to an AP. The ACK is sent to the original station.
The address 3 contains the final destination of the frame (in another BSS).

Case-4:11

In this case, To DS = 1 and From DS = 1 (Figure 15.11d).
This is the case in which the distribution-system is also wireless.
The frame is going from one AP to another AP in a wireless distribution-system.
We do not need to define addresses if the distribution-system is a wired LAN because the frame in these cases has the format of a wired LAN frame (for example: Ethernet,).
Here, we need four addresses to define
original sender
final destination, and
two intermediate APs.

4.11.3.1 Exposed Station Problem

In this problem, a station refrains from using a channel even when the channel is available for use.
In the figure 14.12, station A is transmitting to station B.
Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.
However, station C is exposed to transmission from A i.e. station C hears what A is sending and thus refrains from sending.
In other words, C is too conservative and wastes the capacity of the channel.

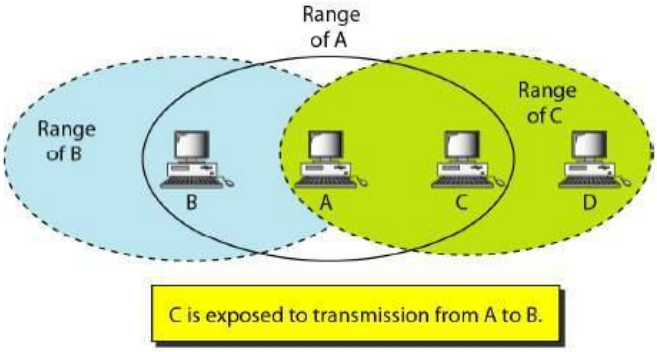


Figure 14.12 *Exposed station problem*

The handshaking messages RTS and CTS cannot help in this case.
Station C hears the RTS from A, but does not hear the CTS from B.
Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D.
Both stations B and A may hear this RTS, but station A is in the sending state, not the receiving state.
However, Station B responds with a CTS.
The problem is here (Figure 15.12).
If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D. It remains exposed until A finishes sending its data as the figure shows.

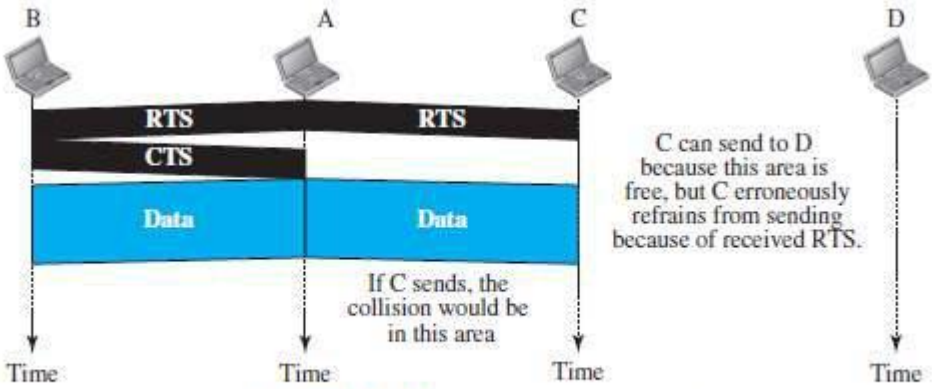


Figure 15.12 *Exposed station problem*

4.11.4 Physical Layer

Table 15.4 *Specifications*

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.400–4.835 GHz	FSK	1 and 2
	DSSS	2.400–4.835 GHz	PSK	1 and 2
	None	Infrared	PPM	1 and 2
802.11a	OFDM	5.725–5.850 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.400–4.835 GHz	PSK	5.5 and 11
802.11g	OFDM	2.400–4.835 GHz	Different	22 and 54
802.11n	OFDM	5.725–5.850 GHz	Different	600

All implementations, except the infrared, operate in the ISM band.
ISM band defines 3 unlicensed bands in the 3 ranges.
902-928 MHz,
2.400--4.835 GHz, and
5.725-5.850 GHz. (ISM → industrial, scientific, and medical)

4.11.4.1 IEEE 802.11 FHSS

IEEE 802.11 FHSS uses the FHSS method (Figure 15.13).
FHSS uses the 2.4-GHz ISM band.
The band is divided into 79 subbands of 1 MHz (and some guard bands).
A pseudorandom number generator selects the hopping sequence.
The modulation technique is either two-level FSK or four-level FSK with 1 or 2 bits/baud.
This results in a data-rate of 1 or 2 Mbps

(FHSS → frequency-hopping spread spectrum DSSS → direct sequence spread spectrum)

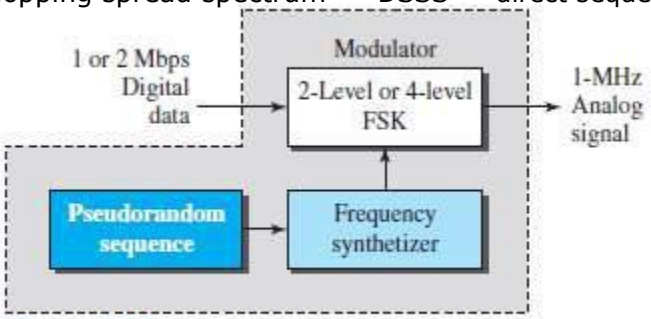


Figure 15.13 *Physical layer of IEEE 802.11 FHSS*

4.11.4.2 IEEE 802.11 DSSS

IEEE 802.11 DSSS uses the DSSS method (Figure 15.14).
DSSS uses the 2.4-GHz ISM band.
The modulation technique in this specification is PSK at 1 Mbaud/s.
The system allows 1 or 2 bits/baud (BPSK or QPSK).
This results in a data-rate of 1 or 2 Mbps.

Figure 15.14 *Physical layer of IEEE 802.11 DSSS*

(HRDSSS → high-rate direct sequence spread spectrum CCK → complementary code keying)
(OFDM → orthogonal frequency-division multiplexing)

4.11.4.3 IEEE 802.11 Infrared

IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm (Figure 15.15).

The modulation technique is called pulse position modulation (PPM).

For a 1-Mbps data-rate, a 4-bit sequence is first mapped into a 16-bit sequence in which only one bit is set to 1 and the rest are set to 0.

For a 2-Mbps data-rate, a 2-bit sequence is first mapped into a 4-bit sequence in which only one bit is set to 1 and the rest are set to 0.

The mapped sequences are then converted to optical signals; the presence of light specifies 1, the absence of light specifies 0.

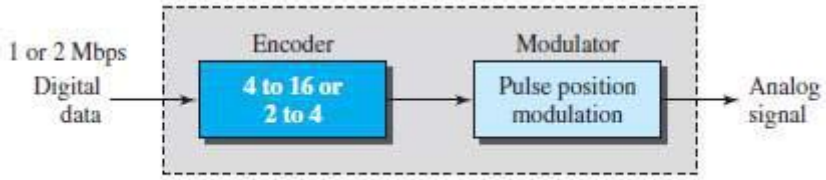


Figure 15.15 *Physical layer of IEEE 802.11 infrared*

4.11.4.4 IEEE 802.11a OFDM

IEEE 802.11a OFDM describes the OFDM method for signal generation in a 5-GHz ISM band.

OFDM is similar to FDM, with 2 major difference:

- All the subbands are used by one source at a given time.
- Sources contend with one another at the data-link-layer for access.

The band is divided into 52 subbands. Out of which,

- 48 subbands are used for sending 48 groups of bits at a time.
- 4 subbands are used for sending control information.

The scheme is similar to ADSL.

Dividing the band into subbands diminishes the effects of interference.

If the subbands are used randomly, security can also be increased.

OFDM uses PSK and QAM for modulation.

The common data-rates are

i) 18 Mbps (PSK) and ii) 54 Mbps (QAM).

4.11.4.5 IEEE 802.11b DSSS

IEEE 802.11 b DSSS describes the HRDSSS method for signal generation in the 2.4-GHz ISM band.

HR-DSSS is similar to DSSS, with 1 major difference: HR-DSSS uses encoding method called CCK.

CCK encodes 4 or 8 bits to one CCK symbol (Figure 15.16).

To be backward compatible with DSSS, HR-DSSS defines 4 data-rates: 1, 2, 5.5, and 11 Mbps.

- The first two versions (1- & 2-Mbps) use the same modulation techniques as DSSS.
- The 5.5-Mbps version
  - uses BPSK and
  - transmits at 1.375 Mbaud/s with 4-bit CCK encoding.
- The 11-Mbps version
  - uses QPSK and
  - transmits at 1.375 Mbps with 8-bit CCK encoding.

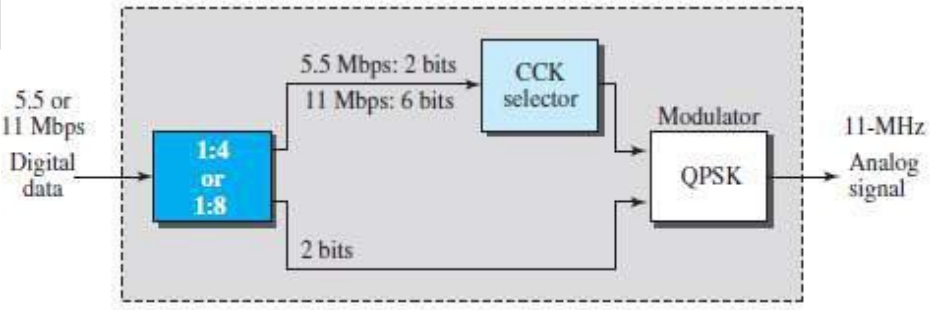


Figure 15.16 *Physical layer of IEEE 802.11b*

4.11.4.6 IEEE 802.11g

This new specification defines forward error correction and OFDM using the 2.4-GHz ISM band.

The modulation technique achieves a 22- or 54-Mbps data-rate.

It is backward compatible with 802.11b, but the modulation technique is OFDM.

4.12 BLUETOOTH

Bluetooth is a wireless-LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on.

A Bluetooth LAN is an ad hoc network. This means the network is formed spontaneously.

The devices

find each other and

make a network called a piconet (Usually, devices are called gadgets)

A Bluetooth LAN can even be connected to the Internet if one of the devices has this capability.

By nature, a Bluetooth LAN cannot be large.

If there are many devices that try to connect, there is confusion.

Bluetooth technology has several applications.

Peripheral devices such as a wireless mouse/keyboard can communicate with the computer.

In a small health care center, monitoring-devices can communicate with sensor-devices.

Home security devices can connect different sensors to the main security controller.

Conference attendees can synchronize their laptop computers at a conference.

Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.

The standard defines a wireless PAN operable in an area the size of a room or a hall.

(PAN → personal-area network)

4.12.1 Architecture

• Bluetooth defines 2 types of networks: 1) Piconet and 2) Scatternet.

4.12.1.1 Piconets

A Bluetooth network is called a piconet, or a small net. (Figure 15.17).

A piconet can have up to 8 stations. Out of which

One of station is called the primary.

The remaining stations are called secondaries.

All the secondary-stations synchronize their clocks and hopping sequence with the primary station.

A piconet can have only one primary station.

The communication between the primary and the secondary can be one-to-one or one-to-many.

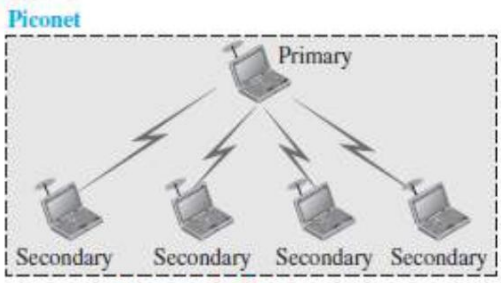


Figure 15.17 *Piconet*

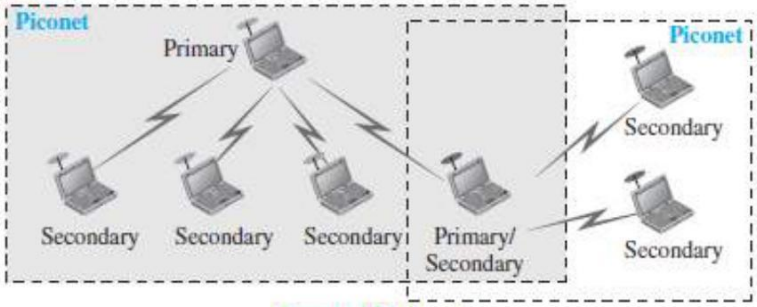


Figure 15.18 *Scatternet*

Although a piconet can have a maximum of 7 secondaries, an additional 8 secondaries can be in the parked state.

A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state.

Because only 8 stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

4.12.1.2 Scatternet

Piconets can be combined to form a scatternet (Figure 15.18).

A station can be a member of 2 piconets.

A secondary station in one piconet can be the primary in another piconet. This is called mediator station.

Acting as a secondary, mediator station can receive messages from the primary in the first piconet.

Acting as a primary, mediator station can deliver the message to secondaries in the second piconet.

4.12.1.3 Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter.

The current data-rate is 1 Mbps with a 2.4-GHz bandwidth.

This means that there is a possibility of interference between the IEEE 802.11b wireless-LANs and Bluetooth LANs.

4.12.2 Bluetooth Layers

• Bluetooth uses several layers that do not exactly match those of the Internet model (Figure 15.19).

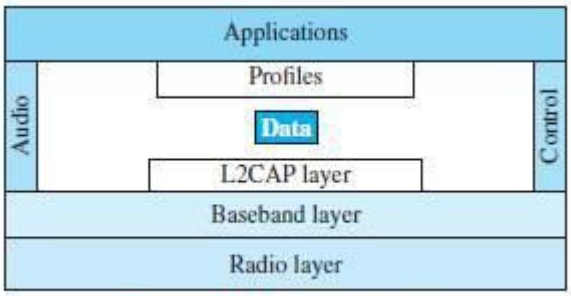


Figure 15.19 *Bluetooth layers*

4.12.2.1 Radio Layer

• The radio layer is roughly equivalent to the physical layer of the Internet model.

• Bluetooth devices are low-power and have a range of 10 m.

1) Band

Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

2) FHSS

Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.

Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second.

A device uses a frequency for only 625 μs (1/1600 s) before it hops to another frequency; the dwell time is 625 μs.

3) Modulation

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering).

GFSK has a carrier frequency.

Bit 1 is represented by a frequency deviation above the carrier; bit „a" is represented by a frequency deviation below the carrier.

The frequencies, in megahertz, are defined according to the following formula for each channel:

$$f_c = 2402 + n \text{ MHz} \qquad n = 0, 1, 2, 3, \ldots, 78$$

For example,

The first channel uses carrier frequency 2402 MHz (2.402 GHz).

The second channel uses carrier frequency 2403 MHz (2.403 GHz).

4.12.2.2 Baseband Layer

The baseband layer is roughly equivalent to the MAC sublayer in LANs.
The access method is TDMA.
The primary and secondary communicate with each other using time slots.
The length of a time slot is exactly the same as the dwell time, 625 μs.
This means that during the time that one frequency is used, a sender sends a frame to a secondary, or a secondary sends a frame to the primary.
The communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

4.12.2.2.1 TDMA

Bluetooth uses a form of TDMA that is called TDD-TDMA (timedivision duplex TDMA).
TDD-TDMA is a kind of half-duplex communication in which the secondary and receiver send and receive data, but not at the same time (halfduplex);
However, the communication for each direction uses different hops.
This is similar to walkie-talkies using different carrier frequencies.

Single-Secondary Communication

If the piconet has only one secondary, the TDMA operation is very simple (Fig 15.21).
The time is divided into slots of 625 μs.
The primary uses even numbered slots (0, 2, 4, ...); the secondary uses odd-numbered slots (1, 3, 5,...).
TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode.
In slot 0, the primary sends, and the secondary receives; in slot 1, the secondary sends, and the primary receives. The cycle is repeated.

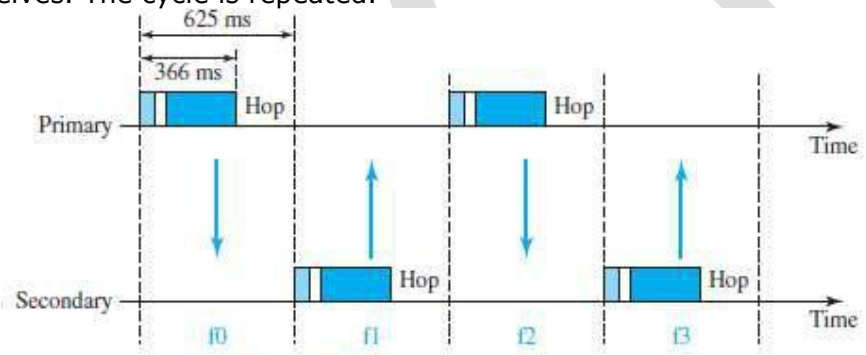


Figure 15.21 *Single-secondary communication*

4.12.2.2.2 Links

Two types of links can be created between a primary and a secondary:

SCQ link (Synchronous Connection-oriented Link) and
ACL links (Asynchronous Connectionless Link).

1) SCA

- This link is used when avoiding latency is more important than data-integrity. (Latency → delay in data delivery Integrity → error-free delivery)

A physical-link is created between the primary and a secondary by reserving specific slots at regular intervals.
The basic unit of connection is 2 slots. One slot is used for each direction.
If a packet is damaged, it is never retransmitted.
Application: Used for real-time audio where avoiding delay is all-important.
A secondary

can create up to 3 SCQ links with the primary
can send digitized audio (PCM) at 64 kbps in each link.

2) ACL

This link is used when data-integrity is more important than avoiding latency.
If a payload encapsulated in the frame is corrupted, it is retransmitted.
A secondary returns an ACL frame in the available odd-numbered slot if and only if the previous slot has been addressed to it.
ACL can use one, three, or more slots and can achieve a maximum data-rate of 721 kbps.

4.12.2.2.3 Frame Types

• A frame in the baseband layer can be one of 3 types: 1) one-slot 2) three-slot or 3) five-slot.

1) One-slot frame

- A slot is 625 μs.
- However, in a one-slot frame exchange, 259 μs is needed for hopping & control mechanisms.
- This means that a one-slot frame can last only 625 - 259, or 366 μs.
- With a 1-MHz bandwidth and 1 bit/Hz, the size of a one-slot frame is 366 bits.

2) Three-slot frame

A three-slot frame occupies 3 slots.
However, since 259 μs is used for hopping, the length of the frame is 3 x 625 - 259 = 1616 μs or 1616 bits.
A device that uses a three-slot frame remains at the same hop (at the same carrier frequency) for 3 slots.
Even though only once hop number is used, 3 hop numbers are consumed.
That means the hop number for each frame is equal to the first slot of the frame.

3) Five-slot frame

- A five-slot frame also uses 259 bits for hopping, which means that the length of the frame is 5 x 625 - 259 =2866 bits.

4.12.2.2.4 Frame Format

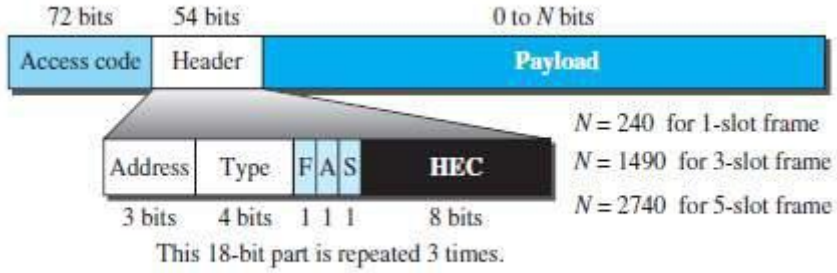


Figure 15.23 *Frame format types*

- The following describes each field (Figure 15.23):

1) Access code

- This field contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from anothe

2) Header

- This field is a repeated I8-bit pattern. Each pattern has the following subfields: **i)**

Address

This subfield can define up to 7 secondaries (1 to 7).

If the address is zero, it is used for broadcast communication from the primary to all secondaries.

ii) Type

This subfield defines the type of data coming from the upper layers.

iii) F

This subfield is for flow control.

When set (1), it indicates that the device is unable to receive more frames (buffer is full).

iv) A

This subfield is for acknowledgment.

Bluetooth uses Stop-and-Wait ARQ.

- 1 bit is sufficient for acknowledgment.

v) S

This subfield holds a sequence number.

Bluetooth uses Stop-and-Wait ARQ

1 bit is sufficient for sequence numbering.

vi) HEC (header error correction)

This subfield is a checksum to detect errors in each 18-bit header section.

The header has three identical 18-bit sections.
The receiver compares these three sections, bit by bit.

If each of the corresponding bits is the same, the bit is accepted; if not, the majority opinion rules.

This is a form of forward error correction (for the header only).

This double error control is needed because the nature of the communication, via air, is very noisy.

There is no retransmission in this sublayer.

3) Payload

This subfield can be 0 to 2740 bits long.
It contains data or control information coming from the upper layers.

4.12.2.3 L2CAP

The L2CAP is roughly equivalent to the LLC sublayer in LANs (Figure 15.20).
It is used for data exchange on an ACL link. (L2CAP → Logical Link Control and Adaptation Protocol)
SCQ channels do not use L2CAP"(Figure 14.25)

Figure 15.20 *L2CAP data packet format*

The following describes each field:

Length

- This field defines the size of the data, in bytes, coming from the upper layers.
  Data can be up to 65,535 bytes.

2) CID (Channel ID)

This field defines a unique identifier for the virtual channel created at this level.

The L2CAP has specific duties: 1) Multiplexing
Segmentation and reassembly
QoS (quality of service) and
Group management.

1) Multiplexing

The L2CAP can do multiplexing.
At the sender site, L2CAP
accepts data from one of the upper-layer protocols
frames the data and
delivers the data to the baseband layer.
At the receiver site, L2CAP
accepts a frame from the baseband layer
extracts the data, and
delivers the data to the appropriate protocol layer.
It creates a kind of virtual channel.

2) Segmentation and Reassembly

In the baseband layer, the maximum size of the payload field is 2774 bits, or 343 bytes.
This includes 4 bytes to define the packet and packet-length.
Therefore, the size of the packet that can arrive from an upper layer can only be 339 bytes.
However, application layers sometimes need to send a data packet that can be up to 65,535 bytes (for example: an Internet packet).
The L2CAP divides the large packets into segments and adds extra information to define the location of the segments in the original packet.
The L2CAP segments the packet at the source and reassembles them at the destination.

3) QoS

Bluetooth allows the stations to define a QoS level.
If no QoS level is defined, Bluetooth defaults to best-effort service; it will do its best under the circumstances.

4) Group Management

Another functionality of L2CAP is to allow devices to create a type of logical addressing between themselves.
This is similar to multicasting.
For example:
2 or 3 secondary devices can be part of a multicast group to receive data from the primary.

MODULE-WISE QUESTIONS

MODULE 4: MULTIPLE ACCESS

Explain random access protocol. (4)
Explain pure ALOHA. (6*)
Explain slotted ALOHA. (4*)
Explain CSMA. (6*)
Explain different persistence methods of CSMA. (6*)
Explain CSMA/CA. (6*)
Explain CSMA/CD. (10*)
List & explain different controlled access protocols. (10*)
Explain reservation access method. (4*)
Explain polling access method. (6*)
Explain token passing access method. (6*)
List & explain channelization protocols. (10*)
Explain FDMA. (6*)
Explain TDMA. (6*)
Explain CDMA. (8*)

MODULE 4(CONT.): WIRED LANS -- ETHERNET

Explain frame format of standard ethernet. (8*)
Explain frame length of standard ethernet. (4*)
Explain addressing in standard ethernet. (6*)
Explain encoding in standard ethernet. (8)
Explain changes in the standard ethernet. (6)
List out 5 goals of fast-ethernet. Explain autonegotiation. (6*)
Explain encoding in fast-ethernet. (8)
Explain MAC Sublayer in gigabit-ethernet (6*)
Explain encoding in gigabit-ethernet. (4)

MODULE 4(CONT.): WIRELESS-LANS

Differentiate b/w wireless LAN & wired LAN with reference to architectural comparison (6)
Explain characteristics of wireless medium. (4)
Explain hidden station problem. (6*)
Explain architecture of IEEE 802.11 (10*)
Explain DCF in IEEE 802.11 (6)
Explain PCF in IEEE 802.11 (6)
Explain frame format of IEEE 802.11 (8*)
Explain frame types of IEEE 802.11 (8*)
Explain addressing in IEEE 802.11 (8*)
Explain exposed station problem. (6*)
Explain physical Layer of IEEE 802.11 (8)
Explain architecture of Bluetooth. (6*)
Explain layers of Bluetooth. (8*)
Explain radio Layer in Bluetooth. (6)
Explain baseband Layer in Bluetooth. (6)
Explain 2 types of links in Bluetooth. (6)
Explain frame format of Bluetooth. (6)
Explain L2CAP in Bluetooth. (6)

MODULE 5: TABLE OF CONTENTS

- Three Phases
  - Agent Discovery
  - Registration
    - Request and Reply
  - Data Transfer
- Inefficiency in Mobile IP
  - Double Crossing
  - Triangle Routing

IPv6 ADDRESSING
- Representation
- Address-space
  - Three Address Types
- Address-space Allocation
  - Global Unicast Addresses
  - Special Addresses
  - Other Assigned Blocks
- Autoconfiguration

THE IPv6 PROTOCOL
- Changes from IPv4 to IPv6 (Advantages of IPv6)
- Packet Format
  - Concept of Flow and Priority in IPv6
  - Fragmentation and Reassembly
- Extension Header
  - Comparison of Options between IPv4 and IPv6

THE ICMPv6 PROTOCOL
- Error Reporting Messages
- Informational Messages
- Neighbor Discovery Messages
- Group Membership Messages

TRANSITION FROM IPv4 TO IPv6
- Strategies

MODULE 5: OTHER WIRELESS NETWORKS

5.1 WiMAX

WiMAX stands for Worldwide Interoperability for Microwave Access.

Purpose of WiMAX:

People want to have access to the Internet from home or office (fixed) where the wired access to the Internet is either not available or is expensive.

People need to access the Internet when they are using their cellular phones (mobiles).

WiMAX provides the "last mile" broadband wireless access.

5.1.1 Services

WiMAX provides 2 types of services to subscribers: 1) Fixed and 2) Mobile.

1) Fixed WiMAX

A base-station can use 3 different types of antenna to optimize the performance:

Omni-directional 2) Sector or 3) Panel (Figure 16.1).

WiMAX uses a beam-steering AAS (Adaptive Antenna System).

While transmitting, antenna can focus its energy in the direction of the subscriber-station.

While receiving, antenna can focus in the direction of the subscriber-station to receive maximum energy sent by the subscriber.

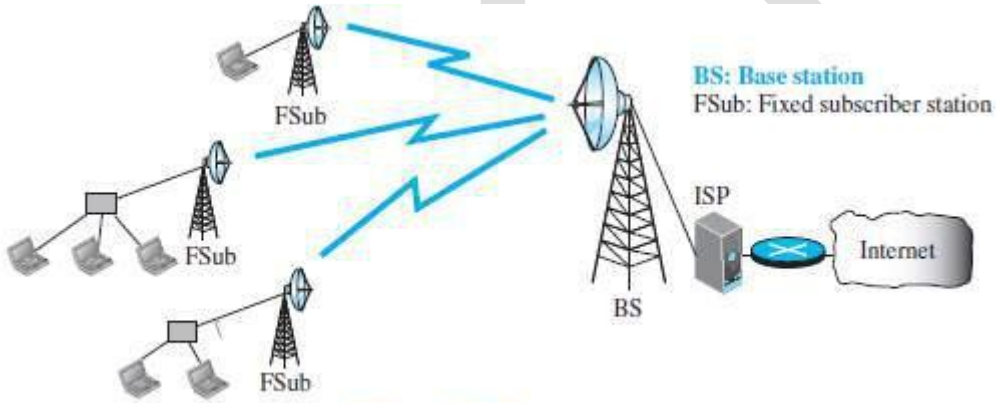


Figure 16.1 *Fixed WiMAX*

2) Mobile WiMAX

• The subscribers are mobile-stations that move from one place to another (Figure 16.2).

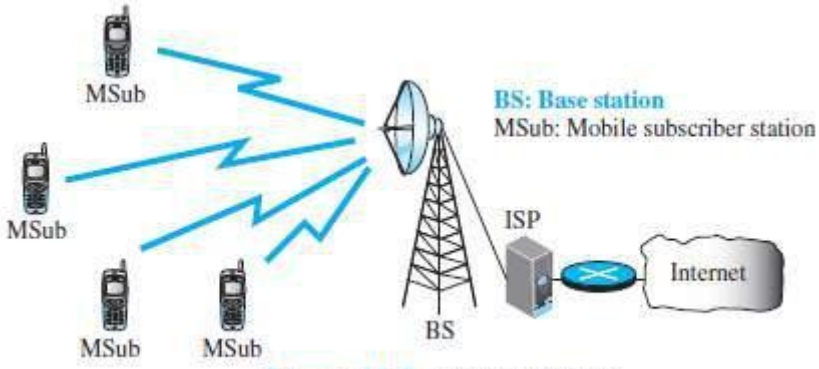


Figure 16.2 *Mobile WiMAX*

5.1.2 IEEE Project 802.16

WiMAX is the result of the IEEE 802.16 project.
The standard is also referred to as wireless local loop.

802.11 Projects	802.16 Projects
Standard for a wireless LAN	Standard for a wireless WAN
Defines a connectionless communication	Defines a connection-oriented service
Distance b/w base-station & host is very limited	Distance b/w base-station & host is above 10 km

IEEE 802.16 was revised into 2 new standards:
IEEE 802.16d which concentrates on the fixed WiMAX.
IEEE 802.16e which defines the mobile WiMAX.

5.1.3 Layers in Project 802.16

Here we discuss, following 2 layers (Figure 16.3):
Data-link layer &
Physical layer.
The data-link layer is divided into 3 sublayers:
Service Specific Convergence Sublayer
Security Sublayer &
MAC Sublayer.
The physical layer is divided into 2 sublayers:
Transmission Convergence Sublayer &
Physical Medium Dependent Sublayer.

5.1.3.1 Data Link layer

1) Service Specific Convergence Sublayer

This is actually the DLC sublayer revised for broadband wireless communication.
It is devised for a connection-oriented service where each connection may benefit from a specific QoS

2) Security Sublayer

This sublayer provides security for communication using WiMAX.
The nature of wireless communication requires security.
Security provided using encryption for information exchanged b/w subscriber-station & base-station.

3) MAC Sublayer

The MAC sublayer defines the access method and the format of the frame.
This sublayer is designed for connection-oriented service.
The packets are routed from the base-station to the subscriber-station using a connection identifier.
Connection identifier remains same during the duration of the communication.

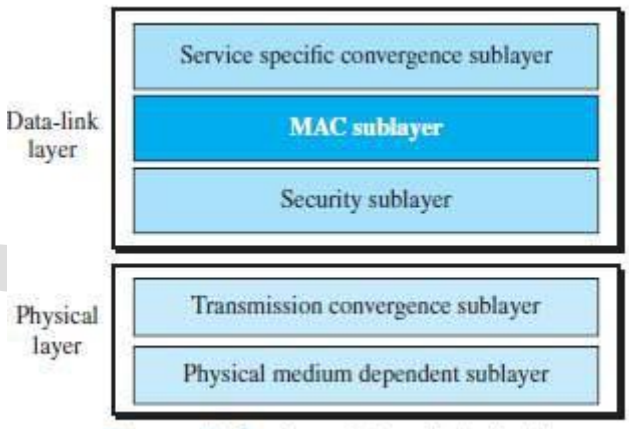


Figure 16.3 *Data-link and physical layers*

5.1.3.2 Physical Layer

1) Transmission Convergence Sublayer

This sublayer uses TDD.

TDD a variation of TDM designed for duplex (bidirectional) communication.

Each frame is made of 2 subframes (Figure 16.5):

Downstream Subframes: carry data from the base-station to the subscribers.

Upstream Subframes: carry data from the subscribers to the base-station.

Each subframe is divided into slots.

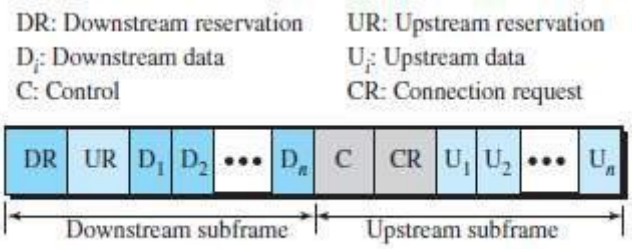


Figure 16.5 *WiMAX frame structure at the physical layer*

2) Physical Medium Dependent Sublayer

This sublayer is in continuous revision.

Originally, 802.16 defined the band 10-66 GHz.

defined following modulations:

QPSK used for long-distance communication.

QAM-16 used for medium-distance communication.

QAM-64 used for short-distance communication.

Later, IEEE defined 802.16d (fixed WiMAX), which added the band 2-11 GHz (compatible with wireless LANs) using the OFDM.

Sometime later, IEEE defined 802.16e (mobile WiMAX) and added SOFDM.

(TDD → Time-Division Duplex FEC → forward error correction) (OFDM → Orthogonal Frequency-Division Multiplexing)

(SOFDM → scalable orthogonal frequency division multiplexing)

5.1.3.3 MAC Sublayer

The MAC sublayer defines the access method and the format of the frame.
This sublayer is designed for connection-oriented service.
The packets are routed from the base-station to the subscriber-station using a connection identifier.
Connection identifier remains same during the duration of the communication.
Here we discuss, following issues: 1) Access Method 2) Frame Format 3) Addressing

1) Access Method

WiMAX uses the reservation (scheduling) access method.
Base-station needs to make a slot-reservation before sending a data to a subscriber-station
Each subscriber-station needs to make a reservation before sending a data to the base-station

2) Frame Format

Two types of frames (Figure 16.4):
Generic Frame is used to send and receive payload.
Control Frame is used only during the connection establishment.
Both frame-types use a 6-byte generic header.
However, some bytes have different interpretations in different frame types.

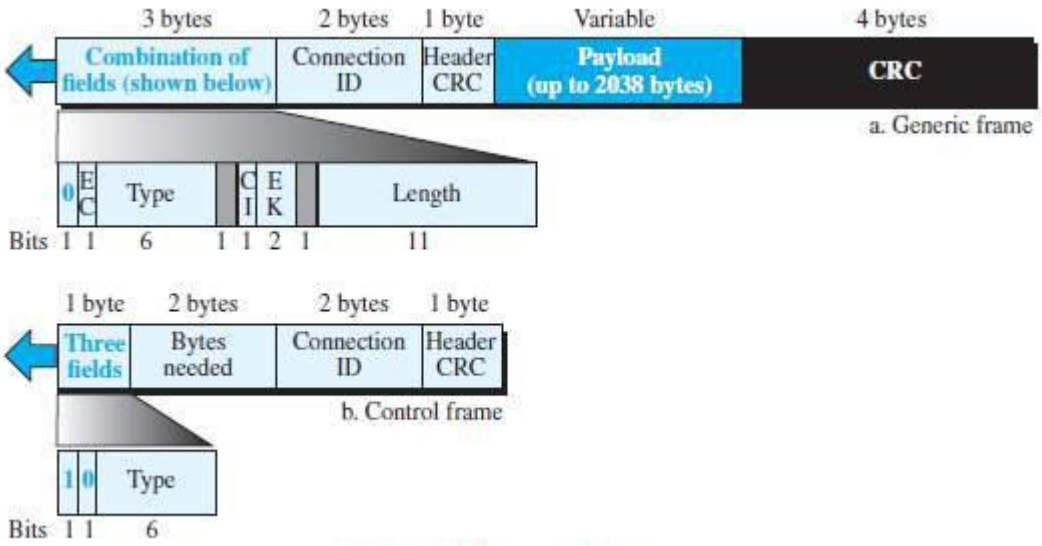


Figure 16.4 *WiMAX MAC frame format*

- The frame contains following fields:

1) First bit
The first bit in a frame is the frame identifier.
If first bit = 0, the frame is a generic frame.
If first bit = 1, the frame is a control frame.

2) EC (Encryption Control)
This field uses one bit to define whether the frame should be encrypted for security purpose.
If EC = 0, it means no encryption.
If EC = 1, it means the frame needs to be encrypted at the security sublayer.

3) Type
This field is used to define the type of the payload.
This field is only present in the generic frame.
The payload can be a packed-load or a fragmented-load.

4) CI (Checksum ID)
This field defines whether the checksum field should be present or not.
If the payload is multimedia, FEC is applied to the frame and there is no need for checksum.

5) EK (Encryption Key)
This field defines one of the 4 keys for encryption if encryption is required.

6) Length
This field defines the total length of the frame.
This field is only present in the generic frame.
This field is replaced by the bytes needed field in the control frame.

DATA COMMUNICATION

7) Bytes Needed
This field defines the number of bytes needed for allocated slots in the physical layer.

8) Connection ID
This field defines the connection identifier for the current connection.

9) Header CRC
Both types of frames need to have header CRC field.
Header CRC is used to check whether the header itself is corrupted.
This field uses the polynomial ($x^8 + x^2 + x + 1$) as the divisor.

10) Payload
This field defines the payload.
Payload is encapsulated in the frame from the service specific convergence sublayer.
This field is not needed in the control frame.

11) CRC
This field is used for error detection over the whole frame.

Addressing

Each subscriber and base-station typically has a 48-bit MAC address.

However, there is no source or destination address field.

The reason is that the combination of source and destination addresses are mapped to a VCI during the connection-establishing phase.

This protocol is a connection-oriented protocol that uses a VCI (Virtual Connection Identifier).

Then, each frame uses the same connection identifier for the duration of data transfer

16.2 CELLULAR TELEPHONY

Cellular telephony is designed to provide communications
between two moving units called mobile-stations (MSs) or
between one mobile-station and one stationary unit called a land unit (Figure 16.6).

A service-provider is responsible for
locating & tracking a caller
assigning a channel to the call and
transferring the channel from base-station to base-station as the caller moves out-of-range.

Each cellular service-area is divided into small regions called cells.

Each cell contains an antenna.

Each cell is controlled by AC powered network-station called the base-station (BS).

Each base-station is controlled by a switching office called a mobile-switching-center (MSC).

MSC coordinates communication between all the base-stations and the telephone central office.

MSC is a computerized center that is responsible for
connecting calls
recording call information and
billing.

Cell-size is not fixed; Cell-size can be increased or decreased depending on population of the area.

Cell-radius = 1 to 12 mi.

Compared to low-density areas, high-density areas require many smaller cells to meet traffic demands.

Cell-size is optimized to prevent the interference of adjacent cell-signals.

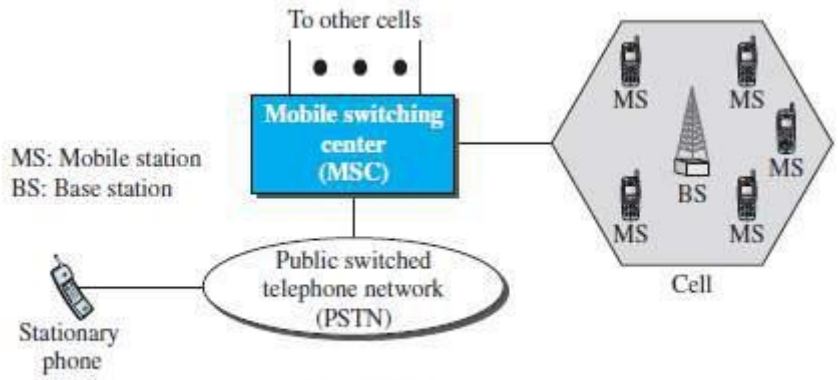


Figure 16.6 *Cellular system*

5.2.1 Operation

5.2.1.1 Frequency-Reuse Principle

In general, neighboring-cells cannot use the same set of frequencies for communication.
Using same set of frequencies may create interference for the users located near the cell-boundaries.
However,
set of frequencies available is limited and
frequencies need to be reused.
A frequency reuse pattern is a configuration of N cells. Where N = reuse factor
Each cell uses a unique set of frequencies.
When the pattern is repeated, the frequencies can be reused.
There are several different patterns (Figure 16.7).
The numbers in the cells define the pattern.
The cells with the same number in a pattern can use the same set of frequencies. These cells are called the reusing cells.

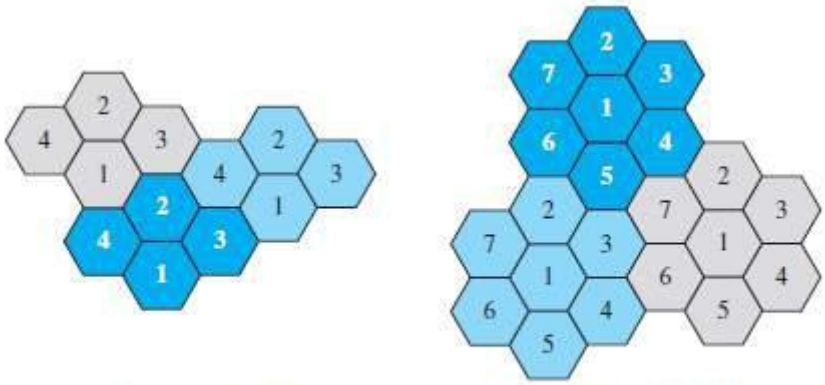


Figure 16.7 *Frequency reuse patterns*

5.2.1.2 Transmitting

Procedure to place a call from a mobile-station:
The caller
enters a phone number and
presses the send button.
The mobile-station
scans the band to determine setup channel with a strong signal and
sends the data (phone number) to the closest base-station.
The base-station sends the data to the MSC.
The MSC sends the data on to the telephone central office.
If called party is available, a connection is made and the result is relayed back to the MSC.
The MSC assigns an unused voice channel to the call, and a connection is established.
The mobile-station automatically adjusts its tuning to the new channel.
Finally, voice communication can begin.

5.2.1.3 Receiving

Procedure to receive a call from a mobile-station:
When a mobile phone is called, the telephone central office sends phone number to the MSC.
MSC searches for the location of the mobile-station by sending query-signals to each cell in a process. This is called paging.
When the mobile-station is found, the MSC transmits a ringing signal.
When the mobile-station answers, the MSC assigns a voice channel to the call.
Finally, voice communication can begin.

5.2.1.4 Handoff

During a conversation, the mobile-station may move from one cell to another.
Problem: When the mobile-station goes to cell-boundary, the signal becomes weak.
To solve this problem, the MSC monitors the level of the signal every few seconds.
If signal-strength decreases, MSC determines a new cell to accommodate the communication.
Then, MSC changes the channel carrying the call (hands signal off from old channel to a new one).

- Two types of Handoff: 1) Hard Handoff 2) Soft Handoff

1) Hard Handoff

Early systems used a hard handoff.
A mobile-station only communicates with one base-station.
When the MS moves from one cell to another cell,
Firstly, communication must be broken with the old base-station.
Then, communication can be established with the new base-station.
This may create a rough transition.

2) Soft Handoff

New systems use a soft handoff.
A mobile-station can communicate with two base-stations at the same time.
When the MS moves from one cell to another cell,
Firstly, communication must be broken with the old base-station.
Then, the same communication may continue with the new base-station.

Roaming

Roaming means that the user
can have access to communication or
can be reached where there is coverage.
Usually, a service-provider has limited coverage.
Neighboring service-providers can provide extended coverage through a roaming contract.

5.2.2 First Generation (1G)

The first generation was designed for voice communication using analog signals.

The main system evolved in the first generation: AMPS (Advanced Mobile Phone System).

5.2.2.1 AMPS

This system is a 1G analog cellular system.

The system uses FDMA to separate channels in a link.

- Here we discuss, two issues: 1) Bands 2) Transmission

1) Bands

The system operates in the ISM 800-MHz band.

The system uses 2 separate channels (Figure 16.8):

First channel is used for forward communication (base-station to mobile-station) Band range: 869 to 894 MHz

Second channel is used for reverse communication (mobile-station to base-station). Band range: 824 to 849 MHz

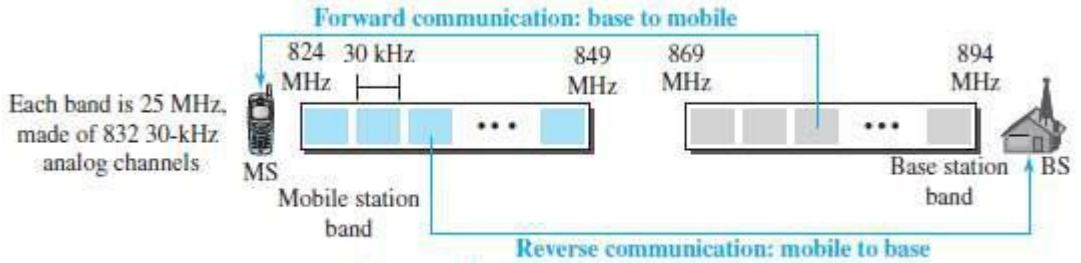


Figure 16.8 *Cellular bands for AMPS*

2) Transmission

The system uses FM and FSK for modulation (Figure 16.9).

Voice channels are modulated using FM.

Control channels are modulated using FSK to create 30-kHz analog signals.

The system uses FDMA to divide each 25-MHz band into 30-kHz channels.

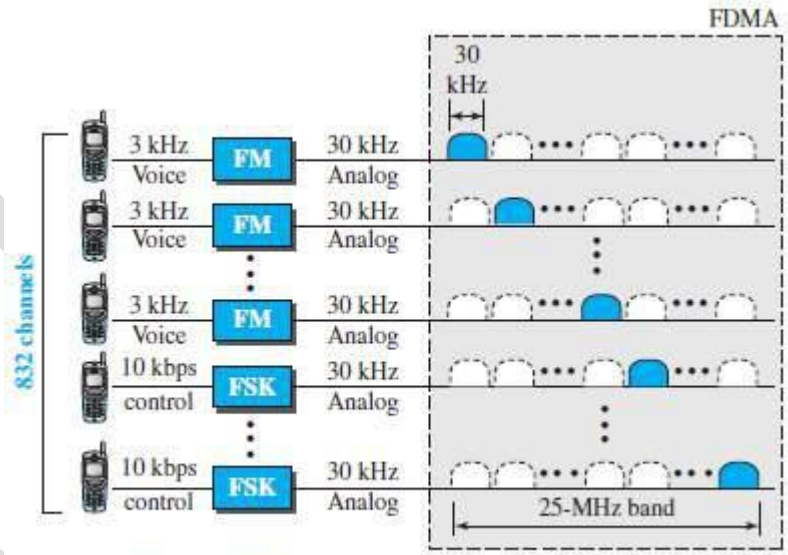


Figure 16.9 *AMPS reverse communication band*

5.2.3 Second Generation (2G)

The second generation was designed for higher-quality voice communication using digital signals.

1G vs. 2G:

The first generation was designed for analog voice communication.

The second generation was mainly designed for digital voice communication.

Three major systems evolved in the second generation:

D-AMPS (digital AMPS)

GSM (Global System for Mobile communication) and

IS-95 (Interim Standard).

5.2.3.1 D-AMPS

D-AMPS (Digital AMPS) was improved version of analog AMPS.

D-AMPS was backward-compatible with AMPS.

Thus, in a cell,

First telephone may use AMPS and

Second telephone may use D-AMPS.

- Here we discuss, two issues: 1) Bands 2) Transmission

1) Band

The system uses the same bands and channels as AMPS (Figure 16.10).

2) Transmission

Each voice channel is digitized using a very complex PCM and compression technique.

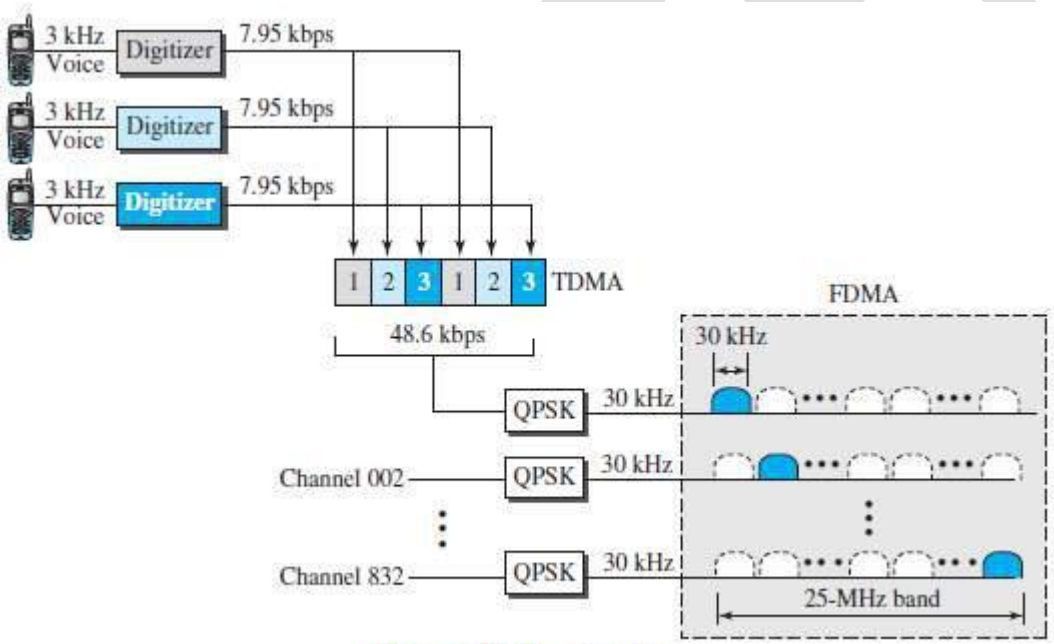


Figure 16.10 *D-AMPS*

5.2.3.2 GSM

- Aim of GSM: to replace a number of incompatible 1G technologies.
- Here we discuss, two issues: 1) Bands 2) Transmission

1) Bands

The system uses two bands for duplex communication (Figure 16.11).
Each band is 25 MHz in width.
Each band is divided into 124 channels of 200 kHz.

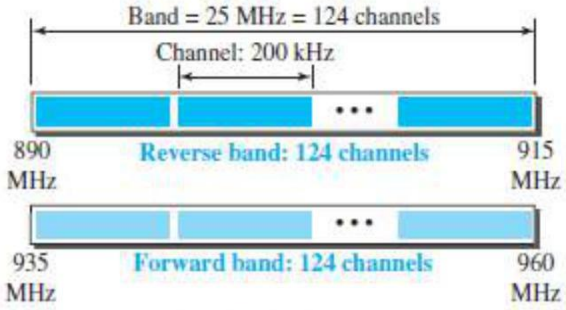


Figure 16.11 *GSM bands*

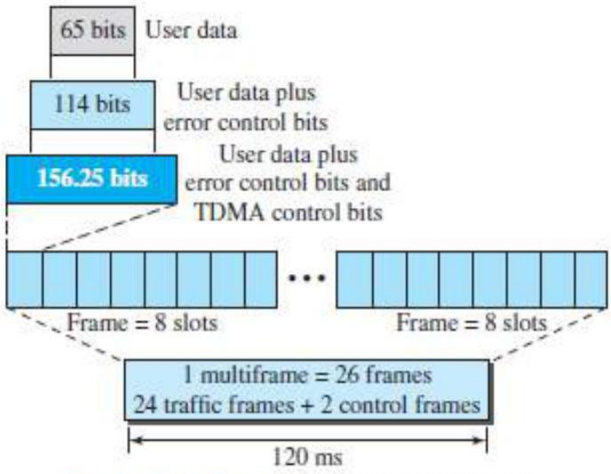


Figure 16.13 *Multiframe components*

2) Transmission

Each voice channel is digitized and compressed to a 13-kbps digital signal (Figure 16.12).
Each slot carries 156.25 bits.
Eight slots share a frame (TDMA).
26 frames also share a multiframe (TDMA).
We can calculate the bit rate of each channel as follows.

$$\text{Channel data rate} = (1/120\text{ ms}) \times 26 \times 8 \times 156.25 = 270.8\text{ kbps}$$

Each 270.8-kbps digital channel modulates a carrier using GMSK (a form of FSK); the result is a 200-kHz analog signal.

Finally, 124 analog channels of 200 kHz are combined using FDMA. The result is a 25-MHz band (Figure 16.13).

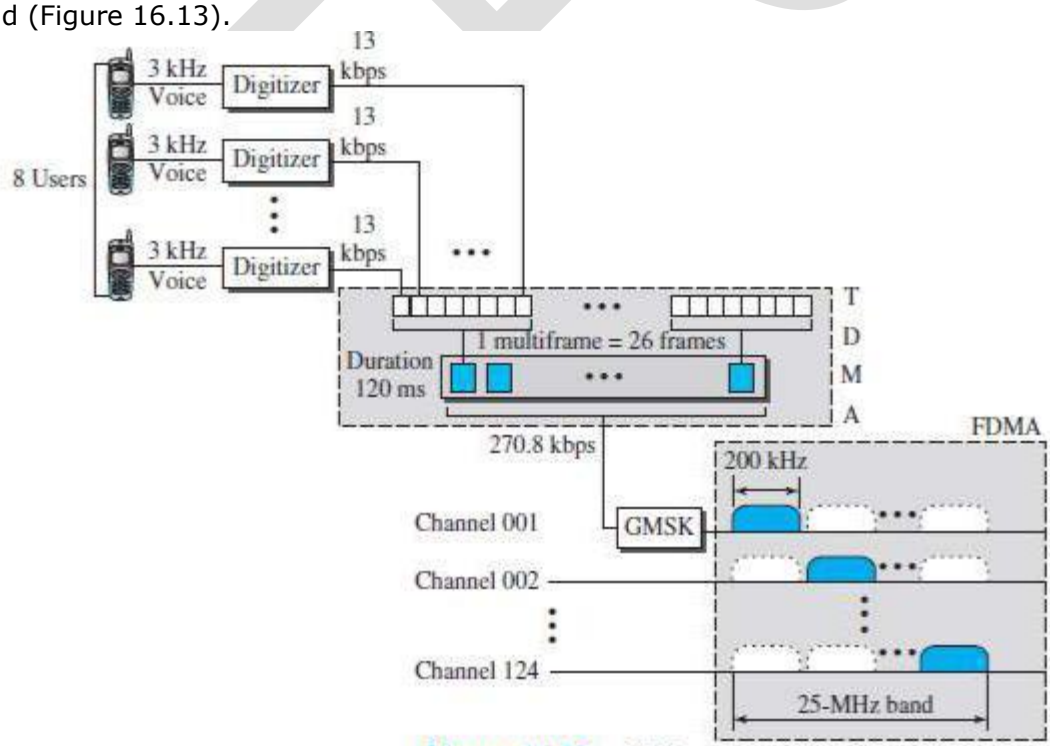


Figure 16.12 *GSM*

5.2.3.3 IS-95

- The system is based on CDMA and DSSS.
- Here we discuss, following 6 issues: 1) Bands 2) Transmission 3) Synchronization 4) Two Data-rate Sets 5) Frequency-Reuse Factor 6) Soft Handoff

1) Bands

- The system uses two bands for duplex communication.
- The bands can be ISM 800-MHz band or ISM 1900-MHz band.

Each band is divided into 20 channels of 1.228 MHz.

- Each service-provider is allotted 10 channels.

IS-95 can be used in parallel with AMPS.

- Each IS-95 channel is equivalent to 41 AMPS channels (41 × 30 kHz = 1.23 MHz).

2) Transmission

- Two types of Transmission:

i) Forward Transmission (base to mobile)

¤ Communications between the base and all mobiles are synchronized.

The base sends synchronized data to all mobiles (Figure 16.14).

ii) Reverse Transmission (mobile to base)

The use of CDMA in the forward direction is possible because the pilot channel sends a continuous sequence of 1s to synchronize transmission.

The synchronization is not used in the reverse direction because we need an entity to do that, which is not feasible.

Instead of CDMA, the reverse channels use DSSS (Figure 16.15).

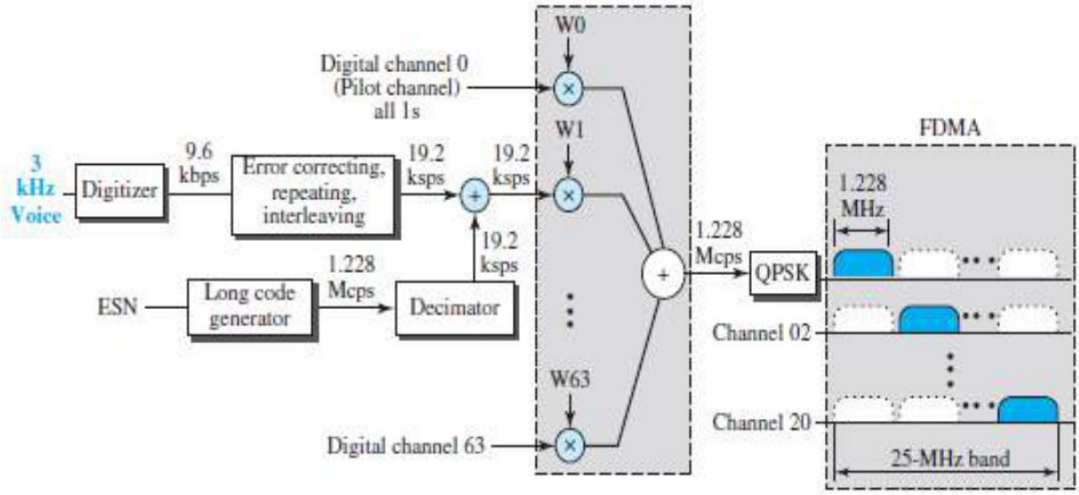


Figure 16.14 *IS-95 forward transmission*

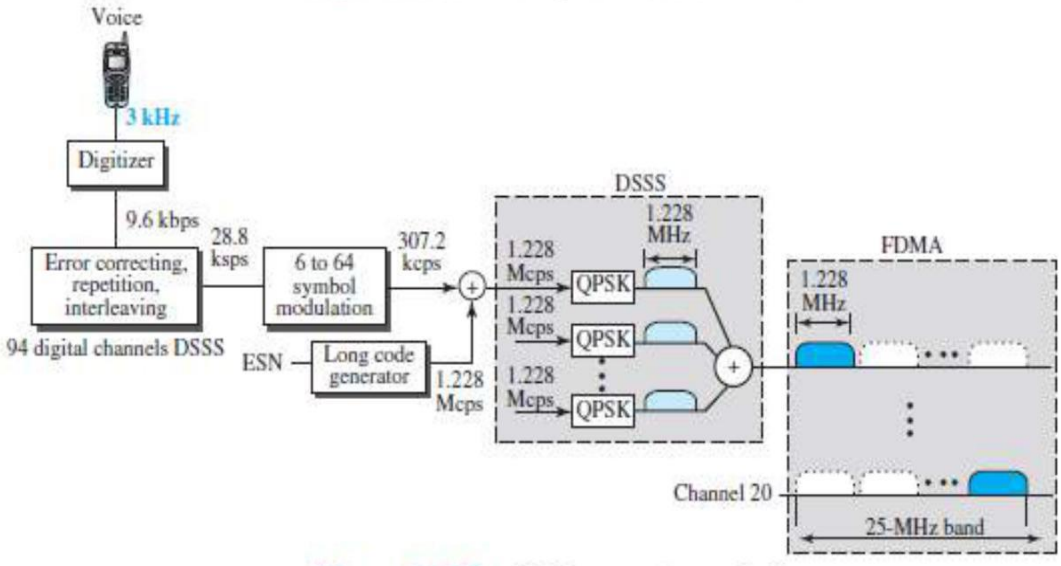


Figure 16.15 *IS-95 reverse transmission*

3) Synchronization

All base channels need to be synchronized to use CDMA.
To provide synchronization, bases use the services of a satellite system (GPS).

4) Two Data Rate Sets

IS-95 defines two data-rate sets:

The first set defines 9600, 4800, 2400, and 1200 bps.
The second set defines 14,400, 7200, 3600, and 1800 bps.

5) Frequency-Reuse Factor

The frequency-reuse factor is normally 1 because the interference from neighboring cells cannot affect CDMA or DSSS transmission.

6) Soft Handoff

Every base-station continuously broadcasts signals using its pilot channel.
Thus, a mobile-station can detect the pilot signal from its cell and neighboring cells.
This enables a mobile-station to do a soft handoff.

5.2.4 Third Generation (3G)

3G cellular telephony provides both digital data and voice communication.

For example: Using a Smartphone,

A person can talk to anyone else in the world.

A person can download a movie, surf the Internet or play games.

Interesting characteristics: the Smartphone is always connected; we do not need to dial a number to connect to the Internet. (IMT → Internet Mobile Communication)

Some objectives defined by the blueprint IMT-2000 (3G working group):

Voice quality comparable to that of the existing public telephone network.

Data-rate of

144 kbps for access in a moving vehicle (car)

384 kbps for access as the user walks (pedestrians) and

2 Mbps for the stationary user (office or home).

Support for packet-switched and circuit-switched data services.

A band of 2 GHz.

Bandwidths of 2 MHz.

Interface to the Internet

5.2.4.1 IMT-2000 Radio Interfaces

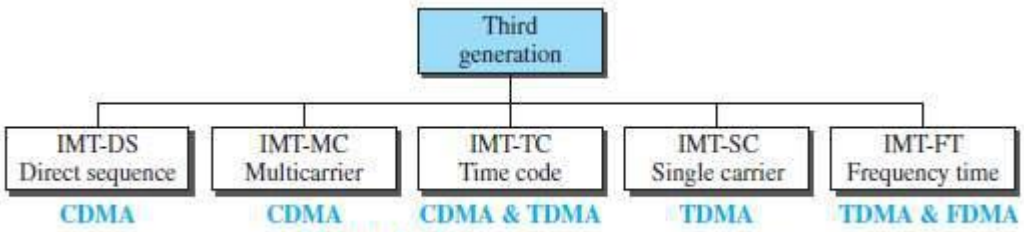


Figure 16.16 *IMT-2000 radio interfaces*

Radio interfaces (wireless standards) adopted by IMT-2000 (Figure 16.16):

IMT-DS

This uses a version of CDMA called W-CDMA (wideband CDMA).
W-CDMA uses a 5-MHz bandwidth.
It is compatible with the CDMA used in IS-95.

2) IMT-MC

This was known as CDMA 2000.
It is an evolution of CDMA technology used in IS-95 channels.
It combines

new wideband (15-MHz) spread spectrum &
narrowband (1.25-MHz) CDMA of IS-95.

It is backward-compatible with IS-95.
It allows communication on multiple 1.25-MHz channels up to 15 MHz.

3) IMT-TC

This uses a combination of W-CDMA and TDMA.
It tries to reach the IMT-2000 goals by adding TDMA multiplexing to W-CDMA.

4) IMT-SC

This uses only TDMA.

5) IMT-FT

This uses a combination of FDMA and TDMA.

5.2.5 Fourth Generation (4G)

4G cellular telephony is expected to be a complete evolution in wireless communications.

Some objectives defined by the 4G working group:

- A spectrally efficient system.
- High network capacity.
- Data-rate of
  - 100 Mbps for access in a moving vehicle
  - 1 Gbps for stationary users and
  - 100 Mbps between any two points in the world.
- Smooth handoff across heterogeneous networks.
- Seamless connectivity and global roaming across multiple networks.
- High quality of service for next generation multimedia support.
- Interoperability with existing wireless standards.
- All IP, packet-switched, networks.

4G is only packet-based networks.

4G supports IPv6.

4G provides better multicast, security, and route optimization capabilities.

- Here we discuss, following issues: 1) Access Scheme 2) Modulation 3) Radio System 4) Antenna 5) Applications

1) Access Scheme

- To increase efficiency,
  i) capacity, ii) scalability & iii) new access techniques are being considered for 4G.
- For example:
  i) OFDMA and IFDMA are being considered for the downlink & uplink of the next generation UMTS. ii) MC-CDMA is proposed for the IEEE 802.20 standard.

2) Modulation

More efficient 64-QAM is being proposed for use with the LTE standards.

3) Radio System

The 4G uses a SDR system.

The components of an SDR are pieces of software and thus flexible.

The SDR can change its program to shift its frequencies to mitigate frequency interference.

4) Antenna

The MIMO and MU-MIMO antenna system is proposed for 4G.

Using this antenna, 4G allows independent streams to be transmitted simultaneously from all the antennas to increase the data-rate.

MIMO also allows the transmitter and receiver coordinates to move to an open frequency when interference occurs.

5) Applications

At the present rates of 15-30 Mbps, 4G is capable of providing users with streaming high-definition television.

At 100 Mbps, the content of a DVD-5 can be downloaded within about 5 minutes for offline access.

(OFDMA → Orthogonal FDMA IFDMA → interleaved FDMA)
(LTE → Long Term Evolution SDR → Software Defined Radio)
(MIMO → multiple-input multiple-output MU-MIMO → multiuser MIMO)
(UMTS → Universal Mobile Telecommunications System)
(MC-CDMA → multicarrier code division multiple access)

5.3 SATELLITE NETWORKS

A satellite network is a combination of nodes that provides communication from one point on the Earth to another.

A node can be
- Satellite
- Earth station or
- End-user terminal/telephone

Like cellular networks, satellite networks divide the planet into cells.

Satellites can provide transmission capability to and from any location on Earth.

Advantages:
- Satellite makes high-quality communication available to undeveloped parts of the world.
- Cost effective: A huge investment in ground-based infrastructure is not required.

General Issues for Operation of Satellites

- Three issues related to the operation of satellites:

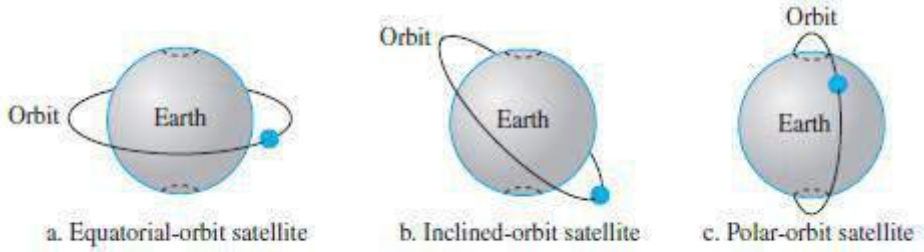
1) Orbits 2) Footprint 3) Frequency Bands for Satellite Communication

1) Orbits

An artificial satellite needs to have an orbit.

An orbit is the path in which the satellite travels around the Earth.

The orbit can be equatorial, inclined, or polar (Figure 16.17.)



a. Equatorial-orbit satellite b. Inclined-orbit satellite c. Polar-orbit satellite

Figure 16.17 *Satellite orbits*

The period means the time required for a satellite to make a complete trip around the Earth.

The period of a satellite is determined by Kepler"s law.

Kepler"s law defines period as a function of the distance of the satellite from the center of the Earth.

Example 5.1

What is the period of the moon, according to Kepler's law?

$$\text{Period} = C \times \text{distance}^{1.5}$$

Here C is a constant approximately equal to 1/100. The period is in seconds and the distance in kilometers.

Solution

The moon is located approximately 384,000 km above the Earth. The radius of the Earth is 6378 km. Applying the formula, we get the following.

$$\text{Period} = (1/100) \times (384{,}000 + 6378)^{1.5} = 2{,}439{,}090 \text{ s} = 1 \text{ month}$$

Example 5.2

According to Kepler's law, what is the period of a satellite that is located at an orbit approximately 35,786 km above the Earth?

Solution

Applying the formula, we get the following.

$$\text{Period} = (1/100) \times (35{,}786 + 6378)^{1.5} = 86{,}579 \text{ s} = 24 \text{ h}$$

This means that a satellite located at 35,786 km has a period of 24 h, which is the same as the rotation period of the Earth. A satellite like this is said to be *stationary* to the Earth.

The orbit is called a *geostationary orbit*.

2) Footprint

- Satellites process microwaves with bidirectional antennas (line-of-sight).
- Normally, the signal from a satellite is aimed at a specific area called the footprint.
- The signal-power at the center of the footprint is maximum.
- The signal-power decreases, as we move out from the footprint-center.
- The boundary of the footprint is the location where the power-level is at a predefined threshold.

3) Frequency Bands for Satellite Communication

For satellite communication, the frequencies reserved are in the GHz range.
Each satellite sends and receives over 2 different bands (Table 16.1):

Uplink: refers to the transmission from the Earth to the satellite.
Downlink: refers to the transmission from the satellite to the Earth.

Table 16.1 *Satellite frequency bands*

Band	*Downlink, GHz*	*Uplink, GHz*	*Bandwidth, MHz*
L	1.5	1.6	15
S	1.9	2.2	70
C	4.0	6.0	500
Ku	11.0	14.0	500
Ka	20.0	30.0	3500

4) Three Categories of Satellites

- Three categories of satellites based on the location of the orbit (Figure 16.18):

1) Geostationary Earth orbit (GEO)
There is only one orbit, at an altitude of 36000 km, for the GEO satellite.

2) Low-Earth-orbit (LEO)
LEO satellites are below an altitude of 2000 km.

3) Medium-Earth-orbit (MEO)

➢ MEO satellites are located at altitudes between 5000 and 15,000 km.

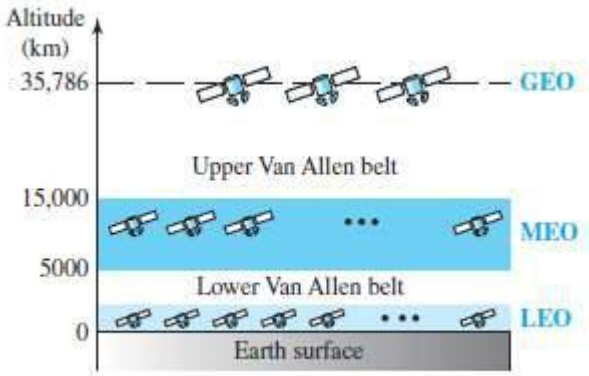


Figure 16.18 *Satellite orbit altitudes*

5.3.2 GEO Satellites

There is only one orbit at an altitude of 36,000 km (Figure 16.19).
Because orbital speed is based on the distance from the planet, only one orbit can be geostationary.
The orbit occurs at the equatorial plane.
Sending-antenna must have receiving-antenna in LOS (Line-of-sight).
Problem: A satellite that moves faster/slower than Earth"s rotation is useful only for short periods.
Solution: To ensure constant communication, the satellite must move at same speed as the Earth.
Thus, the satellite seems to remain fixed above a certain spot.

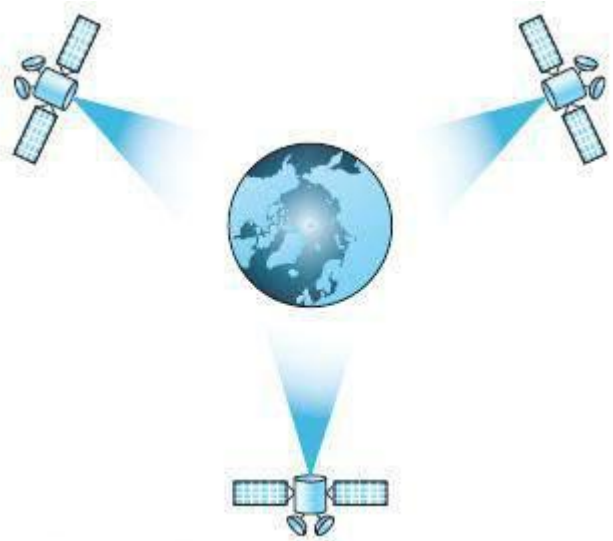


Figure 16.19 *Satellites in geostationary orbit*

5.3.3 MEO Satellites

MEO satellites are located at altitudes between 5000 and 15,000 km.
Example: Global Positioning System (GPS)

5.3.3.1 Global Positioning System

GPS consists of 24 satellites in 6 orbits (Figure 16.20).
GPS is used for land, sea, and air navigation to provide time and location for vehicles and ships.
The orbits and the locations of the satellites in each orbit are designed systematically.
For example: At any time, 4 satellites are visible from any point on Earth.

- A GPS receiver has an almanac (or calendar) that tells the current position of each satellite.
- Here we discuss, 4 issues: 1) Trilateration 2) Measuring the Distance 3) Synchronization 4) Application

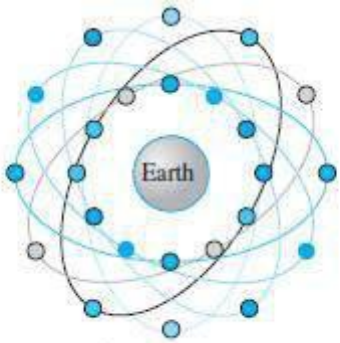


Figure 16.20 *Orbits for global positioning system (GPS) satellites*

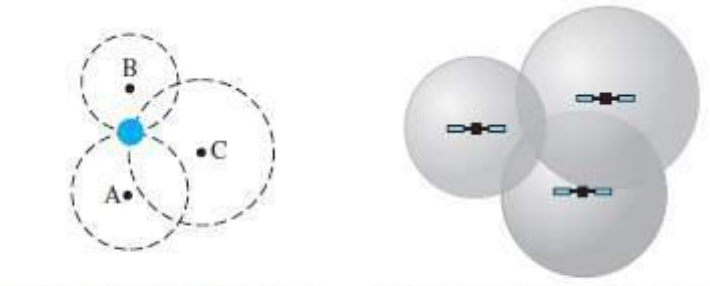
1) Trilateration

GPS is based on a principle called trilateration.
Trilateration means using three distances.
For example (Figure 16.21a):

- On a plane, if we know our distance from three points, we know exactly where we are.

Assume we are 10 miles away from point A,
12 miles away from point B, and
15 miles away from point C.

If we draw three circles with the centers at A, B, and C, we must be somewhere on circle A, somewhere on circle B, and somewhere on circle C.
These three circles meet at one single point; this is our position (Figure 16.21a).



a. Two-dimensional trilateration b. Three-dimensional trilateration

Figure 16.21 *Trilateration on a plane*

In three-dimensional space, the situation is different.
Three spheres meet in two points, (Figure 16.21b).
We need at least four spheres to find our exact position in space (longitude, latitude, and altitude).

2) Measuring the Distance

- Trilateration principle can find our location on the Earth if we know
  → our distance from 3 satellites and
  → position of each satellite.
- The position of each satellite can be calculated by a GPS receiver.
- Then, the GPS receiver needs to find its distance from at least three GPS satellites.
- The distance is measured using a principle called one-way ranging.

3) Synchronization

- Satellites use atomic clocks, which are precise and can function synchronously with each other.
- The receiver"s clock is a normal quartz clock.
- However, there is no way to synchronize receiver"s clock with the satellite"s clock.
- There is an unknown offset between the satellite-clocks and the receiver-clock.
- The unknown offset introduces a corresponding offset in the distance calculation.
- Because of the offset, the measured distance is called a pseudo-range.

4) Applications

1) GPS is used by military forces.
For example:
Thousands of portable GPS receivers were used during the WW2 by foot soldiers, vehicles, and helicopters.
2) GPS is used in navigation.
For example:
The driver of a car can find the location of the car. 3) GPS is used for clock synchronization.

5.3.4 LEO Satellites

LEO satellites have polar orbits.

Usually, a LEO system has a cellular type of access (similar to the cellular telephone system).

Specifications:

Altitude = 500 to 2000 km
Rotation Period = 90 to 120 min
Satellite Speed =20,000 to 25,000 km/h
Footprint Diameter = 8000 km
Round-Trip Time < 20 ms

Because LEO satellites are close to Earth, 20 ms RTT is normally acceptable for audio communication.

A LEO system is made of a group of satellites that work together as a network.

Each satellite acts as a switch.

Different types of links (Figure 16.22):

1) ISLs (Inter-Satellite Links)
Satellites that are close to each other are connected through ISLs.

2) UML (User Mobile Link)
A mobile system communicates with the satellite through a UML.

3) GWL (Gate Way Link)
A satellite communicates with the Earth station (gateway) through a GWL.

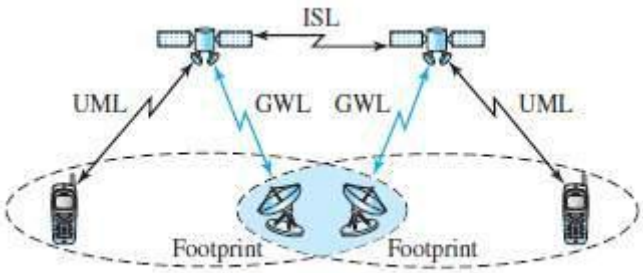


Figure 16.22 *LEO satellite system*

- LEO satellites can be divided into three categories:

1) Little LEO
Operating frequency < 1 GHz.
They are mostly used for low data-rate messaging.

2) Big LEO
Operating frequency = 1 to 3 GHz.
Examples: Globalstar & Iridium

	Globalstar	Iridium
Orbit-Altitude	1400 km	750 km
No. of Satellites	48	66
No. of Orbits	6	6
Satellites per Orbit	8	11

3) Broadband LEO
Broadband LEO provides communication similar to fiber-optic networks.
Example: Teledesic
Teledesic satellite provides fiber-optic-like communication (broadband channels, low error rate, and low delay).
Main purpose: To provide broadband Internet access for users all over the world.

MODULE 5: NETWORK LAYER PROTOCOLS

5.4 Network Layer Protocols

The network layer contains following 4 protocols (Figure 19.1):

Internet Protocol (IP)

IP is the main protocol responsible for packetizing, forwarding, and delivery of a packet at the network layer.

2) Internet Control Message Protocol (ICMP)

ICMP helps IP to handle some errors that may occur in the network-layer delivery.

3) Internet Group Management Protocol (IGMP)

IGMP is used to help IPv4 in multicasting.

4) Address Resolution Protocol (ARP)

ARP is used to glue the network and data-link layers in mapping network-layer addresses to link-layer addresses.

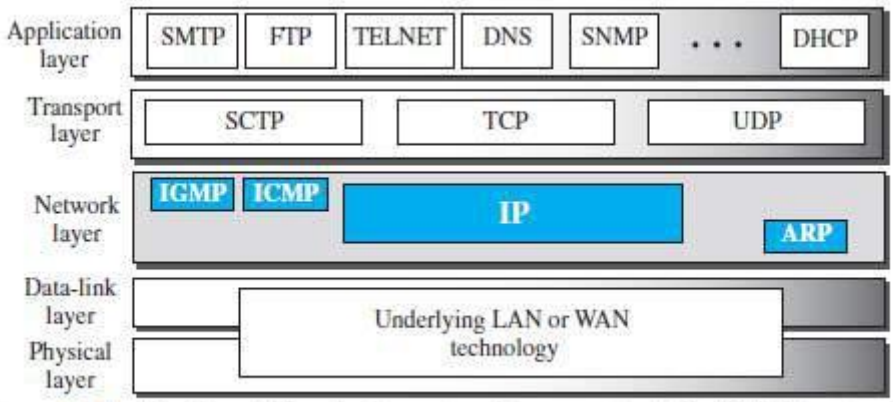


Figure 19.1 *Position of IP and other network-layer protocols in TCP/IP protocol suite*

5.5 INTERNET PROTOCOL (IP)

5.5.1 Internet Protocol (IP)

IP is main protocol responsible for packetizing, forwarding & delivery of a packet at network layer.
IP is an unreliable datagram protocol.
IP provides a best-effort delivery service.
The term best-effort means that the packets can
- be corrupted
- be lost or
- arrive out-of-order.

If reliability is important, IP must be paired with a TCP which is reliable transport-layer protocol.
IP is a connectionless protocol.
IP uses the datagram approach.
- Each datagram is handled independently.
- Each datagram can follow a different route to the destination.
- Datagrams may arrive out-of-order at the destination.

5.5.2 Datagram Format

- IP uses the packets called datagrams.
- A datagram consist of 2 parts (Figure 19.2): 1) Payload 2) Header.

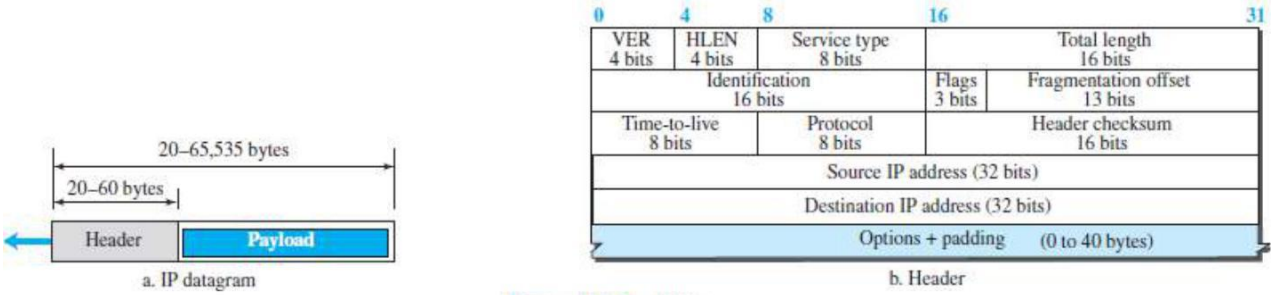


Figure 19.2 *IP datagram*

1) Payload

Payload (or Data) is the main reason for creating a datagram.
Payload is the packet coming from other protocols that use the service of IP.

2) Header

Header contains information essential to routing and delivery.
IP header contains following fields:

1) Version Number (VER)
This field indicates version number used by the packet. Current version=4

2) Header Length (HLEN)
This field specifies length of header.
When a device receives a datagram, the device needs to know
when the header stops and
when the data starts.

3) Service Type
This field specifies priority of packet based on delay, throughput, reliability & cost requirements.

4) Total Length
This field specifies the total length of the datagram (header plus data).
Maximum length=65535 bytes.

5) Identification, Flags, and Fragmentation Offset
These 3 fields are used for fragmentation and reassembly of the datagram.
Fragmentation occurs when the size of the datagram is larger than the MTU of the network.

6) Time-to-Live (TTL)
This field is indicates amount of time, the packet is allowed to remain in the network.
If TTL becomes 0 before packet reaches destination, the router
discards packet and
sends an error-message back to the source.

7) Protocol
This field specifies upper-layer protocol that is to receive the packet at the destination-host.
For example (Figure 19.3):
For TCP, protocol = 6 For UDP, protocol = 17

8) Header Checksum
This field is used to verify integrity of header only.
If the verification process fails, packet is discarded.

9) Source and Destination Addresses
These 2 fields contain the IP addresses of source and destination hosts.

10) Options
This field allows the packet to request special features such as
security level
route to be taken by packet and
timestamp at each router.
This field can also be used for network testing and debugging.

11) Padding

- This field is used to make the header a multiple of 32-bit words.

Example 5.3

An IPv4 packet has arrived with the first 8 bits as $(01000010)_2$. The receiver discards the packet. Why?

Solution

There is an error in this packet. The 4 leftmost bits $(0100)_2$ show the version, which is correct. The next 4 bits $(0010)_2$ show an invalid header length $(2 \times 4 = 8)$. The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

Example 5.4

In an IPv4 packet, the value of HLEN is $(1000)_2$. How many bytes of options are being carried by this packet?

Solution

The HLEN value is 8, which means the total number of bytes in the header is 8×4, or 32 bytes. The first 20 bytes are the base header, the next 12 bytes are the options.

Example 5.5

In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is $(0028)_{16}$. How many bytes of data are being carried by this packet?

Solution

The HLEN value is 5, which means the total number of bytes in the header is 5×4, or 20 bytes (no options). The total length is $(0028)_{16}$ or 40 bytes, which means the packet is carrying 20 bytes of data $(40 - 20)$.

(Comparing a datagram to a postal package.
Payload is the content of the package.
Header is only the information written on the package).

5.5.3 Fragmentation

5.5.3.1 Maximum Transfer Unit (MTU)

Each network imposes a restriction on maximum size of packet that can be carried. This is called the MTU (maximum transmission unit).

For example:

For Ethernet, MTU = 1500 bytes

For FDDI, MTU = 4464 bytes

When IP wants send a packet that is larger than MTU of physical-network, IP breaks packet into smaller fragments. This is called fragmentation (Figure 19.5).

Designers have decided to make the maximum length of IP datagram = 65,535 bytes. This ensures that the IP protocol is independent of the physical network,

When a datagram is fragmented, each fragment has its own header.

A fragmented-datagram may itself be fragmented if it encounters a network with an even smaller MTU.

Source host or router is responsible for fragmentation of original datagram into the fragments.

Destination host is responsible for reassembling the fragments into the original datagram.

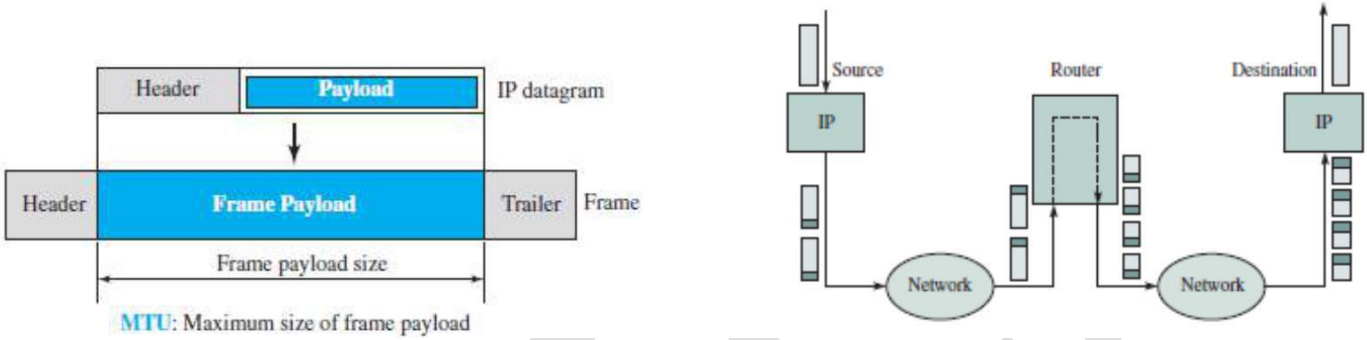


Figure 19.5b: Packet Fragmentation

5.5.3.2 Fields Related to Fragmentation & Reassembly

• Three fields in the IP header are used to manage fragmentation and reassembly:

1) Identification 2) Flags 3) Fragmentation offset.

1) Identification

• This field is used to identify to which datagram a particular fragment belongs to (so that fragments for different packets do not get mixed up).

• To guarantee uniqueness, the IP protocol uses an up-counter to label the datagrams.

• When the IP protocol sends a datagram, IP protocol

→ copies the current value of the counter to the identification field and

→ increments the up-counter by 1.

• When a datagram is fragmented, the value in the identification field is copied into all fragments.

• The identification number helps the destination in reassembling the datagram.

2) Flags

This field has 3 bits.

The leftmost bit is not used.

DF bit (Don't Fragment):

If DF=1, the router should not fragment the datagram. Then, the router discards the datagram and sends an error-message to the source host.

If DF=0, the router can fragment the datagram if necessary.

MF bit (More Fragment):

If MF=1, there are some more fragments to come.

If MF=0, this is last fragment.

3) Fragmentation Offset

This field identifies location of a fragment in a packet.

This field is the offset of the data in the original datagram.

Example 5.6

A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

If the M bit is 0, it means that there are no more fragments; the fragment is the last one. However, we cannot say if the original packet was fragmented or not. A nonfragmented packet is considered the last fragment.

Example 5.7

A packet has arrived with an M bit value of 1. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

If the M bit is 1, it means that there is at least one more fragment. This fragment can be the first one or a middle one, but not the last one. We don't know if it is the first one or a middle one; we need more information (the value of the fragmentation offset).

Example 5.8

A packet has arrived with an M bit value of 1 and a fragmentation offset value of 0. Is this the first fragment, the last fragment, or a middle fragment?

Solution

Because the M bit is 1, it is either the first fragment or a middle one. Because the offset value is 0, it is the first fragment.

Example 5.9

A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?

Solution

To find the number of the first byte, we multiply the offset value by 8. This means that the first byte number is 800. We cannot determine the number of the last byte unless we know the length of the data.

Example 5.10

A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte?

Solution

The first byte number is $100 \times 8 = 800$. The total length is 100 bytes, and the header length is 20 bytes (5×4), which means that there are 80 bytes in this datagram. If the first byte number is 800, the last byte number must be 879.

5.5.4 Options

This field allows the packet to request special features such as
security level
route to be taken by packet and
timestamp at each router.

This field can also be used for network testing and debugging.

As the name implies, options are not required for a datagram.

The header is made of two parts: 1) Fixed part and 2) Variable part.
Maximum size of Fixed part = 20 bytes.
Maximum size of Variable part = 40 bytes

Options are divided into two broad categories: 1) Single-byte options and 2) Multiple-byte options.

1) Single Byte Options

i) No Operation
This option is used as filler between options.

ii) End of Option
This option is used for padding at the end of the option field.

Multiple Byte Options

i) Record Route
- This option is used to record the routers that handle the datagram.

This option can list up to 9 router-addresses.

ii) Strict Source Route
This option is used by the source to pre-determine a route for the datagram.
Useful purposes: The sender can choose a route with a specific type of service, such as
minimum delay
maximum throughput or
more secure/reliable.
All the defined-routers must be visited by the datagram.
If the datagram visits a router that is not on the list, the datagram is discarded.

iii) Loose Source Route
This option is similar to the strict source route, but it is less rigid.
Each router in the list must be visited, but the datagram can visit other routers as well.

iv) Timestamp
This option is used to record the time of datagram processing by a router.
The time is expressed in milliseconds from midnight GMT (Greenwich Mean Time).
The recorded-time can help the managers to track the behavior of the routers in the Internet.

5.5.5 Security of IPv4 Datagrams

Nowadays, the Internet is not secure anymore.

Three security issues applicable to the IP protocol:

Packet sniffing
Packet modification and
IP spoofing.

1) Packet Sniffing

Attackers may

capture certain packets
intercept the packets and
make a copy of the packets.

Packet sniffing is a passive attack.

Passive attack means the attacker does not modify the contents of the packet.

The attack is difficult to detect „." sender & receiver may never know that the packet has been copied.

Solution:

Although the attack cannot be stopped, encryption of packet may make the attacker"s job difficult.

The attacker may still sniff the packet, but the content is not detectable (or understandable).

2) Packet Modification

Attackers may succeed in accessing the content of a packet.

Then, the attacker can

change the address of the packet or
change the data of the packet

Solution:

The attack can be prevented by data integrity mechanism.

Data integrity guarantees that the packet is not modified during the transmission.

3) IP Spoofing

The attacker pretends as a trusted entity and obtains all the secret information.

For example:

An attacker sends an IP packet to a bank pretending as legitimate customers.

- Solution:

The attack can be prevented using an origin-authentication mechanism.

5.5.5.1 IPSec (IP Security)

- IP packets can be protected from the various network-attacks using a protocol called IPSec.
- IPSec protocol & IP protocol can be used to create a connection-oriented service between 2 entities.
- Four services of IPSec:

1) Defining Algorithms & Keys

To create a secure channel b/w two entities, the two entities can agree on some available algorithms and keys.

2) Packet Encryption

To provide privacy, the packets exchanged b/w two parties can be encrypted using the encryption-algorithms and a shared key.

This prevents the packet sniffing attack.

3) Data Integrity

Data integrity guarantees that the packet is not modified during the transmission.
If the received packet does not pass the data integrity test, the packet is discarded.
This prevents the packet modification attack.

4) Origin Authentication

Origin Authentication guarantees that the packet is not created by a pretender.
This prevents the IP Spoofing attack.

5.6 ICMP

ICMP is a network-layer protocol.

This is used to handle error and other control messages.

5.6.1 MESSAGES

ICMP messages are divided into 2 broad categories:

Error-Reporting Messages

These messages report problems that a router or a host may encounter during the processing of datagram.

2) Query Messages

These messages help a host or a network manager get specific information from a router or another host.

For example:

Nodes can discover their neighbors.

Hosts can discover and learn about routers on their network. Routers can help a node redirect the messages.

Fields of ICMP messages (Figure 19.8):

Type: This field identifies the type of message.

Code: This field specifies the reason for the particular message type.

For example,

Type 03 = problem reaching the destinations

Type 11 = problem related to time exceeded.

Checksum: This field is used to detect errors in the ICMP message.

Data section: This field can be used for diagnostic purposes by matching the information in the ICMP message with the original data in the IP packet.

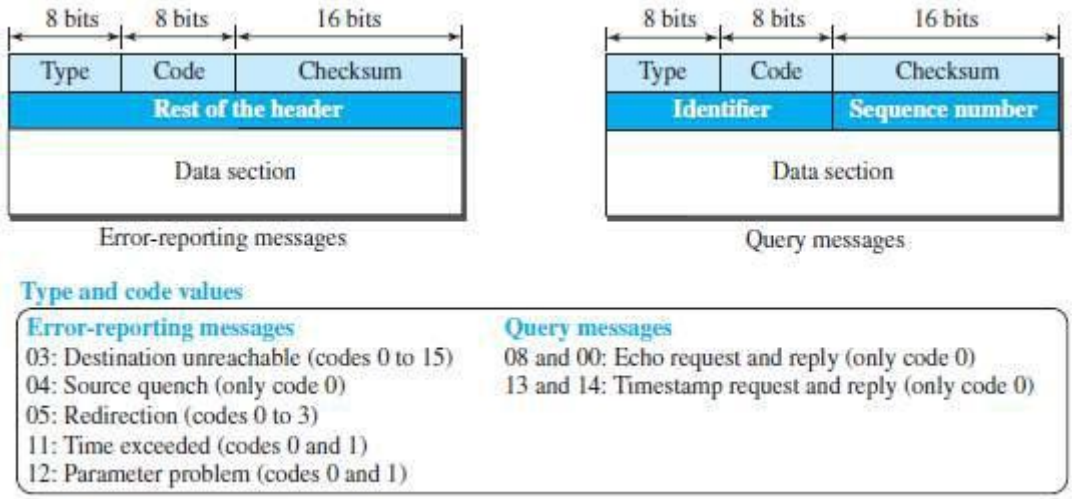


Figure 19.8 *General format of ICMP messages*

5.6.1.1 Error Reporting Messages

Main responsibility of ICMP: To report some errors that may occur during the processing of the datagram (Figure 19.9).

These messages report problems that a router or a host may encounter during the processing of datagram.

ICMP does not correct errors; ICMP simply reports the errors to the source.

Error correction is left to the higher-level protocols (such as TCP or UDP)

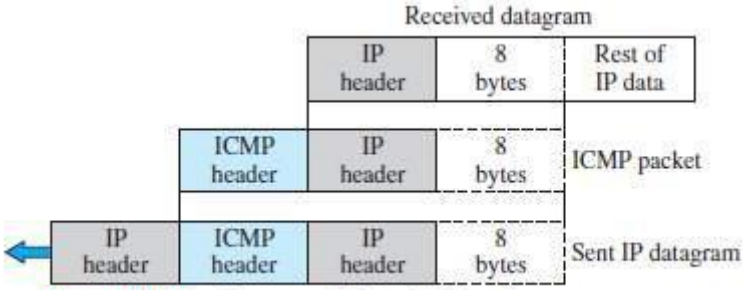


Figure 19.9 *Contents of data field for the error messages*

Rules for reporting messages:

No error-message will be generated for a datagram having a multicast address (or special address).

No error-message will be generated in response to a datagram carrying an ICMP error-message.

No error-message will be generated for a fragmented datagram that is not the first fragment.

1) Destination Unreachable (Type=3)

This message is related to problem reaching the destinations.

This message uses different codes (0 to 15) to define type of error-message.

Possible values for code field:

Code 0 = network unreachable
Code 1 = host unreachable
Code 2 = protocol unreachable
Code 3 = port unreachable

2) Source Quench (Type=4)

This message informs the sender that
network has encountered congestion and
datagram has been dropped.

The source needs to slow down sending more datagrams.

In other words, ICMP adds a kind of congestion control mechanism to the IP protocol.

3) Redirection Message (Type=5)

This is used when the source uses a wrong router to send out its message.

The router
redirects the message to the appropriate router &
informs the source to change its default router in the future.

The IP address of the default router is sent in the message.

TTL prevents a datagram from being aimlessly circulated in the Internet.

When TTL becomes 0,
the datagram is dropped by the visiting router and
a time exceeded message (type 11) is sent to the source.

4) Parameter Problem (Type=12)

This message can be sent when either
there is a problem in the header of a datagram (code 0) or
some options are missing or cannot be interpreted (code 1).

5.6.1.2 Query Messages

- These messages help a network manager to get specific information from a router or host.
- Two types of query messages: request (type 8) and reply (type 0).

1) Echo Request & Echo Reply

- These messages are used to determine whether a remote-host is alive.
- A source-host sends an echo request message to destination-host;

If the destination-host is alive, it responds with an echo reply message.

Type=8 is used for echo request
Type=0 is used for echo reply.
These messages can be used in two debugging tools: ping and traceroute.

2) Timestamp Request & Timestamp Reply

These messages are used to

find the round-trip time between two devices or
check whether the clocks in two devices are synchronized.

The timestamp request sends a number, which defines the time the message is sent.
The timestamp reply resends another number, which defines the time the message is sent.
The timestamp reply also includes 2 new numbers representing

the time the request was received and
the time the response was sent.

Type=13 is used for timestamp request
Type=14 is used for timestamp reply.

5.6.2 Debugging Tools

There are several tools that can be used in the Internet for debugging.
We can determine the viability of a host or router.
We can trace the route of a packet.
Two tools used for debugging: 1) Ping and 2) Traceroute.

5.6.2.1 Ping

The ping program can be used to find if a host is alive and responding
Here, ping is used to see how it uses ICMP packets
The source host sends ICMP echo-request messages;
The destination, if alive, responds with ICMP echo-reply messages.
The ping program
sets the identifier field in the echo-request and echo-reply message and
starts the sequence number from 0; this number is incremented by 1 each time a new message is sent.
Ping can calculate the round-trip time.
It inserts the sending time in the data section of the message.
When the packet arrives, it subtracts the arrival time from the departure time to get the round-trip time (RTT).

5.6.2.2 Traceroute

The traceroute program can be used to trace the path of a packet from a source to the destination.
It can find the IP addresses of all the routers that are visited along the path.
The program is usually set to check for the maximum of 30 hops (routers) to be visited.

Traceroute

The traceroute program is different from the ping program.
The ping program gets help from 2 query messages;
The traceroute program gets help from two error-reporting messages: time-exceeded and destination-unreachable.
The traceroute is an application layer program, but only the client program is needed. In other words, there is no traceroute server program.
The traceroute application program is encapsulated in a UDP user datagram, but traceroute intentionally uses a port number that is not available at the destination.

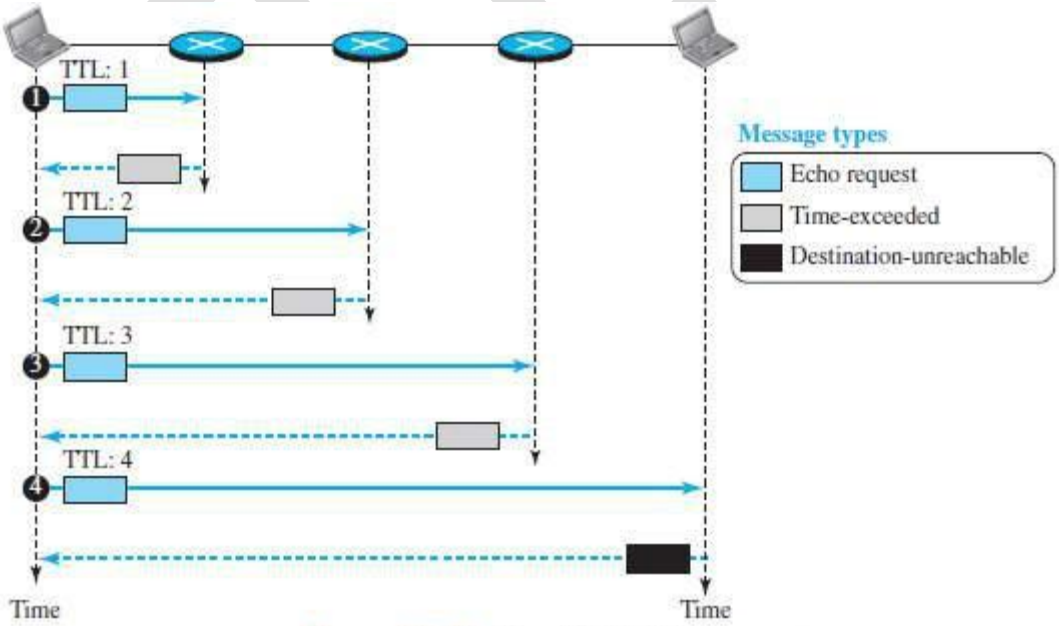


Figure 19.10 *Use of ICMPv4 in traceroute*

5.7 MOBILE IP

Mobile IP is the extension of IP protocol.
Mobile IP allows mobile computers to be connected to the Internet.

5.7.1 Addressing

In Mobile IP, the main problem that must be solved is addressing.

5.7.1.1 Stationary Hosts

The original IP addressing assumed that a host is stationary.
A router uses an IP address to route an IP datagram.
An IP address has two parts: a prefix and a suffix.
The prefix associates a host with a network.

For example, the IP address 10.3.4.24/8 defines a host attached to the network 10.0.0.0/8.

- The address is valid only when the host is attached to the network.

If the network changes, the address is no longer valid.

5.7.1.2 Mobile Hosts

When a host moves from one network to another, the IP addressing structure needs to be modified.
The host has two addresses (Figure 19.12):

Home address &
Care-of address

Home Address

Original address of host called the home address.
The home address is permanent.
The home address associates the host with its home network.
Home network is a network that is the permanent home of the host.

2) Care-of-Address

The care-of address is temporary.
The care-of address changes as the mobile-host moves from one network to another.
Care-of address is associated with the foreign network.
Foreign network is a network to which the host moves.

When a mobile-host visits a foreign network, it receives its care-of address during the agent discovery and registration phase.

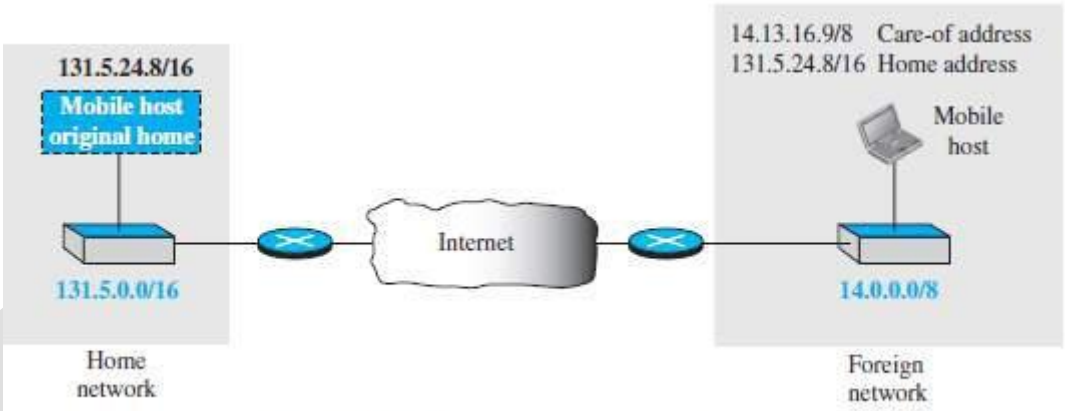


Figure 19.12 *Home address and care-of address*

5.7.2 Agents

Two agents are required to make change of address transparent to rest of the Internet (Fig 19.13):

Home-agent and
Foreign-agent.

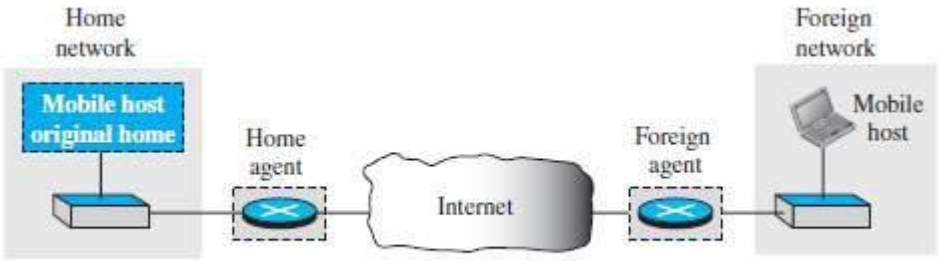


Figure 19.13 *Home agent and foreign agent*

1) Home Agent

- The home-agent is a router attached to the home network.
- The home-agent acts on behalf of mobile-host when a remote-host sends a packet to mobile-host.
- The home-agent receives and delivers packets sent by the remote-host to the foreign-agent.

2) Foreign Agent

The foreign-agent is a router attached to the foreign network.

The foreign-agent receives and delivers packets sent by the home-agent to the mobile-host.

The mobile-host can also act as a foreign-agent i.e. mobile-host and foreign-agent can be the same. However, to do this, a mobile-host must be able to receive a care-of address by itself.

In addition, the mobile-host needs the necessary software to allow it to communicate with the home-agent and to have two addresses: i) its home address and ii) its care-of address.

This dual addressing must be transparent to the application programs.

Collocated Care-of-Address

When the mobile-host and the foreign-agent are the same, the care-of-address is called a collocated care-of-address.

Advantage:

mobile-host can move to any network w/o worrying about availability of a foreign-agent.

Disadvantage:

The mobile-host needs extra software to act as its own foreign-agent.

5.7.3 Three Phases

To communicate with a remote-host, a mobile-host goes through 3 phases (Figure 19.14):

Agent Discovery: involves the mobile-host, the foreign-agent, and the home-agent.
Registration: involves the mobile-host, the foreign-agent, and the home-agent.
Data Transfer: Here, the remote-host is also involved.

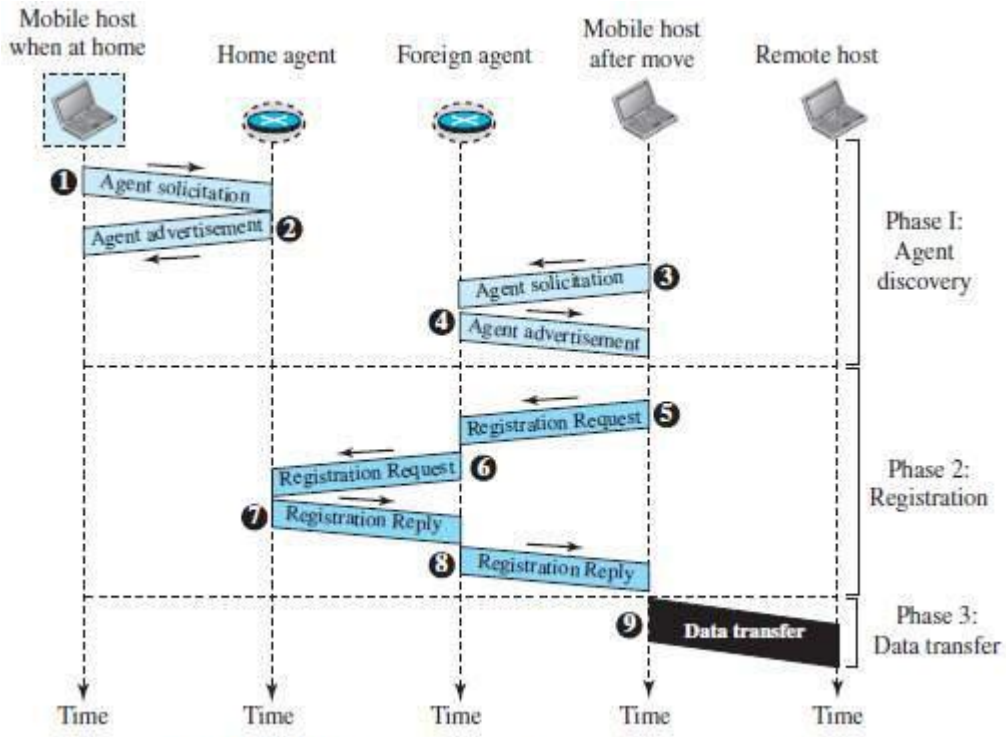


Figure 19.14 *Remote host and mobile host communication*

5.7.3.1 Agent Discovery

Agent discovery consists of two subphases:

A mobile-host must discover (learn the address of) a home-agent before it leaves its home network.

A mobile-host must also discover a foreign-agent after it has moved to a foreign network.

This discovery consists of learning the care-of address as well as the foreign-agent"s address.

Two types of messages are used: i) advertisement and ii) solicitation.

1) Agent Advertisement

• When a router advertises its presence on a network using an ICMP router advertisement, it can append an agent advertisement to the packet if it acts as an agent.

Figure 19.15 *Agent advertisement*

• Various fields are (Figure 19.15):

1) Type
This field is set to 16.

2) Length
This field defines the total length of the extension message.

3) Sequence Number
This field holds the message number.
The recipient can use the sequence number to determine if a message is lost.

4) Lifetime
This field defines the number of seconds that the agent will accept requests.
If the value is a string of 1s, the lifetime is infinite.

5) Code

➢ This field is a flag in which each bit is set (1) or unset (0) (Table 19.1).

Table 19.1 *Code Bits*

Bit	*Meaning*
0	Registration required. No collocated care-of address.
1	Agent is busy and does not accept registration at this moment.
2	Agent acts as a home agent.
3	Agent acts as a foreign agent.
4	Agent uses minimal encapsulation.
5	Agent uses generic routing encapsulation (GRE).
6	Agent supports header compression.
7	Unused (0).

6) Care-of Addresses
This field contains a list of addresses available for use as care-of addresses.
The mobile-host can choose one of these addresses.
The selection of this care-of address is announced in the registration request.

Agent Solicitation

When a mobile-host has moved to a new network and has not received agent advertisements, it can initiate an agent solicitation.

It can use the ICMP solicitation message to inform an agent that it needs assistance

5.7.3.2 Registration

After a mobile-host has moved to a foreign network and discovered the foreign-agent, it must register.

Four aspects of registration:

The mobile-host must register itself with the foreign-agent.

The mobile-host must register itself with its home-agent. This is normally done by the foreign-agent on behalf of the mobile-host.

The mobile-host must renew registration if it has expired.

The mobile-host must cancel its registration (deregistration) when it returns home.

5.7.3.2.1 Request & Reply

To register with the foreign-agent and the home-agent, the mobile-host uses a registration request and a registration reply.

1) Registration Request

A registration request is sent from the mobile-host to the foreign-agent

to register its care-of address and
to announce its home address and home-agent address.

Foreign-agent, after receiving and registering the request, relays the message to the home-agent.

The home-agent now knows the address of the foreign-agent because the IP packet that is used for relaying has the IP address of the foreign-agent as the source address.

Figure 19.16 *Registration request format*

Various fields are (Figure 19.16):

Type

This field defines the type of message.
For a request message the value of this field is 1.

2) Flag

This field defines forwarding information.
The value of each bit can be set or unset (Table 19.2).

Table 19.2 *Registration request flag field bits*

Bit	*Meaning*
0	Mobile host requests that home agent retain its prior care-of address.
1	Mobile host requests that home agent tunnel any broadcast message.
2	Mobile host is using collocated care-of address.
3	Mobile host requests that home agent use minimal encapsulation.
4	Mobile host requests generic routing encapsulation (GRE).
5	Mobile host requests header compression.
6–7	Reserved bits.

3) Lifetime

- This field defines the number of seconds the registration is valid.
  - i) If the field is a string of 0s, the request message is asking for deregistration.
  - ii) This field If the field is a string of 1s, the lifetime is infinite.

4) Home Address

- This field contains the permanent (first) address of the mobile-host.

5) Home Agent Address

- This field contains the address of the home-agent.

6) Care-of-Address
This field is the temporary (second) address of the mobile-host.

7) Identification
This field contains a 64-bit number that is inserted into the request by the mobile-host.
This field matches a request with a reply.

8) Extensions
This field is used for authentication.
This field allows a home-agent to authenticate the mobile agent.

Registration Reply

A registration reply is sent from home-agent to foreign-agent and then relayed to the mobile-host. The reply confirms or denies the registration request. (Figure 19.17)

The fields are similar to registration request with the 3 exceptions:

The value of the type field is 3.

The code field replaces the flag field and shows the result of the registration request (acceptance or denial).

The care-of address field is not needed.

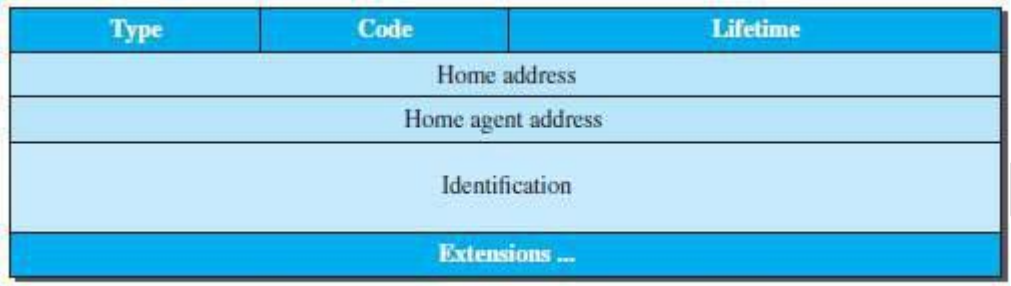


Figure 19.17 *Registration reply format*

5.7.3.3 Data Transfer

• After agent discovery & registration, a mobile-host can communicate with a remote-host (Fig 19.17).

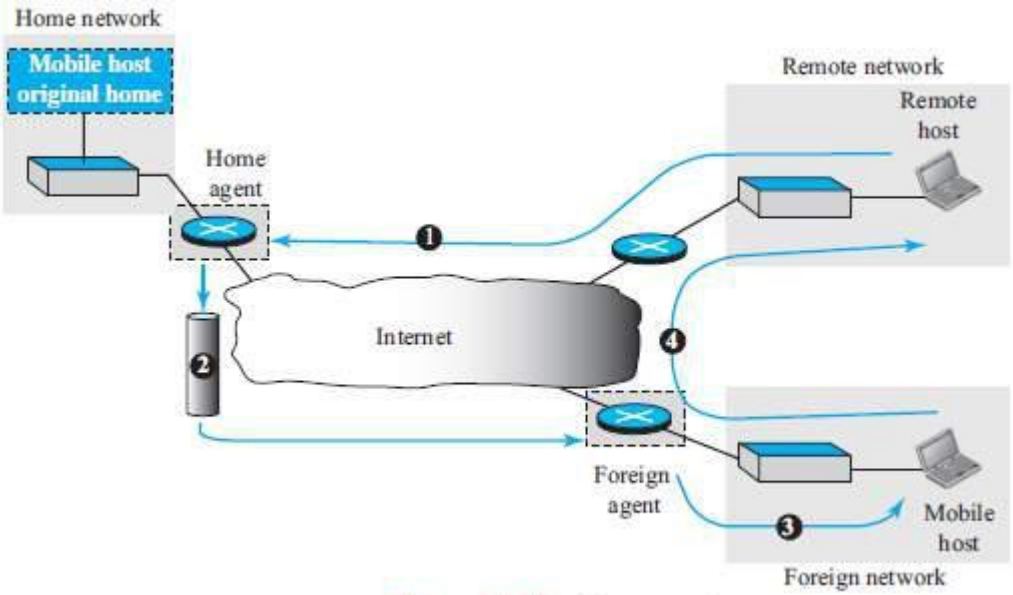


Figure 19.18 *Data transfer*

Here we have 4 cases (Figure 19.18):

1) From Remote-host to Home Agent

When a remote-host wants to send a packet to the mobile-host, the remote-host uses
address of itself as the source address and
home address of the mobile-host as the destination address.

In other words, the remote-host sends a packet as though the mobile-host is at its home network.

The packet is intercepted by the home-agent, which pretends it is the mobile-host.

This is done using the proxy ARP technique (Path 1 of Figure 19.18).

2) From Home Agent to Foreign Agent

After receiving the packet, the home-agent sends the packet to the foreign-agent, using the tunneling concept.

The home-agent encapsulates the whole IP packet inside another IP packet using its address as the source and the foreign-agent"s address as the destination. (Path 2 of Figure 19.18).

3) From Foreign Agent to Mobile Host

When the foreign-agent receives the packet, it removes the original packet.

However, since the destination address is the home address of the mobile-host, the foreign-agent consults a registry table to find the care-of address of the mobile-host. (Otherwise, the would just be sent back to the home network.)

The packet is then sent to the care-of address (Path 3 of Figure 19.18).

4) From Mobile Host to Remote Host

When a mobile-host wants to send a packet to a remote-host (for example, a response to the packet it has received), it sends as it does normally.

The mobile-host prepares a packet with its home address as the source, and the address of the remote-host as the destination.

Although the packet comes from the foreign network, it has the home address of the mobile-host (Path 4 of Figure 19.18).

5.7.4 Inefficiency in Mobile IP

Communication involving mobile IP can be inefficient.

The inefficiency can be severe or moderate.

The severe case is called double crossing or 2X.

The moderate case is called triangle routing or dog-leg routing.

5.7.4.1 Double Crossing

Double crossing occurs when a remote-host communicates with a mobile-host that has moved to the same network (or site) as the remote-host (Figure 19.19).

When the mobile-host sends a packet to the remote-host, there is no inefficiency; the communication is local.

However, when remote-host sends a packet to mobile-host, the packet crosses the Internet twice.

Since a computer usually communicates with other local computers (principle of locality), the inefficiency from double crossing is significant.

5.7.4.2 Triangle Routing

Triangle routing occurs when the remote-host communicates with a mobile-host that is not attached to the same network (or site) as the mobile-host.

When the mobile-host sends a packet to the remote-host, there is no inefficiency.

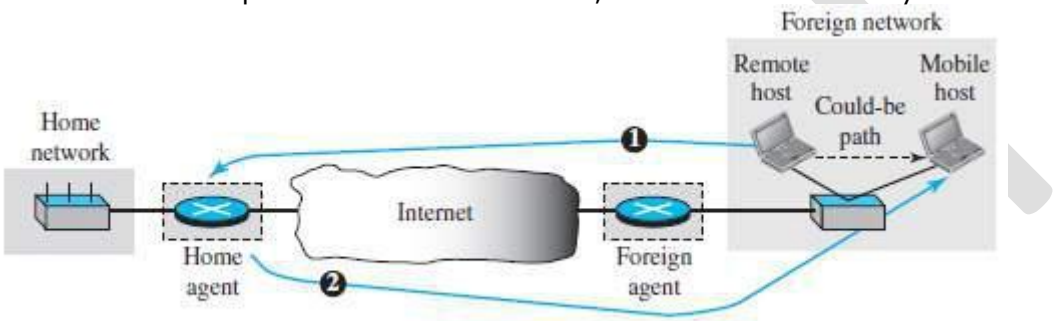


Figure 19.19 *Double crossing*

However, when the remote-host sends a packet to the mobile-host, the packet goes from the remote-host to the home-agent and then to the mobile-host.

The packet travels the two sides of a triangle, instead of just one side (Figure 19.20).

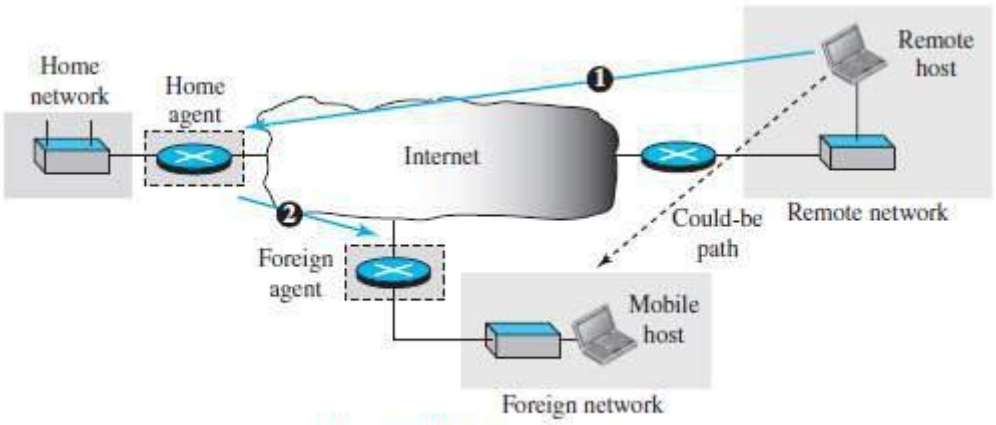


Figure 19.20 *Triangle routing*

Solution

One solution to inefficiency is for the remote-host to bind the care-of address to the home address of a mobile-host.

For example, when a home-agent receives the first packet for a mobile-host, it forwards the packet to the foreign-agent; it could also send an update binding packet to the remote-host so that future packets to this host could be sent to the care-of address.

The remote-host can keep this information in a cache.

The problem with this strategy is that the cache entry becomes outdated once the mobile-host moves.

In this case, the home-agent needs to send a warning packet to the remote-host to inform it of the change.

MODULE 5: NEXT GENERATION IP

5.8 IPv6 ADDRESSING

The main reason for migration from IPv4 to IPv6 is the small size of the address-space in IPv4.
Size of IPv6 address =128 bits (four times the address length in IPv4, which is 32 bits).

5.8.1 Representation

- Two notations can be used to represent IPv6 addresses: 1) binary and 2) colon hexadecimal.

Binary (128 bits)	1111111011110110 ... 1111111100000000
Colon Hexadecimal	FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00

5.8.2 Address Space

The address-space of IPv6 contains 2^{128} addresses.

5.8.2.1 Three Address Types

Three types of destination address: 1) Unicast 2) Anycast and 3) Multicast.

1) Unicast Address

- A unicast address defines a single interface (computer or router).
  The packet with a unicast address will be delivered to the intended recipient.

2) Anycast Address

An anycast address defines a group of computers that all share a single address.
A packet with an anycast address is delivered to only one member of the group.
The member is the one who is first reachable.

3) Multicast Address

A multicast address also defines a group of computers.
Difference between anycasting and multicasting.

In anycasting, only one copy of the packet is sent to one of the members of the group.
in multicasting each member of the group receives a copy.

5.8.3 Address Space Allocation

The address-space is divided into several blocks of varying size.
Each block is allocated for a special purpose.

Table 22.1 *Prefixes for assigned IPv6 addresses*

Block prefix	CIDR	Block assignment	Fraction
0000 0000	0000::/8	Special addresses	1/256
001	2000::/3	Global unicast	1/8
1111 110	FC00::/7	Unique local unicast	1/128
1111 1110 10	FE80::/10	Link local addresses	1/1024
1111 1111	FF00::/8	Multicast addresses	1/256

5.8.3.1 Global Unicast Addresses

The block in the address-space used for unicast communication b/w 2 hosts in the Internet is called global unicast address block.

CIDR for the block is 2000::/3. This means that the three leftmost bits are the same for all addresses in this block (001).

The size of this block is 2^{125} bits, which is more than enough for Internet expansion for many years to come.

An address in the block is divided into 3 parts (Figure 22.1):

Global routing prefix (n bits)
Subnet identifier (m bits) and
Interface identifier (q bits).

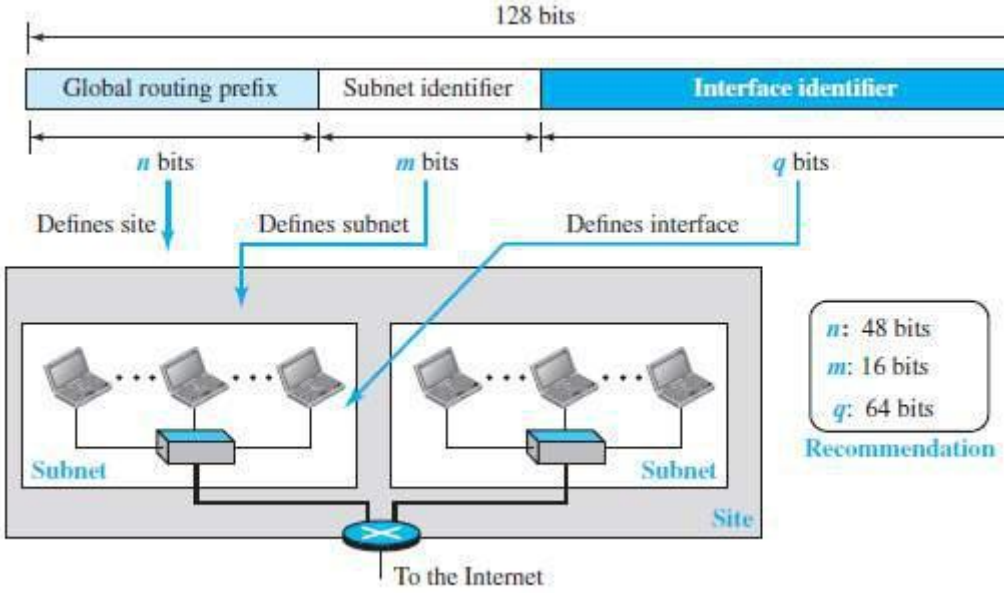


Figure 22.1 *Global unicast address*

The global routing prefix is used to route the packet through the Internet to the organization site, such as the ISP that owns the block.

Since the first 3 bits in this part are fixed (001), the rest of the 45 bits can be defined for up to 2^{45} sites (a private organization or an ISP).

The global routers in Internet route a packet to its destination site based on the value of n.
The next m bits define a subnet in an organization.
The last q bits define the interface identifier.

Two link layer addressing schemes:

64-bit extended unique identifier (EUI-64) defined by IEEE and
48-bit link-layer address defined by Ethernet.

1) Mapping EUI-64

• To map a 64-bit physical address, the global/local bit of this format needs to be changed from 0 to 1 (local to global) to define an interface address (Figure 22.2).

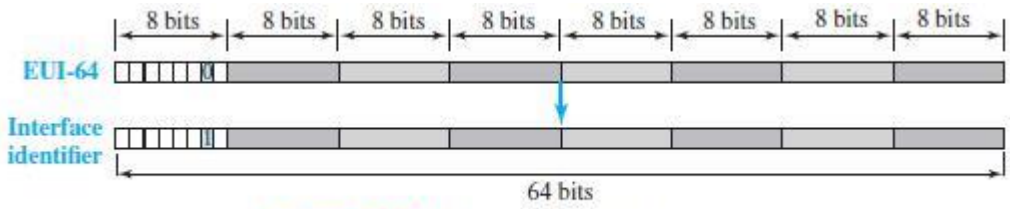


Figure 22.2 *Mapping for EUI-64*

2) Mapping Ethernet MAC Address

Mapping a 48-bit Ethernet address into a 64-bit interface identifier is more involved.

We need to change the local/global bit to 1 and insert an additional 16 bits.

The additional 16 bits are defined as 15 ones followed by one zero, or $FFFE_{16}$ (Figure 22.3).

5.8.3.2 Special Addresses

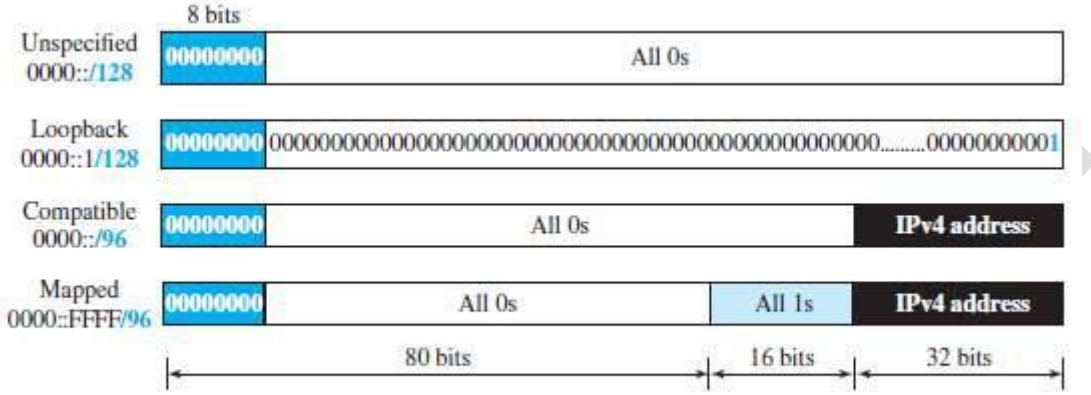


Figure 22.4 *Special addresses*

Following are different special addresses (Figure 22.4):

1) Unspecified Address

The unspecified address is a subblock containing only one address.

This address is used during bootstrap when a host does not know its own address and wants to send an inquiry to find it.

2) Loopback Address

The loopback address also consists of one address.

3) Transition Address

• During the transition from IPv4 to IPv6, hosts can use their IPv4 addresses embedded in IPv6 addresses.

• Two formats have been designed for this purpose: compatible and mapped.

1) Compatible Address

A compatible address is an address of 96 bits of zero followed by 32 bits of IPv4 address.

It is used when a computer using IPv6 wants to send a message to another computer using IPv6.

2) Mapped Address

A mapped address is used when a computer already migrated to version 6 wants to send an address to a computer still using version 4.

5.8.3.3 Other Assigned Blocks

IPv6 uses 2 large blocks for private addressing and one large block for multicasting (Figure 22.5).

1) Unique Local Unicast Block

A subblock in a unique local unicast block can be privately created and used by a site.
The packet carrying this type of address as the destination address is not expected to be routed.
This type of address has the identifier 1111 110.
The next bit can be 0 or 1 to define how the address is selected (locally or by an authority).

2) Link Local Block

A subblock in link local block can be used as a private address in a network.
This type of address has the block identifier 1111111010.
The next 54 bits are set to zero.
The last 64 bits can be changed to define the interface for each computer.

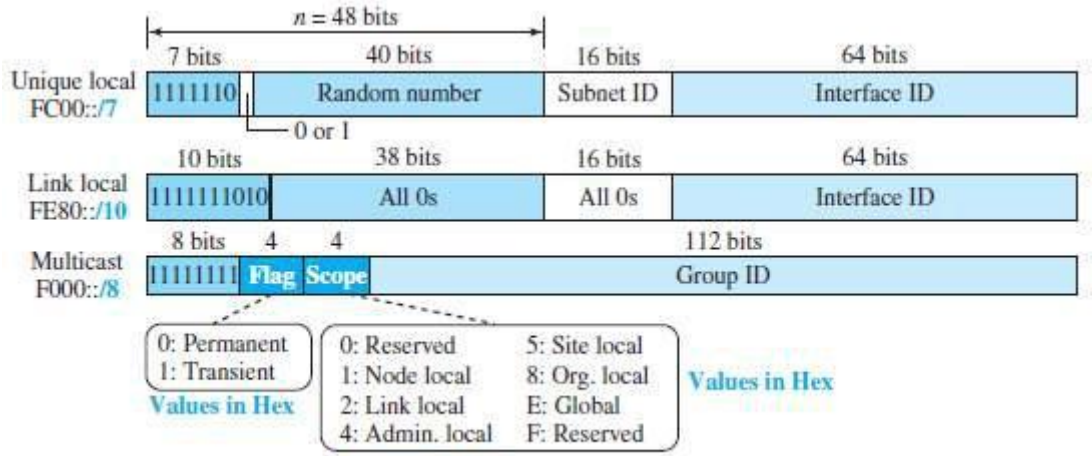


Figure 22.5 *Unique local unicast block*

5.8.4 Autoconfiguration

- When a host in IPv6 joins a network, it can configure itself using the following process:

The host first creates a link local address for itself.
This is done by
taking the 10-bit link local prefix (1111 1110 10)
adding 54 zeros and
adding the 64-bit interface identifier.
The result is a 128-bit link local address.

The host then tests to see if this link local address is unique and not used by other hosts.
Since the 64-bit interface identifier is supposed to be unique, the link local address generated is unique with a high probability.
To check uniqueness, the host
sends a neighbor solicitation message and
waits for a neighbor advertisement message.
If any host in the subnet is using this link local address, the process fails and the host cannot auto-configure itself.

If the uniqueness of the link local address is passed, the host stores this address as its link local address (for private communication), but it still needs a global unicast address.
The host then sends a router solicitation message to a local router.
If there is a router running on the network, the host receives a router advertisement message that includes
global unicast prefix and
subnet prefix that the host needs to add to its interface identifier to generate its global unicast address.

➢ If the router cannot help the host with the configuration, it informs the host in the router advertisement message (by setting a flag).

5.9 THE IPv6 PROTOCOL

5.9.1 Changes from IPv4 to IPv6 (Advantages of IPv6)

Header Format

IPv6 uses a new header format.
Options are
separated from the base-header and
inserted between the base-header and the data.
This speeds up the routing process (because most of the options do not need to be checked by routers).

New Options

IPv6 has new options to allow for additional functionalities.

Extension

IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

Resource Allocation

In IPv6,
type-of-service (TOS) field has been removed
two new fields: 1) traffic class and 2) flow label, are added to enable the source to request special handling of the packet.
This mechanism can be used to support real-time audio and video.

Security

The encryption option provides confidentiality of the packet.
The authentication option provides integrity of the packet.

5.9.2 Packet Format

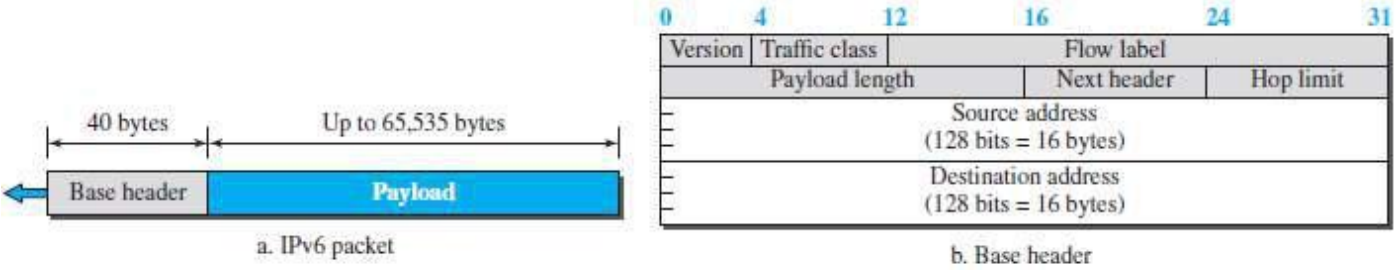


Figure 22.6 *IPv6 datagram*

IP header contains following fields (Figure 22.6):

Version

This specifies version number of protocol. For IPv6, version=6.

2) Traffic Class

This field is used to distinguish different payloads with different delivery requirements.

(Traffic class replaces the type-of-service field in IPv4).

3) Flow Label

This field is designed to provide special handling for a particular flow of data.

4) Payload Length

This indicates length of data (excluding header). Maximum length=65535 bytes.

The length of the base-header is fixed (40 bytes); only the length of the payload needs to be defined.

5) Next Header

This identifies type of extension header that follows the basic header.

6) Hop Limit

- This specifies number of hops the packet can travel before being dropped by a router. (Hop limit serves the same purpose as the TTL field in IPv4).

7) Source and Destination Addresses

- These identify source host and destination host respectively.

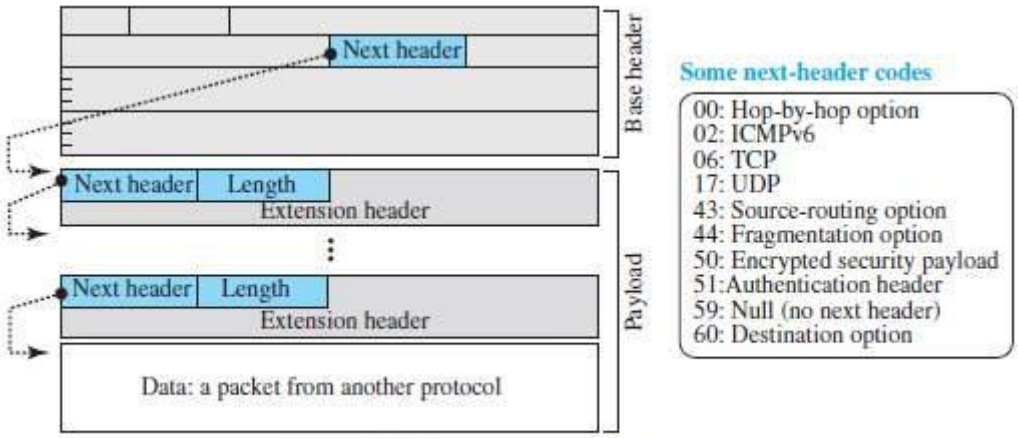


Figure 22.7 *Payload in an IPv6 datagram*

8) Payload

The payload contains zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on).

The payload can have many extension headers as required by the situation.

Each extension header has 2 mandatory fields (Figure 22.7):

Next header and

Length

Two mandatory fields are followed by information related to the particular option.

5.9.2.1 Concept of Flow & Priority in IPv6

To a router, a flow is a sequence of packets that share the same characteristics such as
- traveling the same path
- using the same resources or
- having the same kind of security

A router that supports the handling of flow labels has a flow label table.
The table has an entry for each active flow label.
Each entry defines the services required by the corresponding flow label.
When a router receives a packet, the router consults its flow label table.
Then, the router provides the packet with the services mentioned in the entry.
A flow label can be used to support the transmission of real-time audio/video.
Real-time audio/video requires resources such as
- high bandwidth
- large buffers or
- long processing time

Resource reservation guarantees that real-time data will not be delayed due to a lack of resources.

5.9.2.2 Fragmentation & Reassembly

Fragmentation of the packet is done only by the source, but not by the routers.
The reassembling is done by the destination.
At routers, the fragmentation is not allowed to speed up the processing in the router.
Normally, the fragmentation of a packet in a router needs a lot of processing. This is because
- The packets need to be fragmented.
- All fields related to the fragmentation need to be recalculated.

The source will
- check the size of the packet and
- make the decision to fragment the packet or not.

If packet-size is greater than the MTU of the network, the router will drop the packet.
Then, the router sends an error message to inform the source.

5.9.3 Extension Header

An IP packet is made of
base-header &
some extension headers.

Length of base header = 40 bytes.

To support extra functionalities, extension headers can be placed b/w base header and payload.

Extension headers act like options in IPv4.

Six types of extension headers (Figure 22.8):

1) Hop-by-hop option 2) Source routing 3) Fragmentation
4) Authentication 5) Encrypted security payload 5) Destination option.

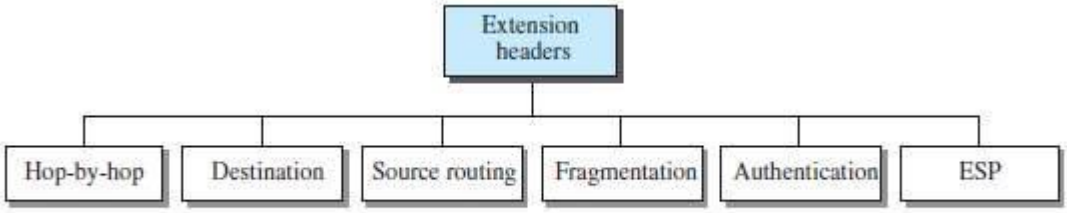


Figure 22.8 *Extension header types*

1) Hop-by-Hop Option

This option is used when the source needs to pass information to all routers visited by the datagram.

Three options are defined: i) Pad1, ii) PadN, and iii) Jumbo payload.

i) Pad1
This option is designed for alignment purposes.
Some options need to start at a specific bit of the 32-bit word.
Pad1 is added, if one byte is needed for alignment.

ii) PadN
PadN is similar in concept to Pad1.
The difference is that PadN is used when 2 or more bytes are needed for alignment. **iii)**

Jumbo Payload
This option is used when larger packet has to be sent. (> 65,535 bytes)
Large packets are referred to as jumbo packets.
Maximum length of payload = 65,535 bytes.

Destination Option

This option is used when the source needs to pass information to the destination only.

Intermediate routers are not allowed to access this information.

Two options are defined: i) Pad1 & ii) PadN

3) Source Routing

This option combines the concepts of
strict source routing and
loose source routing.

4) Fragmentation

In IPv6, only the original source can fragment.

A source must use a "Path MTU Discovery technique" to find the smallest MTU along the path from the source to the destination.

Minimum size of MTU = 1280 bytes. This value is required for each network connected to the Internet.

If a source does not use a Path MTU Discovery technique, the source fragments the datagram to a size of 1280 bytes.

5) Authentication

This option has a dual purpose:

Validates the message sender: This is needed so the receiver can be sure that a message is from the genuine sender and not from an attacker.

Ensures the integrity of data: This is needed to check that the data is not altered in transition by some attacker.

6) Encrypted Security Payload (ESP)

- This option provides confidentiality and guards against attacker.

Comparison of Options between IPv4 and IPv6

The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.

The record route option is not implemented in IPv6 because it was not used.

The timestamp option is not implemented because it was not used.

The source route option is called the source route extension header in IPv6.

The fragmentation fields in the base-header section of IPv4 have moved to the fragmentation extension header in IPv6.

The authentication extension header is new in IPv6.

The encrypted security payload extension header is new in IPv6.

5.10 THE ICMPv6 PROTOCOL

ICMP, ARP & IGMP protocols in IPv4 are combined into one single protocol called ICMPv6 (Fig 22.9).

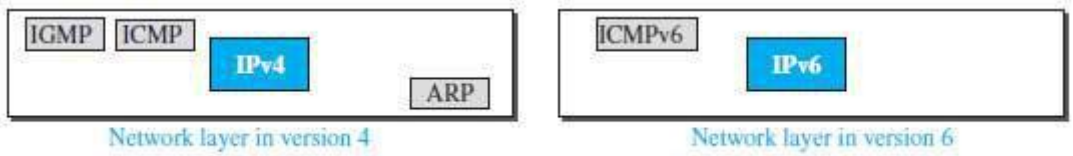


Figure 22.9 *Comparison of network layer in version 4 and version 6*

Four groups of messages (Figure 22.10):
- Error-reporting messages
- Informational messages
- Neighbor-discovery messages and
- Group-membership messages.

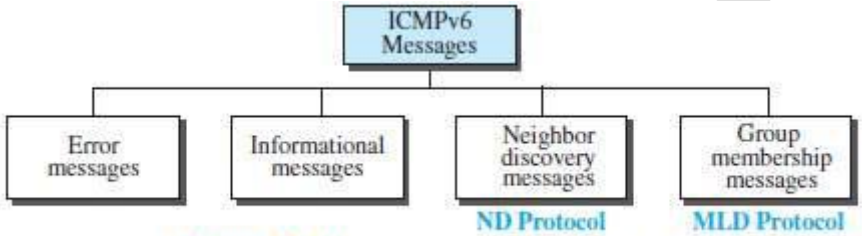


Figure 22.10 *Categories of ICMPv6 messages*

5.10.1 Error-Reporting Messages

- Main responsibility of ICMP: Report errors.
- ICMP forms an error packet, which is then encapsulated in the datagram.
- The encapsulated datagram is delivered to the original source.
- Four types of errors:
  1) Destination unreachable
  2) Packet too big
  3) Time exceeded and
  4) Parameter problems.

1) Destination-Unreachable Message

➢ Here, a router cannot forward a datagram or a host cannot deliver the datagram to the upper layer protocol.
➢ So, the router/host
→ discards the datagram and
→ sends a destination-unreachable message to the source.

2) Packet-Too-Big Message

➢ Fragmentation of the packet is done only by the source, but not by the routers. ➢ If a router receives a datagram larger than MTU size of the network, the router
→ discards the datagram and
→ sends a packet-too-big message to the source.

3) Time-Exceeded Message

➢ A time-exceeded error message is generated in 2 cases: i) When the TTL value becomes zero and
ii) When not all fragments of a datagram have arrived in the time-limit.

4) Parameter-Problem Message

➢ Any missing value in the datagram-header can create serious problems. ➢ If a router discovers any missing value in any field, the router
→ discards the datagram and
→ sends a parameter-problem message to the source.

5.10.2 Informational Messages

Two types of messages: i) echo request and ii) echo reply.
These 2 messages are used to check whether 2 devices can communicate with each other.
A source-host can send an echo-request message to another host.
The destination-host can respond with the echo-reply message to the source-host.

5.10.3 Neighbor-Discovery Messages

Two new protocols are used:
Neighbor-Discovery (ND) protocol and
Inverse-Neighbor-Discovery (IND) protocol.
These 2 protocols are used by nodes on the same link for 3 main purposes:
Hosts use the ND protocol to find routers in the neighborhood that will forward packets for them.
Nodes use the ND protocol to find the link-layer addresses of neighbors.
Nodes use the IND protocol to find the IPv6 addresses of neighbors.
Seven types of errors:

Router-Solicitation Message

A host/router uses router-solicitation message to find a router in n/w that can forward a datagram.
Physical address of the host/router is included to make the response easier for the router.

2) Router-Advertisement Message

A host/router sends the router-advertisement message in response to a router solicitation message.

3) Neighbor-Solicitation Message

The neighbor solicitation message has the same duty as the ARP request message.
A host uses the neighbor solicitation message when the host has a message to send to a neighbor.
The sender knows the IP address of the receiver, but needs the physical address of the receiver.
The physical address is needed for the datagram to be encapsulated in a frame.

4) Neighbor-Advertisement Message

A host sends the neighbor-advertisement message in response to a neighbor solicitation message.

5) Redirection Message

The purpose of the redirection message is the same as for version 4.
However, the format of the packet now accommodates the size of the IP address in version 6.
Also, an option is added to let the host know the physical address of the target router.

6) Inverse-Neighbor-Solicitation Message

- A host uses inverse-neighbor-solicitation message to know the physical address of a neighbor, but not the neighbor"s IP address.
- The message is encapsulated in a datagram using a multicast address.
- The node must send the following 2 information in the option field:
  i) Physical address of the sender and
  ii) Physical address of the target node.
- The sender can also include its IP address and the MTU value for the link.

7) Inverse-Neighbor-Advertisement Message

- A host sends the inverse-neighbor-advertisement message in response to a inverse-neighbor-discovery message.

5.10.4 Group Membership Messages

The management of multicast delivery handling in IPv4 is given to the IGMPv3 protocol.
In IPv6, this responsibility is given to the Multicast Listener Delivery protocol.
MLDv2 has 2 types of messages:

Membership-query message and
Membership-report message.

The first type can be divided into 3 subtypes: i) General, ii) Group-specific, and iii) Group-and-source specific.

1) Membership-Query Message

A router sends a membership-query message to find active group-members in the network.
The format of the membership-query in MLDv2 is exactly the same as the one in IGMPv3 three exceptions:

Size of the multicast address & source address has been changed from 32 bits to 128 bits.
The field size is in the maximum response code field, in which the size has been changed from 8 bits to 16 bits.
The format of the first 8 bytes matches the format for other ICMPv6 packets because MLDv2 is considered to be part of ICMPv6.

2) Membership-Report Message

The format of the membership-report in MLDv2 is exactly the same as the one in IGMPv3 one exception:

Size of the multicast address & source address has been changed from 32 bits to 128 bits.

In particular, the record type is the same as the one defined for IGMPv3 (types 1 to 6).

5.11 TRANSITION FROM IPv4 TO IPv6

5.11.1 Strategies

Three strategies have been devised for transition:

Dual stack
Tunneling and
Header translation.

1) Dual Stack

• Recommended: All hosts must run IPv4 and IPv6 (dual stack) simultaneously until all the Internet uses IPv6 (Figure 22.11).

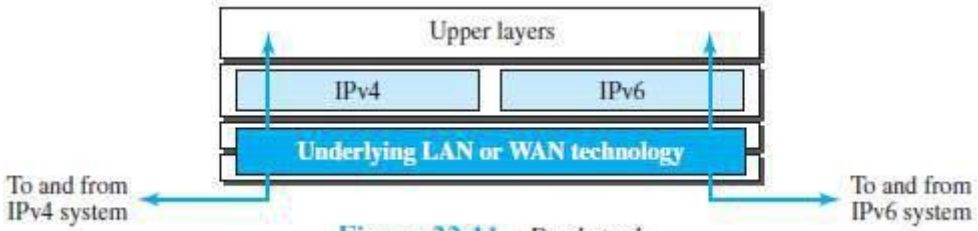


Figure 22.11 *Dual stack*

To determine which version to use, the source queries the DNS.

If the DNS returns an IPv4 address, the source sends an IPv4 packet.
If the DNS returns an IPv6 address, the source sends an IPv6 packet.

2) Tunneling

Tunneling is a strategy used when

two computers using IPv6 want to communicate with each other and
the packet must pass through an IPv4 network.

To pass through IPv4 network, the packet must have an IPv4 address (Figure 22.12).

So,

IPv6 packet is encapsulated in an IPv4 packet when the packet enters the IPv4 network.
IPv6 packet is decapsulated from an IPv4 packet when the packet exits the IPv4 network.

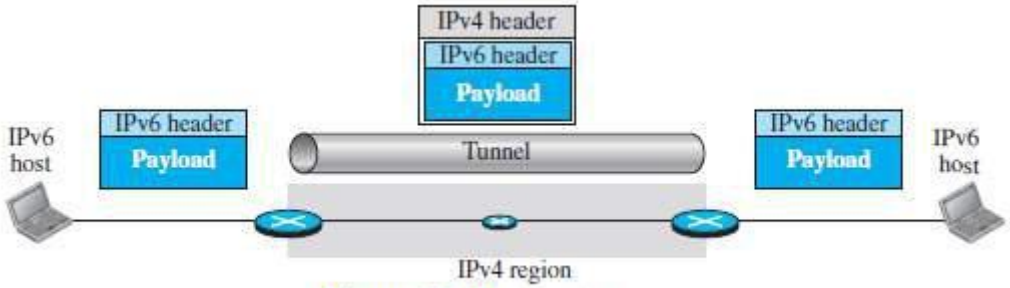


Figure 22.12 *Tunneling strategy*

3) Header Translation

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4 (Figure 22.13).

The sender wants to use IPv6, but the receiver does not understand IPv6.

Tunneling does not work in this situation because

the packet must be in the IPv4 format to be understood by the receiver.

In this case, the header format must be totally changed through header translation.

The header of the IPv6 packet is converted to an IPv4 header/

Figure 22.13 *Header translation strategy*

MODULE-WISE QUESTIONS

MODULE 5: OTHER WIRELESS NETWORKS

Explain two types of services of WiMAX. (2)
Explain layers in Project 802.16. (6)
Explain WiMAX MAC frame format. (6*)
Discuss the operation of the cellular telephony. (6*)
Explain first generation 1G of cellular telephony. (6)
Explain second generation 2G of cellular telephony (6)
Explain third generation 3G of cellular telephony. (6*)
Explain fourth generation 4G of cellular telephony (6*)
Explain the following terms with reference to satellite (4*)
i) Orbits ii) Footprint
10. Explain the 3 categories of satellites. (8*)

MODULE 5 NETWORK LAYER PROTOCOLS

Explain various field of IPv4. (8*)
Explain fragmentation. Explain 3 fields related to fragmentation (6*)
Explain options of IPv4. (6*)
Explain three network attacks to IP protocol. Also, explain four services of IPSec. (8*)
With general format, explain various ICMPv4 messages. (6*)
Explain two tools that use ICMP for debugging. (6)
Explain the following term with reference to Mobile IP: (4*)
i) Home address ii) Care-of address iii) Home-agent iv) Foreign-agent 18.
Explain three phases for communication in Mobile IP. (8*)

MODULE 5 NEXT GENERATION IP

Explain 3 address types of IPv6. (6)
Explain changes from IPv4 to IPv6. (4*)
Explain various field of IPv6. (8*)
Explain various extension header of IPv6. (8)
Explain various ICMPv6 messages. (6)
Explain various group membership messages. (6)
Explain 3 ways to make transition from IPv4 to IPv6. (6)