

SYLLABUS

OBJECTIVES:

- To learn the Network Models and data link layer functions.
- To understand routing in the Network Layer.
- To explore methods of communication and congestion control by the Transport Layer.
- To study the Network Security Mechanisms.
- To learn various hardware security attacks and their countermeasures.

UNIT I NETWORK MODELS AND DATALINK LAYER

9

Overview of Networks and its Attributes – Network Models – OSI, TCP/IP, Addressing – Introduction to Data link Layer – Error Detection and Correction – Ethernet(802.3)- Wireless LAN – IEEE 802.11, Bluetooth – Flow and Error Control Protocols – HDLC – PPP.

UNIT II NETWORK LAYER PROTOCOLS

9

Network Layer – IPv4 Addressing – Network Layer Protocols (IP, ICMP and Mobile IP) Unicast and Multicast Routing – Intra domain and Inter domain Routing Protocols – IPv6 Addresses – IPv6 – Datagram Format - Transition from IPv4 to IPv6.

UNIT III TRANSPORT AND APPLICATION LAYERS

9

Transport Layer Protocols – UDP and TCP Connection and State Transition Diagram - Congestion Control and Avoidance (DEC bit, RED) - QoS - Application Layer Paradigms – Client – Server Programming – Domain Name System – World Wide Web, HTTP, Electronic Mail.

UNIT IV NETWORK SECURITY

9

OSI Security Architecture – Attacks – Security Services and Mechanisms – Encryption –Advanced Encryption Standard – Public Key Cryptosystems – RSA Algorithm – Hash Functions – Secure Hash Algorithm – Digital Signature Algorithm.

UNIT V HARDWARE SECURITY

9

Introduction to hardware security, Hardware Trojans, Side – Channel Attacks – Physical Attacks and Countermeasures – Design for Security. Introduction to Block chain Technology.

OUTCOMES:

Upon successful completion of the course the student will be able to

C01: Explain the Network Models, layers and functions.

C02: Categorize and classify the routing protocols.

C03: List the functions of the transport and application layer.

C04: Evaluate and choose the network security mechanisms.

C05: Discuss the hardware security attacks and countermeasures.

TEXTBOOKS

1. Behrouz.A.Forouzan, Data Communication and Networking, Fifth Edition, TMH, 2017.(Unit – I,II,III)

2. William Stallings, Cryptography and Network Security, Seventh Edition, Pearson Education, 2017(Unit- IV)

3. Bhunia Swarup, Hardware Security –A Hands On Approach,Morgan Kaufmann, First edition, 2018.(Unit – V).

REFERENCES

1. James.F.Kurose and Keith.W.Ross, Computer Networking – A Top – Down Approach, Sixth Edition, Pearson, 2017.
2. Douglas. E.Comer, Computer Networks and Internets with Internet Applications, Fourth Edition, Pearson Education, 2008.

UNIT I NETWORK MODELS AND DATALINK LAYER

Overview of Networks and its Attributes – Network Models – OSI, TCP/IP, Addressing – Introduction to Data link Layer – Error Detection and Correction – Ethernet(802.3)- Wireless LAN – IEEE 802.11, Bluetooth – Flow and Error Control Protocols – HDLC – PPP.

1.1 OVERVIEW OF NETWORKS AND ITS ATTRIBUTES

Q1. Write the criteria for effective data communications.(2 marks)[MAY/JUNE 2016]

Q2. Define the term protocol and interface.(2 marks) [NOV/DEC 2019]

Q3. Define the term protocol.(2 marks) [NOV/DEC 2015]

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).

Characteristics of Data Communications

The effectiveness of a data communications system depends on four characteristics: delivery, accuracy, timeliness, and jitter.

- **Delivery.** The system must deliver data to the correct destination. Data must be received by the receiver device.
- **Accuracy.** The system must deliver the data accurately. Data that have been altered (changed during transmission) in transmission and left uncorrected are unusable.
- **Timeliness.** The system must deliver data in exact time. 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 (any delay) significant delay. This kind of delivery is called real-time transmission.
- **Jitter.** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio and 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 occurs.

Components Required

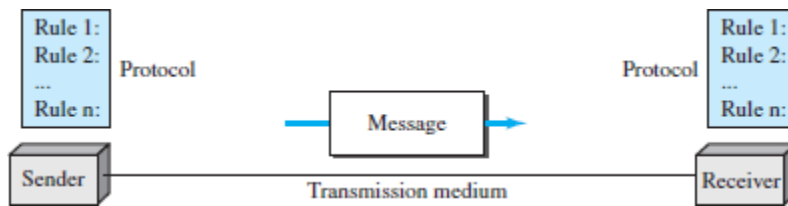


Fig 1.1: Five components for Communication

The components required for communication is shown in Fig1.1. They are:

a) Message:

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

b) Sender:

The **sender** is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

c) Receiver:

The **receiver** is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

d) 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.

e) Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices (Between sender and Receiver). Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Representation:

Information today (**available**) comes in different forms such as text, numbers, images, audio, and Video.

A) Text:

Text is represented as a bit pattern, a sequence of bits (0s or 1s).

What is bit pattern? All data inside a computer is transmitted as a series of electrical signals that are either on or off. Therefore, in order for a computer to be able to process any kind of data, including text, images and sound, they must be converted into binary form. 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**.

B) Numbers:

Numbers are also represented by bit patterns. The number is directly converted to a binary number to simplify mathematical operations. ie: Conversion of decimal to binary.

C) Images:

Images are also represented by bit patterns.

Representing image by bit pattern: Images also need to be converted into binary in order for a computer to process them so that they can be seen on our screen. Digital images are made up of pixels. Each pixel in an image is made up of binary numbers. If we say that 1 is black (or on) and 0 is white (or off), then a simple black and white picture can be created using binary.

D) Audio:

Audio refers to the recording or broadcasting of sound or music. It is continuous, not discrete.

E) Video:

Video refers to the 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, which is a discrete entity and can be arranged to convey the idea of motion.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex and is shown in Fig 1.2.

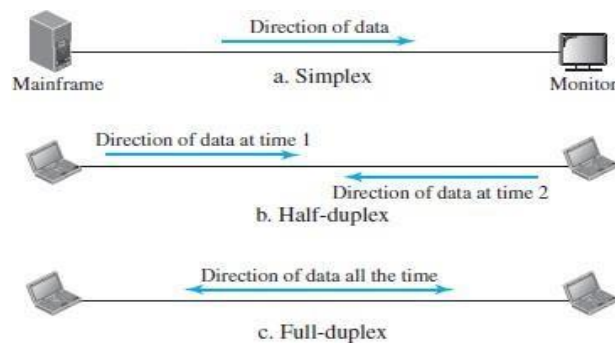


Fig1.2: Mode of communication

a) Simplex:

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a). **Keyboards and traditional monitors** are examples of simplex devices. In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.

- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
- This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.
- The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.

b) 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 (see Figure 1.2b). Messages flow in both the directions, but not at the same time.

- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data. **Walkie-talkies are half-duplex systems.**

c) Full-Duplex:

In full-duplex mode (**also called duplex**), both stations can transmit and receive simultaneously (at the same time), (see Figure 1.2c).

Example of full-duplex communication is the **telephone network**.

When two people are communicating by a telephone line, both can talk and listen at the same time.

COMPARISON - SIMPLEX, HALF-DUPLEX AND FULL-DUPLEX MODE

BASIS FOR COMPARISON	SIMPLEX MODE	HALF-DUPLEX MODE	FULL-DUPLEX MODE
Direction of communication	Communication is unidirectional.	Communication is bidirectional, but one at a time.	Communication is bidirectional.
Send/Receive	A device can only send the data but cannot receive it or it can only receive the data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
Example	Radio, Keyboard, and monitor.	Walkie-Talkie	Telephone network.

NETWORKS

Q1. Present the evolution and the types of Networks. (13 marks)[Nov/dec 2021]

What is a Network?

A **network** is the interconnection of a set of devices capable of communication. A device can be a **host** (called as end system) such as a large computer, desktop, laptop, workstation, cellular phone, or security system.

Network Criteria

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

A) 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.

1. the number of users.
2. the type of transmission medium.
3. the capabilities of the connected hardware.
4. the efficiency of the software.

Performance is often evaluated by two networking metrics: **throughput** and **delay**.

B) 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.

C) Security

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

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.

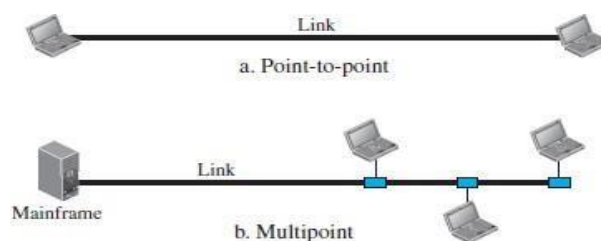


Fig1.3: Types of Connections

Multipoint: A multipoint (also called multidrop) connection is one in which **more than two specific devices share a single link** (see Figure 1.3 below). 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.

Physical Topology (Network 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: mesh, star, bus, and ring.

A. Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device as shown in Fig 1.4. A fully connected mesh network with n nodes has $n(n-1)/2$ physical channels.

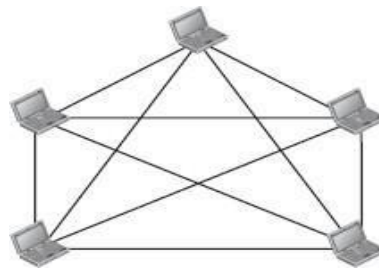


Fig1.4: Mesh topology

Advantages:

- 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.
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- Privacy or security.
- Point-to-point links make fault identification and fault isolation easy.

Disadvantages:

- Every device must be connected to every other device. Installation and reconnection are difficult.
- More number of wire connections make it greater than the available space (in walls, ceilings, or floors) which can accommodate.
- The hardware required to connect each link (I/O ports and cable) can be expensive.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

B. 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 connected 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 (see Figure 1.5).



Fig1.5: Star topology

Advantages:

- Less expensive than a mesh topology.
- Easy to install and reconfigure.
- Less cables are required, and additions, and deletions involve only one connection: between that device and the hub.
- It is Robust. If one link fails, only that link is affected. All other links remain active.

Disadvantages:

- The topology depends on one single point, the hub. If the hub goes down, the whole system is dead.
- A star requires far less cable than a mesh; each node must be linked to a central hub. The star topology is used in local-area networks (LANs). High-speed LANs also use a star topology with a central hub.

C. Bus Topology:

A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure 1.6). **Nodes are connected to the bus cable** by drop lines and taps. **A drop line** is a connection 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, the signal becomes weaker and weaker as it travels farther and farther. For this reason, there is a limit on the number of taps used in this topology.



Fig1.6: Bus Topology

Advantages:

- Ease of installation.
- Less cabling

Disadvantages:

- Difficult reconfiguration and fault isolation.
- Difficult to add new devices.
- Signal reflection at top can cause degradation in quality.
- If any fault in backbone occurs, then it can stop all transmission.

Ethernet LANs can use a bus topology, but they are less popular now.

D. 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 (see Figure 1.7).

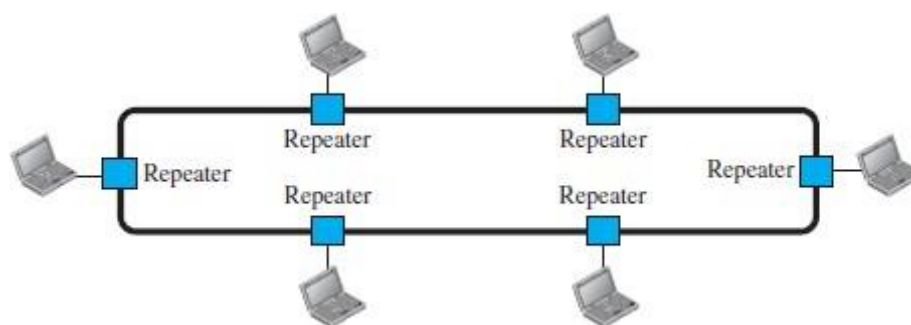


Fig1.7: Ring Topology

Advantages:

- Easy to install.
- Easy to reconfigure.
- Fault identification is easy.

Disadvantages:

- Unidirectional traffic.
- Break in a single ring can break entire network.

Ring topologies are found in some office buildings or school campuses. Today high-speed LANs made this topology less popular.

E. Tree Topology

Tree topology is shown in Fig 1.8.

- It has a root node and all other nodes are connected to it forming a hierarchy.
- It is also called hierarchical topology.
- It should at least have three levels to the hierarchy.
- Tree topology is ideal if workstations are located in groups.
- They are used in Wide Area Network.

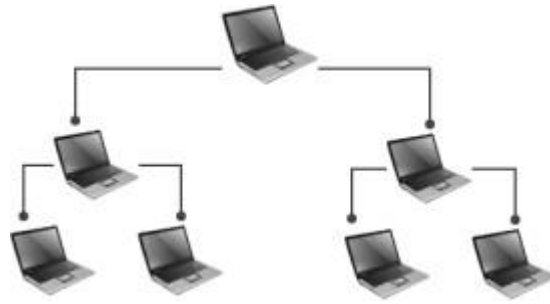


Fig 1.8: Tree Topology

F. Hybrid Topology

- Hybrid Topology (see Fig 1.9) is a combination of one or more basic topologies.
 - For example if one department in an office uses ring topology, the other departments use star and bus topology, then connecting these topologies will result in Hybrid Topology.
 - Hybrid Topology inherits the advantages and disadvantages of the topologies included.

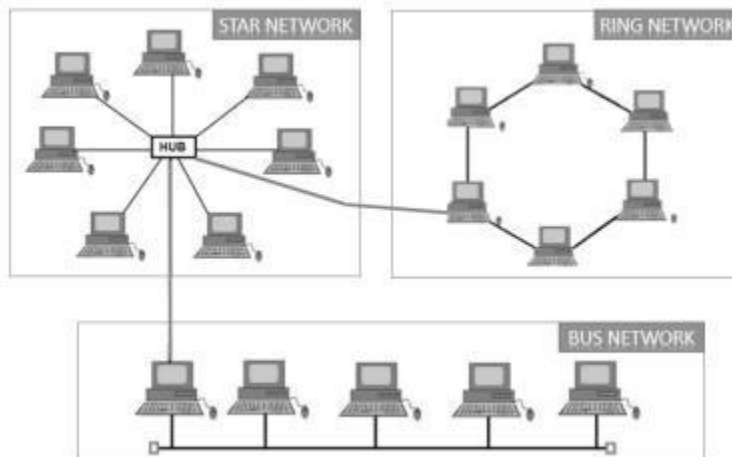


Fig 1.9: Hybrid Topology

1.2. BUILDING NETWORK AND ITS TYPES

Q1. Explain the challenges in building an network. (10 marks) [APR/MAY 2017]

Q2. Explain the challenges faced in building a network. What are the essential requirements to be taken into consideration for building a network in an organization

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A computer network is mainly of three types:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)

Local Area Network

- Local Area Network is a group of computers connected to each other in a small area such as building, office. LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely fast rate in Local Area Network.
- LAN can be connected using a common cable or a Switch.

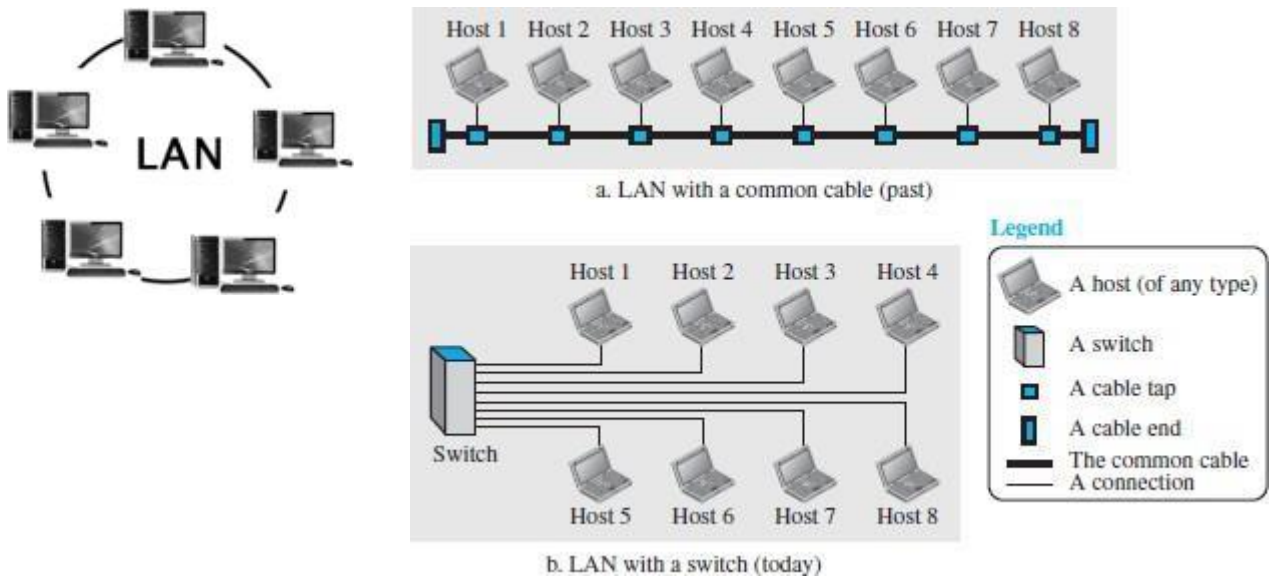


Fig1.10: LAN connections

B. Wide Area Network (WAN)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A wide area network is an interconnection of devices capable of communication.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of business, government, and education.
- WAN can be either a point-to-point WAN or Switched WAN.

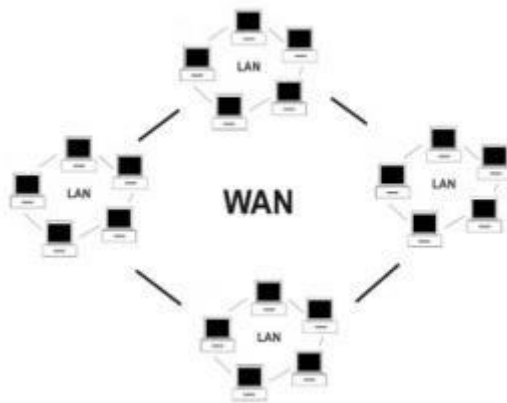


Fig 1.11 Wide Area Network

A) Point-to-Point WAN

A point-to-point WAN (see Fig1.12) is a network that connects two communicating devices through a transmission media (cable or air).

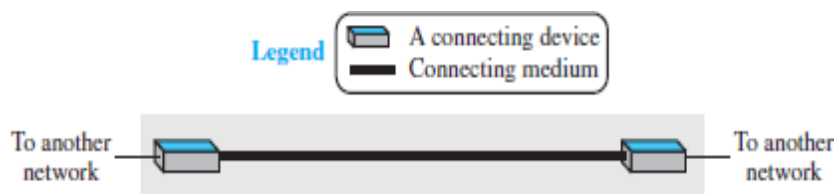


Fig1.12: point-to-point WANS.

B) Switched WAN

A switched WAN is a network with more than two ends (see Fig1.13). A switched WAN is a combination of several point-to-point WANs that are connected by switches.

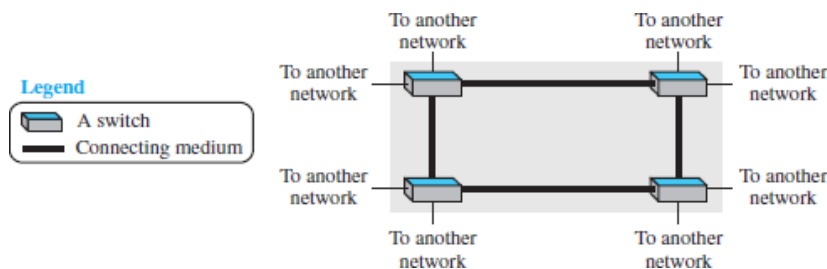


Fig1.13: Switched WAN.

There are some differences between a LAN and a WAN.

1. A LAN is normally limited in size, spanning an office, a building, or a campus; A WAN has a wider geographical span, spanning a town, a state, a country, or even the world.
2. A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems.
3. A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it.

C. Metropolitan Area Network (MAN)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a

different LAN to form a larger network.

- It generally covers towns and cities (50 km)
- In MAN, various LANs are connected to each other through a telephone exchange line.
- Communication medium used for MAN are optical fibers, cables etc.
- It has a higher range than Local Area Network (LAN). It is adequate for distributed computing applications.

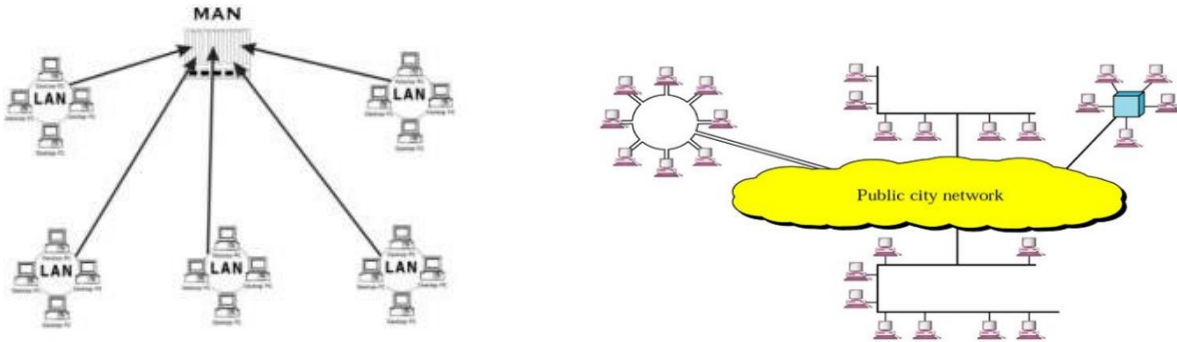


Fig 1.14 Metropolitan Area Network

Internetwork

When two or more networks are connected, they make 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.

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**.

A) Circuit-Switched Network

In a **circuit-switched network**, a dedicated connection, called a circuit, is always available between the two end systems (or between two computers).

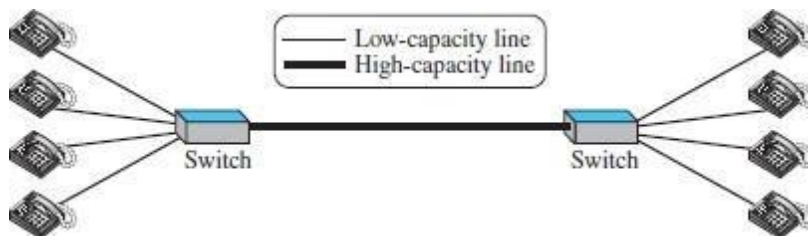


Fig1.15: Circuit-switched network

The four telephones at each side are connected to a switch. The switch connects a telephone set at one side to a telephone set at the other side. The thick line connecting two switches is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets.

B) 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 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.
- A router in a packet-switched network has a queue that can store and forward the packet.

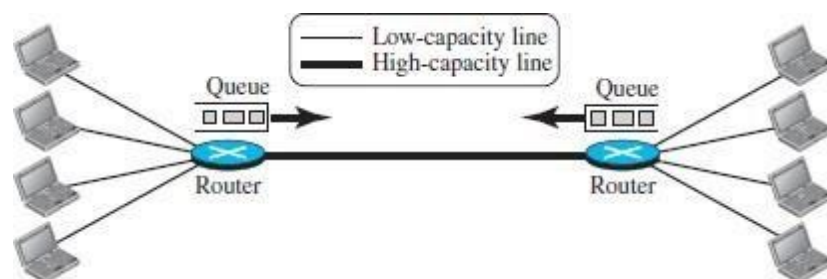


Fig1.16: Packet-Switched Network

OVERVIEW OF INTERNET

The Internet

An internet (lower case i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase I), and is composed of thousands of interconnected networks. Figure 1.17 shows a conceptual view of the Internet.

It 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.

Accessing the Internet

- The Internet today is an internet network that allows any user to become part of it. The user, however, needs to be physically connected to an ISP. The physical connection is

done through a point-to-point WAN.

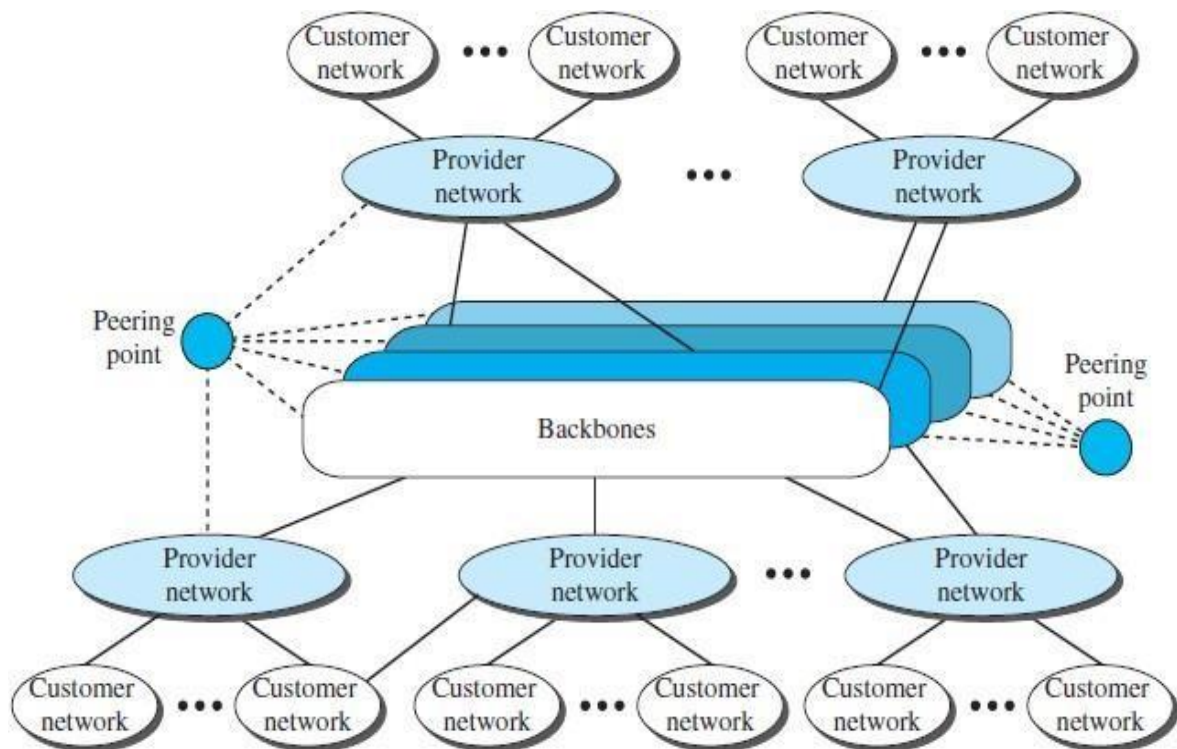


Fig1.17: Internet

b. Using Telephone Networks

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.
- **DSL Service.**
The DSL service allows the line to be used simultaneously for voice and data communication.

c. Using Cable Networks

The cable companies have been upgrading their cable networks and connecting to the Internet.

d. Using Wireless Networks

A household or a small business can use a combination of wireless and wired

connections to access the Internet. Small business centers can be connected to the Internet through a wireless WAN.

e. Direct Connection to the Internet

A large organization can 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 (Internet service provider). For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

1.2 NETWORK MODELS

PROTOCOL LAYERING

Q1. What are the key benefits of layered network?(2 marks)[NOV/DEC 2019]

When communication is simple, we 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 a teach layer, or protocol layering. Dividing the task between different layers is called Protocol layering.

Need of layering:

- It decomposes the problem of building a network into more manageable components. Each layer solves one part of the problem.
- It provides a more modular design. i.e, If we want to add new service, it require only modifying the functionality at the respective layers and refusing the functions provided at all other layers.

Scenarios

Two simple scenarios are available to understand the need for protocol layering.

First Scenario

In the first scenario, communication is 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 Figure1.18.

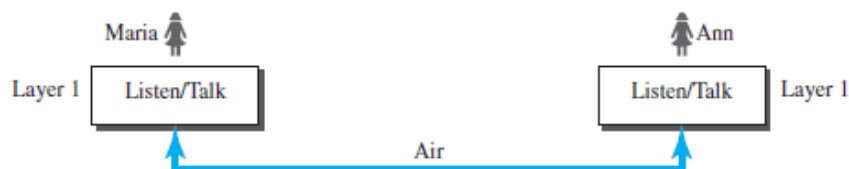


Fig1.18: Single layer protocol Set of rules followed in this scenario:

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 (not talking) from speaking when the other party is speaking.

Fourth, each party knows that the conversation should be a dialog.

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.

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.

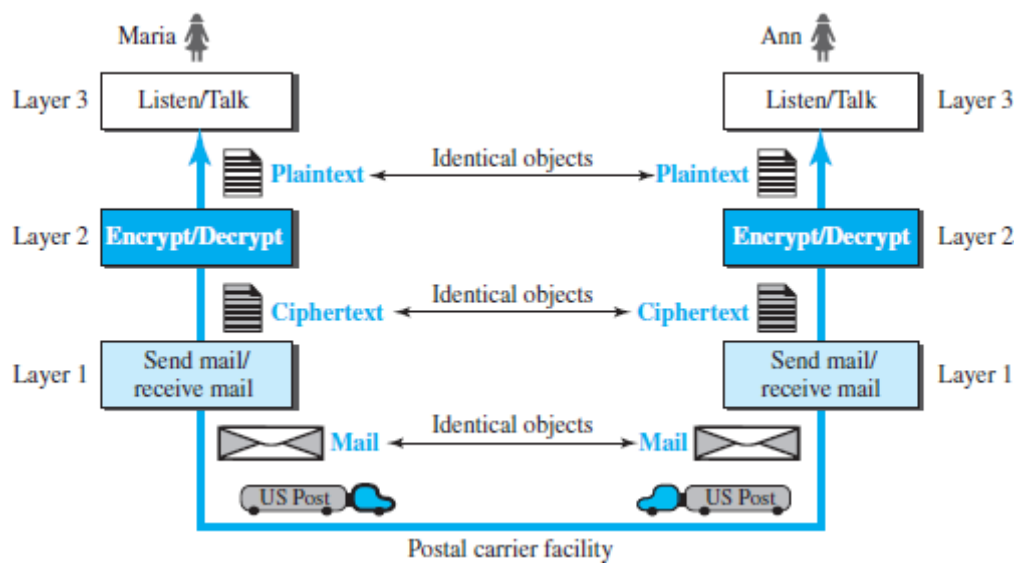


Fig1.19: Three layer protocol

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, takes the ciphertext, puts it in an envelope, adds the sender and receiver addresses, and mails it. Protocol layering enables us to divide a complex task into several smaller and simpler tasks. For example, in the Figure 1.19, 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.

Principles of Protocol Layering

First Principle

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 cipher text letter. The object under layer 1 at both sites should be a piece of mail.

Logical Connections

Logical connection between each layer is shown in Figure 1.20.

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.

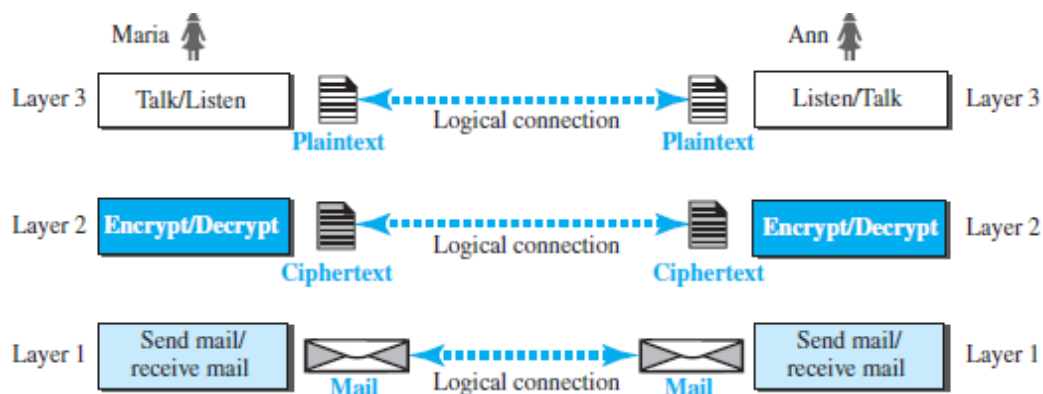


Fig1.20: the concept of logical connection between layers.

THE OSI MODEL

Q1. Draw the OSI network architecture and explain the functionalities of every layer in detail. (13 MARKS) [NOV/DEC 2015]

Q2. Draw the block diagram and explain the functionalities of different OSI layers. (13 MARKS) [NOV/DEC 2019]

Q3. Data Link Control (DLC) and Media Access Control (MAC) are part of which layer in OSI model? What is their role? (13 MARKS) [NOV/DEC 2020]

Q4. Discuss the layering principles of OSI mode of communication networks. (13 MARKS) [NOV/DEC 2021]

ISO defines a common way to connect computer by the architecture called Open System Interconnection(OSI) architecture. Network functionality is divided into seven layers.

Organization of the layers

The 7 layers can be grouped into 3 subgroups

A. Network Support Layers

Layers 1,2,3 - Physical, Data link and Network are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical addressing, transport timing and reliability.

B. Transport Layer

Layer4, transport layer, ensures end-to-end reliable data transmission on a single link.

C. User Support Layers

Layers 5,6,7 - Session, presentation and application are the user support layers. They allow interoperability among unrelated software systems

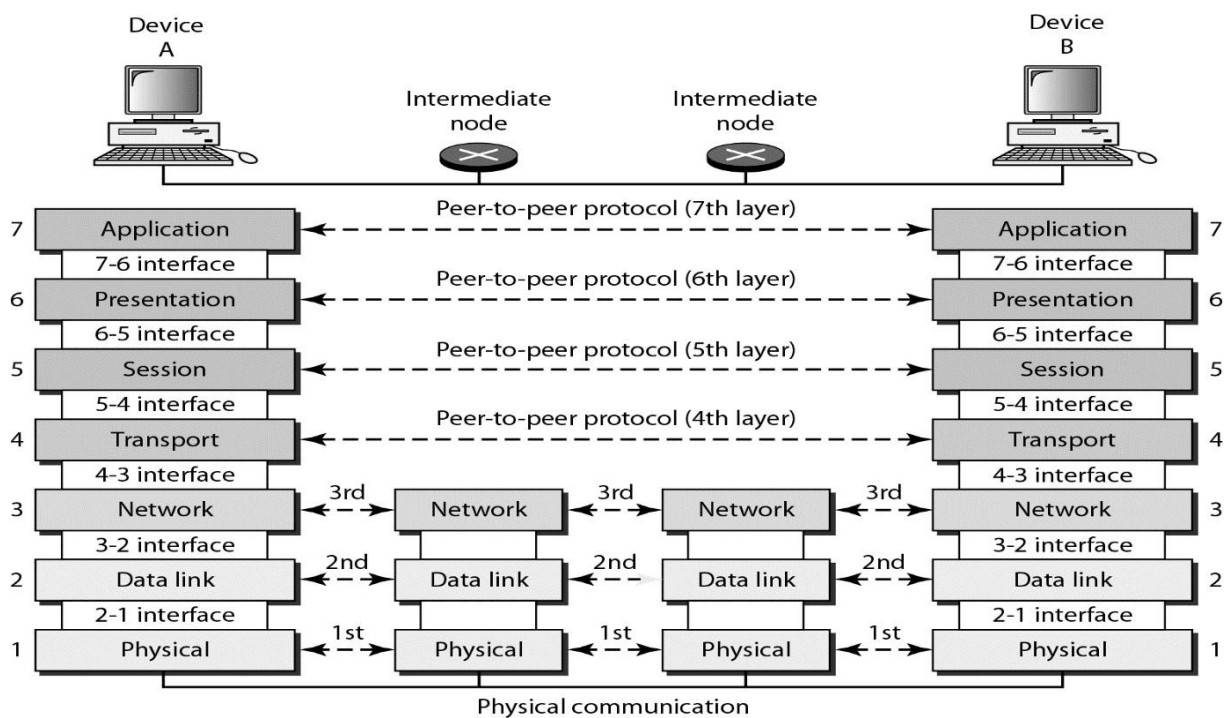


Fig 1.21 The interaction between layers in the OSI model

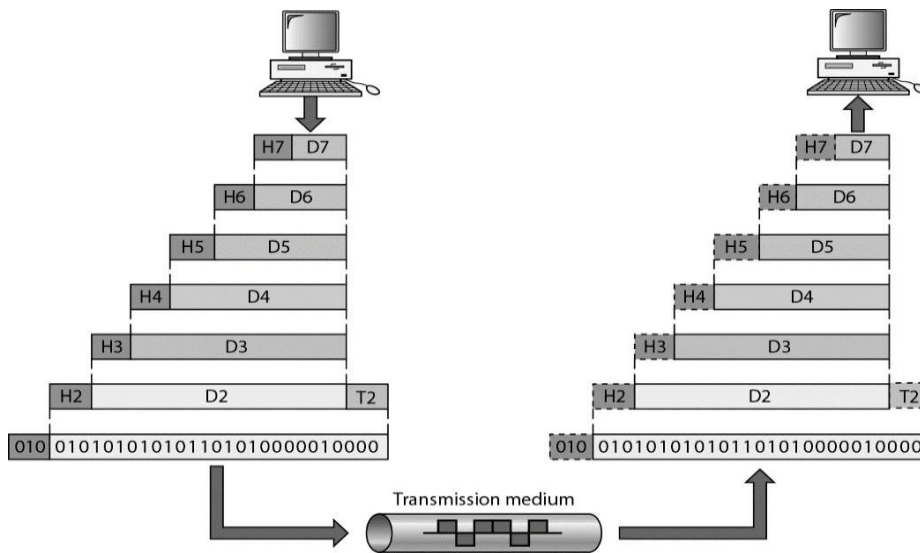


Fig 1.22 A Data exchange using the OSI model

Functions of the Layers

1. PHYSICAL LAYER

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.

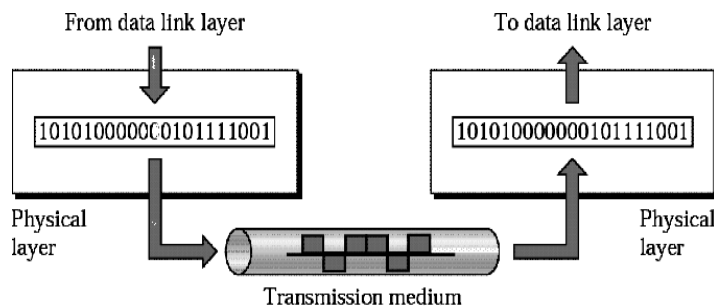


Fig 1.23 Physical Layer

The physical layer is concerned with the following:

- ❑ **Physical characteristics of interfaces and media** - The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- ❑ **Representation of bits** - To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.
- ❑ **Data Rate or Transmission rate** - The number of bits sent each second – is also defined by the physical layer.
- ❑ **Synchronization of bits** - The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.
- ❑ **Line Configuration** - In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
- ❑ **Physical Topology** - The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.

- **Transmission Mode** - The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

2. DATA LINK LAYER

It is responsible for transmitting frames from one node to next node.

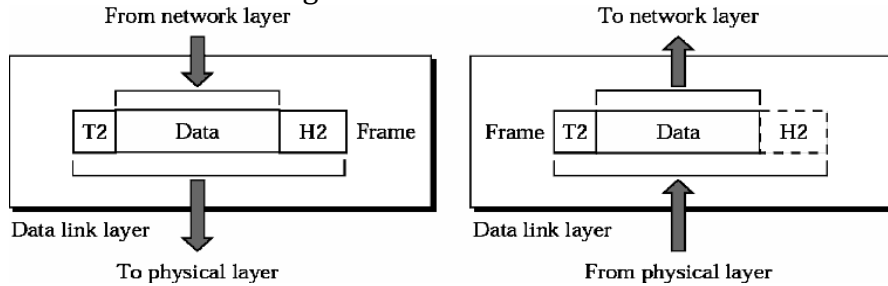


Fig 1.24 Data Link Layer

The other responsibilities of this layer are

- **Framing** - Divides the stream of bits received into data units called frames.
- **Physical addressing** - If frames are to be distributed to different systems on the n/w, data link layer adds a header to the frame to define the sender and receiver.
- **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the data link layer imposes a flow control mechanism.
- **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Access control** -Used to determine which device has control over the link at any given time.

3. NETWORK LAYER

This layer is responsible for the delivery of packets from source to destination.

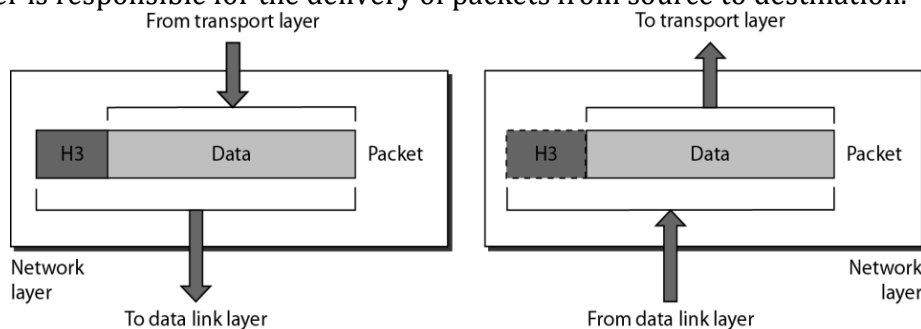


Fig 1.25 Network Layer

The other responsibilities of this layer are

- **Logical addressing** - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** - The devices which connects various networks called routers are responsible for delivering packets to final destination.

4. TRANSPORT LAYER

It is responsible for **Process to Process** delivery. It also ensures whether the message arrives in order or not.

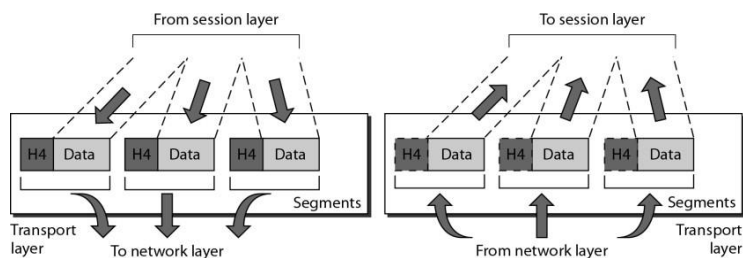


Fig 1.26 Transport Layer

The other responsibilities of this layer are

- **Port addressing** - The header in this must therefore include an address called port address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- **Connection control** - This can either be connectionless or connection-oriented. The connectionless treats each segment as an individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow and error control** - Similar to data link layer, but process to process take place.

5. SESSION LAYER

This layer establishes, manages and terminates connections between applications.

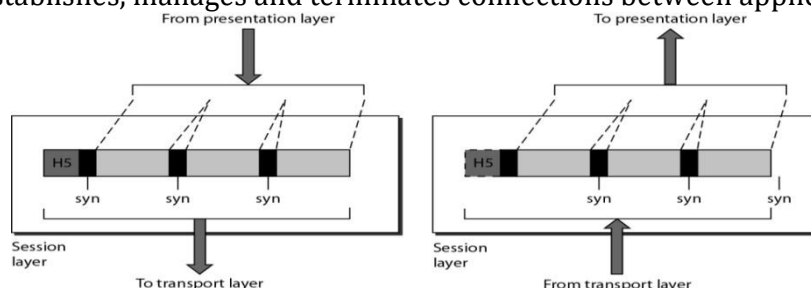


Fig 1.27 Session Layer

The other responsibilities of this layer are

- **Dialog control** - This session allows two systems to enter into a dialog either in half duplex or full duplex.
- **Synchronization** - This allows to add checkpoints into a stream of data.

6. PRESENTATION LAYER

It is concerned with the syntax and semantics of information exchanged between two systems.

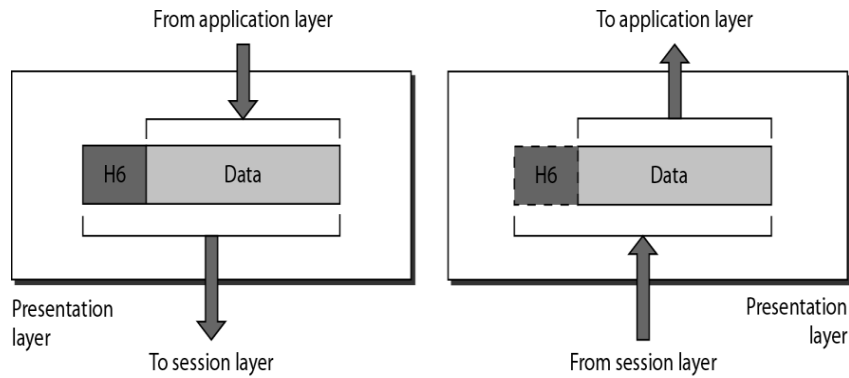


Fig 1.28 Presentation Layer

The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change message into some common format.
- **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

7. APPLICATION LAYER

This layer enable the user to access the n/w. This allow the user to log on to remote user.

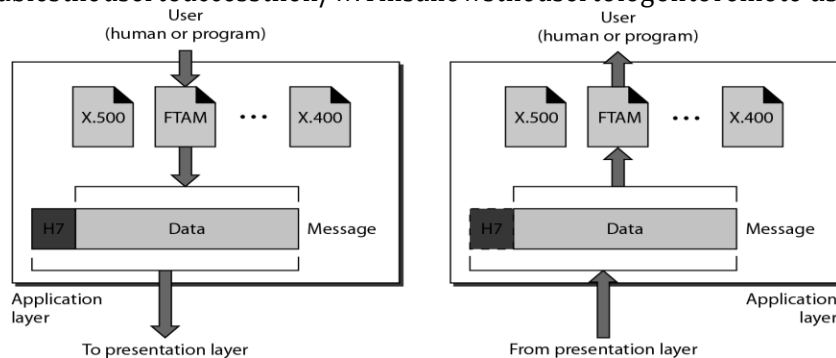


Fig 1.29 Application Layer

The other responsibilities of this layer are

- FTAM (file transfer, access, mgmt.)** -Allows user to access files in a remote host.
- Mail services** - Provides email forwarding and storage.
- Directory services** - Provides database sources to access information about various sources and objects.

TCP/IP PROTOCOL SUITE / TCP/IP REFERENCE MODEL [INTERNET ARCHITECTURE]

Q1. Explain TCP/IP Model with neat sketch.

- The TCP/IP architecture is also called as Internet architecture.
- It is developed by the US Defense Advanced Research Project Agency (DARPA) for its packet switched network (ARPANET).
- TCP/IP is a protocol suite used in the Internet today.
- It is a 5-layer model. The layers of TCP/IP are
 - Application layer
 - Transport Layer (TCP/UDP)
 - Internet Layer
 - Network Interface Layer
- The host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCPIIP taking care of part of the duties of the session layer. So, the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.
- The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCPIIP by a single layer called the application layer.

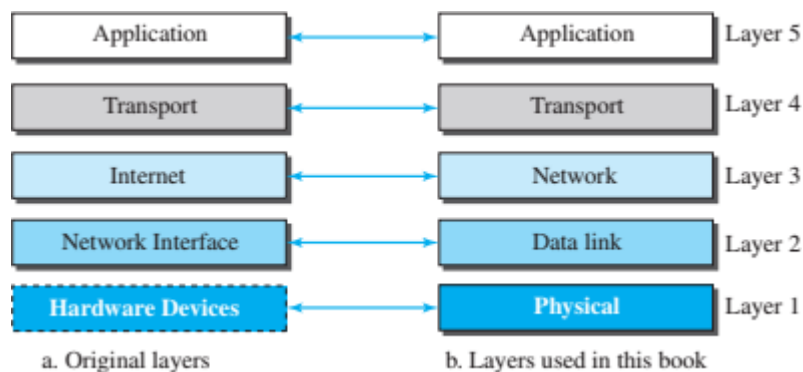


Fig 1.30 Layer Organization

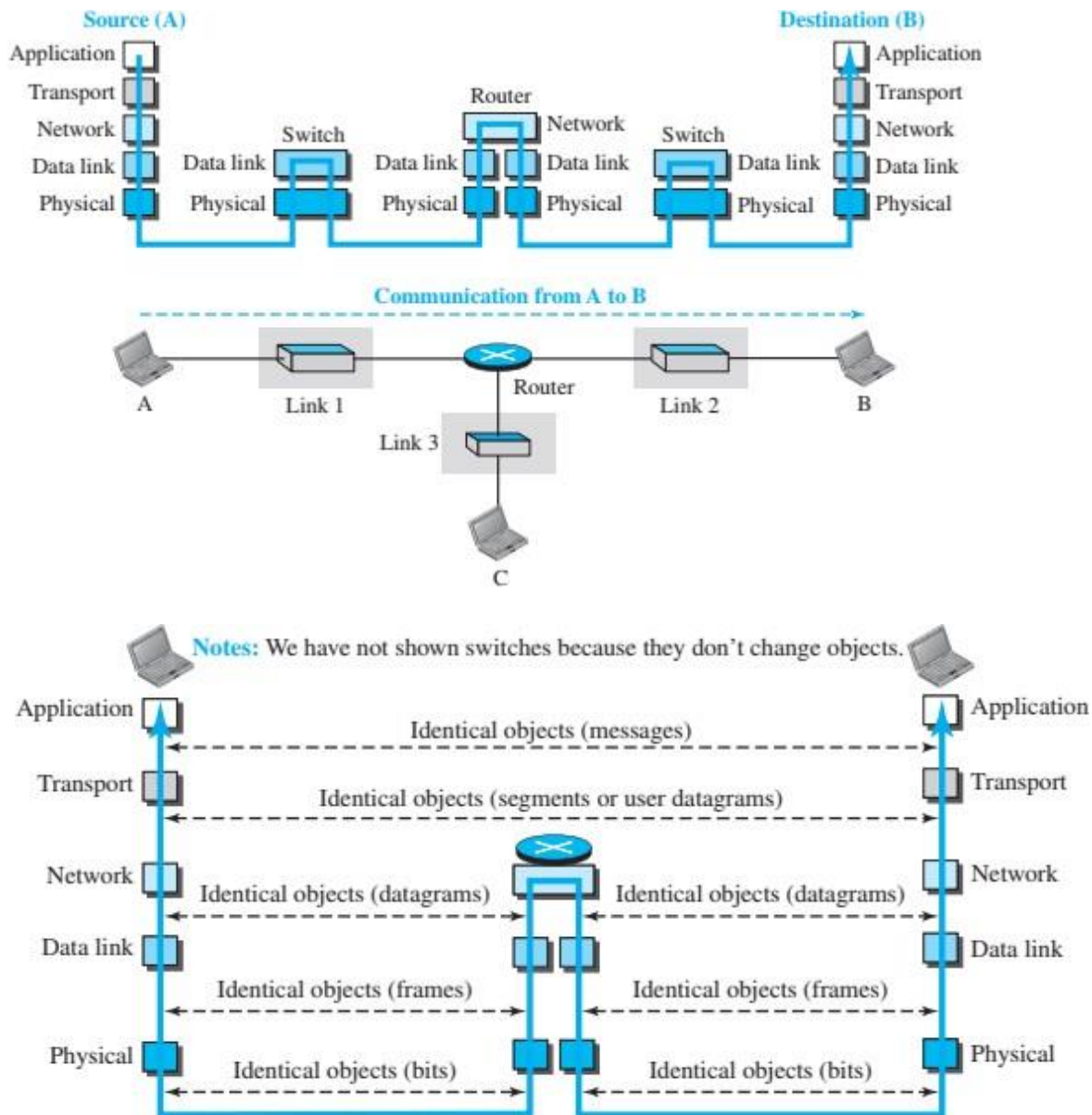


Fig 1.31 Flow of data between layers

Physical Layer

The physical layer is responsible for carrying individual bits in a frame across the link. Although the physical layer is the lowest level in the TCP/IP protocol suite, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer.

- Two devices are connected by a transmission medium (cable or air).
- So, the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but the logical unit between two physical layers in two devices is a bit.
- There are several protocols that transform a bit to a signal.

Data-link Layer

- An internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the destination.
- The routers are responsible for choosing the best links. However, when the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link. The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN. It supports all the standard and proprietary protocols.
- Any protocol that can take the datagram and carry it through the link suffices for the network layer. The data-link layer takes a datagram and encapsulates it in a packet called a frame. Each link-layer protocol may provide a different service. Some link-layer protocols provide complete error detection and correction, some provide only error correction.

Network Layer

- The network layer is responsible for creating a connection between the source computer and the destination computer. The communication at the network layer is host-to-host.
- The network layer in the Internet includes the main protocol, Internet Protocol (IP), that defines the format of the packet, called a datagram at the network layer. IP also defines the format and the structure of addresses used in this layer. IP is also responsible for routing a packet from its source to its destination, which is achieved by each router forwarding the datagram to the next router in its path.
- At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

Transport Layer

- Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another.
- UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.
- The main protocol, Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data.
- TCP provides flow control, error control and congestion control to reduce the loss of segments due to congestion in the network.
- The other common protocol, User Datagram Protocol (UDP), is a connectionless protocol that transmits user datagrams without first creating a logical connection. In UDP, each user datagram is an independent entity without being related to the

- previous or the next one. UDP is a simple protocol that does not provide flow, error, or congestion control.
- A new protocol, Stream Control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia

Application Layer

- The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer.
- Communication at the application layer is between two processes. The application layer in the Internet includes many predefined protocols.
- 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.

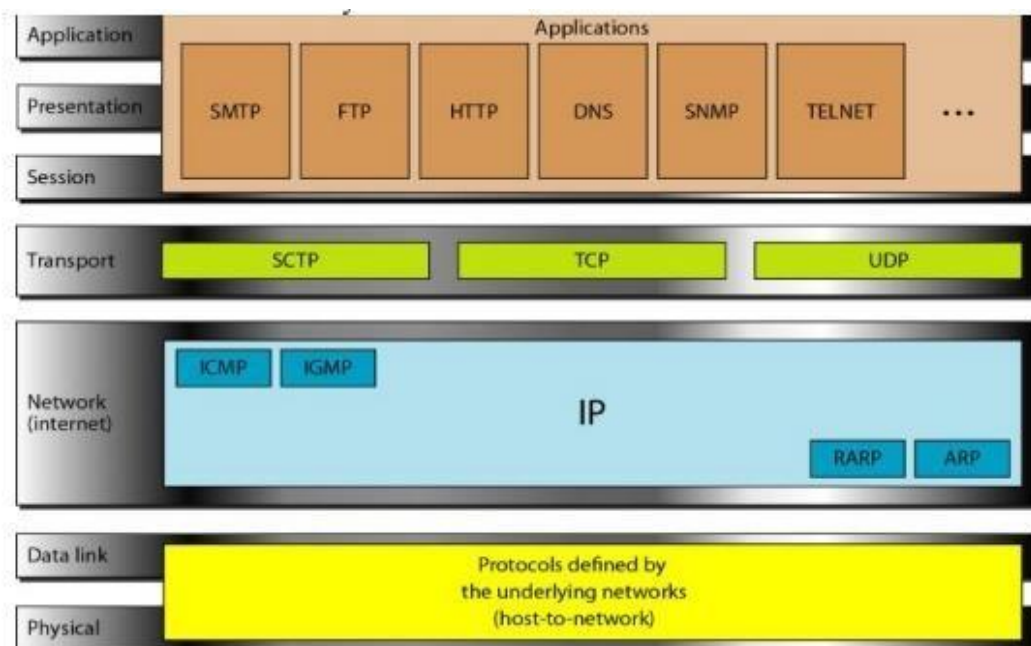
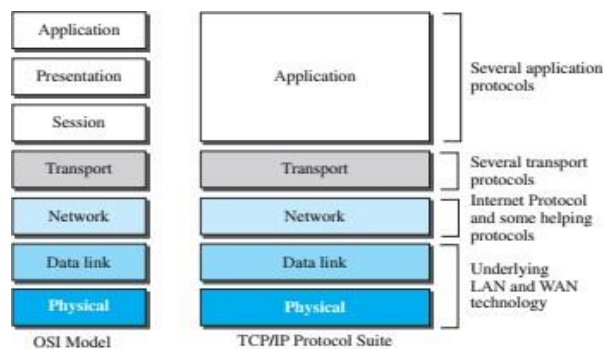
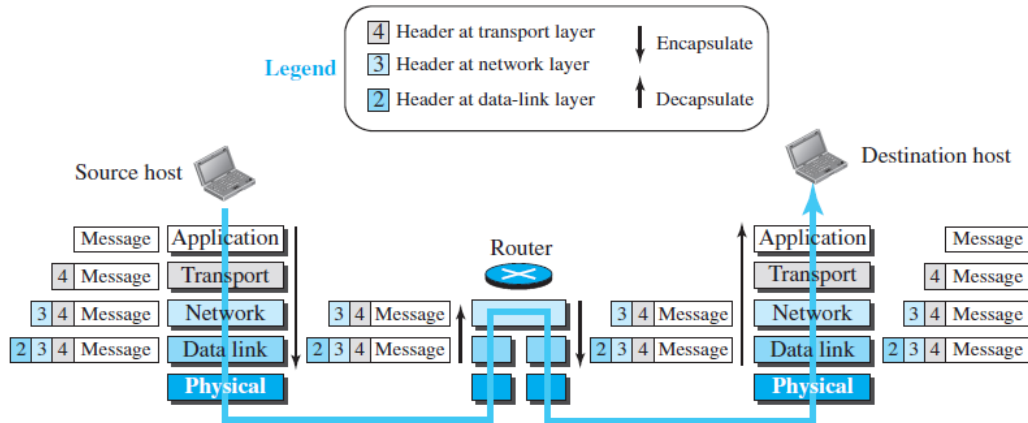


Fig 1.32 OSI Verses TCP/IP

Encapsulation and Decapsulation

One of the important concepts in protocol layering in the Internet is encapsulation/decapsulation.



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.

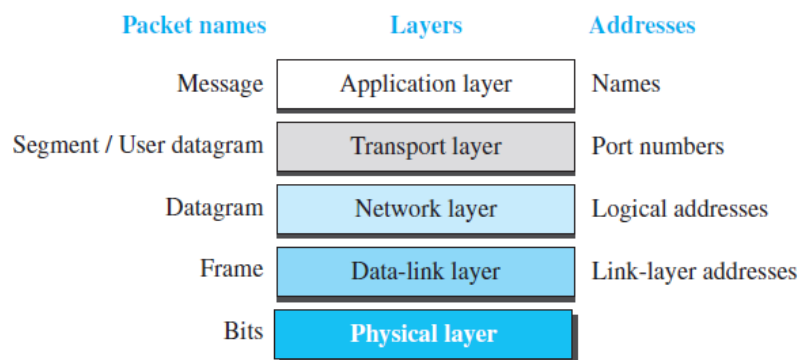
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

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.

Addressing

Addressing in the TCP/IP protocol suite



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).

INTRODUCTION TO DATA LINK LAYER

Q1.State the issues in datalink layer. (2 marks) NOV/DEC 2015

Q2. List the responsibilities of data link layer. (2 marks) NOV/DEC 2019

The Internet is a combination of networks combined together by connecting devices (routers or switches). If a packet is to travel from a host to another host, it needs to pass through these networks. Figure shows the same scenario. Communication at the data-link layer is made up of five separate logical connections between the data-link layers in the path.

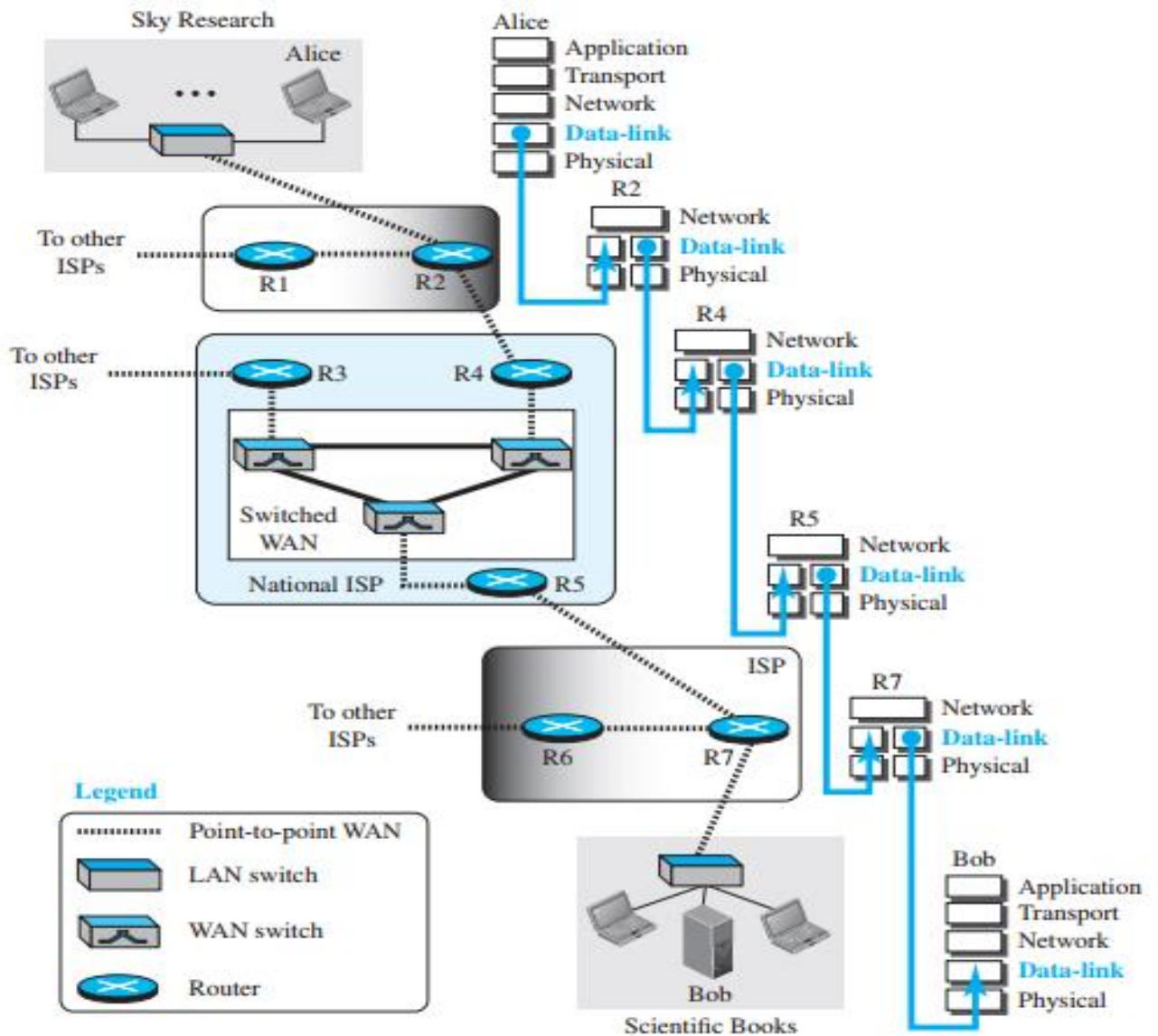


Fig.1.49 Communication at the data-link layer

The data-link layer at Alice's computer communicates with the data-link layer at router R2. The data-link layer at router R2 communicates with the data-link layer at router R4, and so on. Finally, the data-link layer at router R7 communicates with the data-link layer at Bob's computer. Only one data-link layer is involved at the source or the destination, but two data-link layers are involved at each router. The reason is that Alice's and Bob's computers are each connected to a single network, but each router takes input from one network and sends output to another network.

A. Nodes and Links

- Communication at the data-link layer is node-to-node. A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point. These LANs and WANs are connected by routers. It is customary to refer to the two end hosts and the routers as nodes and the networks in between as links.

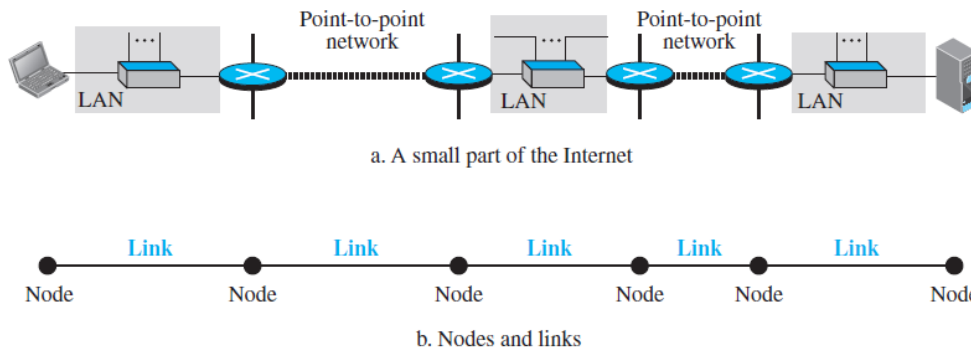


Fig.1.50 Nodes and links.

- Figure 1.50 shows a simple representation of links and nodes when the path of the data unit is only six nodes. The first node is the source host; the last node is the destination host. The other four nodes are four routers. The first, the third, and the fifth links represent the three LANs; the second and the fourth links represent the two WANs.

B. Services

The data-link layer is located between the physical and the network layers. The data link layer provides services to the network layer; it receives services from the physical layer.

- The duty scope of the data-link layer is node-to-node.
- When a packet is travelling in the Internet, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.
- The data-link layer of the source host needs only to encapsulate, the data-link layer of the destination host needs to decapsulate, but each intermediate node needs to both encapsulate and decapsulate.

Services provided by the data-link layer:

- Framing**
- Flow control**
- Error control**
- Congestion control**

A. Framing

- The first service provided by the data-link layer is framing.
- The data-link layer at each node needs to encapsulate the datagram (packet received from the network layer) in a frame before sending it to the next node.
- The node also needs to decapsulate the datagram from the frame received on the logical channel.
- **A packet at the data-link layer is normally called a frame**

B. Flow Control

Controlling the flow of frames at the sender side to avoid overflow and loss of data at the receiver side is called flow control.

If the rate of produced frames is higher than the rate of consumed frames, frames at the receiving end need to be buffered while waiting to be consumed.

C. Error Control

- At the sending node, a frame in a data-link layer needs to be changed to bits, transformed to electromagnetic signals, and transmitted through the transmission media.
- At the receiving node, electromagnetic signals are received, transformed to bits, and put together to create a frame.
- Since electromagnetic signals are affected by error, a frame is also get affected by error. The error should be detected.
- After detection, it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node.

D. Congestion Control

- A link may be congested with frames, which may result in frame loss; most data-link layer protocols do not directly use a congestion control to prevent congestion.
- In general, congestion control is considered an issue in the network layer or the transport layer because of its end-to-end nature.

Two Categories of Links

- Point-to-point link
 - Broadcast link.
-
- In a point-to-point link, the link is dedicated to the two devices; in a broadcast link, the link is shared between several pairs of devices.
 - For example, when two friends use the traditional home phones to chat, they are using a Point-to-point link; when the same two friends use their cellular phones, they are using a broadcast link.

Two Sub layers

The data-link layer has two sub layers:

Data link control (DLC) and media access control (MAC).

The data link control sub layer deals with all issues common to both point-to-point and broadcast links; the media access control sub layer deals only with issues specific to broadcast links.

1.3. LINK-LAYER ADDRESSING

A link-layer address is called a link address, sometimes called a physical address, and sometimes a MAC address. A link is controlled at the data-link layer, the addresses need to belong to the data-link layer.

When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header. These two addresses are changed every time the frame moves from one link

to another.

Figure shows, IP addresses and link-layer addresses in a small internet. In the diagram, three links and two routers. There are only two hosts: Alice (source) and Bob (destination). For each host, we have shown two addresses, the IP addresses (N) and the link-layer addresses (L).

A router has as many pairs of addresses as the number of links the router is connected to. Three frames are shown, one in each link. Each frame carries the same datagram with the same source and destination addresses (N1 and N8), but the link-layer addresses of the frame change from link to link.

In link 1, the link-layer addresses are L1 and L2. In link 2, they are L4 and L5. In link 3, they are L7 and L8.

The IP addresses and the link-layer addresses are not in the same order. For IP addresses, the source address comes before the destination address; for link-layer addresses, the destination address comes before the source.

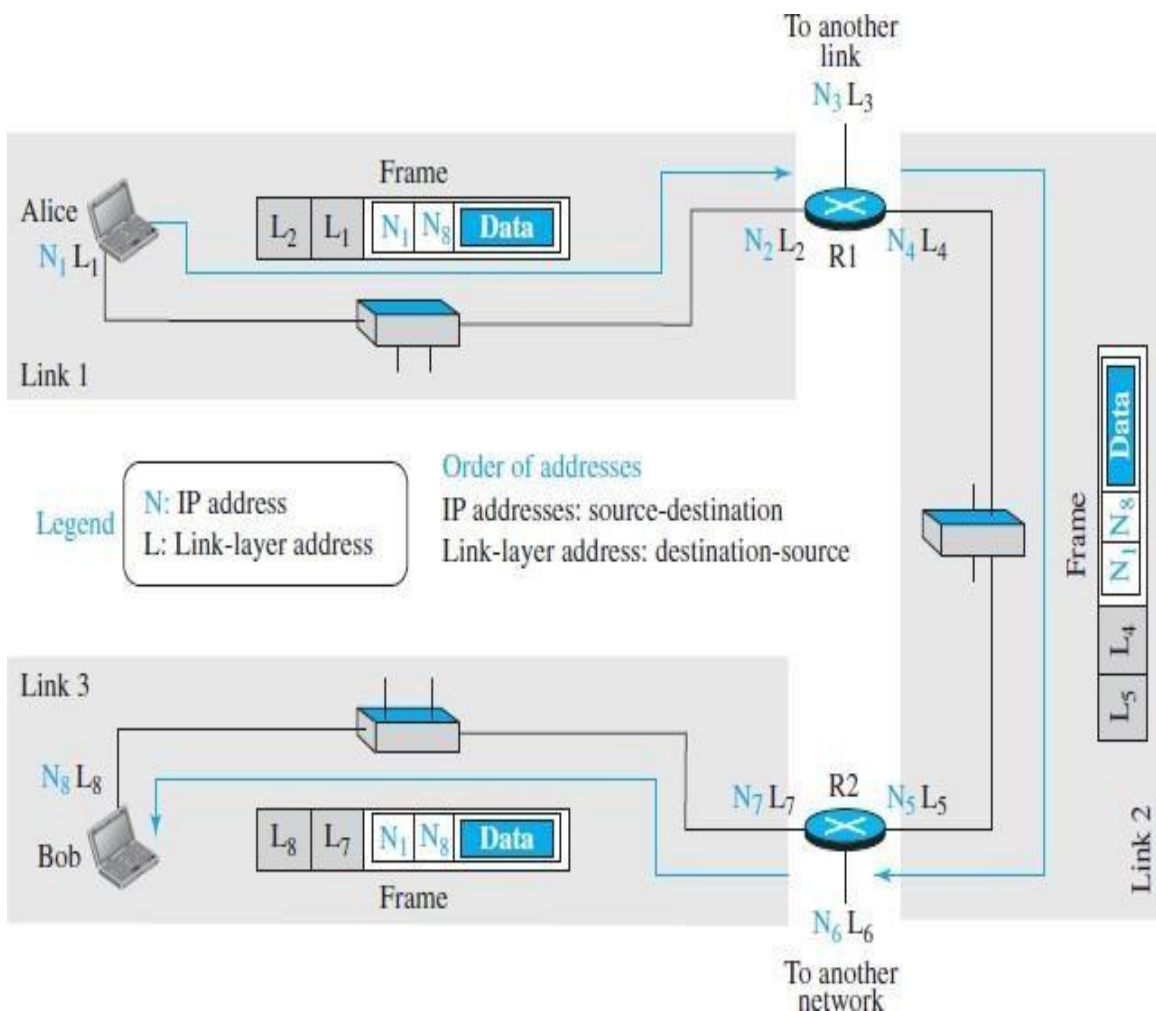


Fig. 1.52 IP addresses and link-layer addresses in a small internet.

Three types of Address:

A. Unicast Address

Each host or each interface of a router is assigned a unicast address. Unicasting means one to-one communication. A frame with a unicast address destination is destined only for one entity in the

link.

Example

The unicast link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons; for example, the following is a link-layer address of a computer.

A3:34:45:11:92:F1

B. Multicast Address

Some link-layer protocols define multicast addresses. Multicasting means one-to-many communications.

Example

The multicast link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons. **The second digit, needs to be an even number in hexadecimal.** The following shows a multicast address:

A2:34:45:11:92:F1

C. Broadcast Address

Some link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

Example

The broadcast link-layer addresses in the most common LAN, Ethernet, are 48 bits, all 1s, that are presented as 12 hexadecimal digits separated by colons.

The following shows a broadcast address:

FF: FF: FF: FF: FF: FF

Address Resolution Protocol (ARP)

The ARP protocol is one of the protocols defined in the network layer, as shown in Figure. It belongs to the network layer. It maps an IP address to a logical-link address.

The main work of ARP:

- ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.

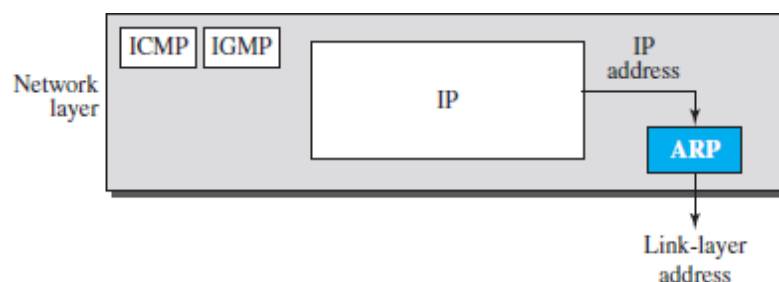


Fig1.53 ARP

- If a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address.

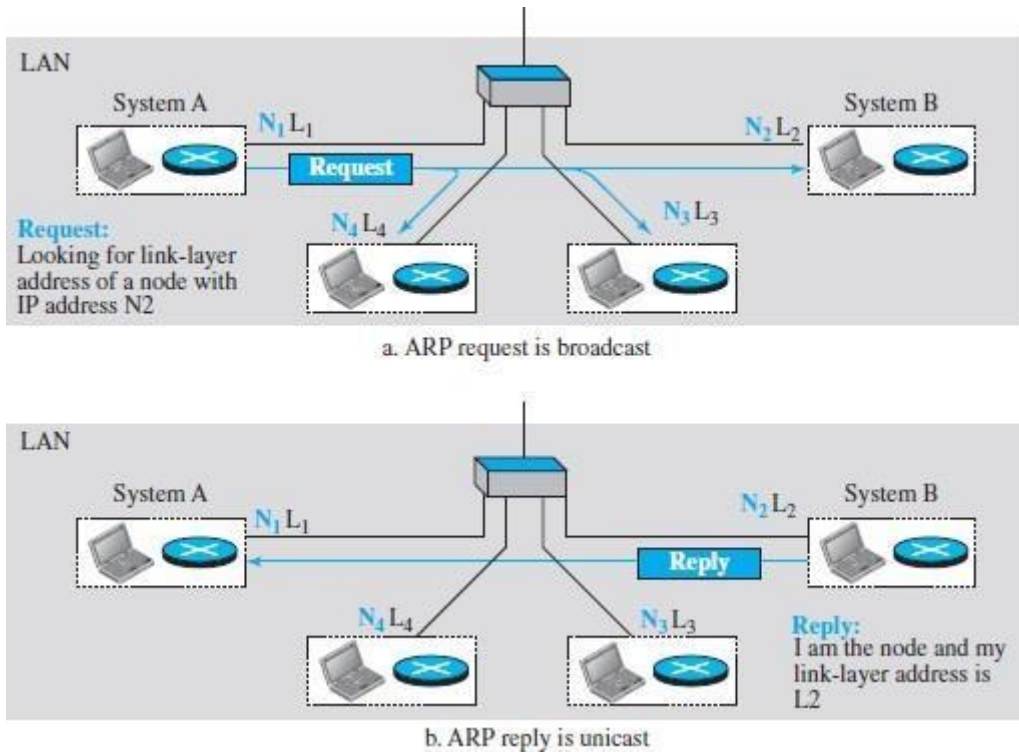


Fig 1.54 ARP operation

- Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an AR response packet.
- The response packet contains the recipient's IP and link-layer addresses. The packet is unicast directly to the node that sent the request packet.
- In Figure, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address N_2 . System A needs to pass the packet to its data-link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of N_2 . This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure above.
- System B sends an ARP reply packet that includes its physical address. Now system A can send all the packets it has for this destination using the physical address it received.

Packet Format

- Figure 1.55 shows the format of an ARP packet.

- The hardware type field defines the type of the link-layer protocol; Ethernet is given the type 1. The protocol type field defines the network-layer protocol: IPv4 protocol is (0800)16.
- The source hardware and source protocol addresses are variable-length fields defining the link-layer and network-layer addresses of the sender. The destination hardware address and destination protocol address fields define the receiver link layer and network-layer addresses.
- An ARP packet is encapsulated directly into a data-link frame. The frame needs to have a field to show that the payload belongs to the ARP and not to the network-layer datagram.

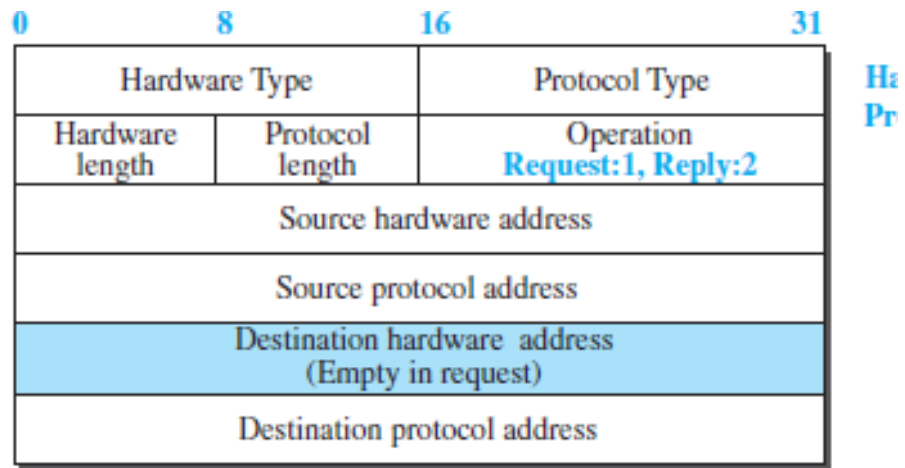
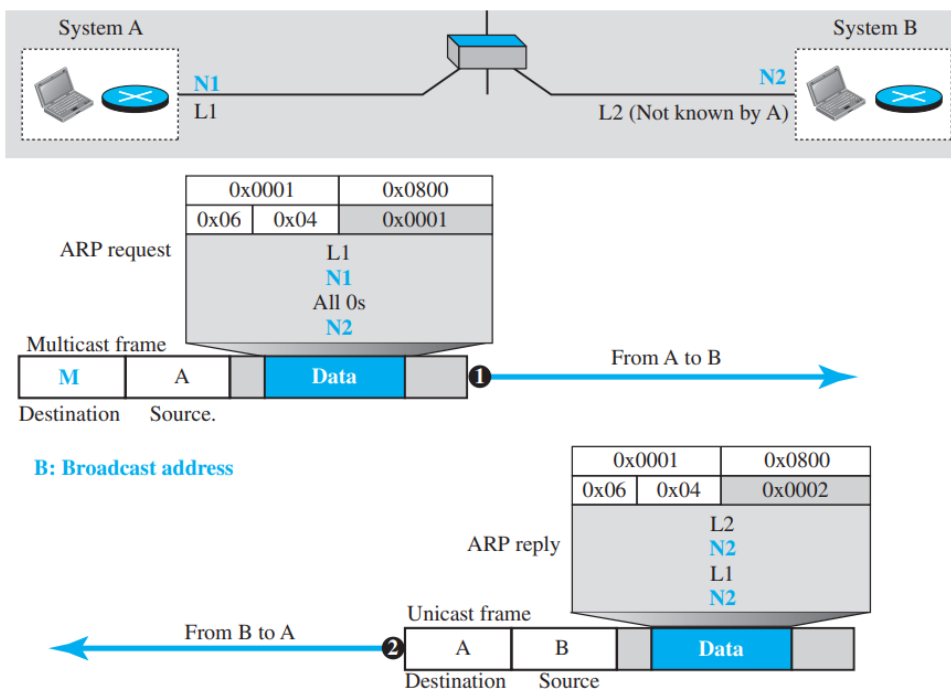


Fig 1.55 ARP packet

Example



1.4. ERROR DETECTION AND CORRECTION

Q1. Explain any two error detection mechanisms in detail. (13 marks)[MAY/JUNE 2016]

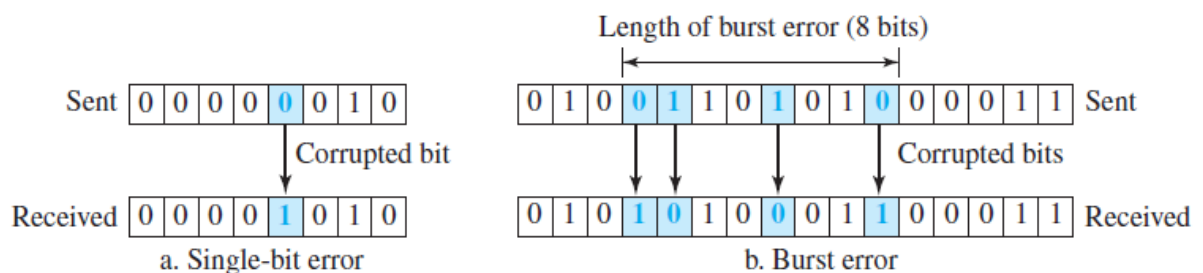
Q2. Obtain the 4 bit CRC for the data sequence 10011011100 using the

polynomial X^4+X^2+1

Q3. Enumerate any one method for error detection and any one method for correction. . (13 marks)[NOV/DEC 2021]

Types of Errors

- Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference.
- 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. Figure shows the effect of a single-bit and a burst error on a data unit.



- A burst error is more likely to occur than a single-bit error because the duration of the noise signal is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits.
- 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.
- In **error detection**, we are only looking to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of corrupted bits. 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.
- Redundancy is achieved through various coding schemes. We can divide coding schemes into two broad categories: **block coding** and **convolution coding**.

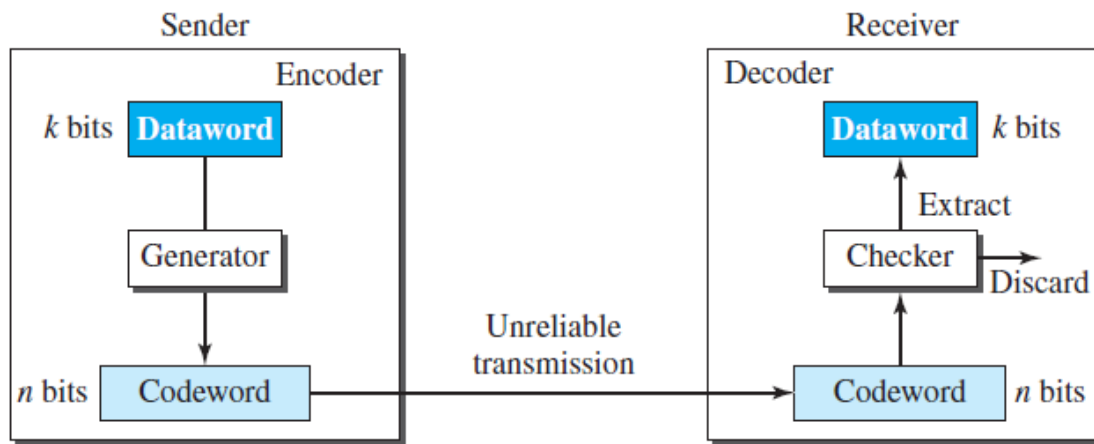
ERROR DETECTION TECHNIQUES:

BLOCK CODING

- In block coding, we divide our message into blocks, each of k bits, called **datawords**. We add r redundant bits to each block to make the length $n = k + r$. The resulting n -bit blocks are called **codewords**.
- Figure shows the role of block coding in error detection. The sender creates codewords out of datawords 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 codewords, the word is accepted; the

corresponding dataword is extracted for use. If the received codeword is not valid, it is discarded.

- However, if the codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected.



Example: Even Parity

Let us assume that $k = 2$ and $n = 3$. Table shows the list of datawords and codewords.

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

Assume the sender encodes the dataword 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 dataword 00. Two corrupted bits have made the error undetectable.

Hamming Distance

- The **Hamming distance** between two words (of the same size) is the number of differences between the corresponding bits.
- 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 $d(00000, 01101) = 3$.
- The Hamming distance can easily be found if we apply the XOR operation on the two words and count the number of 1s in the result.

Example

Let us find the Hamming distance between two pairs of words.

1. The Hamming distance $d(000, 011)$ is 2 because $(000 \oplus 011)$ is 011 (two 1s).
2. The Hamming distance $d(10101, 11110)$ is 3 because $(10101 \oplus 11110)$ is 01011 (three 1s).

Minimum Hamming Distance for Error Detection

- In a set of codewords, the minimum Hamming distance is the smallest Hamming distance between all possible pairs of codewords.
- To guarantee the detection of up to s errors in all cases, the minimum Hamming distance in a block code must be $d_{min} = s + 1$.

LINEAR BLOCK CODES

A linear block code is a code in which the exclusive OR of two valid codewords creates another valid codeword.

Minimum Distance for Linear Block Codes

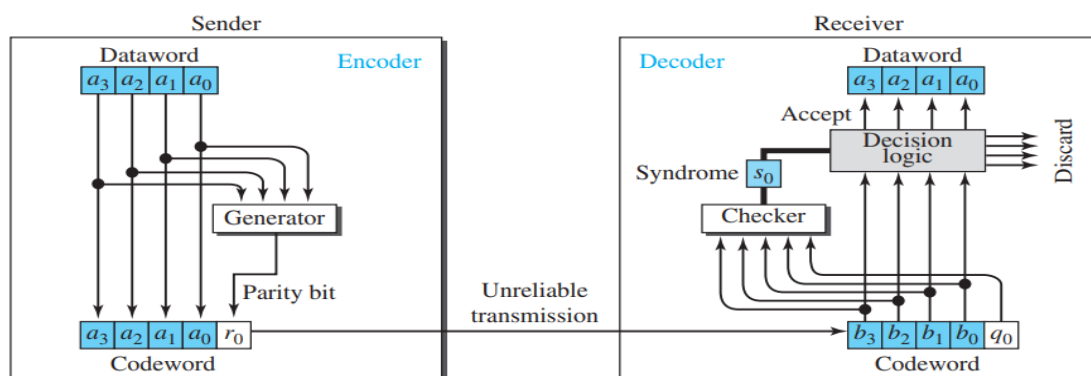
It is simple to find the minimum Hamming distance for a linear block code. The minimum Hamming distance is the number of 1s in the nonzero valid codeword with the smallest number of 1s.

Parity-Check Code

- Perhaps the most familiar error-detecting code is the parity-check code. This code is a linear block 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 1s in the codeword even.
- The minimum Hamming distance for this category is $d_{min} = 2$, which means that the code is a single-bit error-detecting code.

<i>Dataword</i>	<i>Codeword</i>	<i>Dataword</i>	<i>Codeword</i>
0000	0000 0	1000	1000 1
0001	0001 1	1001	1001 0
0010	0010 1	1010	1010 0
0011	0011 0	1011	1011 1
0100	0100 1	1100	1100 0
0101	0101 0	1101	1101 1
0110	0110 0	1110	1110 1
0111	0111 1	1111	1111 0

Figure shows a possible structure of an encoder (at the sender) and a decoder (at the receiver).



The encoder uses a generator that takes a copy of a 4-bit dataword (a0, a1, a2, and a3) and generates a parity bit r0.

$$R_0 = a_3 + a_2 + a_1 + a_0 \text{ (modulo-2)}$$

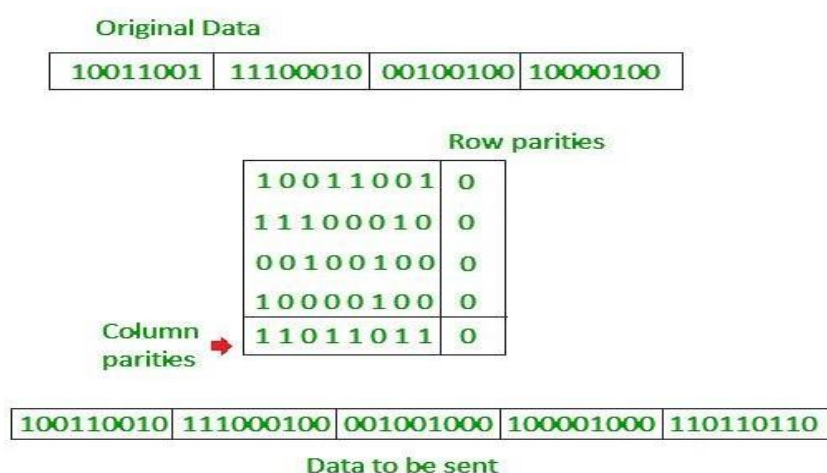
- If the number of 1s is even, the result is 0; if the number of 1s is odd, the result is 1. In both cases, the total number of 1s in the codeword is even.
- The sender sends the codeword, which may be corrupted during transmission. The receiver receives a 5-bit word. The checker at the receiver does 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.

$$S_0 = b_3 + b_2 + b_1 + b_0 + q_0 \text{ (modulo-2)}$$

The syndrome is passed to the decision logic analyzer. If the syndrome is 0, there is no detectable error in the received codeword; the data portion of the received code word is accepted as the dataword; if the syndrome is 1, the data portion of the received codeword is discarded.

TWO-DIMENSIONAL PARITY CHECK (LONGITUDINAL REDUNDANCY CHECK)

Parity check bits are calculated for each row, which is equivalent to a simple parity checkbit. Parity checkbits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.

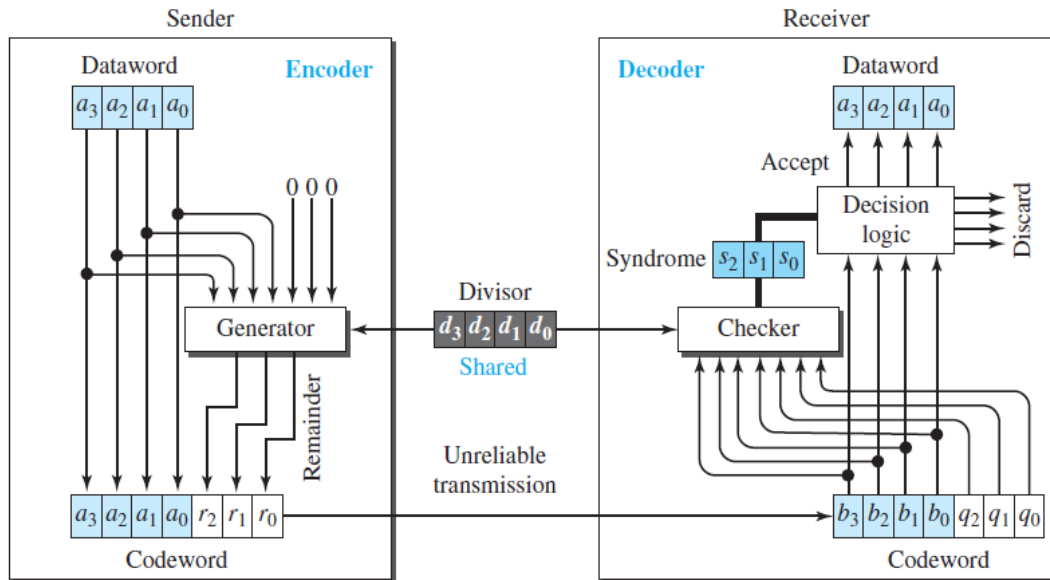


CYCLIC CODES

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.

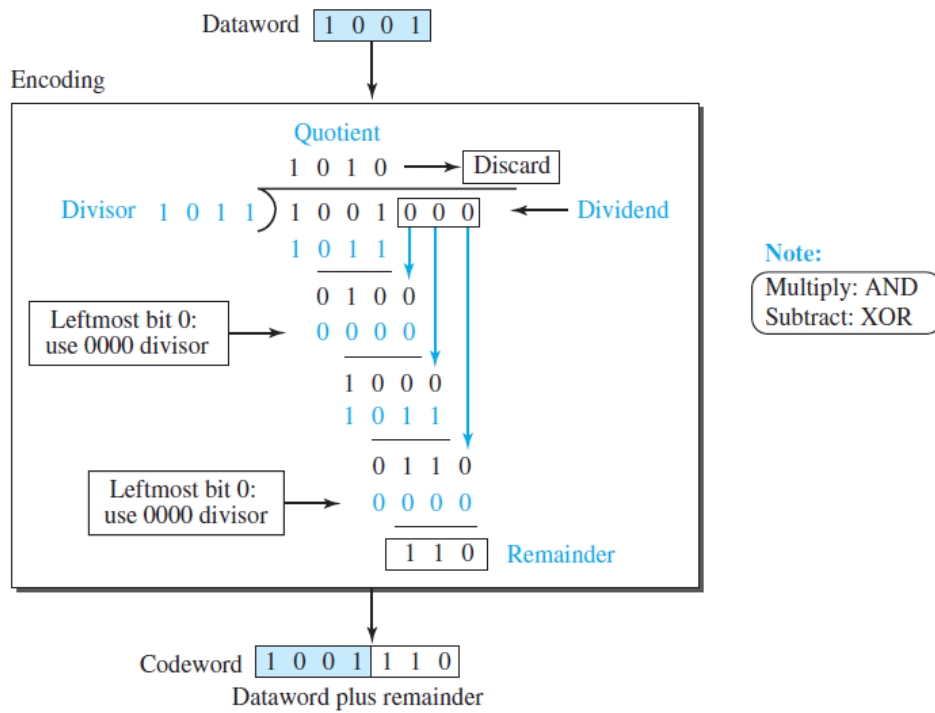
Cyclic Redundancy Check (CRC)

CRC is the subset of cyclic codes which is used in networks such as LANs and WANs.

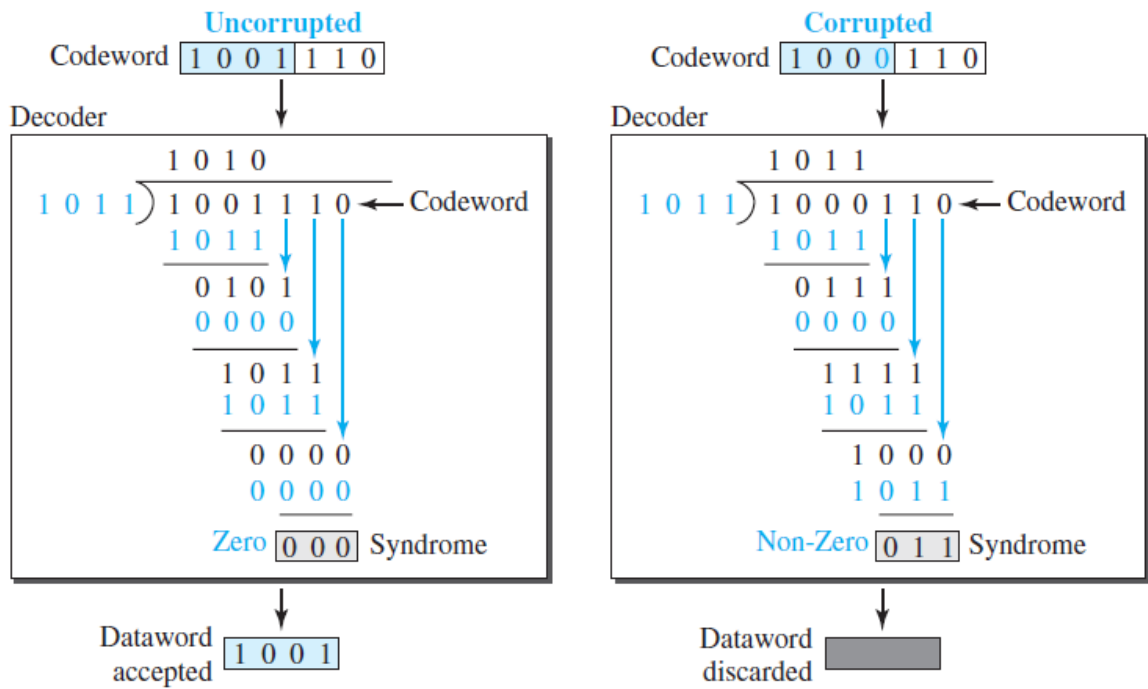


CRC ENCODER and DECODER

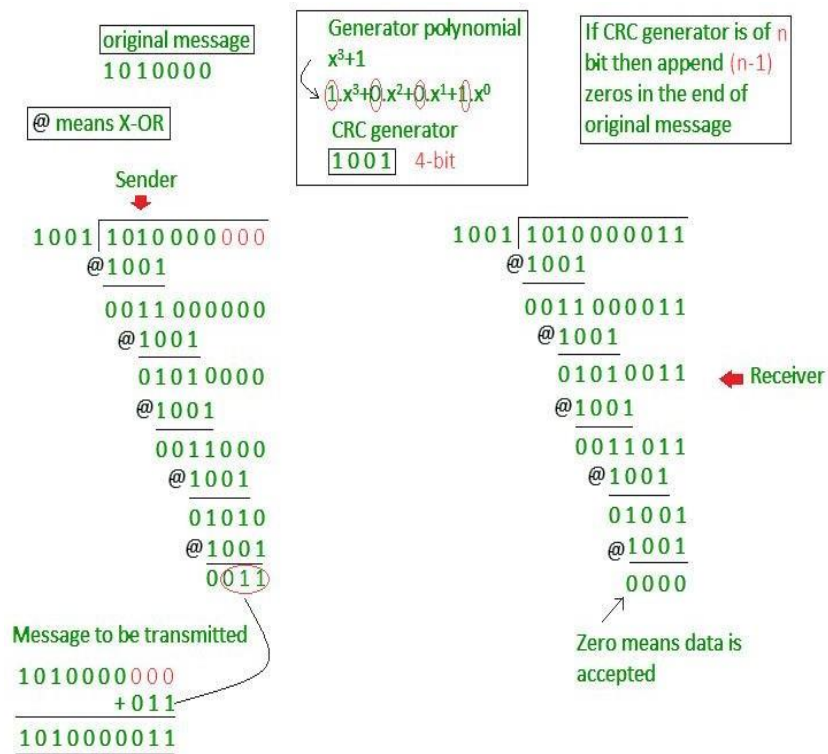
ENCODER



DECODER

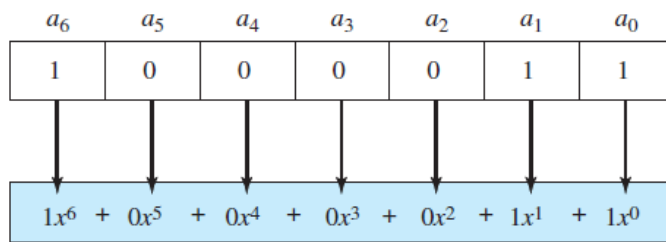


Example 2

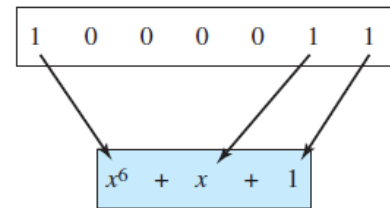


Polynomials

A better way to understand cyclic codes and how they can be analyzed is to represent them as polynomials.



a. Binary pattern and polynomial



b. Short form

A Polynomial to represent a binary word

The degree of a polynomial is the highest power in the polynomial. For example, the degree of the polynomial $x^6 + x + 1$ is 6.

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.
- Addition and subtraction are the same. 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, $x^3 \times x^4$ 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 .

Shifting

Shifting to the left means adding extra 0s as rightmost bits; shifting to the right means deleting some rightmost bits.

Shifting left 3 bits: 10011 becomes 10011000

$x^4 + x + 1$ becomes $x^7 + x^4 + x^3$

Shifting right 3 bits: 10011 becomes 10

$x^4 + x + 1$ becomes x

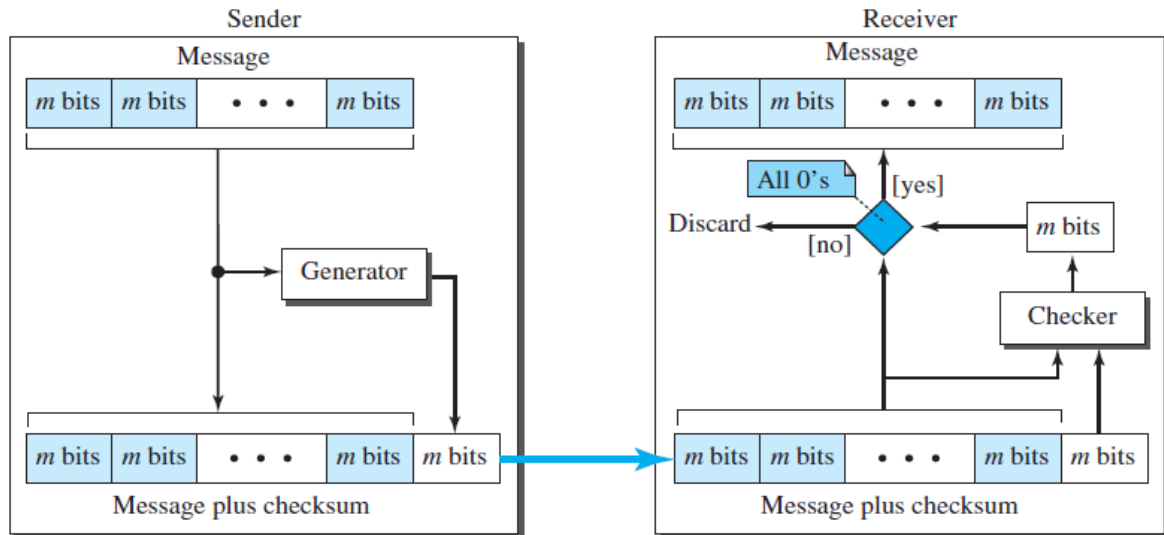
Shifting to the left is accomplished by multiplying each term of the polynomial by x^m , where m is the number of shifted bits; shifting to the right is accomplished by dividing each term of the polynomial by x^m .

Check Sum

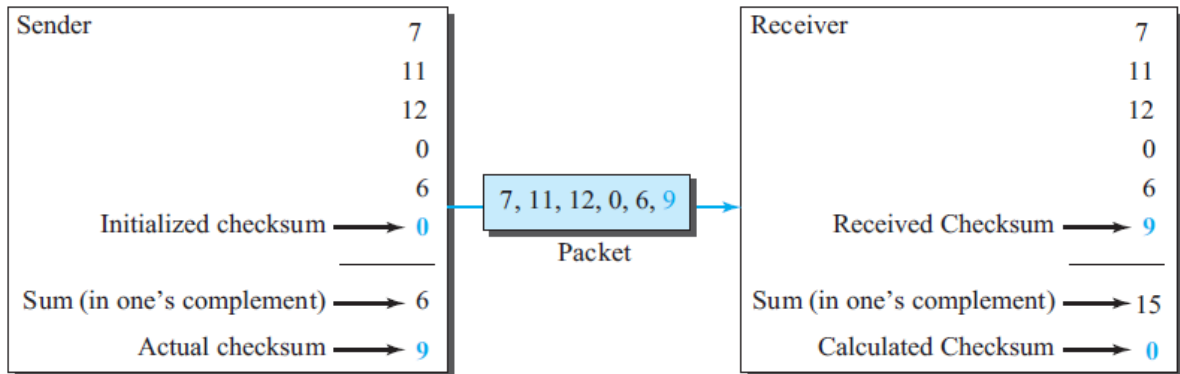
Procedure to calculate Traditional check sum

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

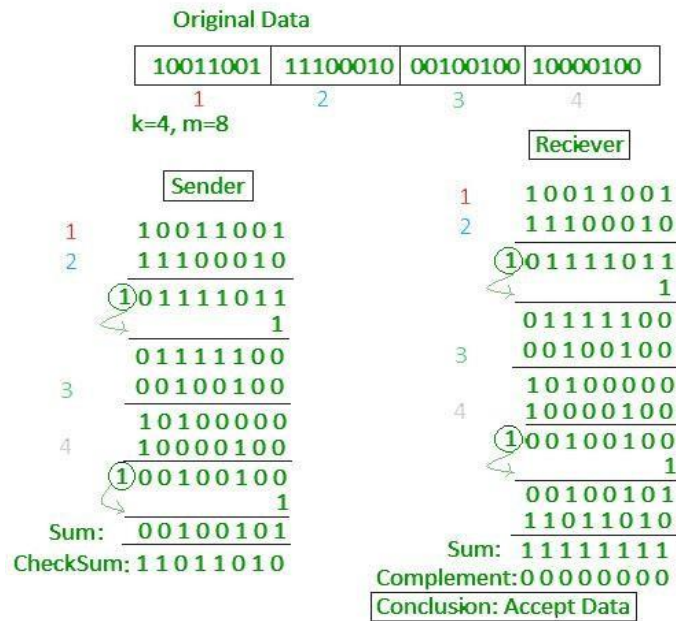
Sender	Receiver
1. The message is divided into 16-bit words.	1. The message and the checksum are received.
2. The value of the checksum word is initially set to zero.	2. The message is divided into 16-bit words.
3. All words including the checksum are added using one's complement addition.	3. All words 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.



Example1



Example 2



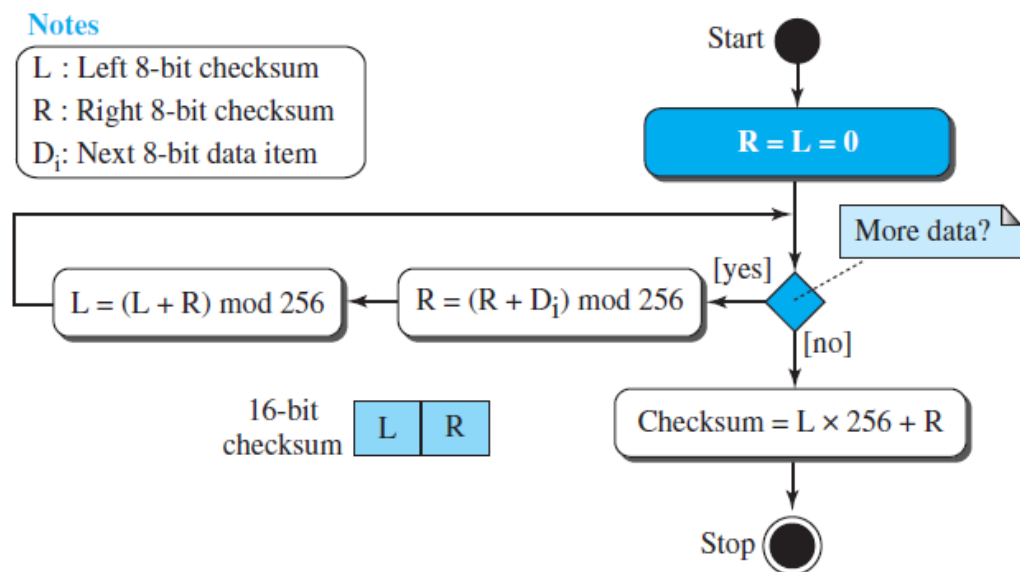
Exercise: nov/dec 2021

i) Answer the following questions: (7)

- I. What is the polynomial representation of 110111?
- II. What is the result of shifting 111000 three bits to the left?
- III Repeat part (ii) using polynomials.
- IV What is the result of shifting 110011 four bits to the right? Repeat part (iv) using polynomials.

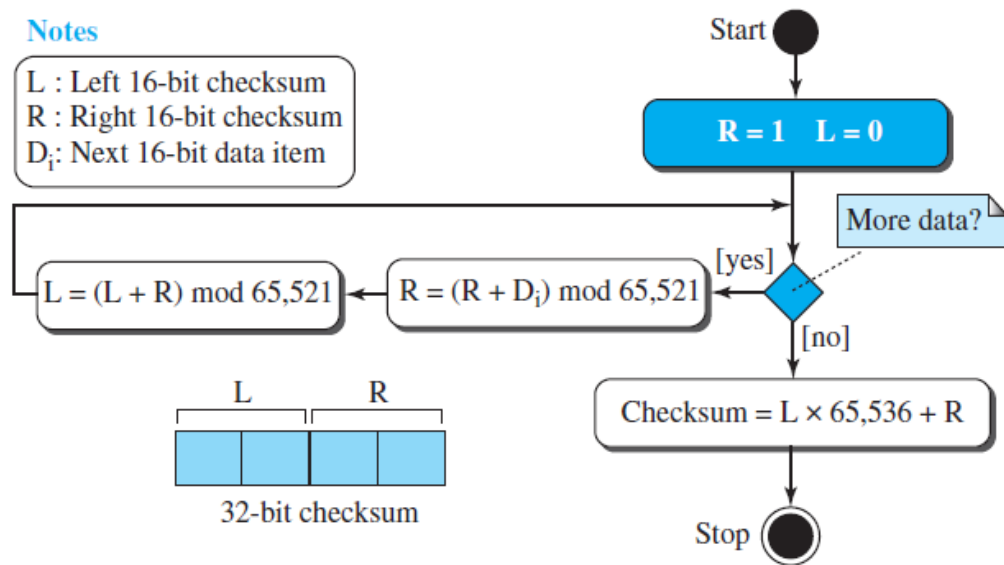
Fletcher Checksum

Figure 10.18 Algorithm to calculate an 8-bit Fletcher checksum



Adler Checksum

Figure 10.19 Algorithm to calculate an Adler checksum



ERROR CORRECTION TECHNIQUES:

FORWARD ERROR CORRECTION: HAMMING CODE

Hamming Code

Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. It is technique developed by R.W. Hamming for error correction.

Redundant bits -

Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:

$$2^r \geq m + r + 1$$

where, r = redundant bit, m = data bit

Suppose the number of data bits is 7, then the number of redundant bits can be calculated using: $2^4 \geq 7 + 4 + 1$

Thus, the number of redundant bits = 4

Parity bits -

A parity bit is a bit appended to a data of binary bits to ensure that the total number of 1's in the data are even or odd. Parity bits are used for error detection. There are two types of parity bits:

1. Even parity bit:

In the case of even parity, for a given set of bits, the number of 1's are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1's an even number. If the total number of 1's in a given set of bits is already even, the parity bit's value is 0.

2. Odd Parity bit

In the case of odd parity, for a given set of bits, the number of 1's are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1's an odd number. If the total number of 1's in a given set of bits is already odd, the parity bit's value is 0.

General Algorithm of Hamming code -

- The Hamming Code is simply the use of extra parity bits to allow the identification of an error.
- Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
- All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
- All the other bit positions are marked as data bits.
- Each data bit is included in a unique set of parity bits, as determined its bit position in binary form.
- Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc).
- Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc).
- Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4-7, 12-15, 20-23, etc).
- Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8-15, 24-31, 40-47, etc).
- In general each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.
- Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.
- Set a parity bit to 0 if the total number of ones in the positions it checks is even.

Determining the position of redundant bits -

These redundancy bits are placed at the positions which correspond to the power of 2. As in the above example:

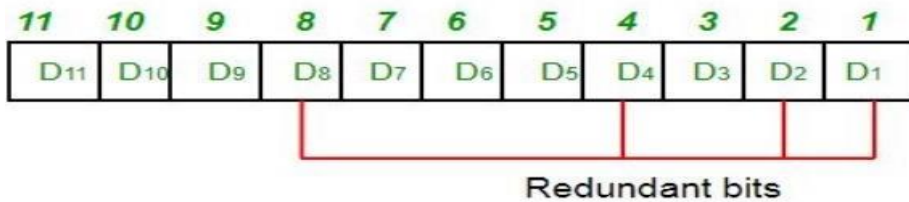
The number of data bits = 7

The number of redundant bits = 4

The total number of bits = 11

The redundant bits are placed at positions corresponding to power of 2- 1, 2, 4, and

8



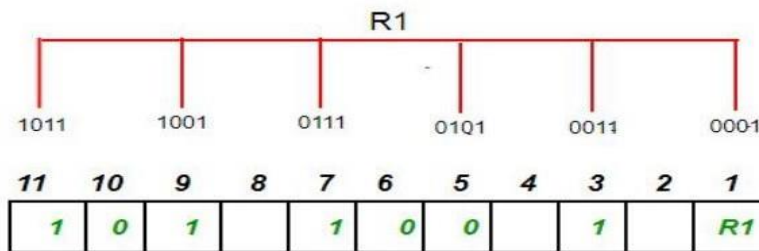
Suppose the data to be transmitted is 1011001, the bits will be placed as follows:



Determining the Parity bits -

- 1 R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.

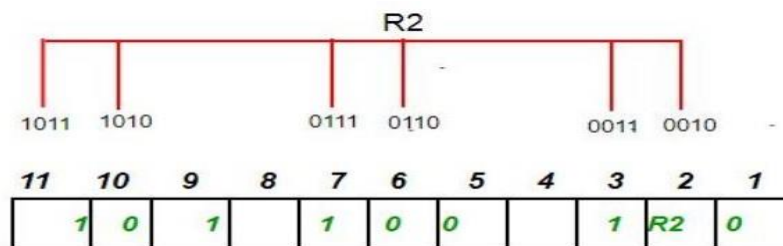
R1: bits 1, 3, 5, 7, 9, 11



To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0

- 2 R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.

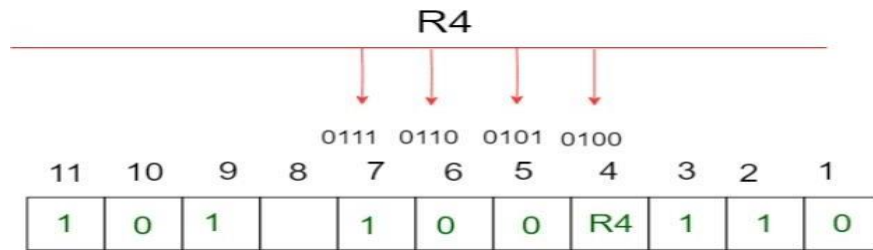
R2: bits 2,3,6,7,10,11



To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is an odd number the value of R2 (parity bit's value) = 1

- 3 R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit.

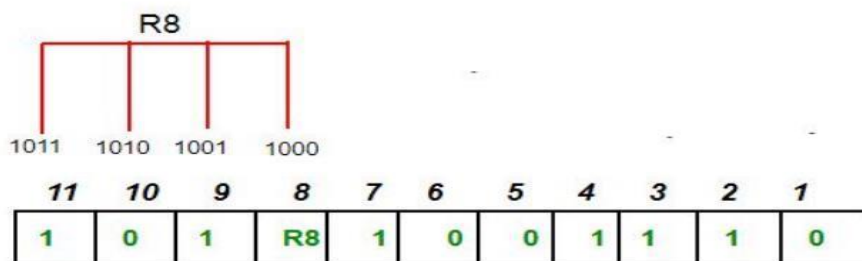
R4: bits 4, 5, 6, 7



To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is an odd number, the value of R4 (parity bit's value) = 1

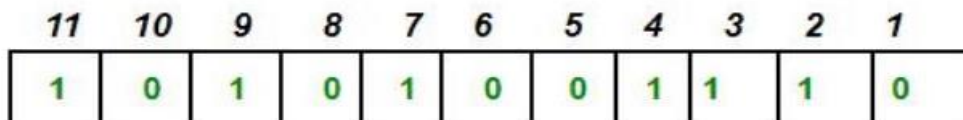
R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.

R8: bit 8,9,10,11



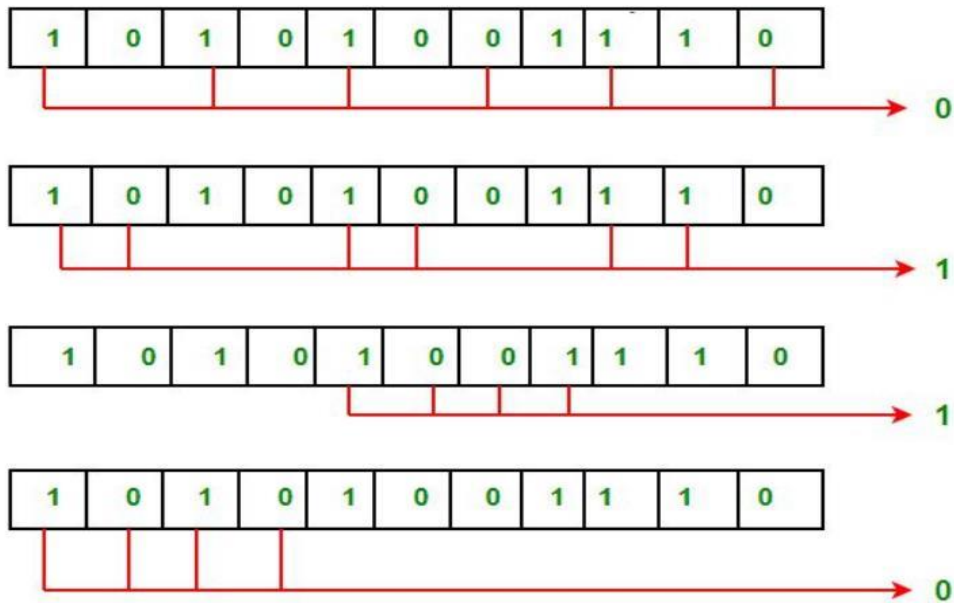
To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number, the value of R8 (parity bit's value) = 0.

Thus, the data transferred is:



Error detection and correction -

Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then it gives new parity values in the binary number:



The bits give the binary number as 0110 whose decimal representation is 6. Thus, the bit 6 contains an error. To correct the error the 6th bit is changed from 1 to 0.

DATA LINK CONTROL LAYER

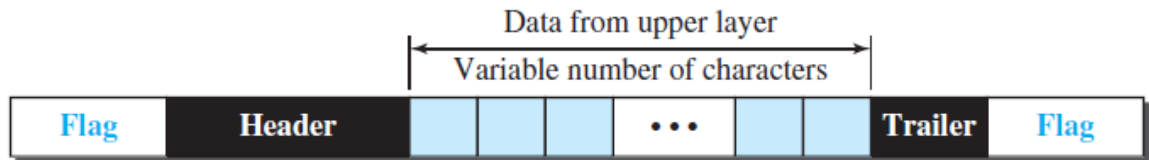
The data-link layer is divided into two sublayers. Data link control (DLC) and Media access control (MAC) layer.

Data link control functions include framing and flow and error control.

Framing

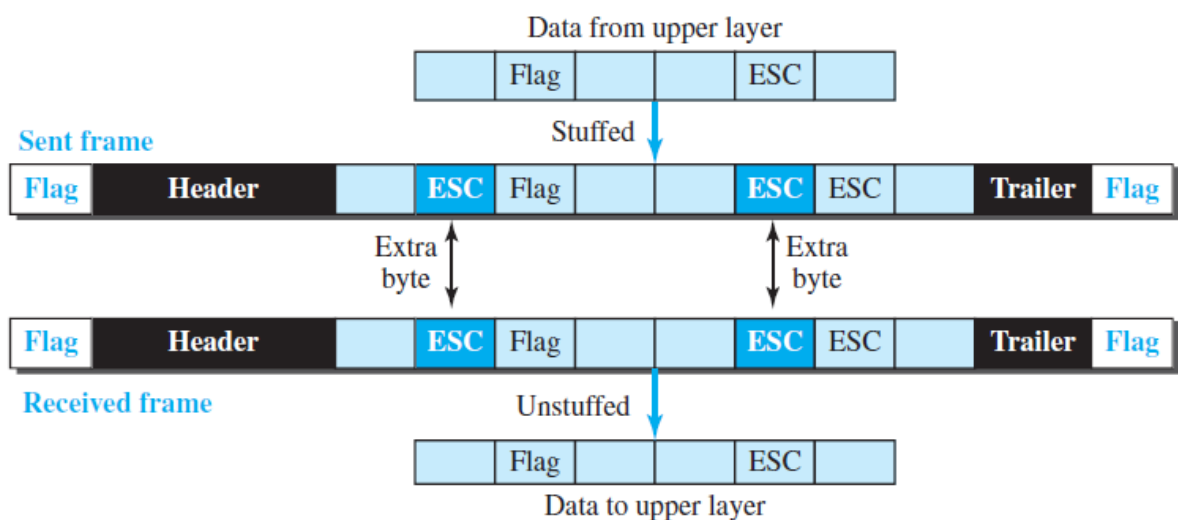
- Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.
- Although the whole message could be packed in one frame, that is not normally done. One reason is that a frame can be very large, making flow and error control very inefficient. When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole frame. When a message is divided into smaller frames, a single-bit error affects only that small frame.
- 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*.
- In variable-size framing, we need a way to define the end of one frame and the beginning of the next. Two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

Character-Oriented Framing



Frame in a Character-Oriented Protocol

- 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.
- Character-oriented framing was popular when only text was exchanged by the data-link layers. The flag could be selected to be any character not used for text communication. Now, however, we send other types of information such as graphs, audio, and video; 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.
- Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text.

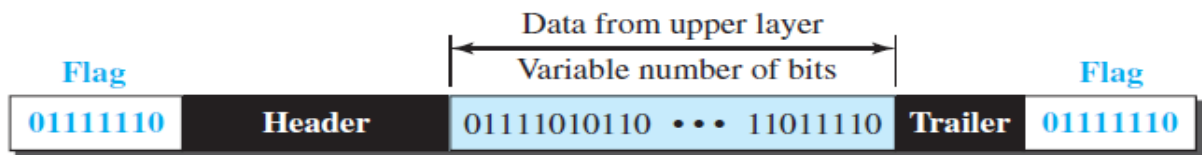


Byte Stuffing and Un stuffing

Bit-Oriented Framing

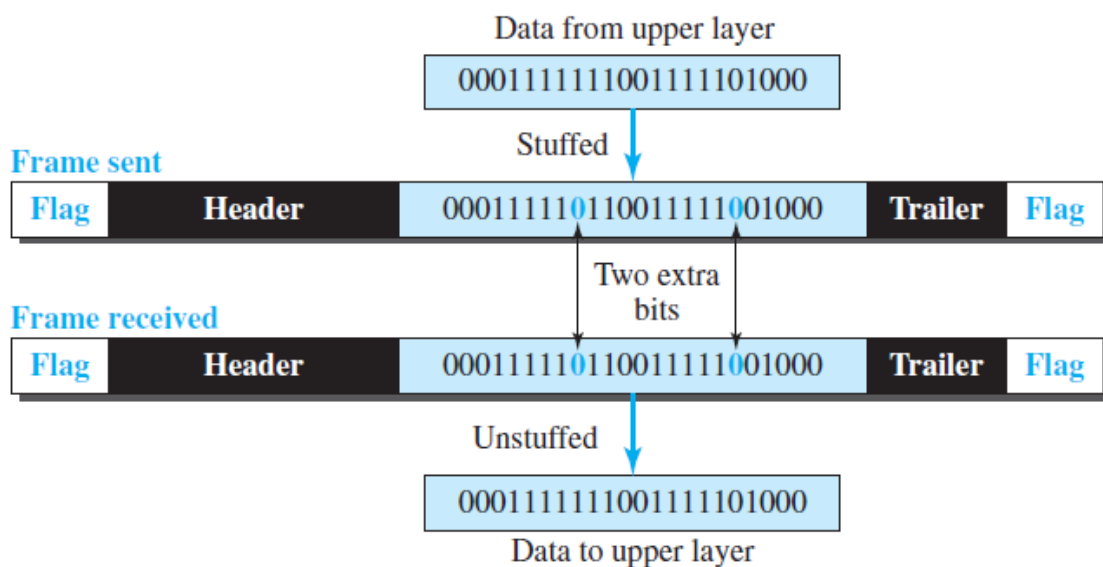
- In *bit-oriented framing*, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on. However, in

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.



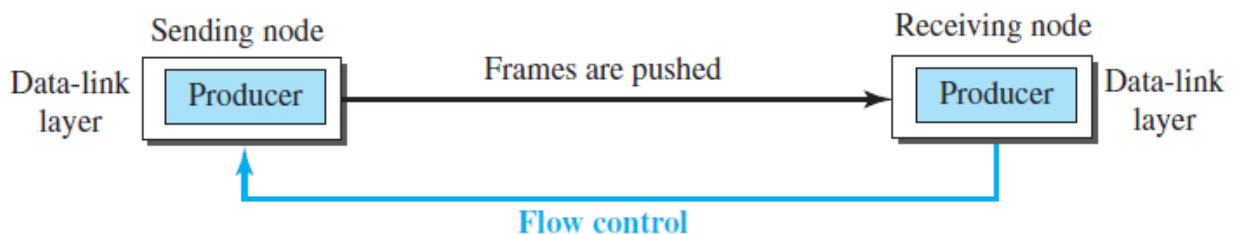
A frame in a bit-oriented protocol

- 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.



Bit stuffing and unstuffing

Flow Control



- 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.
- 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.

Error Control

Error control at the data-link layer is normally very simple and implemented using one of the following two methods. In both methods, a CRC is added to the frame header by the sender and checked by the receiver.

❑ In the first method, if the frame is corrupted, it is silently discarded; if it is not corrupted, the packet is delivered to the network layer. This method is used mostly in wired LANs such as Ethernet.

❑ In the second method, if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent (for the purpose of both flow and error control) to the sender.

Combination of Flow and Error Control

- Flow and error control can be combined. In a simple situation, the acknowledgment that is sent for flow control can also be used for error control to tell the sender the packet has arrived uncorrupted. The lack of acknowledgment means that there is a problem in the sent frame.
- Traditionally three protocols have been defined for the data-link layer to deal with flow and error control: Stop-and-Wait, Go-Back-N, and Selective-Repeat.

1. Stop-and-Wait Automatic Repeat Request

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

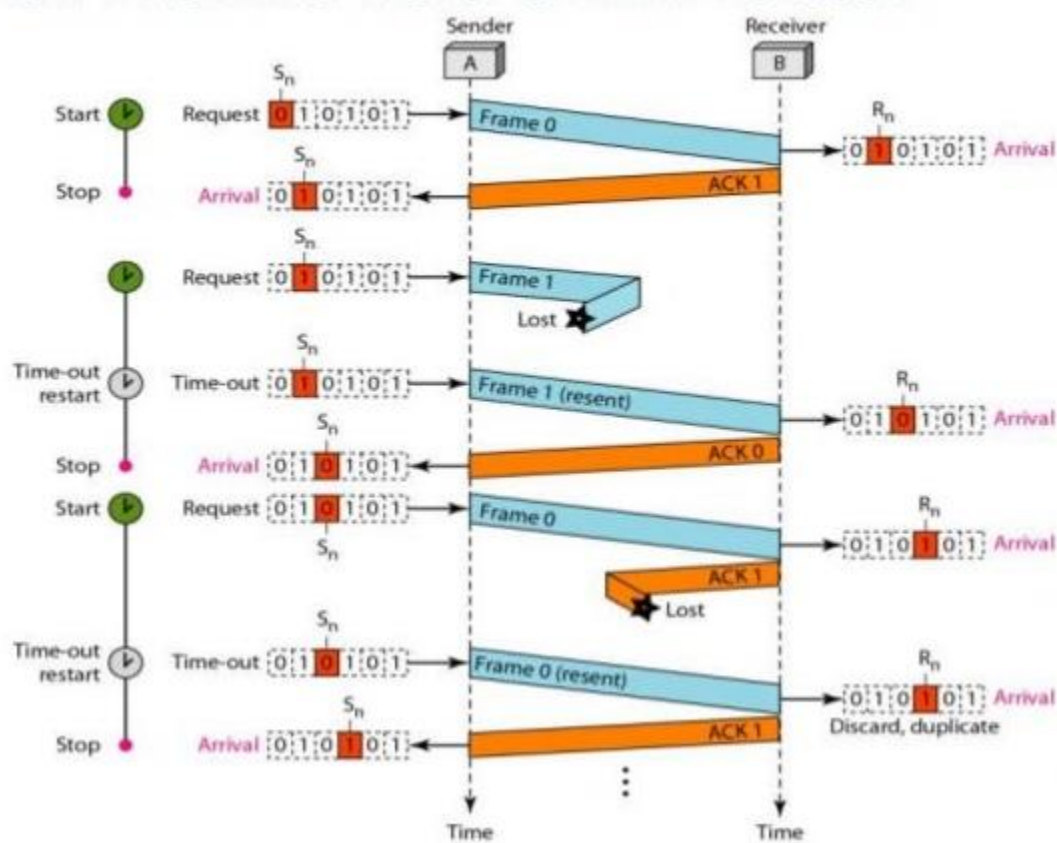
Sequence Numbers

- A field is added to the data frame to hold the sequence number of that frame. For example, if we decide that the field is m bits long, the sequence numbers start from 0, go to $2^m - 1$, and then are repeated.
- In Stop-and-Wait ARQ we use sequence numbers to number the frames. The sequence numbers are based on modul0-2 arithmetic.

Acknowledgment Numbers

- Since the sequence numbers must be suitable for both data frames and ACK frames, we use this convention: The acknowledgment numbers always announce the sequence number of the next frame expected by the receiver. For example, if frame 0 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 1 (meaning frame 1 is expected next). If frame 1 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 0 (meaning frame 0 is expected).

Flow diagram



In the above flow diagram Frame a is sent and acknowledged. Frame 1 is lost and resent after the time-out. The resent frame 1 is acknowledged and the timer stops. Frame a is sent and acknowledged, but the acknowledgment is lost. The sender has no idea if the frame or the acknowledgment is lost, so after the time-out, it resends frame 0, which is acknowledged.

2. Go-Back-N Automatic Repeat Request

In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive.

Sequence Numbers

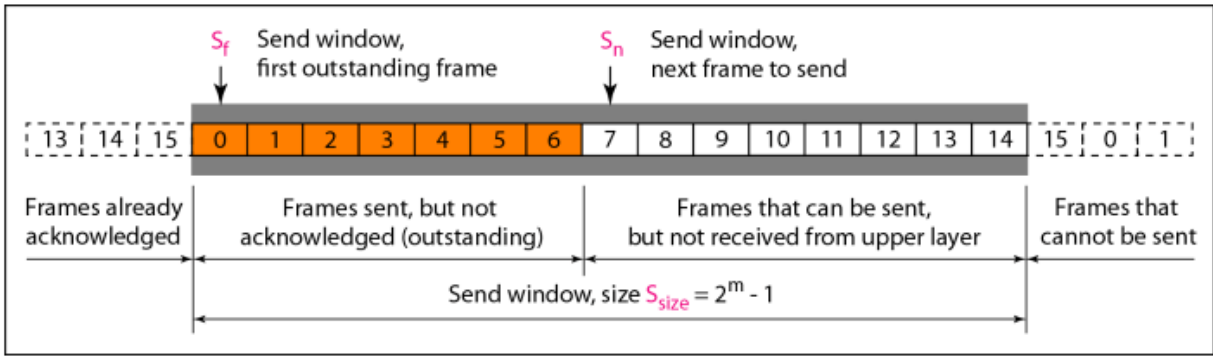
Frames from a sending station are numbered sequentially. If the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to $2^m - 1$. For example, if m is 4, the only sequence numbers are 0 through 15 inclusive. So the sequence numbers are

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ...

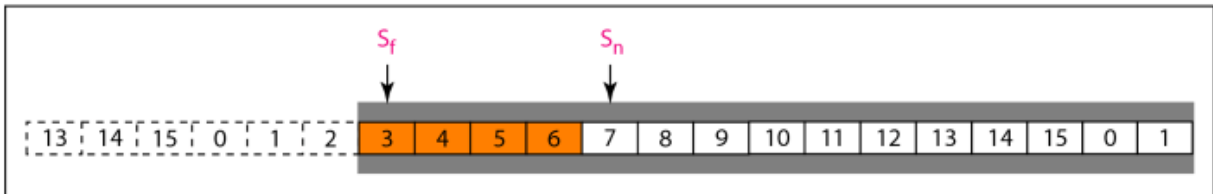
In other words, the sequence numbers are modulo- 2^m

Sliding Window

The sender and receiver need to deal with only part of the possible sequence numbers. The range which is the concern of the sender is called the send sliding window; the range that is the concern of the receiver is called the receive sliding window.

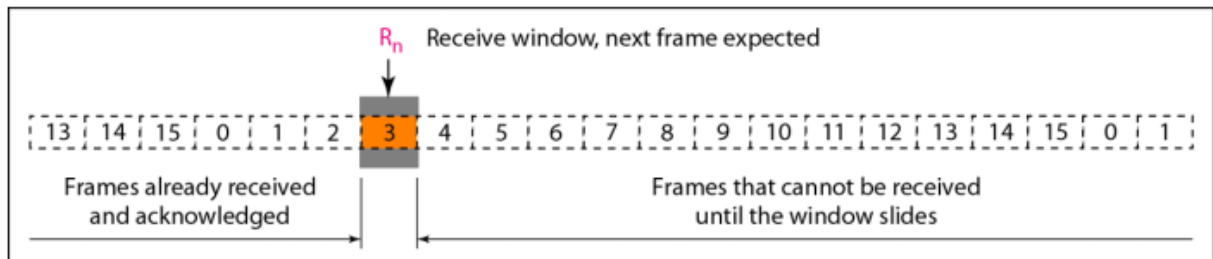


a. Send window before sliding

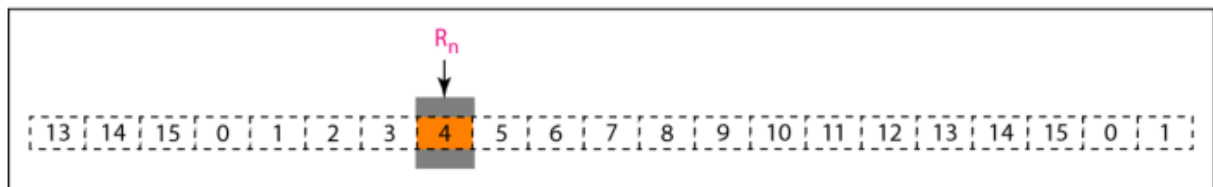


b. Send window after sliding

The send window can slide one or more slots when a valid acknowledgment arrives.



a. Receive window



b. Window after sliding

The receive window is an abstract concept defining an imaginary box of size 1 with one single variable R_n . The window slides when a correct frame has arrived; sliding occurs one slot at a time.

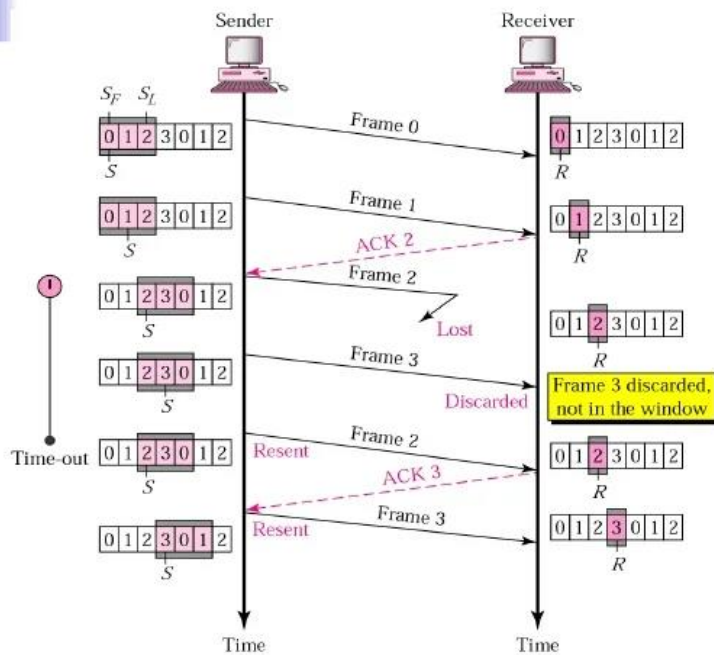
Acknowledgment

The receiver sends a positive acknowledgment if a frame has arrived safe and sound and in order. If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives the one it is expecting. The silence of the receiver causes the timer of the unacknowledged frame at the sender site to expire. This, in turn, causes the sender to go back and resend all frames, beginning with the one with the expired timer.

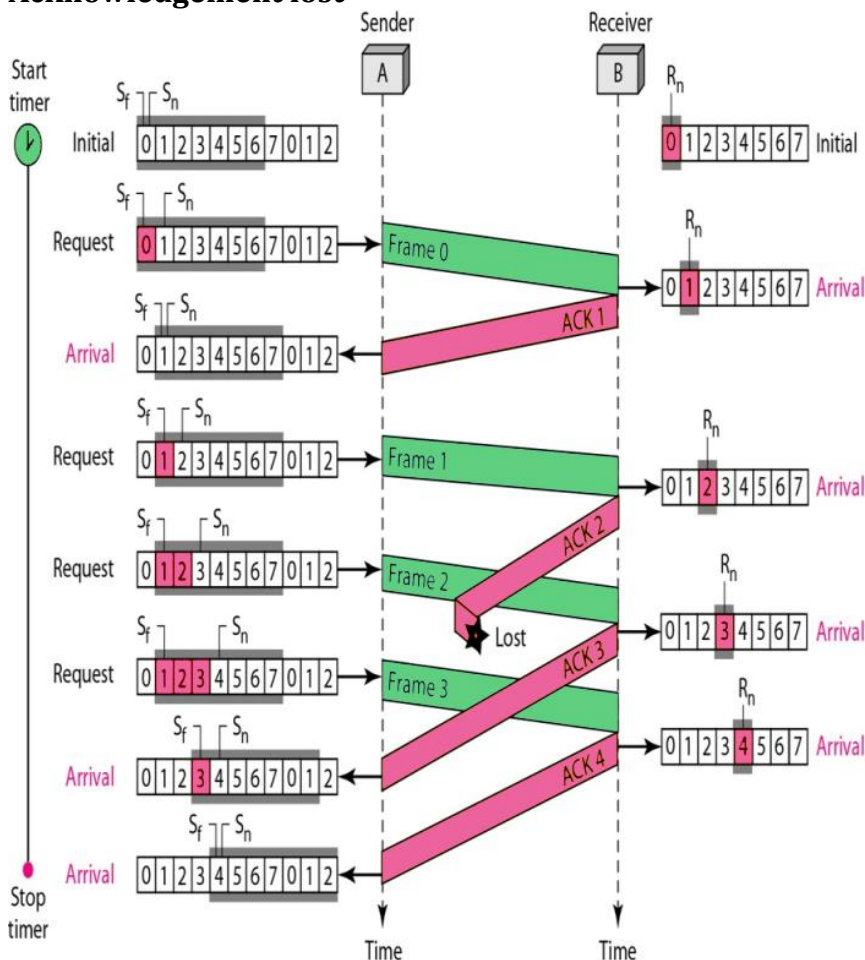
Resending a Frame

When the timer expires, the sender resends all outstanding frames. For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4, 5, and 6 again. That is why the protocol is called *Go-Back-N* ARQ.

Flow diagram Frame lost



Acknowledgement lost



3. Selective Repeat Automatic Repeat Request

Go-Back-N ARQ simplifies the process at the receiver site. The receiver keeps track of only one variable, and there is no need to buffer out-of-order frames; they are simply discarded. However, this protocol is very inefficient for a noisy link. In a noisy link a

frame has a higher probability of damage, which means the resending of multiple frames.

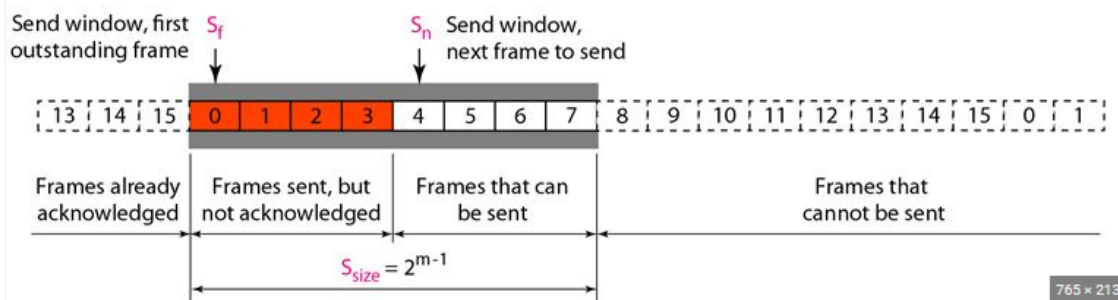
- This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent. This mechanism is called Selective Repeat ARQ.

Windows

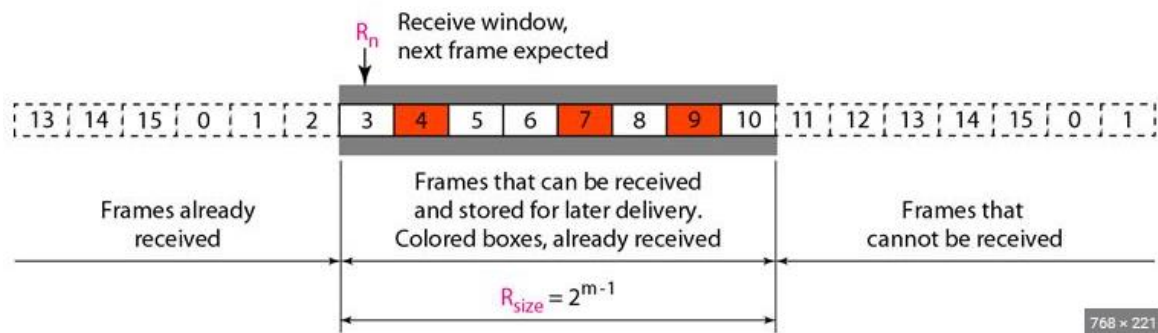
The Selective Repeat Protocol also uses two windows: a send window and a receive window.

The send window maximum size can be 2^{m-1} . For example, if $m = 4$, the sequence numbers go from 0 to 15, but the size of the window is just 8. The receive window is the same size as the send window.

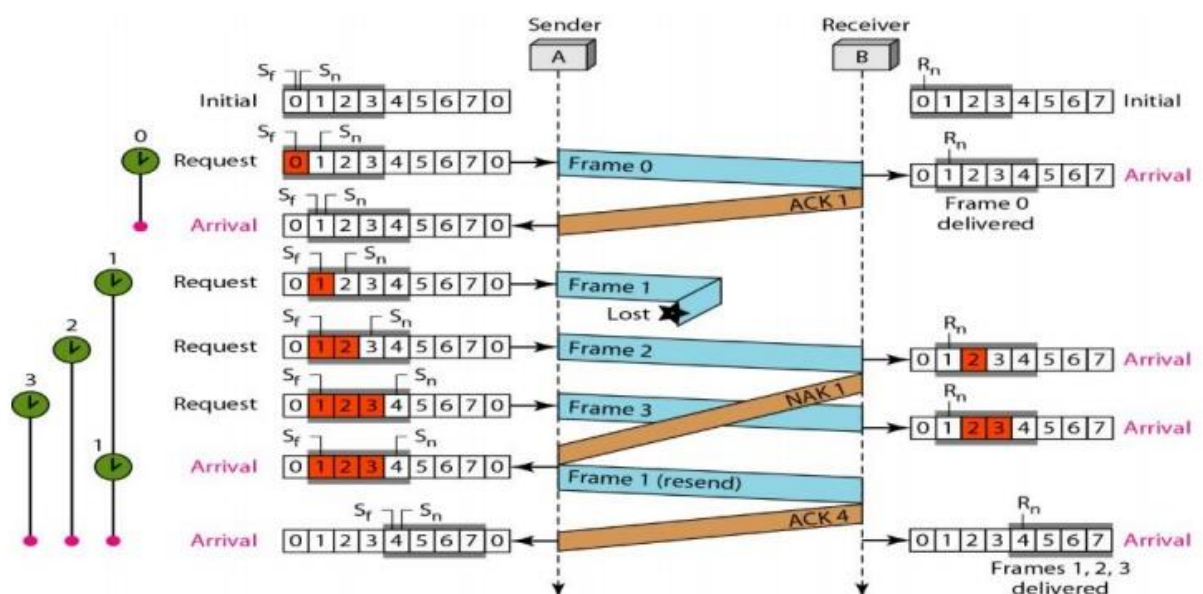
Sent window



Receive window



Flow diagram Frame lost

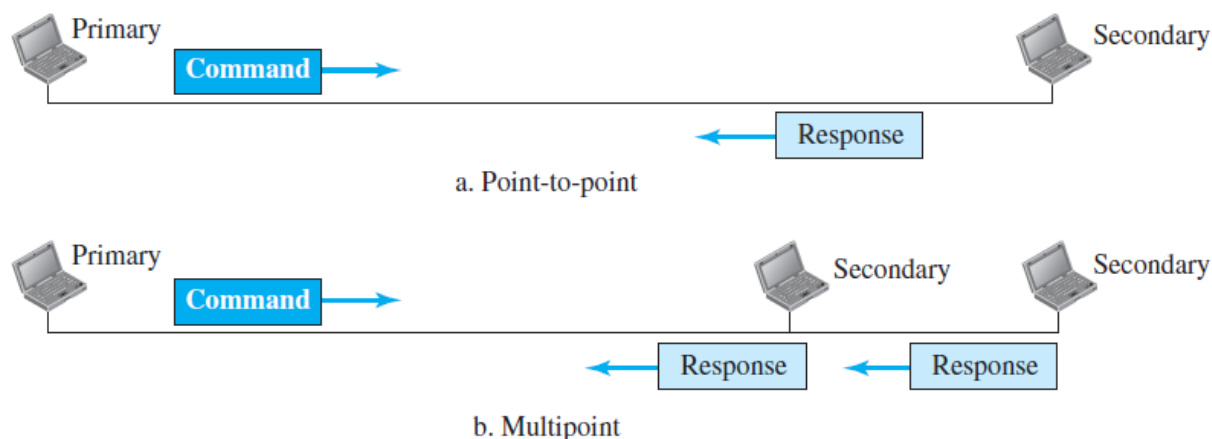


Piggybacking

Protocols have been designed in the past to allow data to flow in both directions. However, to make the communication more efficient, the data in one direction is piggybacked with the acknowledgment in the other direction. In other words, when node A is sending data to node B, Node A also acknowledges the data received from node B.

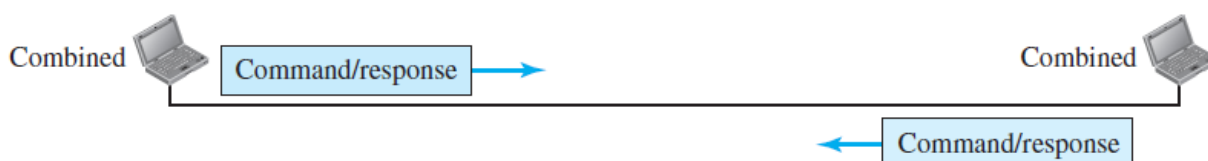
HDLC

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



Normal Response mode

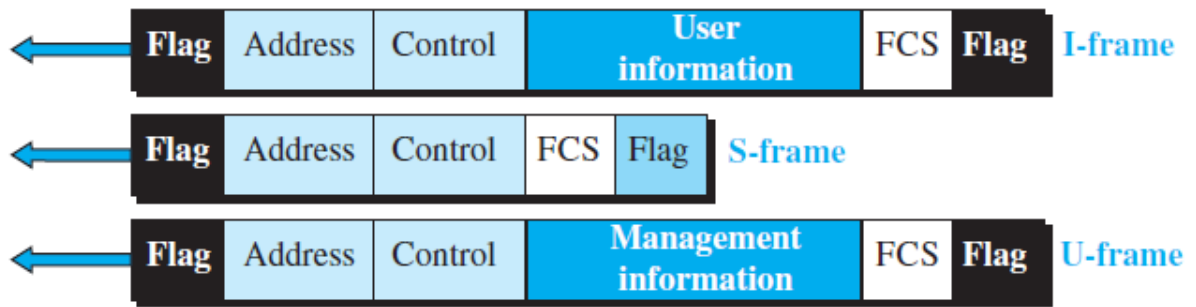
In ABM, the configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary (acting as peers), as shown in Figure.



Asynchronous Balanced mode

Framing

HDLC defines three types of frames: information frames (I-frames), supervisory frames (S-frames), and unnumbered frames (U-frames).



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

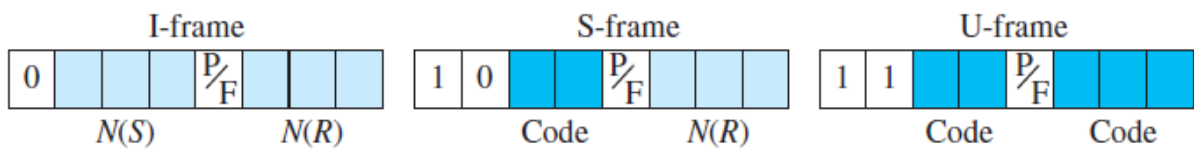
Address field. This field contains the address of the secondary station. If a primary station created the frame, it contains to address. If a secondary station creates the frame, it contains from address.

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.

Control field format for different frame types



Control Field for I-Frames

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. The last 3 bits, called $N(R)$, correspond to the acknowledgment number when piggybacking is used. If $P/F = 1$ it means poll when the frame is sent by a primary station to a secondary. It means final when the frame is sent by a secondary to a primary.

Control Field for S-Frames

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 00- Receive Ready, 01-Reject, 10-Receive not ready, 11-Selective Reject.

Control Field for U-Frames

U-frames contain an information field, but one used for system management information, not user data.

U-frame codes are divided into 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.

POINT-TO-POINT PROTOCOL (PPP)

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

Services Provided by PPP

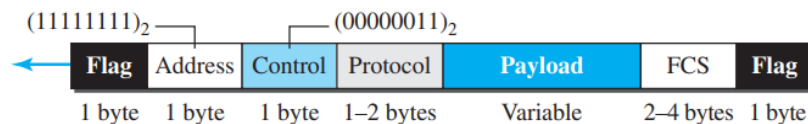
- PPP defines the format of the frame to be exchanged between devices. It also defines how two devices can negotiate the establishment of the link and the exchange of data.
- PPP is designed to accept payloads from several network layers. The new version of PPP, called Multilink PPP, provides connections over multiple links.

Services Not 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.



Flag. A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110.

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

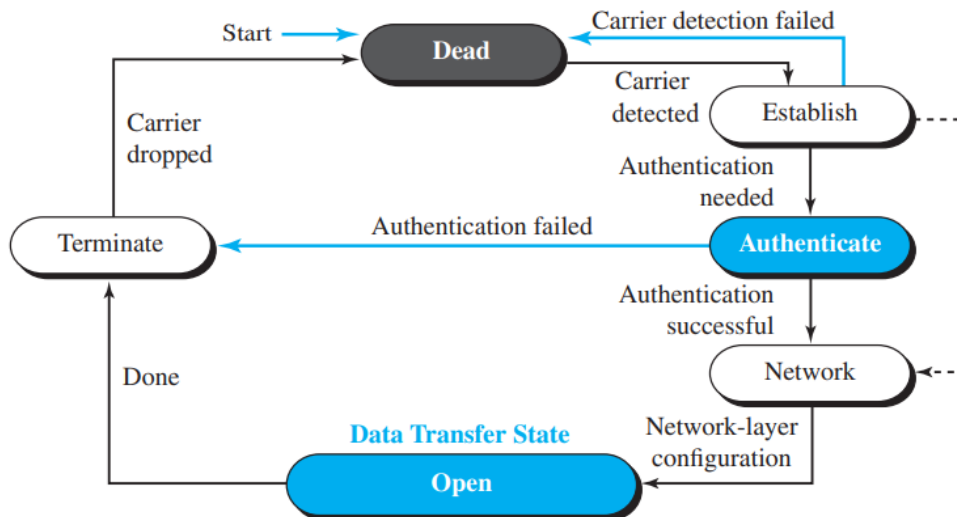
Protocol. The protocol field defines what is being carried in the data field: either user data or other information.

Payload field. This field carries either the user data or other information. The data field is byte-stuffed if the flag byte pattern appears in this field.

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

Byte Stuffing

Since PPP is a byte-oriented protocol, the flag in PPP is a byte that needs to be escaped whenever it appears in the data section of the frame. The escape byte is 01111101,



which means that every time the flaglike pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag.

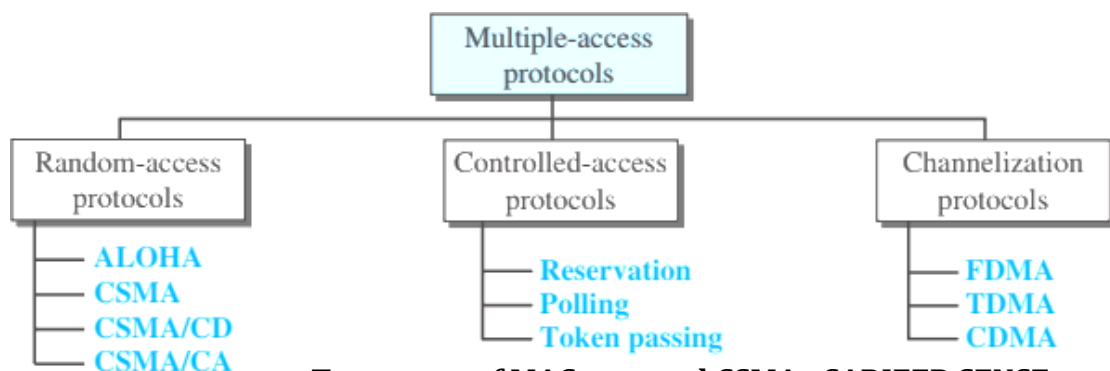
Transition Phases

The transition diagram, which is an FSM, starts with the dead state. In this 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.
- If the two parties agree that they need authentication, then the system needs to do authentication. Otherwise, the parties can simply start communication.
- Data transfer takes place in the open state. When a connection reaches this state, the exchange of data packets can be started.
- The connection remains in this state until one of the endpoints 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

Media Access Control

The taxonomy of medium access protocols is shown in the below figure.

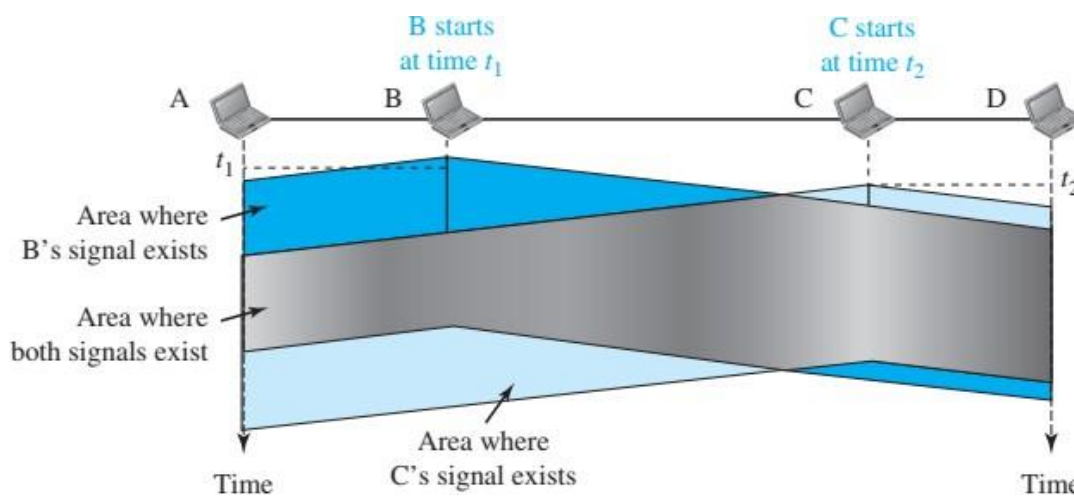


Taxonomy of MAC protocol CSMA : CARRIERS SENSE

MULTIPLE ACCESS

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle “sense before transmit” or “listen before talk.”

CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason for this is shown in Figure below, a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium).



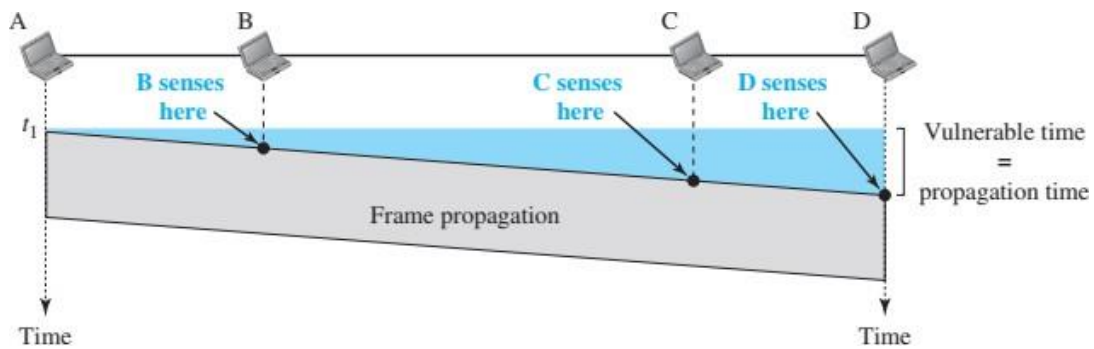
Space/time model of a collision in CSMA

At time t_1 , station B senses the medium and finds it idle, so it sends a frame. At time t_2 ($t_2 > t_1$), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed.

Vulnerable time

- The vulnerable time for CSMA is the propagation time T_p . This is the time needed for a signal to propagate from one end of the medium to the other.
- When a station sends a frame and any other station tries to send a frame during this time, a collision will result.
- But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending. Figure below shows the worst case.

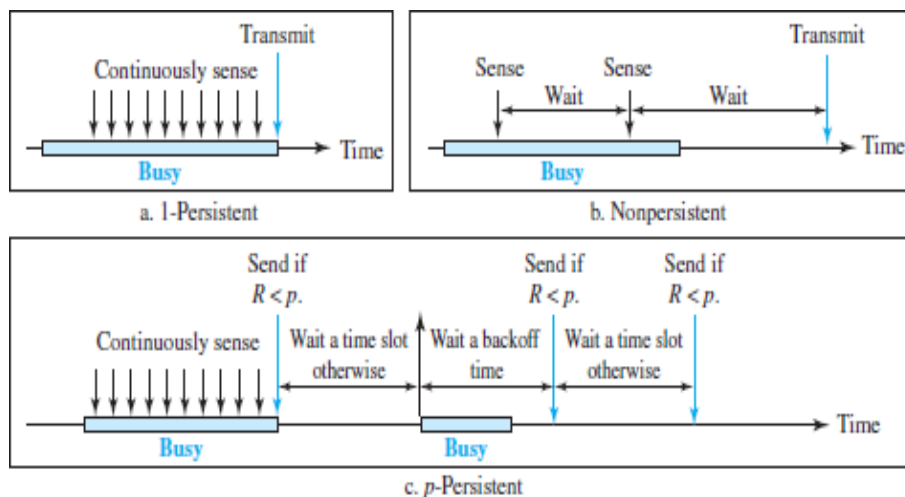
- The leftmost station, A, sends a frame at time t_1 , which reaches the rightmost station, D, at time $t_1 + T_p$. The gray area shows the vulnerable area in time and space.



Vulnerable time in CSMA

Persistence Methods

What should a station do if the channel is busy? What should a station do if the channel is idle? Three methods have been devised to answer these questions: the 1-persistent method, the non-persistent method, and the p-persistent method. Figure below shows the behavior of three persistence methods when a station finds a channel busy.



Persistence methods

1-Persistent

The 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately. We will see later that Ethernet uses this method.

Nonpersistent

In the nonpersistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount

of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

p-Persistent

The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the

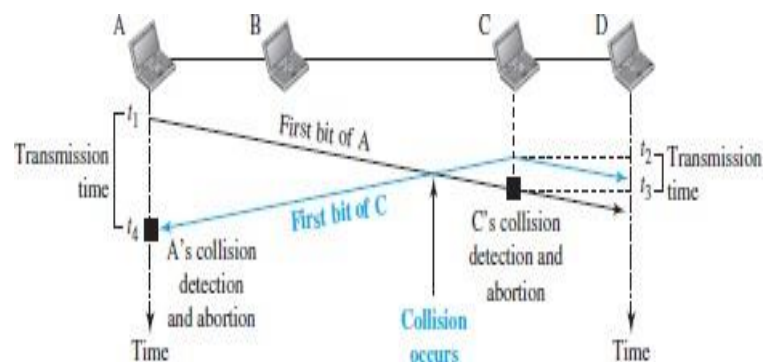
advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability p , the station sends its frame.
2. With probability $q = 1-p$, the station waits for the beginning of the next time slot and checks the line again.
 - a. If the line is idle, it goes to step 1.
 - b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.

CSMA/CD

Explain the concept behind CSMA/CD and name the standard that uses it (2)
April/may 2019

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision. In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.



Collision of the first bits in CSMA/CD

At time t_1 , station A has executed its persistence procedure and starts sending the bits of its frame. At time t_2 , station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs some time 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 (or after a short time, but we assume immediately) aborts

transmission. Station A detects collision at time t_4 when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration $t_4 - t_1$; C transmits for the duration $t_3 - t_2$.

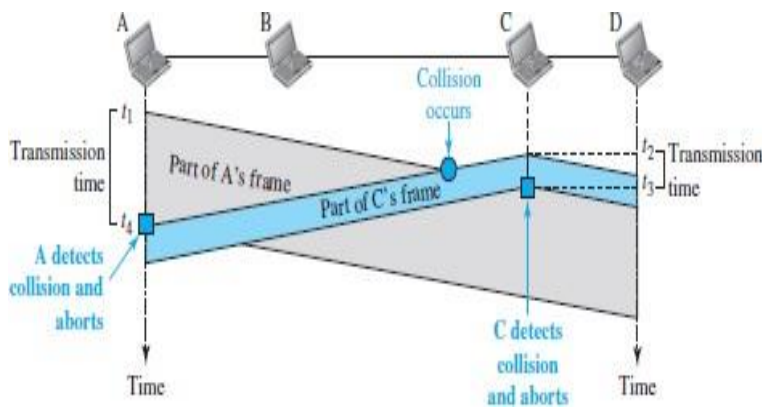
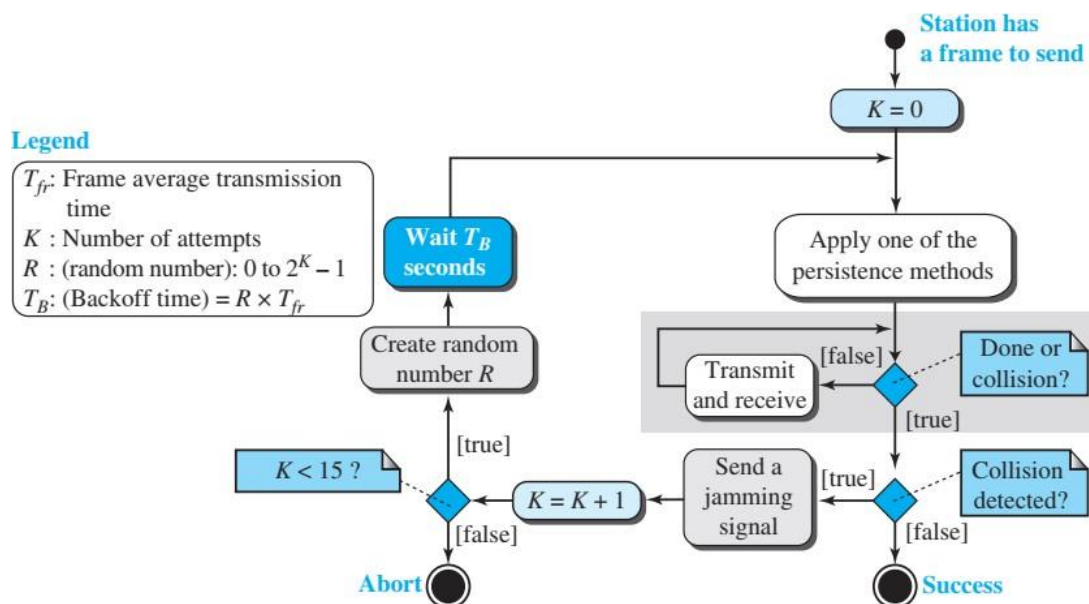


Fig.2.12 Collision and abortion in CSMA/CD

Flow Diagram of CSMA/CD



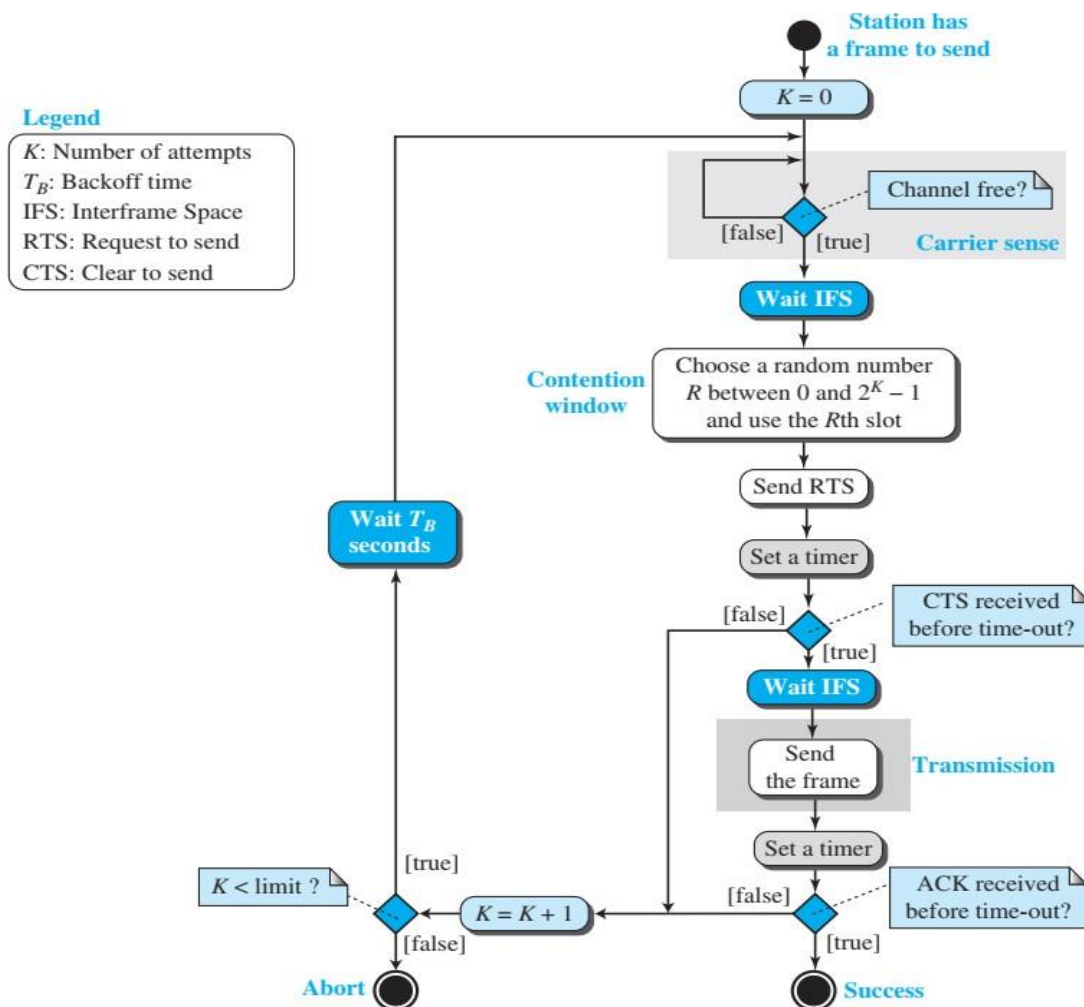
Flow diagram of CSMA/CD

The first difference is the addition of the persistence process. We need to sense the channel before we start sending the frame by using one of the persistence processes (nonpersistent, 1-persistent, or p-persistent). The corresponding box can be replaced by one of the persistence processes. channel before we start sending the frame by using one of the persistence processes we discussed previously (nonpersistent, 1-persistent, or p-persistent). The corresponding box can be replaced by one of the persistence processes.

CSMA/CA

Briefly discuss some of the collision avoidance strategies in CSMA/CA. What is the purpose of NAV in CSMA/CA? (7) Nov/Dec 2020

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks. Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments.

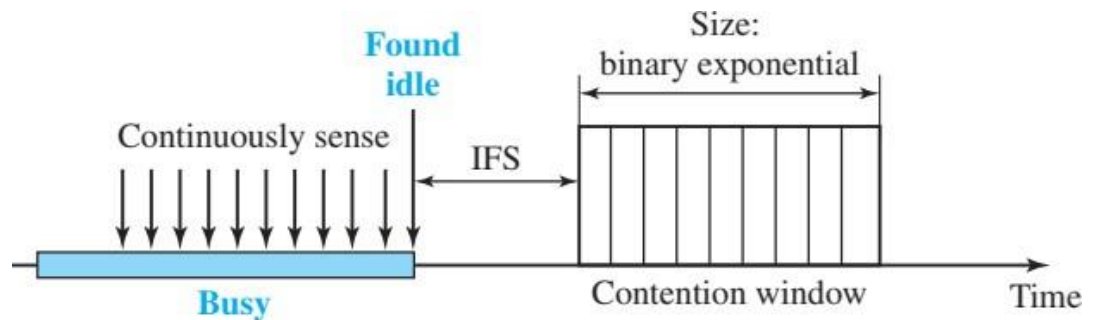


Flow diagram of CSMA/CA

- **Interframe Space (IFS):** When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS. After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window. The 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.
- **Contention Window:** The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential backoff strategy. This means that it is set to one slot the first time and then doubles each time

the station cannot detect an idle channel after the IFS time. This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.

- **Acknowledgment:** In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.



Contention window Frame Exchange Time Line

Figure below shows the exchange of data and control frames in time. 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 backoff until the channel is idle. After the station is found to be idle, the station waits for a period of time called the DCF interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

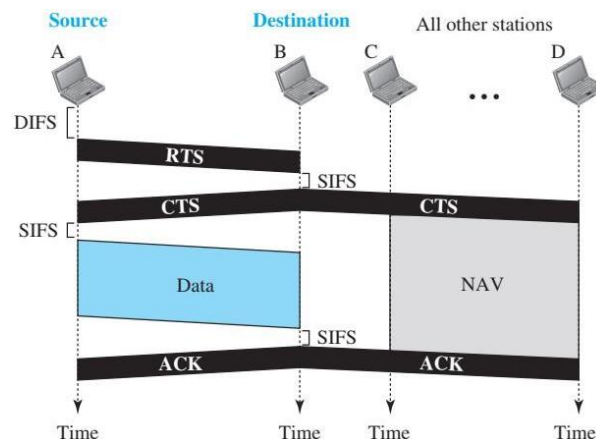


Fig.CSMA/CA and NAV

- After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates 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.

Network Allocation Vector

The other stations defer sending their data if one station acquires access by using a key feature called NAV. When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that 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.

Collision during Handshaking

What happens if there is a collision during the time when RTS or CTS control frames are in transition, often called the handshaking period? 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.

Hidden-Station Problem

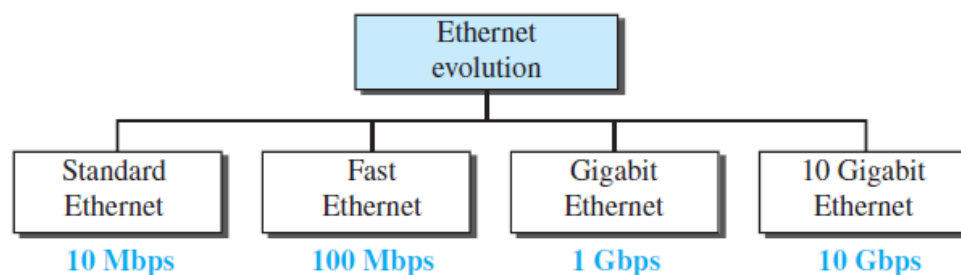
The solution to the hidden station problem is the use of the handshake frames (RTS and CTS). Figure 2.16 also shows that the RTS message from A reaches B, but not C. However, because both A and C are within the range of B, the CTS message, which contains the duration of data transmission from A to B, reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

Wired LAN Ethernet IEEE 802.3

Draw and explain the frame structure of IEEE 802.3 (8)

Elucidate the principles of Ethernet 802.3 protocol (13) Nov/Dec 2021

The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs. Since then, it has gone through four generations: **Standard Ethernet** (10 Mbps), **Fast Ethernet** (100 Mbps), **Gigabit Ethernet** (1 Gbps), and **10 Gigabit Ethernet** (10 Gbps)

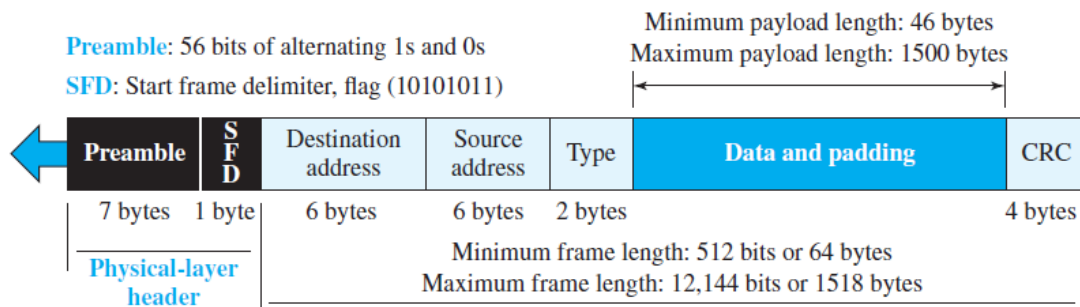


STANDARD ETHERNET

The data rate of 10 Mbps acts as the Standard Ethernet. Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next 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 it. The sender may overwhelm the receiver with frames, which may result in dropping frames. If a frame drops, the sender will not know about it. Since IP, which is using the service of Ethernet, is also connectionless, it will not know about it either.

Frame Format

The Ethernet frame contains seven fields



- ❑ **Preamble.** This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization.
- ❑ **Start frame delimiter (SFD).** This field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits are (11)₂ and alert the receiver that the next field is the destination address.
- ❑ **Destination address (DA).** This field is six bytes (48 bits) and contains the link layer address of the destination station or stations to receive the packet.
- ❑ **Source address (SA).** This field is also six bytes and contains the link-layer address of the sender of the packet.
- ❑ **Type.** This field defines the upper-layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF, and so on.
- ❑ **Data.** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes. If the data coming from the upper layer is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame. If it is less than 46 bytes, it needs to be padded with extra 0s.
- ❑ **CRC.** The last field contains error detection information, in this case a CRC-32. The CRC is calculated over the addresses, types, and data field. If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame.

Minimum frame length: 64 bytes

Maximum frame length: 1518 bytes

Minimum data length: 46 bytes

Maximum data length: 1500 bytes

Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a link-layer address. The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes. For example, the following shows an Ethernet MAC address:

4A:30:10:21:10:1A

The transmission in the standard Ethernet is always broadcast, no matter if the intention is unicast, multicast, or broadcast. In the bus topology, when station A sends a frame to station B, all stations will receive it. In the star topology, when station A sends a frame to station B, the hub will receive it. Since the hub is a passive element, it does not check the destination address of the frame; it regenerates the bits (if they have been weakened) and sends them to all stations except station A. In fact, it floods the network with the frame. The question is, then, how the actual unicast, multicast, and broadcast transmissions are distinguished from each other. The answer is in 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.

(Note: Access Method Explain CSMA CD here.)

FAST ETHERNET (100 MBPS)

The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.

Autonegotiation

A new feature added to Fast Ethernet is called autonegotiation. It allows a station or a hub a range of capabilities. Autonegotiation allows two devices to negotiate the mode or data rate of operation. It was designed particularly to allow incompatible devices to connect to one another. For example, a device with a maximum data rate of 10 Mbps can communicate with a device with a 100 Mbps data rate (but which can work at a lower rate). We can summarize the goal of autonegotiation as follows. It was designed particularly for these purposes:

- 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 (but which can work at a lower rate).
- To allow one device to have multiple capabilities.
- To allow a station to check a hub's capabilities.

GIGABIT ETHERNET

The goals of the Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.

4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Support autonegotiation as defined in Fast Ethernet.

10 GIGABIT ETHERNET

The IEEE committee created 10 Gigabit Ethernet and called it Standard 802.3ae. The goals of the 10 Gigabit Ethernet design can be summarized as upgrading the data rate to 10 Gbps, keeping the same frame size and format, and allowing the interconnection of LANs, MANs, and WAN possible.

Wireless LAN: (WiFi) IEEE802.11

1. Compare the medium of a wired LAN with that of a wireless LAN in today's communication environment. Explain why the MAC protocol is more important in wireless LANs than in wired LANs? (7) Nov/Dec 2020
2. Explain how hidden and exposed station problems are addressed in wireless LANs? (6) Nov/Dec 2020
3. What is exposed station problem. (2) Nov/Dec 2019

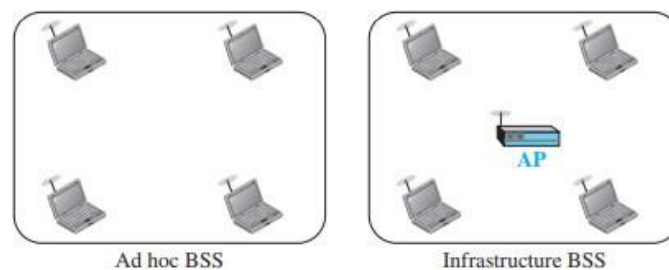
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers. It is sometimes called wireless Ethernet. The term WiFi (short for wireless fidelity) is used as a synonym for wireless LAN. WiFi, however, is a wireless LAN that is certified by the WiFi Alliance, a global, nonprofit industry association of more than 300 member companies devoted to promoting the growth of wireless LANs.

Architecture

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building blocks of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure shows two sets in this standard.



Basic Service Set

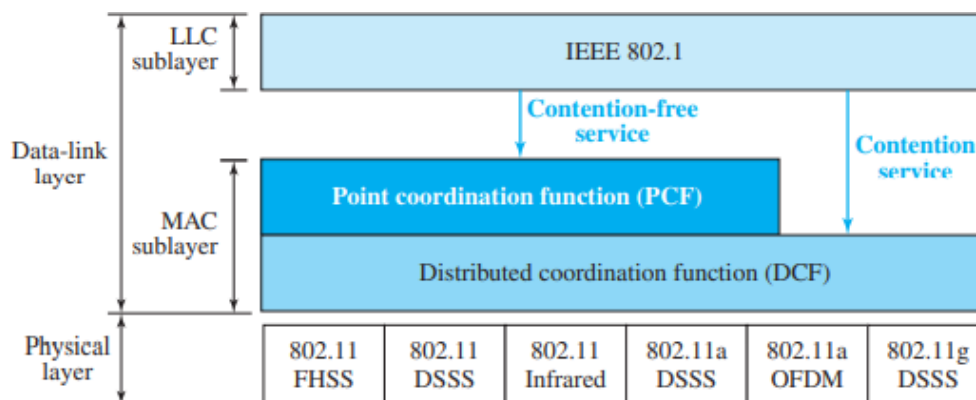
The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure BSS.

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is a wired or a wireless network. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.

MAC Sublayer

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF). Figure shows the relationship between the two MAC sublayers, the LLC sublayer, and the physical layer.



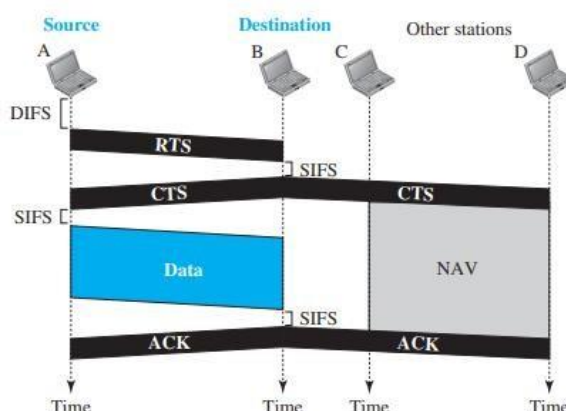
MAC sublayer Distributed Coordination

Function

One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF). DCF uses CSMA/CA as the access method.

Frame Exchange Time Line

Figure shows the exchange of data and control frames in time.



Frame exchange timeline

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 backoff until the channel is idle.

After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station.

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.

Network Allocation Vector

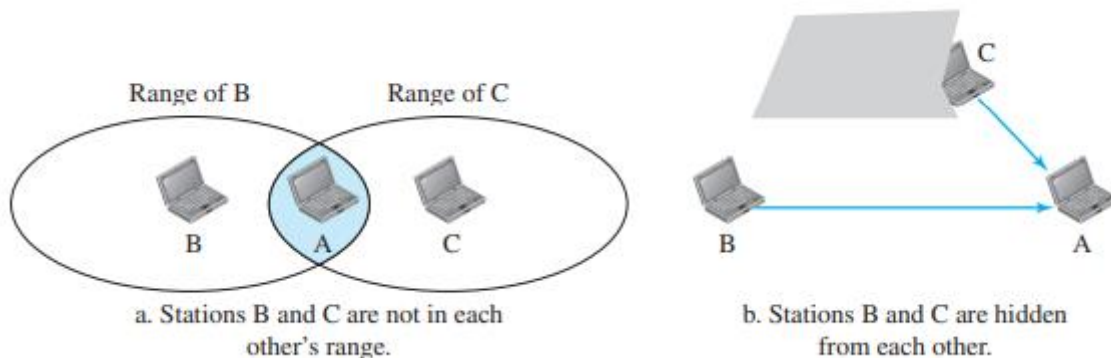
When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

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 backoff strategy is employed, and the sender tries again.

Hidden-Station Problem

The solution to the hidden station problem is the use of the handshake frames (RTS and CTS). In the below figure RTS message from B reaches A, but not C. However, because both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A, reaches Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.



Point Coordination Function (PCF)

The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network. It is implemented on top of the DCF and is used mostly for time-sensitive transmission. PCF has a centralized, contention-free polling access method.

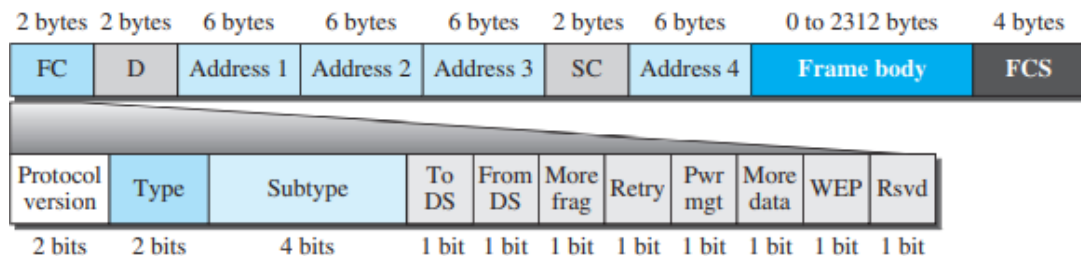
Fragmentation

The wireless environment is very noisy, so frames are often corrupted. 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 send a small frame than a large one.

Frame Format

The MAC layer frame consists of nine fields, as shown in Figure



MAC layer frame format

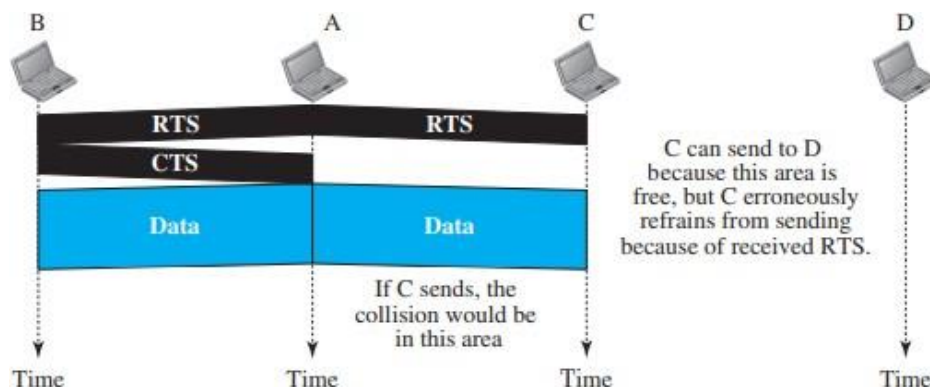
Frame Types A wireless LAN defined by IEEE 802.11 has three categories of frames: **management frames, control frames, and data frames.**

- Management Frames Management frames are used for the initial communication between stations and access points.
- Control Frames Control frames are used for accessing the channel and acknowledging frames
- Data Frames Data frames are used for carrying data and control information.

Exposed Station Problem

In this problem a station refrains from using a channel when it is available. In the below Figure, 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; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.

The handshaking messages RTS and CTS cannot help in this case. Station C hears the RTS from A and refrains from sending, even though the communication between C and D cannot cause a collision in the zone between A and C; station C cannot know that station A's transmission does not affect the zone between C and D.



BLUETOOTH:

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when they are at a short distance from each other. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability.

Architecture:

Bluetooth defines two types of networks: piconet and scatternet.

Piconets

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. A piconet can have only one primary station. The communication between the primary and secondary stations can be one-to-one or one-to-many.

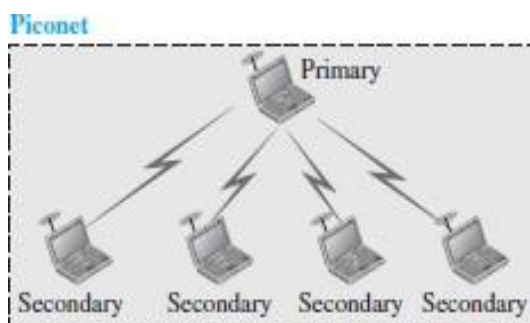


Fig.2.18 Piconets

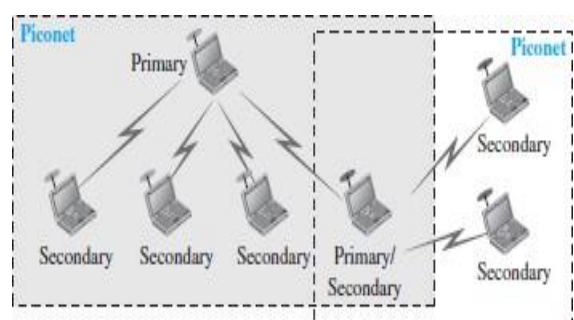


Fig.2.19 Scatternet Scatternet

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. Bluetooth uses several layers that do not exactly match those of the Internet model.

Bluetooth Layers

1. L2CAP

The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs.

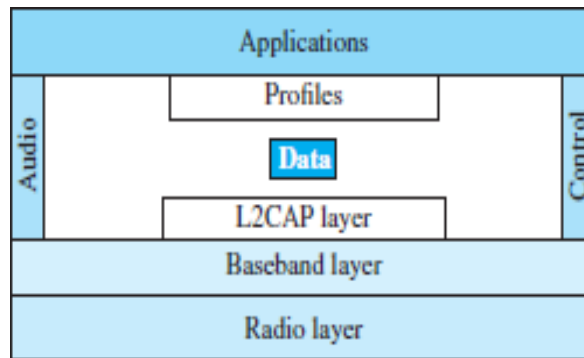


Fig.2.20 Bluetooth Layers

L2CAP data packet format



Fig.2.21 L2CAP data packet format

The 16-bit length field defines the size of the data, in bytes, coming from the upper layers. Data can be up to 65,535 bytes. The channel ID (CID) defines a unique identifier for the virtual channel. The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

Multiplexing

The L2CAP can do multiplexing. At the sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers them to the baseband layer. At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol layer.

Segmentation and Reassembly

The maximum size of the payload field in the baseband layer 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.

QoS

Bluetooth allows the stations to define a quality-of-service level.

Group Management

Another functionality of L2CAP is to allow devices to create a type of logical addressing between themselves. This is similar to multicasting.

2. Baseband Layer

The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA. The primary and secondary stations communicate with each other using time slots. The length of a time slot is exactly the same as the μ s. This means that during the time that one frequency is used, a primary sends a frame to a secondary, or a secondary sends a frame to the primary.

TDMA

Bluetooth uses a form of TDMA that is called TDD-TDMA (time-division duplex TDMA). TDD-TDMA is a kind of half-duplex communication in which the sender and receiver send and receive data, but not at the same time (half-duplex); 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. The time is divided into slots of 625μ s. 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.

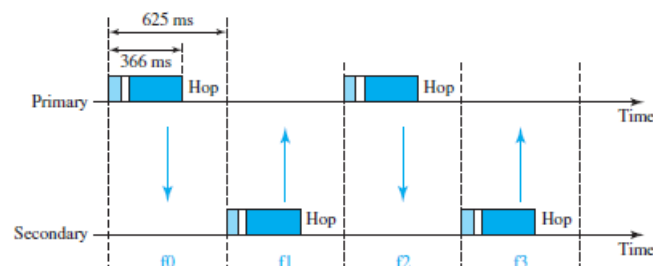


Fig. 2.22 Single-Secondary Communication Multiple-

Secondary Communication

The process is a little more involved if there is more than one secondary in the piconet. Again, the primary uses the even-numbered slots, but a secondary sends in the next odd-numbered slot if the packet in the previous slot was addressed to it. All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot.

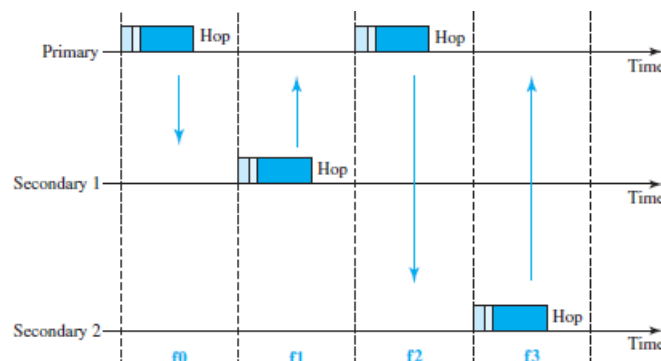


Fig. 2.22 Multiple-Secondary Communication

Links

Two types of links can be created between a primary and a secondary: SCO links and ACL links.

SCO A synchronous connection-oriented (SCO) link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery). In an SCO link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals.

ACL An asynchronous connectionless link (ACL) is used when data integrity is more important than avoiding latency.

Frame Format

A frame in the baseband layer can be one of three types: one-slot, three-slot, or five slot.

A slot, as we said before, is 625 μ s. However, in a one-slot frame exchange, 259 is needed for hopping and control mechanisms. This means that a one-slot frame can last only 625 - 259, or 366 μ s. With a 1-MHz bandwidth and 1 bit/Hz, the size of a one slot frame is 366 bits.

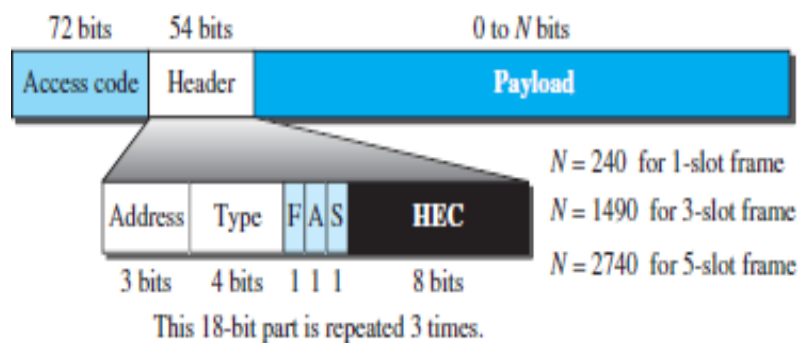


Fig. 2.23 Frame format

Address. The 3-bit address subfield can define up to seven secondaries (1 to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.

Type. The 4-bit type subfield defines the type of data coming from the upper layers.

F. This 1-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (buffer is full).

A. This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.

S. This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.

f. HEC. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.

3. 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 10m. Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

State in brief the Frequency Hopping Spread Spectrum (FHSS) technique. (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

Modulation

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK.