UNIT-I
INTRODUCTION TO NETWORKS & DATA COMMUNICATIONS

Syllabus Contents: The Internet, Protocols & Standards, Layered Tasks, OSI Model, TCP / IP, Addressing, Line Coding Review, Transmission Media: Guided and unguided Media Review.

Important Terminology and concepts related to Networks & Data Communications

Data communication: Data communication is the exchange of data between two devices via some wired or wireless transmission medium. A dialogue between two people is an example of communication. Other examples are phone calls, emails, etc. The main purpose of data communication is to share information.

Components of a data communications system:

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

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

(iii) Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

(iv) 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

(v) Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but cannot communicate with each other.

Data Representation:

It is the means of representing the data. Information today comes in different forms such as text, numbers, images, audio, and video.

Data Flow

It represents how the communication between two devices takes place. The communication can be simplex, half-duplex, or full-duplex as shown in Figure

(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 a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. Entire channel may be used in simplex mode.

(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.

Example: Walkie-talkie. A push-to-talk button is used to select the way of transmission.

(c) Full-Duplex:
In a full-duplex system, sender and receiver can communicate with each other simultaneously. An example of a full-duplex device is a telephone.

Network:
A network is a set of devices connected by communication links. These devices are called nodes. A node can be a computer, server, modem, switch, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Distributed Processing:
Most networks use distributed processing, in which a task is divided among multiple computers. i.e., more than one computer is used to perform a task. Thus, multiple CPUs work on same task. Ex: Cellular communications networks, aircraft control systems

Network Criteria:

A network must be able to meet some of criteria. The most important of these are performance, reliability, and security. The other criteria are number of users, transmission speed and type of physical connection used to connect nodes

Performance:

- Performance can be measured in terms of 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.
- Performance of a network depends on factors like number of users, the type of transmission medium, and hardware and the software capabilities.
- Performance is often evaluated by two networking metrics: throughput and delay. Throughput is the output per unit time. Increase throughput will also increase the delay because of traffic congestion in the network.

Reliability:
Reliability means degree of faithfulness. 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.

Security:
Security means protection of data from unauthorized access and damage. Security issues involve the implementing policies and procedures for recovery from breaches and data losses.

Types of Connections (Configurations):

There are two possible types of connections: point-to-point and multipoint.

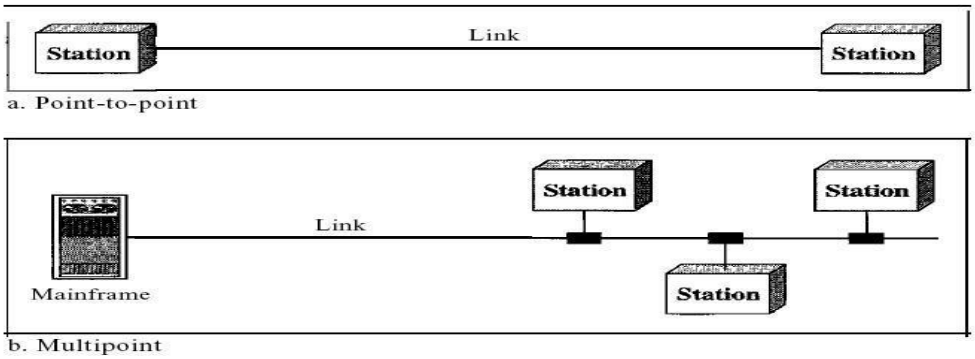
(i) Point-to-Point communication:

- There is a dedicated link between two devices.
- Channel's entire capacity is reserved for the two connected devices.
- One transmitter and one receiver.
- The smallest distance to reach the receiver is most important because the message has to travel through many intermediate devices.
- Provides security and privacy because communication channel is not shared.
- Examples: T-carrier, X.25, etc.

(ii) Multipoint (or multidrop) communication:

- More than two devices share a single link
- The channel's capacity is shared temporarily among the devices connected to the link.
- There is one transmitter and many receivers.

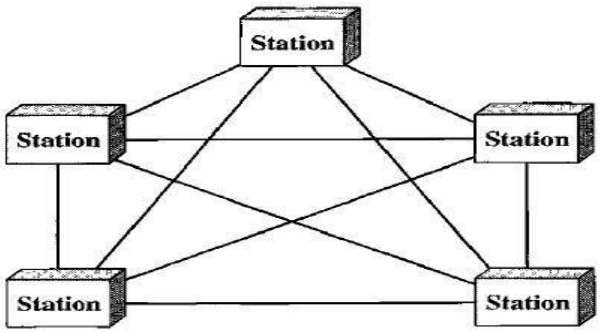
- The smallest distance is not important to reach the receiver.
- It does not provide security and privacy because communication channel is shared.
- Examples: Token ring, Ethernet, ATM, etc.
- It is also called P2MP, PTMP or PMP communication
- Examples: Token ring, Ethernet, ATM, etc



Physical Topology (or Network Topology):

The term physical topology refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. There are four basic topologies possible: mesh, star, bus, and ring.

(a) Mesh Topology (Point-to-point): In a mesh topology, every node is connected to every other node using a dedicated point-to-point link. The term dedicated means that the link carries traffic only between the two devices it connects. If there are n nodes, each node is connected to n - 1 other nodes. Thus, we need n (n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we need n (n -1) /2 duplex-mode links.



Advantages:

1. It is robust (strong and powerful).
2. This eliminates the traffic problems.
3. Offers good security.

Disadvantages:

1. More number of connections are needed. So, installation is complex and costly.
2. Maintenance is also difficult.

Applications: Mesh topologies are used where the reliability of network communication is very important. A few applications include:

- Military organizations to avoid breakdown in communications
- Wireless mesh networks are used
  - In emergency services, such as police and fire services,
  - Monitoring traffic flow, sewage treatment and to help control street lighting

(b) Star Topology (Point-to-Point):

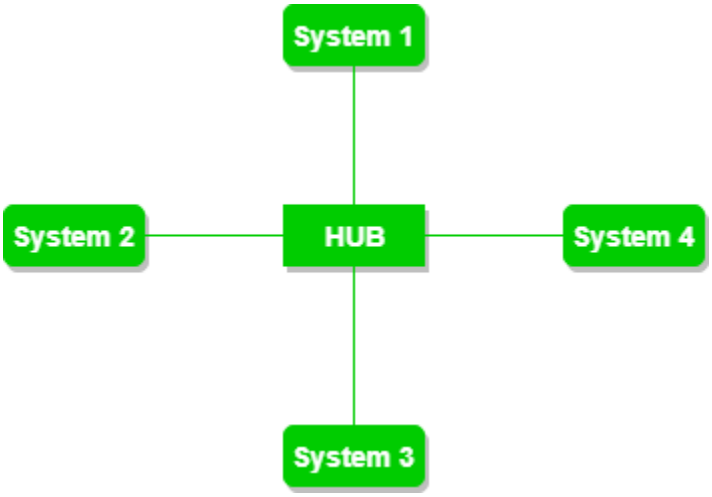
In a star topology, each device has a dedicated point-to-point link only to a central controller, which is usually called a hub. The devices are not directly linked to one another. So, star topology does not allow direct traffic between devices. If one device wants to send data to another, it sends the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

Advantages:

- It is robust. New links can be easily added.
- Less expensive than a mesh topology.
- It is easier to install and reconfigure.
- Cabling is less and simple.
- If one link fails, only that link is affected. All other links remain active.

Disadvantages:

- Extra hardware is required (hubs or switches) which adds to cost
- Whole topology depends on one single point, the hub. If the hub goes down, the whole system is collapsed.



(c) Bus Topology (Multipoint):

One long cable is used as a backbone to link all the devices in the network Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that joins the drop line with main cable.

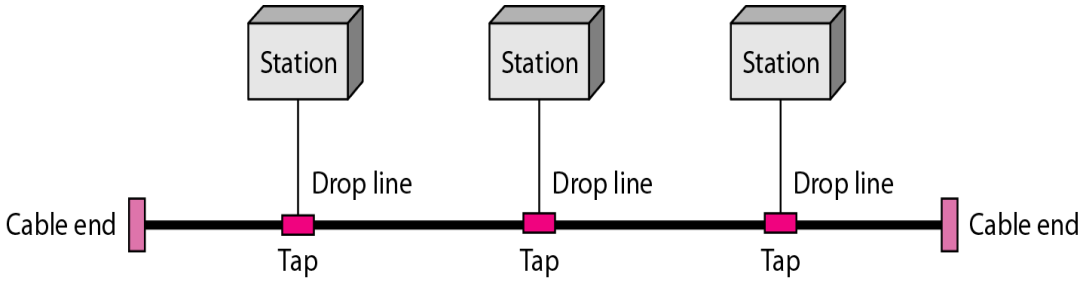
As a signal travels along the cable, some of its energy is transformed into heat. Therefore, signal becomes weaker after sometime. Thus, there is a limit on the number of taps and on the distance between those taps.

Advantages:

- Ease of installation. Length of cable required is less than a star topology.
- It is easy to add or remove devices in this network without affecting any other device.
- Failure of one node does not affect the rest of the network.
- Does not require hubs or switches. Supports multiple nodes.

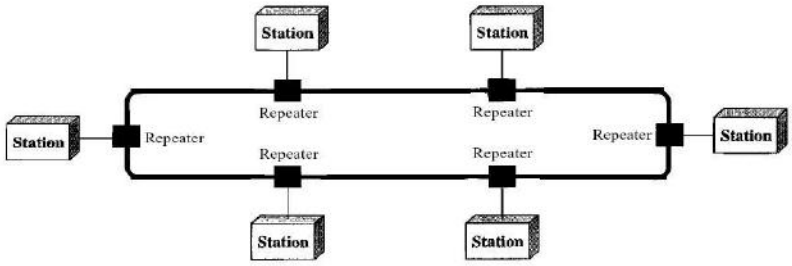
Disadvantages:

- High maintenance cost in the long run
- A break in the backbone can cause an entire network to collapse
- Security options are limited.



(d) Ring Topology (Multipoint):

The devices in the network are arranged in the form of a ring. 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 the ring.



Advantages:

- Relatively easy to install and reconfigure.
- Each device is linked to only its immediate neighbors. Thus, to add/delete a device, we need to change only two connections.
- In addition, a fault can be easily isolated. Generally, in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

- A data packet (token) must have to pass through all the nodes.
- A break in the ring (such as a disabled station) can disable the entire network.
- It is slower in performance as compared to the bus topology.

CATEGORIES (TYPES) OF NETWORKS:

A network can be mainly classified as Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs)

1. Local Area Network (LAN):

A LAN is a group of computers and network devices connected together, usually within a limited area or premises. The main components used in a MAN are server, computers, switches, hubs, routers, access points and printers. High speed inexpensive technology is used for LANs. (e.g., token ring or Ethernet).

Examples for LANs: Networking in home, office, school, laboratory, university campus. Home Wi-Fi networks are wireless LANs

2. Metropolitan Area Networks (MANs):

A MAN is a collection of local-area networks (LANs) or other networks that communicate with one another. Thus, it is a network of networks, It usually covers in the same city or metropolitan area. The main components used in a MAN are Computers, routers, printers, modems and Wire/Cable.

Examples for MANs: cable TV network in a city, high-speed Digital subscriber line (DSL). In general, a MAN is either owned by a user group or by a network service provider

3. Wide Area Network (WAN):

A WAN is a large group of computers and network devices connected together and extends over a state or country. A WAN connects several LANs, and may be limited to an organization or accessible to the public. The high speed and relatively expensive technology is used for WANs.

Example for WAN: Internet is the world's largest WAN.

WANs frequently face security issues like hacking and virus attacks. Firewall and Antivirus software are installed in PCs to prevent the security issues.

4. Campus area network (CAN): They are larger than LANs, but smaller than MANs. These types of networks are typically seen in universities. They can be spread across several buildings that are fairly close to each other.

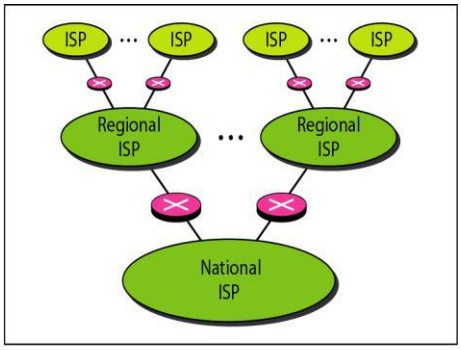
5. Personal area network (PAN): It is a computer network for interconnecting electronic devices within a person's workspace. A PAN may be wired or wireless It connects several devices such as cell phone headsets, wireless keyboards, wireless mice, printers, bar code scanners and game consoles.

Comparison of LAN, MAN and WAN

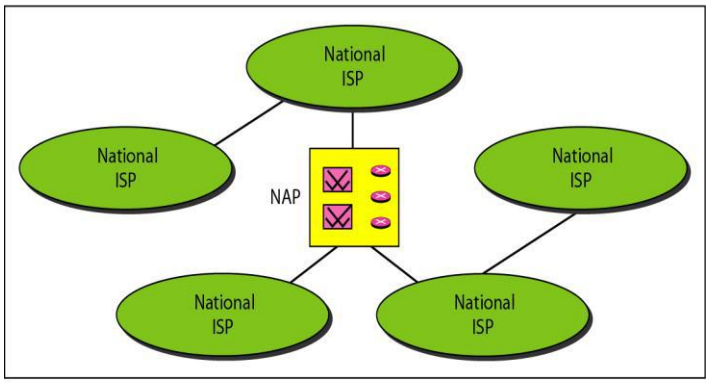
	LAN	MAN	WAN
Coverage	Used for small premises like school, college or hospital	Covers small towns, or a City. Ex: Cable TV network in a city	Country/Continent Ex: Internet
Design and maintenance	Easy	Difficult	Difficult
Speed	High	Moderate	Low
Ownership of Network	Private	Private or Public	Private or Public

THE INTERNET

Today, Internet is being used in in numerous applications in area like defence, business, education, entertainment, industries, research, etc. The Internet has come a long WANs and LANs joined by connecting devices and switching stations. Internet is continuously changing with respect to new addresses, data and technology.
The users can get Internet connection and get services from the Internet service providers (lSPs).
Internet Service Providers (ISPs): These ISPs are classified as international service providers, national service providers, regional service providers, and local service providers. The hierarchy of various types of ISPs at national and international levels are shown in the figures.



a. Structure of a national ISP



b. Interconnection of national ISPs

International ISPs:
At the top of the hierarchy are the international ISPs. They are multinational companies. They connect national ISPs together.
Example: AT &T, Reliance Jio, China Mobile.
National ISPs:
The National ISPs are backbone networks. They operate at national level. They are created and maintained by special organizations. There are many national ISPs operating in India.
Examples; Jio, Airtel, BSNL, Vi
To provide connectivity between the end users, these networks are connected by complex switching stations (normally run by a third party) called “Network access points (NAPs)”. Some national ISP networks are also connected to one another by private switching stations called “peering points”.

Regional ISPs:
They cover multiple locations in a specific region. Regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.
Example: BBNL in Bangalore.
Local ISPs:
Local ISPs provide internet services to a city or a district. They provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Sometimes, they may be cable TV or other service providing companies.

PROTOCOLS AND STANDARDS

Protocols:
A protocol is defined as a set of rules that govern data communications. It determines what is communicated, how it is communicated and when it is communicated. Syntax, semantics and timing are the important elements of a protocol.

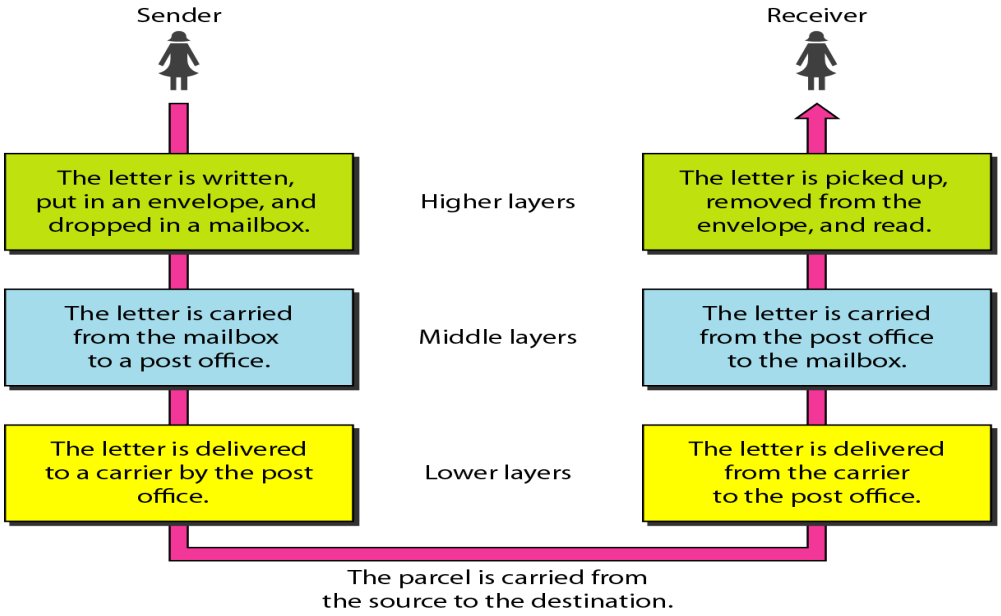
- Syntax
  - Structure or format of the data
  - Field delineation: It tells how to read the bits
- Semantics
  - Interprets the meaning of the bits
  - Knows which fields define what action
- Timing
  - When data should be sent and what data.
  - Speed at which data is sent or received.

Standards:

Different equipment manufacturers produce different equipment. They have to follow some standards in maintaining market. Standards ensure interoperability of data, technology and processes. They provide guidelines to manufacturers, vendors, government agencies, and other service providers while using the equipment and technology in international communications.
Data communication standards are mainly classified as “de facto” standards and “de jure” standards.
De facto standards: De facto means "by fact" or "by convention". These standards have not approved by an organized body. They are established by manufacturers and have been adopted through widespread use.
De jure standards: de jure means meaning "by law" or "by regulation". These standards are legislated by an officially recognized body. (Example: IEEE standards)

LAYERED TASKS

We use the concept of layers in our daily life. As an illustrative example, consider the process of sending a letter through post office. Below Figure shows the steps in this task.



In Figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

Layers at the Sender Site

Higher layer: The sender writes the letter, puts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

Middle layer: The letter is picked up by a letter carrier and delivered to the post office.

Lower layer: The letter is sorted at the post office; a carrier transports the letter.

The letter reaches the recipient's local post office through a central post office by means of a truck, a train, an airplane, boat, or a combination of these.

Layers at the Receiver Site

Lower layer: The carrier transports the letter to the post office.

Middle layer: The letter is sorted and delivered to the recipient's mailbox.

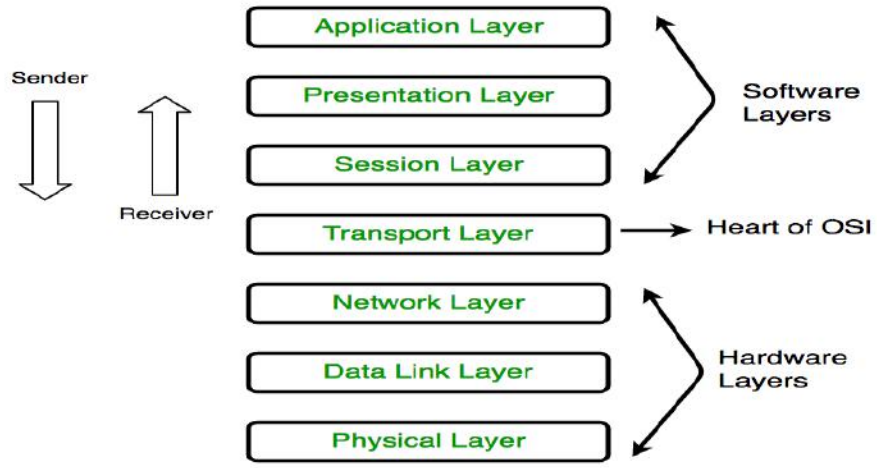
Higher layer: The receiver picks up the letter, opens the envelope, and reads it.

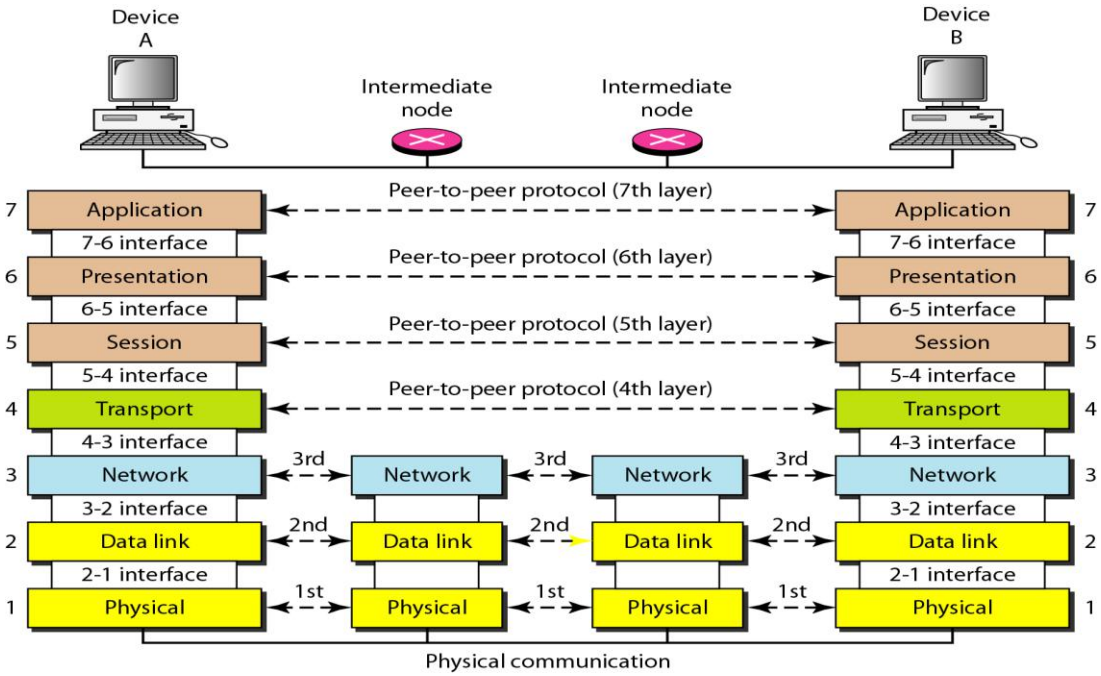
Layered network models: There are two important layered network models: one is OSI Model and other is TCP/IP Model

OPEN SYSTEMS INTERCONNECTION (OSI) MODEL

OSI model was developed by "International Organization for Standardization (ISO)", in the year 1984. It is a conceptual model. It specifies the communication functions of a telecommunication or computing system. It is not concerned with the underlying internal structure and technology. Its goal is the interoperability of various communication systems with standard communication protocols.

The model has 7 abstraction (theoretical) layers (levels). Each layer has specified functionality. Each intermediate layer serves its above layer and is served by its next lower layer.





Note: In OSI model, PDU (Protocol Data Unit) means a unit (block) of information transferred over a network. PDU of datalink layer is called "frame". PDU of network layer is called "packet". PDU of transport layer is called "segment".

1. Physical Layer (Layer 1):

- Physical layer is the lowest layer of the OSI reference model. It is a hardware layer. Data in this layer consists of stream of bits (0s and 1s).
- It is not concerned with the meaning of the bits.

- It is responsible for the physical connection between devices and synchronization between transmitter and receiver.
- Hubs, Ethernet, cabling, repeaters, modems, etc., are the devices used in this layer.

- It defines the transmission medium, type of configuration, network topology and the direction of transmission (Simplex, Half Duplex, or Full Duplex) between two devices

2. Data link Layer (Layer 2): Hop-to-hop data transfer

The data link layer provides node-to-node data transfer.

- Its responsibilities:
  - Framing: Dividing the stream of bits received from the network layer into data units called frames.
  - Physical addressing: Adding a header to the frame with sender's and receiver's addresses.
  - Access control: Providing access to appropriate device.
  - Error control: Detecting and correcting data frames that are corrupted or lost during transmission.
  - Flow control: Allowing two stations working at different speeds to communicate with each other.

- It consists of two sub layers: Medium access control (MAC) layer and Logical link control (LLC) layer.
  - MAC sublayer handles physical addressing.
  - LLC sublayer provides the logic for the data link. It also controls error checking and frame synchronization functions of the data link layer.

3. Network Layer (Layer 3): Host-to-host data transfer

- ✓ Network layer is responsible for connections between different networks, using the addresses in the frame.
- ✓ It divides the message segments from transport layers into packets and assembles incoming packets into message segments.
- ✓ It also takes care of packet routing i.e., selection of the shortest path to transmit the packets.
- ✓ It places the sender's & receiver's IP addresses in the header.
- ✓ It controls the operation of the subnets (part or portion of a larger network such as internet)

4. Transport Layer (Layer 4): End-to-End data transfer

- It is responsible for the reliable transfer of data between end users.
- It divides messages into small segments. Each segment contains a sequence number.
- It manages the delivery and error checking of data packets.
- It also provides reliable services to the upper layers, through flow control, segmentation and error control.
- It may also provide the acknowledgement of the successful data transmission.

5. Session Layer: (Layer 5):

- The session layer controls the session (dialog or conversation) among different computers.

- It provides the mechanism for opening, closing (terminating) and managing a session between the local and remote applications.
- It allows the systems to communicate in half-duplex or full-duplex mode.
- It establishes procedures for check pointing.
- It also includes authentication, and reconnection in case of a network interruption.

6. Presentation Layer (Layer 6)

It extracts data from the application layer, converts (translates) it in to suitable format and transmits it over the network. Thus, it is also called "syntax layer" or "translation layer.
The main functions of the presentation layer are:

- ✓ Translation: Translation converts data sent by an application layer into an acceptable and compatible data format. It is based on the application network protocol and architecture.
- ✓ Encryption/Decryption: Data encryption translates the data into another form or code. Decryption transforms encrypted information into its original form. The purpose of encryption and decryption is to ensure privacy.
- ✓ Compression: Reduces the number of bits in the information.

7. Application Layer (Layer 7)

Application layer is the topmost layer in OSI model. This layer is closest to the end user.
It provides user services needed by an application program to communicate with another application program on a network. Examples:

- It identifies communication partners, resource availability, and synchronizes communication.
- It allows a user to connect to a remote server and perform file Transfer, access, and management (FTAM).
- It is responsible for the browser services, email services and directory services.

Merits of OSI model:

- ✓ It is a generic model and acts as a guidance tool to develop any network model.
- ✓ OSI model distinguishes well between the services, interfaces and protocols.
- ✓ Protocols of OSI model are very well hidden. They can be replaced by new protocols easily, when technology changes.
- ✓ Supports connection-oriented as well as connectionless service.

Demerits of OSI model:

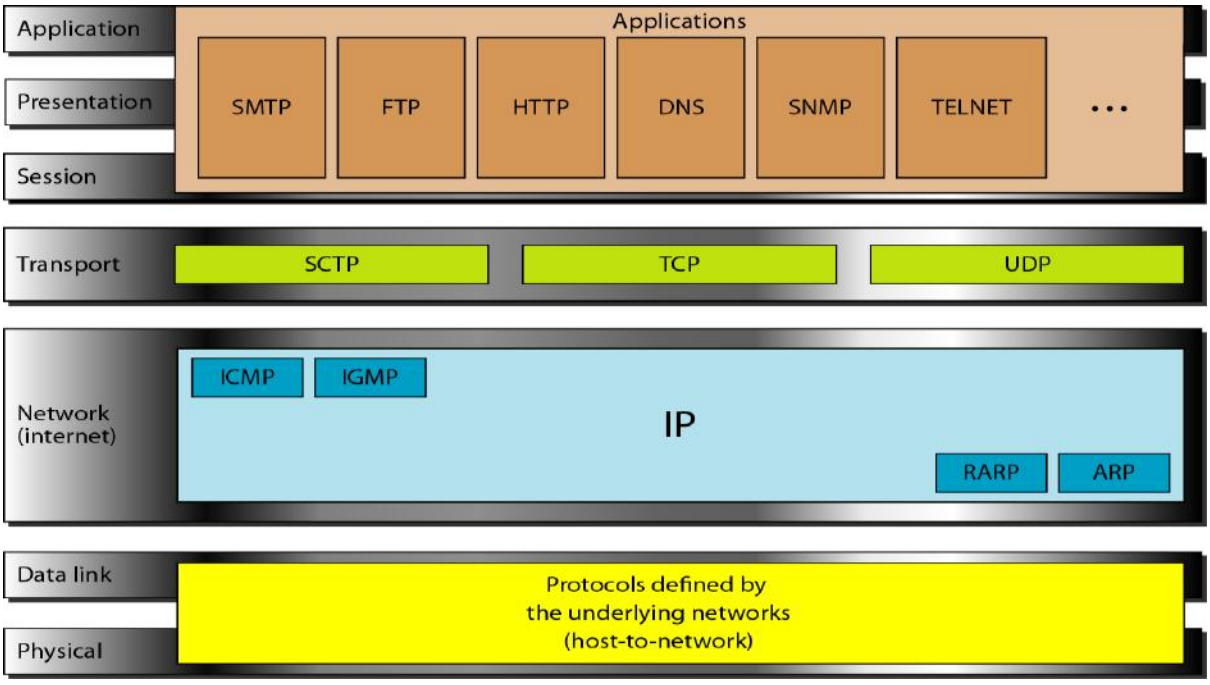
- TCP/IP protocol suite was developed and was in use prior to the OSI model. It is just used as a reference model.
- It is difficult to define the various layers in the model.
- It is difficult to fit a new protocol in this model.
- There is some duplication of services at various layers.
- There is also interdependence among the layers.

TCP/IP Suite (TCP/IP Model)

TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP protocol suite means a set of communications protocols used in the Internet and similar computer networks. TCP/IP suite mainly consists of TCP protocol and IP protocol.
IP Protocol obtains the address to which data is sent. Then, TCP is responsible for data delivery. It specifies how data should be packetized, addressed, transmitted, routed and received on a TCP/IP network.
The TCP/IP protocol suite was developed prior to the OSI model. The original TCP/IP protocol suite was defined with four layers: host-to-network, internet, transport, and application layers. When TCP/IP is compared to OSI,

- Host-to-network layer in TCP/IP model is equivalent to the combination of the physical and data link layers in OSI model. It is also called "network interface layer". or "link layer".
- Internet layer of TCP/IP is equivalent to the network layer of OSI
- Transport layer of TCP/IP is equivalent to the transport layer of OSI
- Application layer of TCP/IP is equivalent to combination of session, presentation, and application layers of OSI

Thus TCP/IP protocol suite can be treated as it is made of five layers: physical, data link, network, transport, and application layers.



Not all layers are completely defined by the model, so these layers are "filled in" by external standards and protocols.
Protocols at various layers are described below.

Physical and Data Link Layers:

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a LAN or a WAN.

Network Layer (Internet layer):

At this layer, TCP/IP supports the Internetworking Protocol (IP). IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP

- **IP Protocol:** IP is the transmission mechanism used by the TCP/IP. It is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. protocols. It doesn't provide error checking or tracking. It is an unreliable and **connectionless protocol**. i.e., it does not guarantee the delivery of message.
- **Address Resolution Protocol**
  ARP is used to find the physical address of the node when its Internet address is known.
- **Reverse Address Resolution Protocol**
  It used to find Internet address of the node when physical address is known.
- **Internet Control Message Protocol (ICMP)**
  ICMP It is used by hosts and gateways to send notification of datagram problems to the sender. It sends query and error reporting messages.
- **Internet Group Message Protocol**
  IGMP is used in sending a message to a group of recipients.

Transport Layer:

Transport layer represents two protocols: TCP and UDP. They are responsible for delivery of a message from a process (running program) to another process.

- **User Datagram Protocol (UDP)**
  UDP is a simpler transport protocol. It adds only port addresses, checksum error control, and length information to the data from the upper layer. It is a connection-less protocol.
- **Transmission Control Protocol (TCP)**
  TCP provides full transport-layer services to applications. TCP is a reliable stream transport protocol. Here, stream means connection-oriented. i.e., it makes a connection and checks whether message is received or not. If errors occurs, it again sends the message after correcting the errors. So, it is highly reliable. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments.
- **Stream Control Transmission Protocol (SCTP)**
  SCTP is a transport layer protocol that combines the best features of UDP and TCP. It provides support for newer applications such as voice over the Internet.

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.

Merits of TCP/IP model

1. It operates independently.
2. It supports a number of routing protocols.
3. It is scalable (can be expanded or upgraded)
4. It supports Client/server architecture.

Demerits of TCP/IP

1. The model cannot be used in any other application.
2. Replacing protocol is not easy.
3. It has not clearly separated its services, interfaces and protocols.

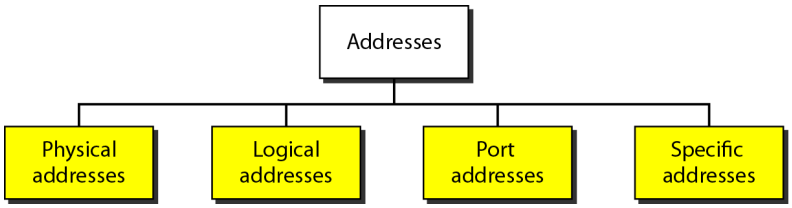
Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP/IP is more reliable OSI model	OSI is less reliable
TCP/IP does not have very strict boundaries. For example, it combines both session and presentation layer in the application layer.	OSI has strict boundaries. For example, OSI uses different session and presentation layers.

ADDRESSING

Reference site:
https://www.youtube.com/watch?v=yDTC6sbYFFE

Four levels of addresses are used in an internet employing the TCP/IP model: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses.



Relationship of layers and addresses in TCP/IP:

TCP/IP Layer	Addresses associated
Host-to-network layer	Physical addresses
Internet layer	Logical addresses
Transport layer	Port addresses
Application layer	Specific addresses

Physical Addresses (or MAC addresses or Link addresses):
Physical address is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). It appears as 12 hexadecimal digits. Every pair of hexadecimal digits is separated by a colon, as shown below:

07:01:02:01:2C:4B
A 6-byte (12 hexadecimal digits) physical address.

Logical Addresses:
Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet.

Logical Address	Physical Address
The logical address is a virtual address since it does not exist physically.. It is generated by CPU, while running program.	Physical address is a location that exists in the memory. It is computed by the hardware component called Memory Management Unit (MMU).
Its length is 32 bits	Its length is 48 bits
It can be viewed by the user.	User can't view the physical address directly. In order to locate a device in an IP network, the logical IP address is used to find physical address by address resolution protocol (ARP).
One device can have only one physical address. It is constant, so tit cannot be changed.	One device can have a variety of logical addresses.

Port Addresses:
Computers can run multiple applications (processes) at the same time. The end objective of Internet is a process-to-process communication between hosts. For example, computer A can communicate with a remote computer C by using TELNET protocol. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to run simultaneously, each process is assigned a logical address called port address or 'port number'. A port address in TCP/IP is 16 bits in length as shown below.

753

A 16-bit port address represented as one single number.

Example: Port number of FTP is 21. Port number of TELNET protocol is 23.

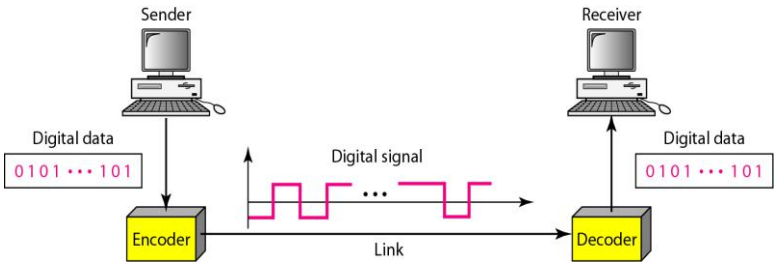
Specific Addresses:
Some applications have user-friendly addresses that are designed for specific purpose. They are called specific addresses. There are two types of specific addresses: Universal Resource Locator (URL) and Email address
Example for URL: www.mhhe.com
Example email address: rao_123@gmail.com
URL is used to find a document on the World Wide Web. Email address defines the recipient of an e-mail. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.
Summary on addresses: *Through logical address the system identifies a network. after identifying the network physical address is used to identify the host on that network. The port address is used to identify the particular application running on the destination host. Specific address is a user-friendly address such as URL and Email address.*

Line Coding Review

Line coding is **the process of converting digital data to digital signals**. It converts a sequence of bits to a digital signal. It is also called "digital baseband modulation" or "digital baseband transmission". Line coding process is carried out by a transmitter.

The data may be in the form of text, numbers, graphical images, audio, or video-stored in computer memory as sequences of bits. Line coding converts this sequence of bits to a digital signal.

At the sending end, digital data are encoded into a digital signal. At the receiver, the digital data is recovered (reconstructed) from the digital signal.



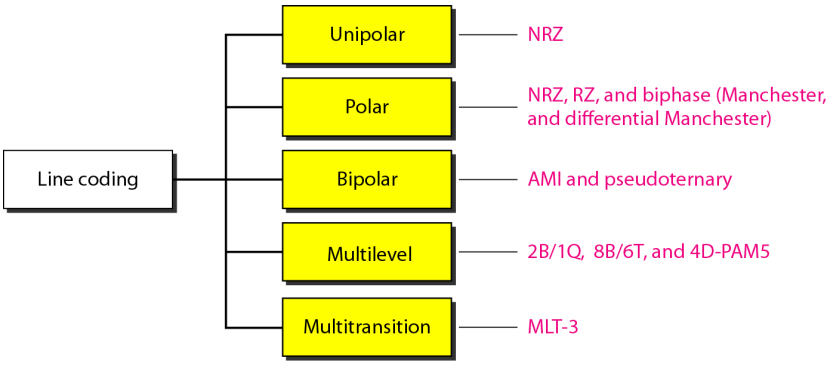
Data rate: Data rate defines the number of bits sent per sec (bps). It is also called "bit rate".

Signal rate: Signal rate is the number of signal elements sent in a second or number of symbol changes per second and is measured in bauds. It is also known as "baud rate" or "modulation rate". In other words. baud rate is the number of pulses sent per second. It is the unit used to measure the speed of signaling. Our aim is to increase the data rate while reducing the baud rate.

Bit rate = Baud rate x the number of bits per baud (per pulse)

Line coding schemes:

There are five types of line coding schemes available.



1. Unipolar Coding:

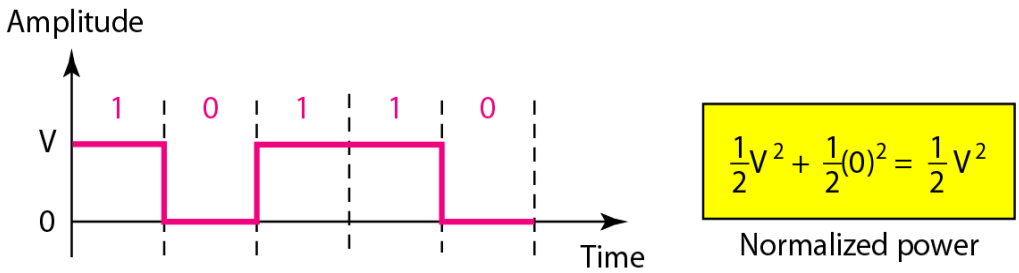
It is the simplest line code and it requires less bandwidth for transmission. It is analogous to on-off keying in modulation. Its drawbacks are that it is not self-clocking (needs a separate clock signal for decoding) and it has a significant DC component. So, it is not normally used in data communications today.

All signal levels are present on one side of the time axis - either above or below.

A positive voltage represents a binary 1, and zero volts indicates a binary 0.

Non-Return-to-Zero (NRZ) scheme is an example of this code, where the signal level does not return to zero during a symbol transmission (at the middle of the bit). NRZ is commonly used with serial ports.

Example: 10110



2. Polar Coding: NRZ

The voltages are on both sides of the time axis.

Polar NRZ scheme can be implemented with two voltages- positive and negative.

Example: +V for 0 and -V for 1

There are two versions of Polar NRZ scheme:

NRZ - Level (NRZ-L): Positive voltage for one symbol and negative for the other

NRZ - Inversion (NRZ-I): ‘Change in polarity’ means 1 and ‘no change in polarity’ means 0. In other words, a “1” symbol inverts the polarity and a “0” does not.

Example: 01001110. Here 0 is representing +ve level and 1 is representing -ve level.

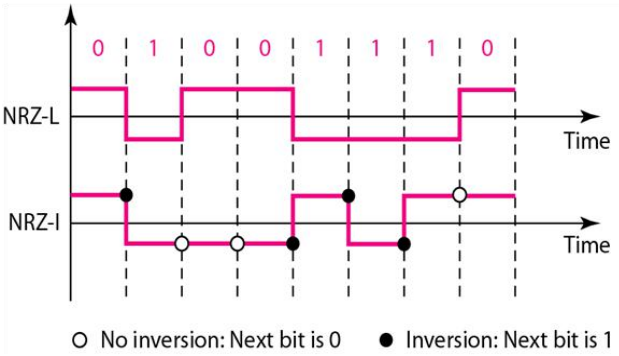


Figure: Polar NRZ type coding

Polarity Coding: Return to Zero (RZ):

Return-to-zero (RZ or RTZ) describes a line code used in telecommunications signals in which the signal drops (returns) to zero between each pulse. This takes place even if a number of consecutive 0s or 1s occur in the signal. The signal is self-clocking.

The Return to Zero (RZ) scheme uses three voltage values. +, 0, -.

Each symbol has a transition in the middle-either from high to zero or from low to zero

Example: 01001

.

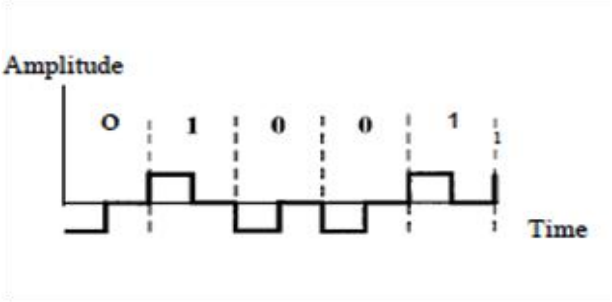


Figure: Polar RZ type coding

Manchester and Differential Manchester codings:

Manchester coding:

Manchester coding consists of combining the NRZ-L and RZ schemes.

Every symbol has a level transition in the middle: from high to low or low to high. Uses only two voltage levels.

Differential Manchester coding:

Differential Manchester coding consists of combining the NRZ-I and RZ schemes. Every symbol has a level transition in the middle. But the level at the beginning of the symbol is determined by the symbol value. One symbol causes a level change the other does not.

Example: 010011

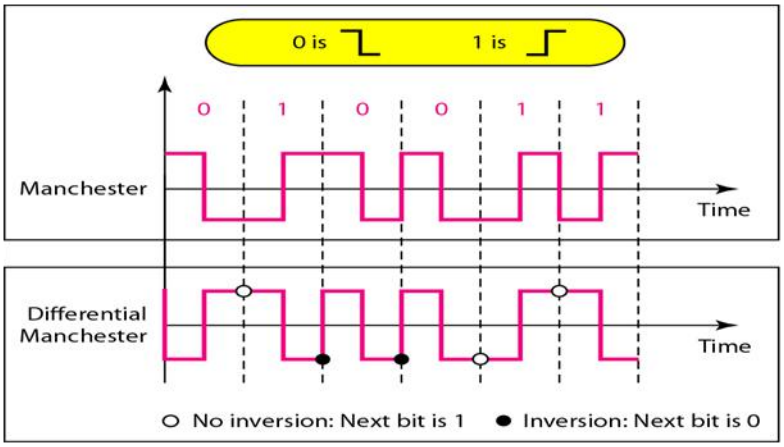


Figure: Manchester and differential Manchester Coding

3. Bipolar Schemes:

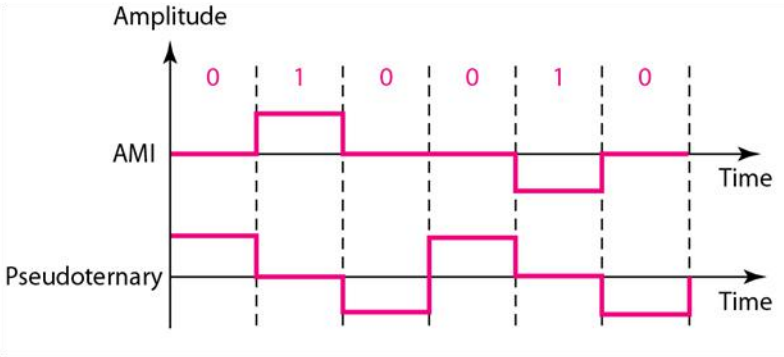
Code uses 3 voltage levels: +, 0, -, to represent the symbols (note no transitions to zero).

Voltage level for one symbol is at "0" and the other alternates between + & -.

Bipolar Alternate Mark Inversion (AMI) - the "0" symbol is represented by zero voltage and the "1" symbol alternates between +V and -V.

Pseudoternary is the reverse of AMI. "1" symbol is represented by zero voltage and the "0" symbol alternates between +V and -V.

Example: 010010



Bipolar Scheme

4. Multilevel Schemes:

In these schemes we increase the number of data bits per symbol thereby increasing the bit rate.

Since we are dealing with binary data we only have 2 types of data element a 1 or a 0.

(i) Multilevel:2B1Q (2-Binary-1-Quaternary)

Data patterns of size "2" bits are encoded as "1" signal element belonging to a "4" level signal

The following transition table is used to draw/interpret the signal wave form

Data is sent two times faster than with NRZ-

	Previous level: positive	Previous level: negative
Next bits	Next level	Next level
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3

Transition table

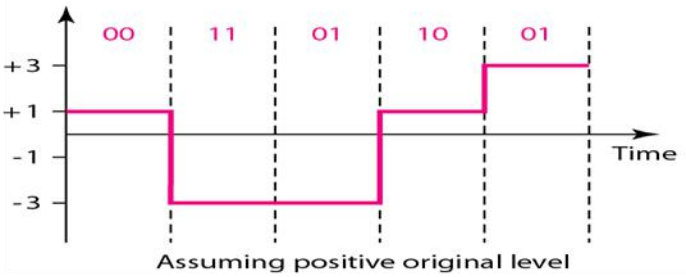


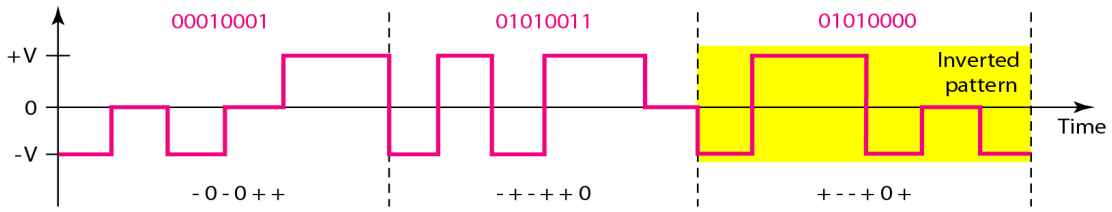
Figure: Multilevel: 2B1Q scheme

(ii) Multilevel: 8B6T scheme

8 Binary 6 Ternary

Encodes 8 bits as a pattern of 6 signal elements, where the signal has three levels (ternary).

Each signal pattern has a weight of 0 or +1 DC values



Note: Some example patters are given below: (from hexadecimal 00 to 26)

Table D.1 *8B/6T code*

Data	*Code*	*Data*	*Code*	*Data*	*Code*	*Data*	*Code*
00	-+00-+	20	-++-00	40	-00+0+	60	0++0-0
01	0-+-+0	21	+00+--	41	0-00++	61	+0+-00
02	0-+0-+	22	-+0-++	42	0-0+0+	62	+0+0-0
03	0-++0-	23	+-0-++	43	0-0++0	63	+0+00-
04	-+0+0-	24	+-0+00	44	-00++0	64	0++00-
05	+0--+0	25	-+0+00	45	00-0++	65	++0-00
06	+0-0-+	26	+00-00	46	00-+0+	66	++00-0
07	+0-+0-	27	-+++--	47	00-++0	67	++000-
08	-+00+-	28	0++-0-	48	00+000	68	0++-+-
09	0-++-0	29	+0+0--	49	++-000	69	+0++--
0A	0-+0+-	2A	+0+-0-	4A	+-+000	6A	+0+-+-
0B	0-+-0+	2B	+0+--0	4B	-++000	6B	+0+--+
0C	-+0-0+	2C	0++--0	4C	0+-000	6C	0++--+
0D	+0-+-0	2D	++00--	4D	+0-000	6D	++0+--
0E	+0-0+-	2E	++0-0-	4E	0-+000	6E	++0-+-
0F	+0--0+	2F	++0--0	4F	-0+000	6F	++0--+
10	0--+0+	30	+-00-+	50	+--+0+	70	000++-
11	-0-0++	31	0+--+0	51	-+-0++	71	000+-+
12	-0-+0+	32	0+-0-+	52	-+-+0+	72	000-++
13	-0-++0	33	0+-+0-	53	-+-++0	73	000+00

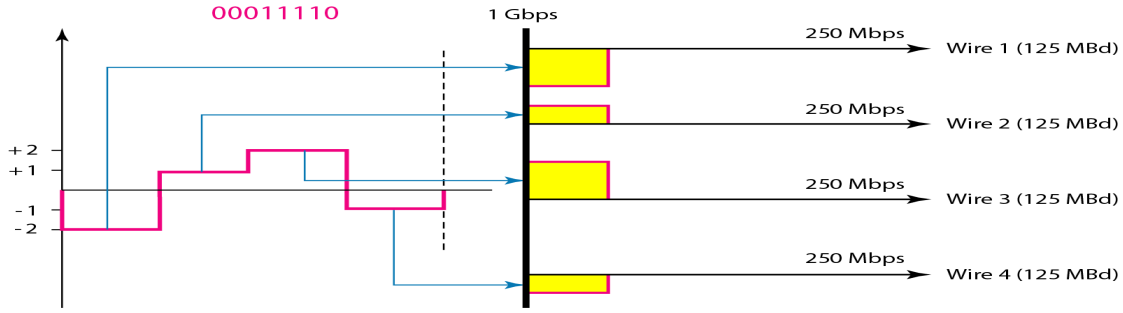
(iii) Multilevel: 4D-PAM5 scheme

Four-dimensional five-level pulse amplitude modulation (4D-PAM5).

The 4D means that data is sent over four wires at the same time

It uses five voltage levels, such as -2, -1, 0, 1, and 2.

Example: 00011110 (00: -2, 01: +1, 11: +2 and 10: -1)



5. Multiline Transmission (MLT-3)

The multiline transmission, three level (MLT-3) scheme uses three levels (+v, 0, and- V) and three transition rules to move between the levels.

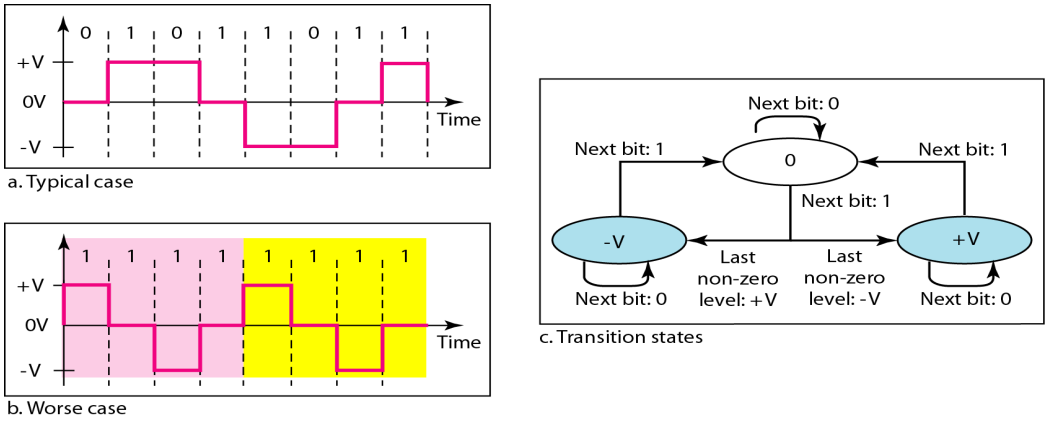
If the next bit is 0, there is no transition.

If the next bit is 1 and the current level is not 0, the next level is 0.

If the next bit is 1 and the level is 0, the next level is the opposite of the last nonzero level.

The behavior of MLT-3 can best be described by the state diagram shown in Figure. The three voltage levels *(-V*, 0, and *+V)* are shown by three states (ovals). The transition from one state (level) to another is shown by the connecting lines. Figure also shows two examples of an MLT-3 signal.

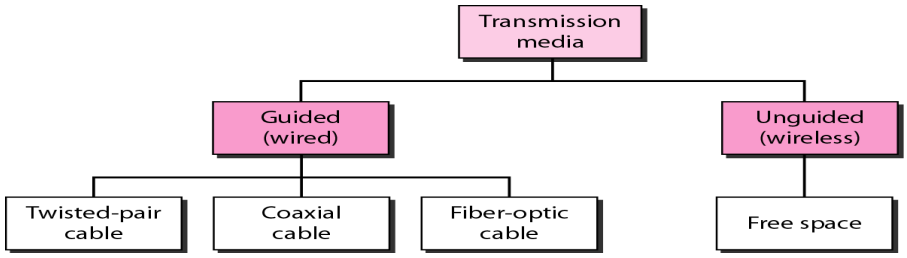
Example: 01011011 and 11111111



Multiline Transmission ML-3

TRANSMISSION MEDIA

In data communications, a transmission medium is a physical path between transmitter and receiver. i.e., it is the channel through which data is sent from one place to another. Transmission media are broadly classified into the following types:



GUIDED MEDIA

It is also called wired or bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links. They are widely used in computer and telephone networks. Guided media has lesser noise and obstacles in comparison to unguided media. This causes guided media to give a faster rate of data transmission than unguided media. Important features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of guided media: Twisted Pair Cable, Coaxial Cable, and Optical Fiber Cable (OFC)

1. Twisted Pair Cable

It is the most widely used transmission media. It consists of two separately insulated conductor wires twisted together. By twisting, both wires are equally affected by noise like external interference and cross talk. These equal effects are cancelled out at the receiver. Quality of the cable also depends on number of twists per inch.

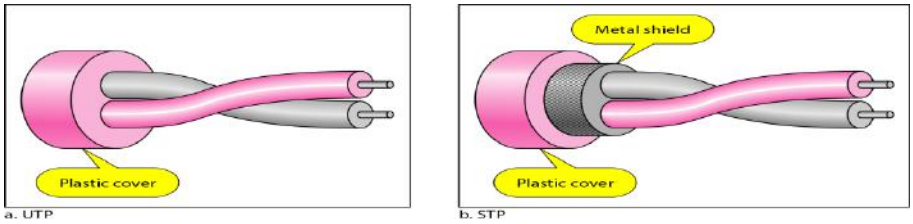
Generally, several such pairs are bundled together in a protective sheath. Twisted Pair is of two types:

(i) Unshielded Twisted Pair (UTP)

UTP It is a pair of insulated copper wires twisted together to reduce noise generated by external interference. It doesn't use additional shielding. Its frequency range is suitable for transmitting

both data and voice signals. Generally, UTPs are used to establish the connection for enterprises over a long distance.

(ii) Shielded Twisted Pair (STP):
This type of cable consists of a special jacket (shield) to block external interference. It is used in fast ethernet and voice and data channels of telephone lines. STPs are used to establish the connection within a short distance, like a home or small industry. STP cables are thicker than UTP cables.



a. UTP b. STP

Advantages of STP over UTP

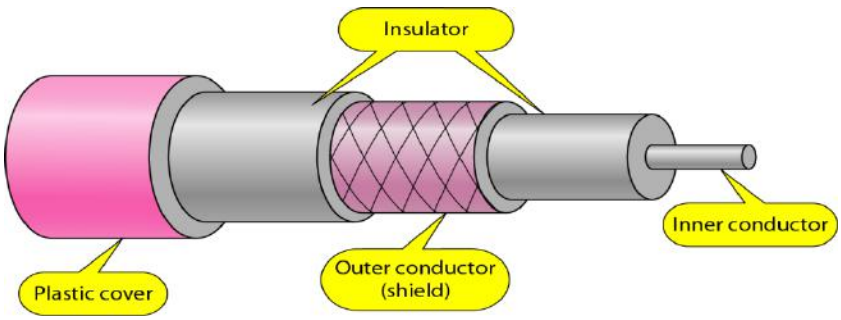
STP	UTP
1.Less electromagnetic interference and low cross talk	1. More electromagnetic interference and high cross talk
2. More data speed (Fast).	2. Less data speed (Slow).

Disadvantages of STP over UTP

STP	UTP
1. More expensive	1. Less expensive
2. It is bulkier. So Installation is difficult.	2. Lighter, small in size, and flexible. so easier to install.
3. Requires more maintenance to reduce the loss of data signals.	3. Requires less maintenance.

Applications:
- ✓ Telephone lines
- ✓ LANs

2. Coaxial Cable



Coaxial cable is a type of cable that has an inner conductor surrounded by an insulating layer, surrounded by a conductive shielding. Many coaxial cables also have an insulating outer jacket (protective outer sheath).
Coaxial cable carries signals of higher frequency ranges than twisted pair cable. widely use Coaxial cables. Coaxial cable transmits information in two modes: baseband mode and broadband mode.

Baseband Transmission	Broadband Transmission
Mostly used for LAN networks.	Mostly used for Telephone networks
Uses digital signaling on wires	Uses analog signals in the form of optical or electromagnetic waves
Dedicated cable bandwidth	Bandwidth is split into separate ranges
Used for short distances.	Used for long distances without attenuation.
Bidirectional: A single cable is used to both send and receive data	Unidirectional: Two cables are used, one to send and one to receive..
Uses with Bus topology.	Used with bus and tree topologies

Advantages of coaxial cable:
- Inexpensive.
- Easy to install and expand.
- Better noise Immunity.
- High bandwidth.

Disadvantages of coaxial cable:
- Single cable failure can disrupt the entire network

Applications:
- LANs
- Cable TV and analog television networks

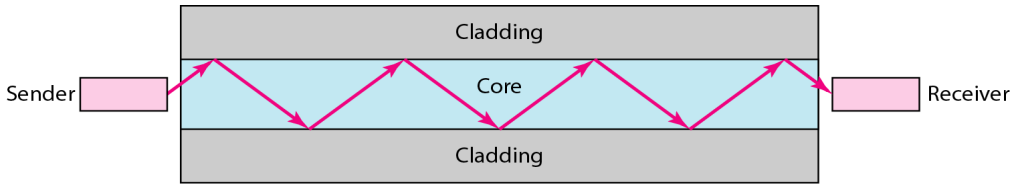
3. Optical Fiber Cable (OFC)

OFC has three basic elements: The core, the cladding and the coating.
Core: Core is the light transmission area of the fiber. It is made of either glass or plastic. OFC uses the concept of reflection of light through the core.
Cladding: The core fiber is coated with a less dense glass called cladding. It has slightly lower refractive index than core. It causes good reflection within the core by increasing critical angle with the fiber. Thus, light waves are efficiently transmitted through the fiber. Cladding also prevents adjacent fibers from touching each other.
Coating: The coating surrounding cladding comprises a plastic material to protect the fiber from the physical environment. Sometimes metallic sheaths are added to the coating for further physical protection.
Advantages of OFC:
- Light weight

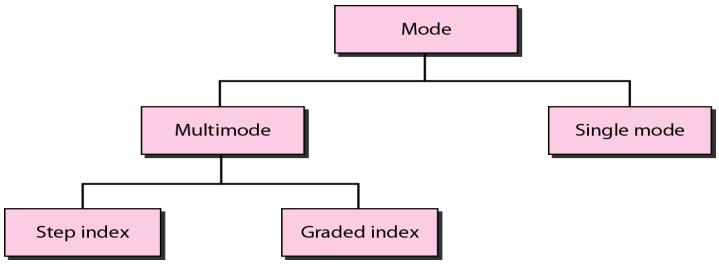
- Better noise immunity.
- Increased capacity and bandwidth
- Less signal attenuation over long distances
- Resistance to corrosive materials

Disadvantages of OFC:

- Difficult to install and maintain.
- High cost.
- It is unidirectional. If we need bidirectional communication, another cable is needed
- Fragile (brittle and easily breakable).



Propagation modes in Optical Fiber Cable:



Single mode and multimode fibers: Single mode means the fiber allows only one type of light mode to propagate at a time, while multimode means the fiber can propagate multiple modes. Single mode fiber has smaller core and high transmission rate and is more suitable for long distances, but more expensive.

Step index and graded index fibers: Step index fiber is a type of fiber where the refractive index of the core is uniform throughout and undergoes an abrupt change at the core-cladding boundary. In graded index fiber the refractive index of the core is maximum at the center of core and then it decreases towards core-cladding interface. Step index fiber is easy to manufacture, less expensive and used for long distances. Graded index fiber has more information-carrying capacity.

2. UNGUIDED MEDIA

It is also referred to as “wireless” or “unbounded” transmission media. No physical medium is required for the transmission of electromagnetic signals.

Important features:

- Signal is broadcasted through air
- Less secure
- Used for larger distances

There are 3 major types of unguided media: Radio waves, Microwaves, and Infrared waves

1. Radio waves

Frequency range:3KHz – 1GHz.

Radio waves are transmitted easily through air. They do not cause damage if absorbed by the human body, and they can be reflected to change their direction. These are easy to generate and can penetrate through nonconducting materials, such as wood, bricks, and concrete, fairly well. They cannot pass through electrical conductors, such as water or metals. The sending and receiving antennas need not be aligned. Applications of radio waves include:

- AM and FM Radio Broadcasting and TV broadcasting
- Military communications,
- Satellite transmissions.
- Mobile phones and wireless networks,

Radio waves are classified as Terrestrial radio and Satellite radio. In terrestrial radio broadcasting the radio waves are broadcast by a land-based radio station, while in satellite radio the radio waves are broadcast by a satellite in earth orbit. To receive the content the listener must have a broadcast radio receiver (radio)

2. Microwaves

Frequency range:1GHz– 300GHz

Microwaves travel by line-of-sight transmission i.e., the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Microwaves are harmful to human body. Applications of Microwaves include:

- Transmission of TV signals
- Mobile phones and Wireless networks
- Radar and navigational systems
- Microwave ovens in cooking and reheating.
- In medical treatment (example: treatment of cancer)

3. Infrared waves (or infrared light)

Frequency range:300GHz– 400THz

Infrared waves have a higher frequency than microwaves. They are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Infrared waves are harmful to human body. Applications of infrared waves include:

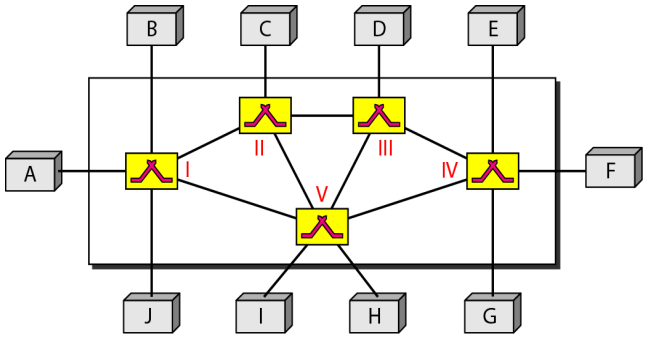
- ✓ Heat sensors and thermal imaging
- ✓ Night vision equipment
- ✓ TV remotes, wireless mouse, keyboard, printer, etc.
- ✓ Infrared radiation is used in cooking, known as broiling or grilling.
- ✓ In medical treatment (example: the relief of muscle pain and tension)

UNIT-2
SWITCHING

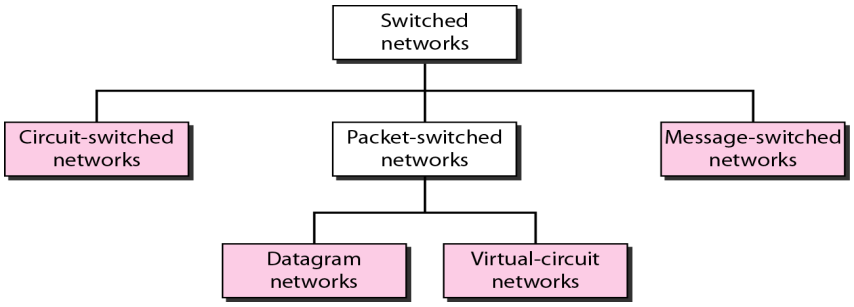
Syllabus contents: Datagram Networks, Virtual Circuit Networks, Structure of a switch, Ethernet Physical Layer, Data Link Layer: Error detection and Correction, Data Link Control: Framing, Flow and Error Control Protocols, Noiseless Channel and Noisy Channel Protocol, HDLC, Point-to-Point Protocol.

Switched Network:

A network switch is hardware component that connects devices in a computer network. A switched network consists of a series of interconnected nodes, called switches. Some of these nodes are connected to the end systems (Examples: computers or telephones). Others are used only for routing. The following figure show a switched network.



Here A, B, C, D, …, H, are end systems and I, II, III, IV, and V are switches. Each switch is connected to multiple links (connecting lines in figure). Based on the method of connection, present networks are broadly classified as Circuit-switched networks, Packet-switched networks, and Message-switched networks. The first two are commonly used today. Packet-switched networks are further classified as Datagram networks and Virtual-circuit networks.



Types of networks

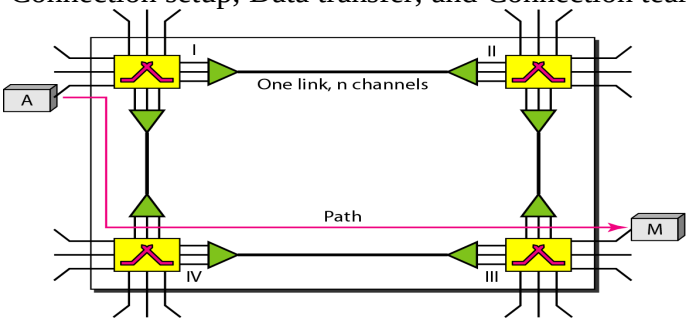
1. CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected by physical links.

- ✓ Two stations are connected by one or more links.
- ✓ Each link is divided into n channels by using FDM or TDM.
- ✓ Each connection uses only one dedicated channel on a link.

Circuit switching is most often used for voice and video calling systems. An example of a circuit-switched network is landline telephone network. A circuit switched network is implemented in physical layer.

Figure shows a circuit-switched network with four switches and four links. Each link is divided into 3 channels by using FDM or TDM. The communication in a circuit-switched network involves three phases: Connection setup, Data transfer, and Connection teardown.



(i) Connection Setup phase: 'connection setup' means creating dedicated channels between the switches. Suppose end system 'A' needs to communicate with end system 'M'. Then, A requests a connection to M. This request must be accepted by M and also all the switches. Then all the required resources are reserved for entire duration of data transfer. These resources include buffers, I/O ports, and processing time of switch, etc.

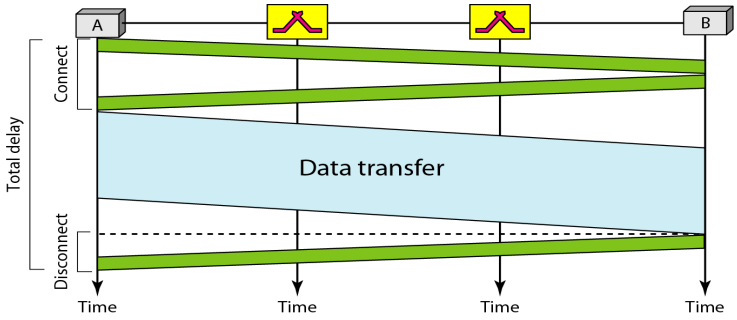
(ii) Data Transfer Phase: After the establishment of the dedicated circuits (channels), data is transferred between end users. The switches route the data based on their occupied band (FDM) or time slot (TDM).

(iii) Connection Teardown Phase: When one of the stations (end users) wants to disconnect, a signal is sent to each switch to release the resources.

Important parameters:

Efficiency: Because resources are allocated for entire duration of the connection, they are unavailable to other connections. Hence, Circuit-switched networks are not as efficient as the other two types of networks

Delay: Here, the delay at each switch is minimal, because all the resources are available during entire connection time.

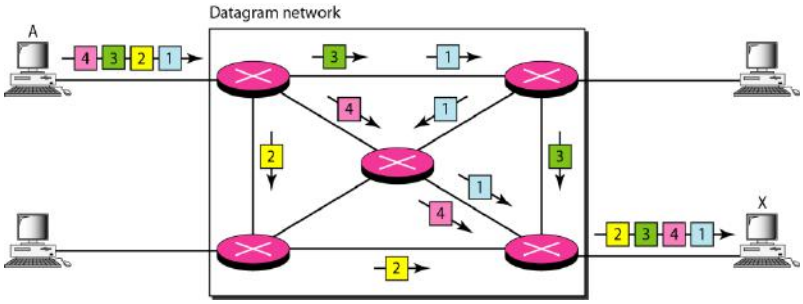


The delay in data transfer involves: the propagation time (slope of the coloured box), and data transfer time. D (height of the coloured box). Delays in other phases are time for connection and time for disconnection.

2. PACKET SWITCHED NETWORKS

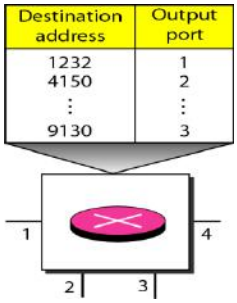
In a packet-switched network, the message is first divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol. These packets are handled in two ways: Datagram and Virtual circuit

(A) DATAGRAM NETWORKS



- Packets can take any practical route.
- Packets may get lost or delayed.
- Packets may arrive out of order.
- It is up to receiver to re-order packets and recover from missing packets

The datagram networks are connectionless networks. There are no setup or teardown phases. A switch in a datagram network uses a routing table. The table is based on the destination address. The destination address is in the header of a packet. This address remains the same during the entire journey of the packet.



Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network. It is because resources are allocated on demand (only when there are packets to be transferred)

Delay

There may be more delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait (for resources) at a switch before it is forwarded.

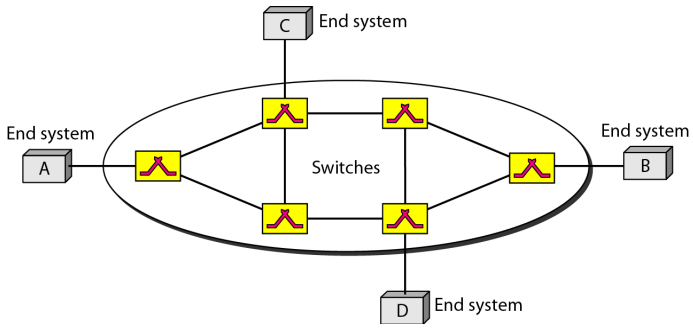
The packet travels through two switches. There are three transmission (say 3T), three propagation delays (say 3t in transmission), and two waiting times (w1 and w2). Ignoring the processing time in each switch,

Total delay =3T + 3t + w1 + w2

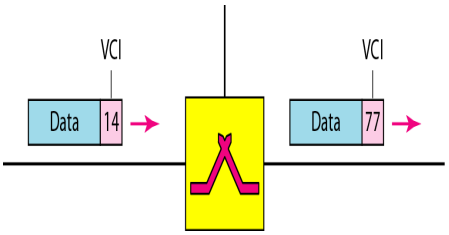
(B) VIRTUAL-CIRCUIT NETWORKS

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some features of both.
Important features:

- As in a circuit switched network, it has setup phase, data transfer phase and teardown phase.
- Resources can be reserved during setup phase similar to a circuit-switched network or allocated on demand like in a datagram network.
- As in a datagram network. data are packetized and each packet carries an address in the header. However. the address in the header will not indicate destination. It indicates the next switch and the channel on which the packet is to be carried. So, no routing decisions are needed for a packet
- As in a circuit-switched network, all packets follow the same path established during the connection.
- Presently, a virtual switching network is implemented in the data link layer, where as a circuit switched network is implemented in physical layer.



Virtual-circuit network



Virtual-circuit identifier

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

Global Address:

If the network is part of an international network, a source or a destination must have a global address, i.e., a globally unique network address. A global address in virtual-circuit networks is used only to create a virtual-circuit identifier.

Virtual-Circuit Identifier (VCI):

A VCI is the address that is actually used for data transfer. It transfers data over a packet-switched network in such a way that it appears as though there is a dedicated physical link between source and destination. That is why it's called 'Virtual'.

In a virtual-circuit network, setup, data transfer, and teardown phases occur. Switches maintain a **connection table** indexed by ⟨VCI, port⟩ pairs. In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection. In the teardown phase, the source and destination inform the switches to delete those entries. Data transfer occurs between these two phases.

At each switch the VCI changes to point the next switch.

Delay in Virtual-Circuit Networks

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Ignoring the processing time in each switch,

Total delay = 3T+ 3t + setup delay + teardown delay

where, 3 ‘T’ s are three transmission times (3T), 3 ‘t’s are three propagation delays, and w1 and w2 are the waiting times.

STRUCTURE OF A CIRCUIT SWITCH

Based on technology, there are 2 types of Circuit Switches: space-division switch and time-division switch. In space-division switching, the paths in the circuit are separated from one another spatially. This technology was originally designed for use in analog networks but is used currently in both analog and digital networks.

1. Space-Division Switches:

Single-stage Crossbar Switch

A crossbar switch connects n inputs to m outputs in a grid, using electronic microswitches (transistors) at each crosspoint as shown in figure. To connect n inputs to m outputs using a crossbar switch requires n x m crosspoints. The major limitation of this design is the number of crosspoints required, which is impractical fewer than 25 percent of the crosspoints are in use at any given time. The rest are idle.

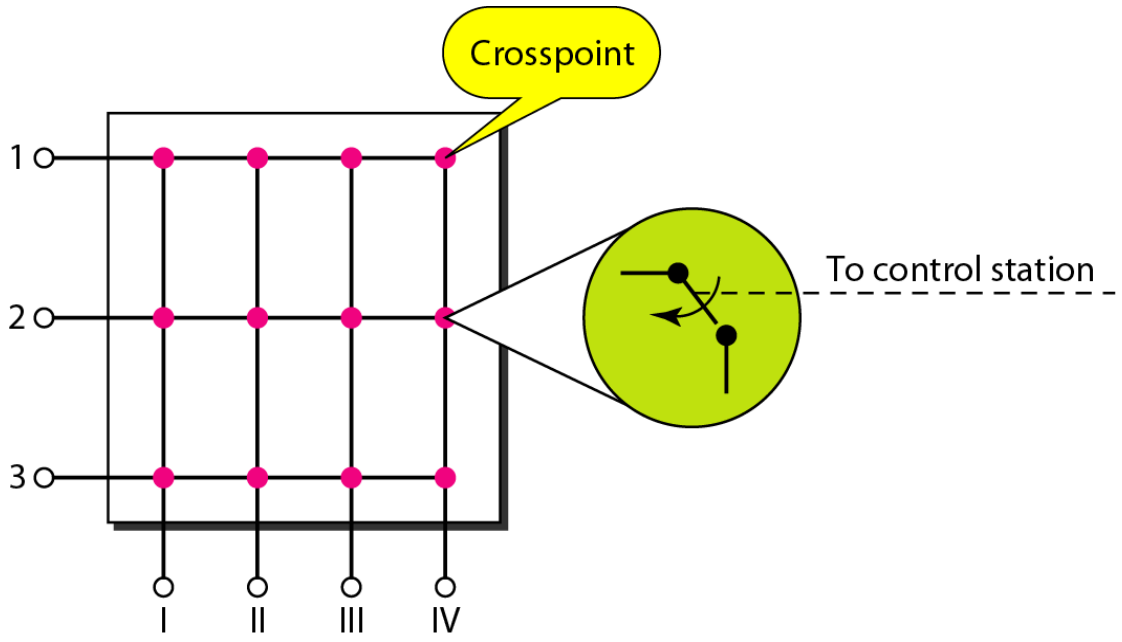
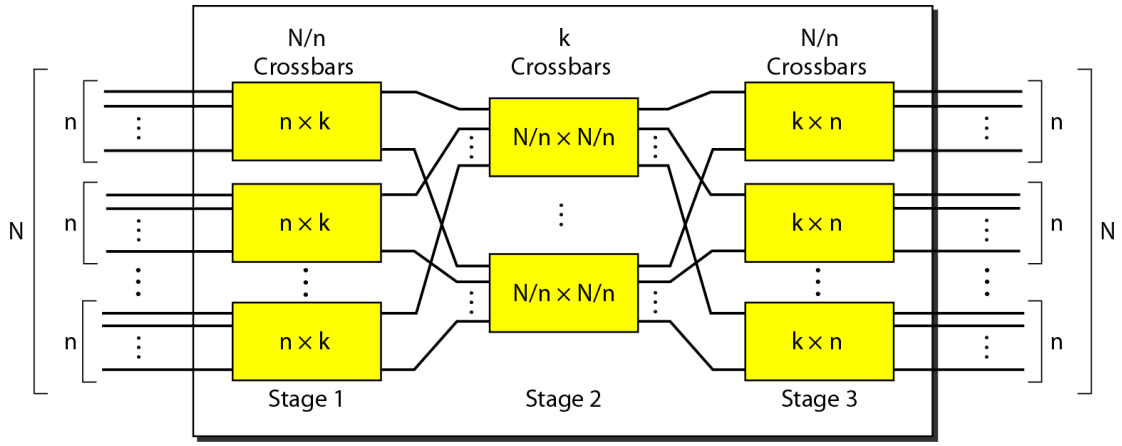


Figure: Crossbar switch with three inputs and four outputs

Multistage crossbar Switch:

This resolves the limitations of the crossbar switch It combines crossbar switches in many stages. Figure shows 3-stage switch.



A three-stage cross switch

Here, we use multiple paths inside the switch, to reduce the number of crosspoints. Each crosspoint in the middle stage can be accessed by multiple crosspoints in the first or third stage.

- We divide the N input lines into n-line groups. For each group, we use one crossbar of size n x k, where k is the number of crossbars in the middle stage. In other words, the first stage has N/n crossbars of n x k crosspoints.
- We use k crossbars, each of size (N/n) x (N/n) in the middle stage.
- In a three-stage switch, the total number of crosspoints = $2kN + k(N/n)^2$

which is much smaller than the number of crosspoints in a single-stage switch (N^2).

Example: Design a three-stage, 200 × 200 switch (N = 200) with k = 4 and n = 20

Solution:

In the first stage we have N/n or 10 crossbars, each of size 20 × 4.

In the second stage, we have 4 crossbars, each of size 10 × 10.

In the third stage, we have 10 crossbars, each of size 4 × 20.

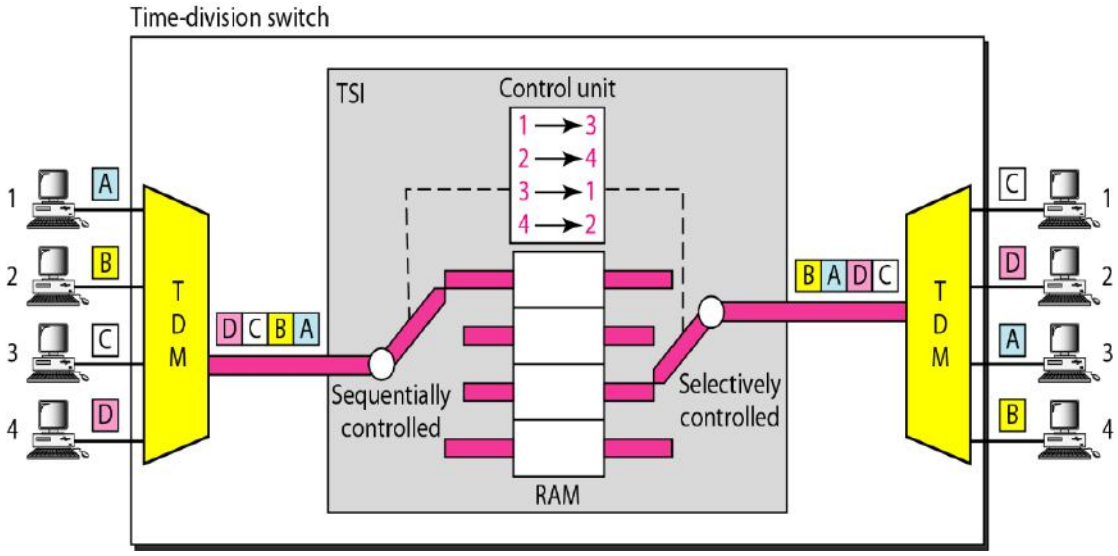
The total number of crosspoints is $2kN + k(N/n)^2$, or 2000 crosspoints.

This is 5 percent of the number of crosspoints in a single-stage switch (200 × 200 = 40,000).

2. Time-Division Switches:

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

1 → 3 2 → 4 3 → 1 4 → 2

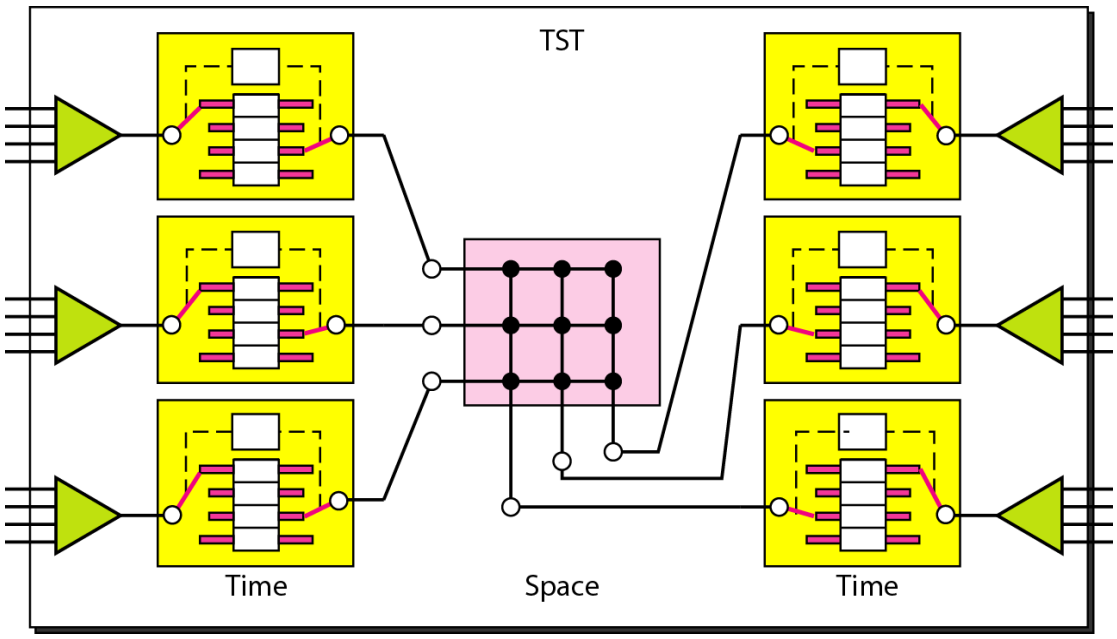


Time-division switch

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

Time-space-time switch

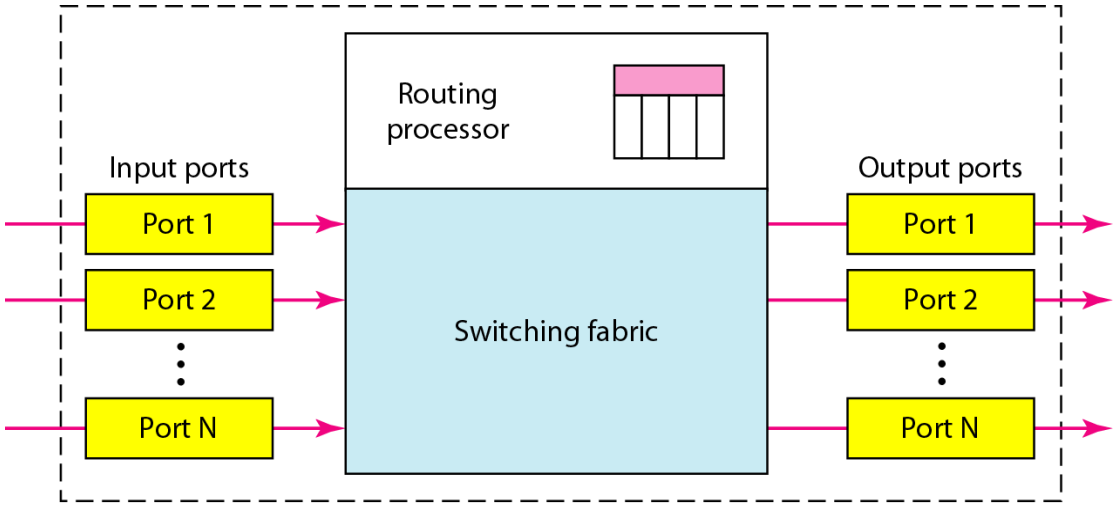
The advantage of space-division switching is that it is instantaneous. The advantage of time-division switching is that it needs no crosspoints. A 'Time-space-time switch' shown in the figure combines the advantages of both.



Time-space-time switch

STRUCTURE OF PACKET SWITCHES

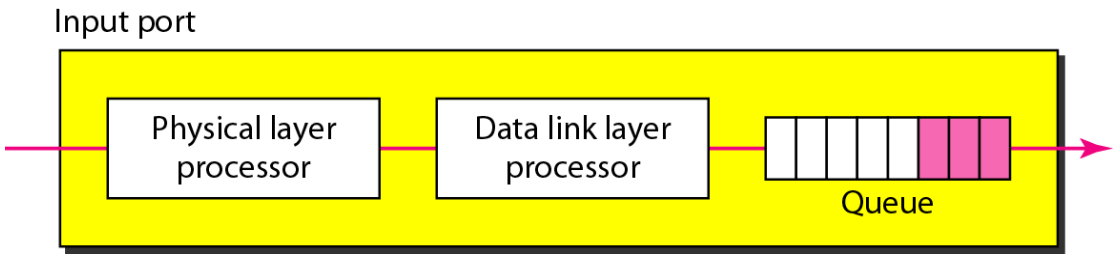
A packet switch has four components: input ports, output ports, the routing processor, and the switching fabric, as shown in Figure.



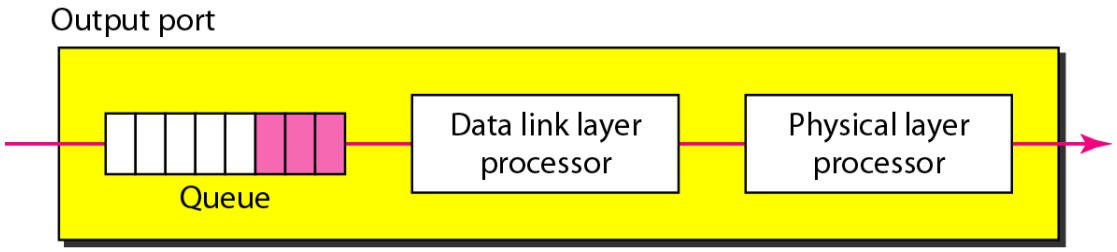
Routing Processor:

Routing Processor: The routing processor performs the functions of the network layer using a routing table containing destination address and output port number.

Input Port: An input port performs the physical and data link functions of the packet switch. ex: Errors are detected and corrected



Output Port: The output port performs the same functions as the input port, but in the reverse order

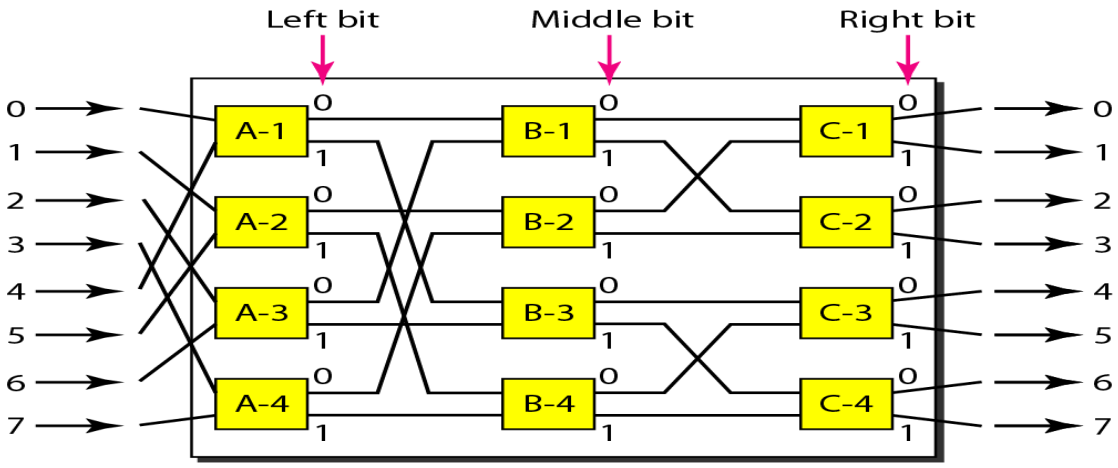


Switching fabric: *Switching fabric* is a network topology, in which different network nodes are connected with each other via one or more network switches. The simplest type of switching fabric is the crossbar switch.

Banyan Switch

It is a more realistic approach than the crossbar switch is the banyan switch. It is a multistage switch with microswitches at each stage that route the packets based on the output port represented as a binary string. For n inputs and n outputs, we have log2 n stages with n/2 microswitches at each stage. The first stage routes the packet based on the high-order bit of the binary string. The second stage routes the packet based on the second high-order bit, and so on. Figure 8.24 shows a banyan switch with eight inputs and eight outputs. The number of stages is Iog2(8) = 3

Note: ($\log_2$ n) is the power to which the number 2 must be raised to obtain the value n.



A banian switch sending a cell to output 6 (110)

Suppose a packet has arrived at input port 1 and must go to output port 6 (110 in binary). The first microswitch (A-2) routes the packet based on the first bit (1), the second microswitch (B-4) routes the packet based on the second bit (1), and the third microswitch (C-4) routes the packet based on the third bit (0).

Batcher-Banyan Switch

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

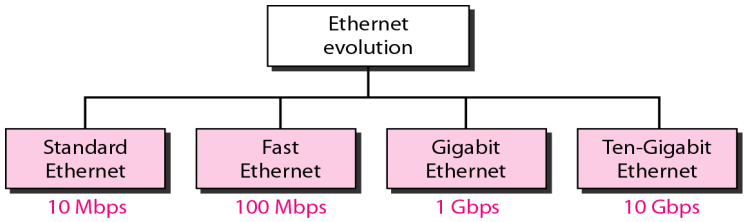
A switch (called Batcher switch) sorts the incoming packets according to their final destinations using hardware merging techniques. Another hardware module called a trap is added between the Batcher switch and the banyan switch prevents duplicate packets (packets with the same output destination) from passing to the banyan switch simultaneously. Then, packets are allowed to reach destination one at a tick.

Batcher switch → **Trap** → **Banian Switch**

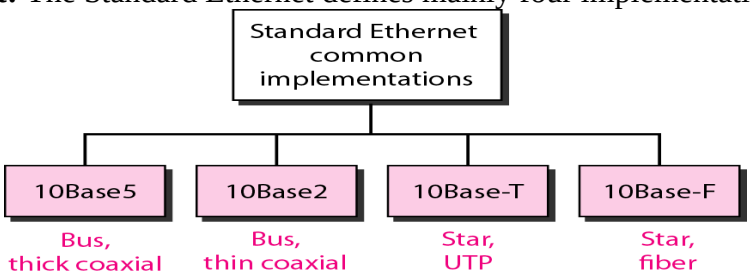
Ethernet Physical Layer

Ethernet: Ethernet is the traditional technology for connecting devices in a wired LAN or WAN using a protocol. Ethernet describes how network devices format and transmit data. We use Ethernet cable to physically connect computer to the internet. Ethernet connections are almost always faster than Wi-Fi connections, and are usually more stable.

Evolution of Ethernet:



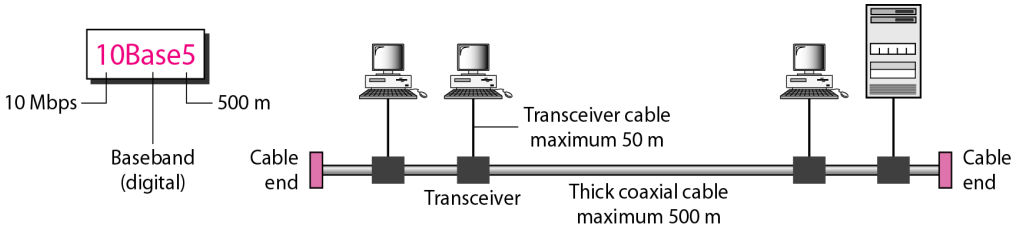
Standard Ethernet: The Standard Ethernet defines mainly four implementations:



Encoding and Decoding: All standard implementations use digital signaling (baseband) at 10 Mbps. Manchester coding is used in standard Ethernet.

Standard Ethernet implementations:

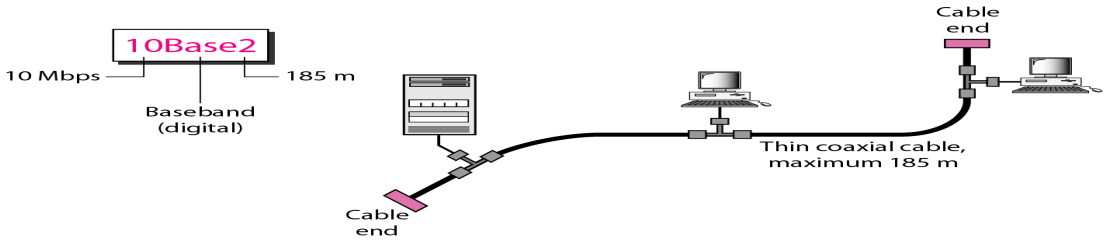
10Base5: Thick Ethernet



- It was the first Ethernet specification. It is also called "Thick net" because it uses a thick coaxial cable like a hose pipe used in garden. It is too stiff to bend with hands.
- 10Base5 means that it operates at 10 Mbps, use baseband signaling, and can support segments of up to 500 meters.
- The maximum length of the coaxial cable must not exceed 500 meters to minimize the effect of attenuation. If a length of more than 500 m is needed, repeaters are used for each segment.
- It uses a **bus topology** with an external transceiver (transmitter/receiver) connected to the station via a transceiver cable.
- The transceiver is responsible for transmitting, receiving, and detecting collisions. It provides separate paths for sending and receiving. This means that collision can only occur in the coaxial cable.

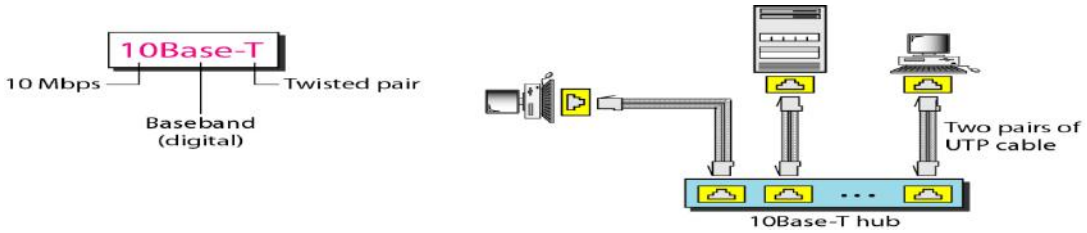
Data collision: When many packets are transmitted between nodes simultaneously, they may cause data collision. The packets are either discarded or sent back to their originating stations and then retransmitted.

10Base2: Thin Ethernet



- 10Base2 means that it operates at 10 Mbps, use baseband signaling, and can support segments of up to 185 meters (nearly 200 meters).
- It is also called "Thin Ethernet", because the coaxial cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. Coaxial cable is terminated with BNC connectors, which are relatively less expensive
- Here, implementation is easy and more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial.
- It also uses a **bus topology.**
- In this, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.
- Any collision here happens in the coaxial cable.

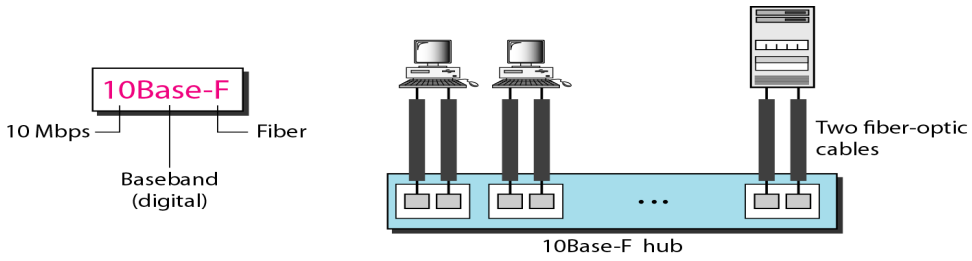
10Base-T: Twisted-Pair Ethernet



The third implementation is called 10Base-T. 10Base-T means that it operates at 10 Mbps, use baseband signaling and Twisted pair cables. The maximum length of the twisted cable is 100 m, to minimize the effect of attenuation in the twisted cable.

- It uses a physical **star topology**.
- The stations are connected to a hub via two pairs of twisted cable. One pair is used for sending and other for receiving,
- Any collision here happens in the hub.

10Base-F: Fiber Ethernet

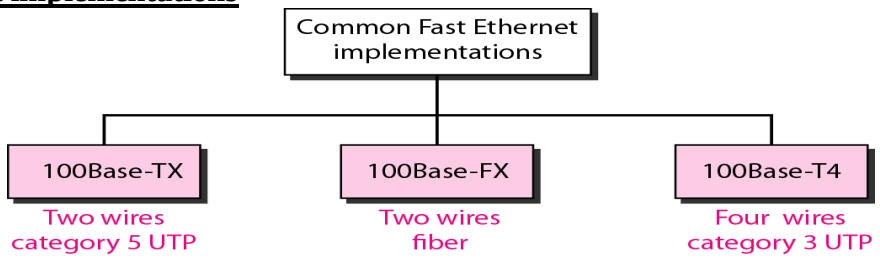


- 10-Mbps Ethernet is the most common Ethernet used. It uses a **star topology** to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables

- It is expensive due to the cost of the connectors and terminators, but it has excellent noise immunity.
- It is the method of choice when running between buildings or widely-separated hubs. Runs of up to Km are allowed. It also offers food security

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

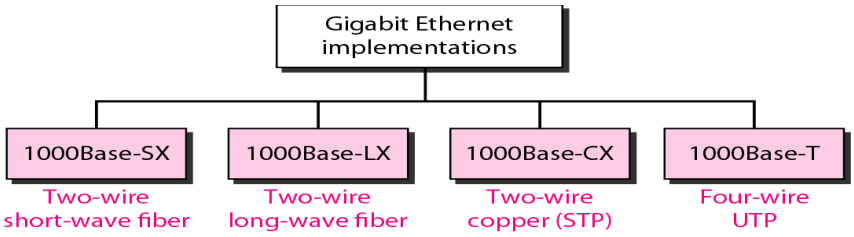
Fast Ethernet implementations



Characteristics	**100Base-TX**	**100Base-FX**	**100Base T-4**
Media	5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

Gigabit Ethernet:

- It offers a speed of 1 gigabit per second (Gbps). Gigabit Ethernet is used to connect computers and servers in local networks.
- Gigabit Ethernet has the limit of 70 km



Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Ten-Gigabit (10Gbe) Ethernet implementations

- ✓ Enterprises use 10 Gigabit Ethernet switches for very high-speed network applications – mostly in the data center or server room.
- ✓ It offers data speeds up to 10 gigabits per second.
- ✓ It was launched in 2002

Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

Data Link Layer
Error detection and Correction

Errors:

During the transmission of digital signals, data may be corrupted due to noise. This results in one or more errors. A single error means a 0 bit may change to 1 or a 1 bit may change to 0.

If only one bit in the data unit (example: packet or frame) has changed, it is called “single error”. If 2 or more bits changed, it is called “Burst”

Bursts are more likely to occur than the single-bit error because the duration of noise is normally longer than the duration of 1 bit. For illustration purpose consider a 4-bit word.

Examples:

1	0	0	1

Data transmitted

1	0	0	0

Single error (1 changed to o)

Two errors (0 in second position from left changed to 1 & 1 in second position from changed to 0)

Redundancy:

To detect or correct errors, we need to send extra (redundant) bits with data. These extra bits are called redundant bits. Receiver uses them to detect or correct the errors.

Block Coding

In block coding, we divide the message into blocks called data words. Let each block has k bits. We add r extra bits (redundant bits) to each block to make the length n = k + r. The resulting n-bit blocks are called code words.

Role of Block coding in error detection

Suppose the original codeword has changed to an invalid one due to errors. If the receiver knows or gets a list of valid code words, block coding can detect the errors.

A generator circuit at the sending end generates a code word for each data word, and sends the code words to receiver.

Each codeword sent to the receiver may change during transmission.

Each received codeword is checked by a checker circuit. If it is a valid code word, the data word is extracted and used. If the received codeword is not valid, it is discarded.

Example:

Let length of data word = k = 2 bits; No. of redundant bits = r = 1 bit.

Then, length of code word = k + r = 2+1 = 3 bits.

Then the following table shows the list of data words and code words. Later, we will see how to derive a codeword from a data word.

Data word	Codeword
00	000
01	011
10	101
11	110

Code for error detection

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

The receiver receives 011. It is a valid codeword. The receiver extracts the data word 01 from it.

The codeword is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is not accepted.

If double error occurs, the above code cannot detect the errors. Let 000 is received instead of 011. Since received word also is a valid codeword, it cannot detect the errors.

Error Correction:

The receiver needs to find (or guess) the original codeword sent. If error occurs during transmission, received code word is compared with the valid code words in the receiver and find out correct code word.

Example:

Add 3 redundant bits to the 2-bit data word to make 5-bit codewords as follows:

Data word	Codeword
00	00000
01	01011
10	10101
11	11110

Assume the dataword is 01.

Then codeword created is 01011.

Suppose the codeword is corrupted during transmission, and 01001 is received. The receiver finds that the received codeword is not in the table. Assuming that there is only 1 bit corrupted, it uses the following strategy to guess the correct dataword.

The receiver compares the received codeword with the first codeword in the table (01001 versus 00000), and decides that the first codeword is not the one that was sent because there are two different bits.

Hamming Distance

The Hamming distance between two words is the number of differences between corresponding bits (number of changes).

The Hamming distance By the same reasoning, the original codeword cannot be the third or fourth one in the table.

The original codeword must be the second one in the table because this is the only codeword with one error. The receiver replaces the differed bit. i.e., it replaces 01001 with 01011 and consults the table to find the dataword 01.

d(000, 011) is 2. It is found by
$000 \oplus 011 = 011$ (two 1's)

The Hamming distance d(10101, 11110) is 3. It is found by
$10101 \oplus 11110 = 01011$ (three 1's)

The minimum Hamming distance is the smallest Hamming distance between all possible pairs in a set of words.

Example: Find the minimum Hamming distance of the coding scheme in above table

Solution:

We first find all the Hamming distances.

d(00000,01011)=3, d(00000,10101)=3, d(00000,11110)=4,
d(01011,10101)=4, d(01011,11110)=3, d(10101,11110)=3

The d_{min} in this case is 3.

Minimum Hamming distance for Error Detection

To guarantee the detection of up to s errors, the minimum Hamming distance in a block code must be

$$d_{min} = s + 1.$$

Minimum Hamming distance for Error Correction

To guarantee correction of up to s errors in all cases, the minimum Hamming distance in a block code must be $d_{min} == 2s+ 1$. Thus minimum distance for error corrections are 3, 5, 7, and so on.

Example: A code scheme has a Hamming distance $d_{min} =4$. What is the error detection and correction capability of this scheme?

Solution: This code guarantees the detection of up to three errors (s = 3), but it can correct up to one error. In other words.

LINEAR BLOCK CODES

Almost all block codes used today belong to a subset called linear block codes. A linear block code is a code in which the exclusive OR (modulo-2 addition) of two valid code words creates another valid codeword.

Parity-Check Code

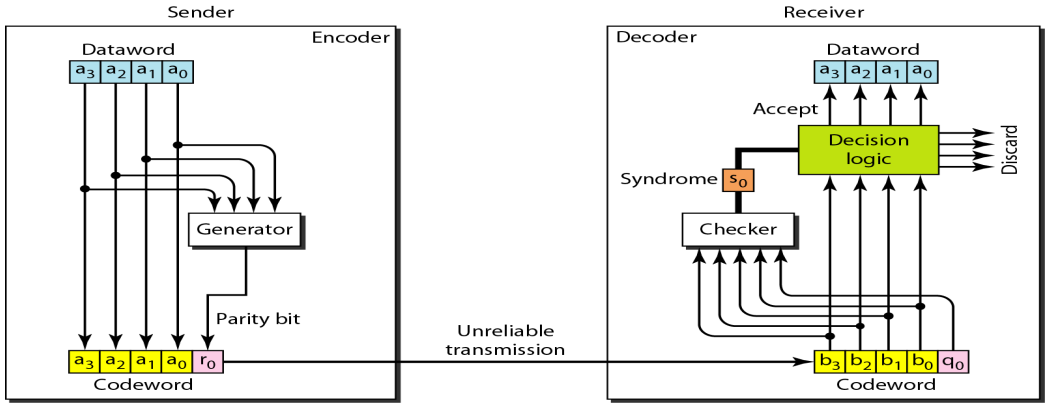
A simple parity-check code is a single-bit error-detecting code in which $n = k + 1$ with $d_{min} = 2$, where k is the length of dataword, n is that of codeword.

It can detect an odd number of errors.

The code in Table 10.2 is also a parity-check code with k = 4 and n = 5.

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

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



The calculation is done in modular arithmetic. The encoder uses a generator that takes a copy of a 4-bit data word (a0, a1, a2, and a3) and generates a parity bit r0. The data word bits and the parity bit create the 5-bit codeword.

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

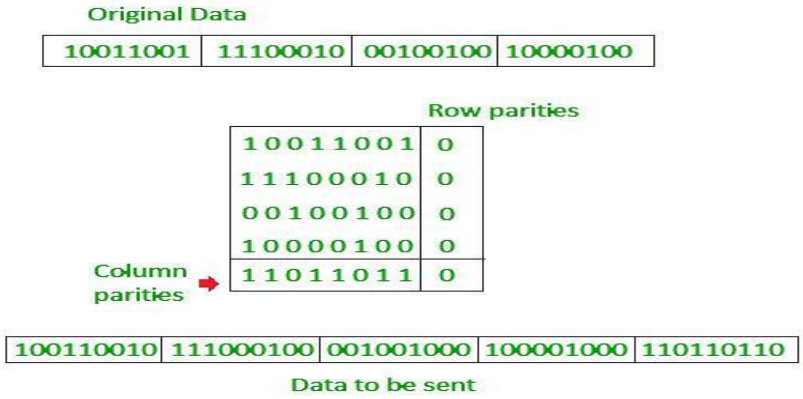
The receiver receives a 5-bit word. The checker at the receiver does the same thing as the generator in the sender with one exception: The addition is done over all 5 bits. The result, which is called the syndrome, is just 1 bit. The syndrome is 0 when the number of 1s in the received codeword is even; 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 codeword is accepted as the data word; if the syndrome is 1, the data portion of the received codeword is discarded. The data word is not created.

Note: A simple parity-check code can detect an odd number of errors

Two-dimensional Parity check
Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits 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.



Hamming Codes

They are used for error correction.

These codes were originally designed with $d_{min} = 3$, which means that they can detect up to two errors or correct one single error. Hamming codes are available to correct more than one error

Let n be the length of codeword and k be that of dataword. Let m is the number of redundant bits to be used.

Then We need to choose an integer m >= 3 (for single error). The values of n and k are then calculated from m using the relation

$$n = 2^m - 1 \text{ and } k = n - m.$$

For example, if m =3, then n =7 and k=4.

This is a Hamming code C(7, 4) with d_{min} =3. Table shows the data words and code words for this code.

Table: Hamming code C

Datawords	*Codewords*	*Datawords*	*Codewords*
0000	0000000	1000	1000110
0001	0001101	1001	1001011
0010	0010111	1010	1010001
0011	0011010	1011	1011100
0100	0100011	1100	1100101
0101	0101110	1101	1101000
0110	0110100	1110	1110010
0111	0111001	1111	1111111

(7, 4)

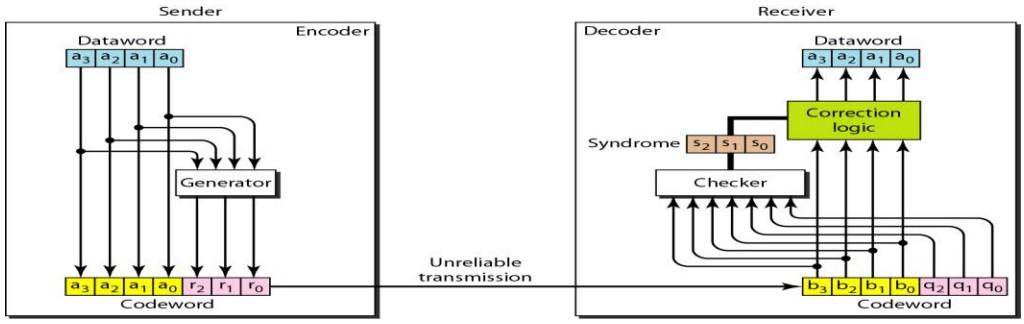


Figure: *The structure of the encoder and decoder for a Hamming code*

A copy of a 4-bit data word is fed into the generator that generate ro, r1, and r2 as shown below:

$r_0 = a_2 + a_1 + a_0$

$r_1 = a_3 + a_2 + a_1$

$r_2 = a_1 + a_0 + a_3$

ro, r1 and r2 add to the data word, create the code word send to the receiver .At receiver checker check the error existing or not .Receiver generate 3 bit syndrome, syndrome is equal to zero there is no error ,syndrome not equal to zero error present in receiving code

$S_0 = b_2 + b_1 + b_0 + q_0$

$S_1 = b_3 + b_2 + b_1 + q_1$

$S_2 = b_1 + b_0 + b_3 + q_2$

The 3-bit syndrome $S_2S_1S_0$ creates eight different bit patterns (000 to 111) that can represent eight different conditions. These conditions in the following table define an error in 1 of the 7 bits of the received codeword, as shown in Table. None means no error.

Syndrome	000	001	010	011	100	101	110	111
Error	None	q_0	q_1	b_2	q_2	b_0	b_3	b_1

This Hamming code can only correct a single error or detect a double error. However, there is a way to make it detect a burst error.

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.

Cyclic Redundancy Check (CRC)

Widely used in data communication

Example of CRC *C*(7,4). Here 7 is the3 length of codeword and 4 is the length of dataword.

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

Table: A CRC code with C(7, 4)

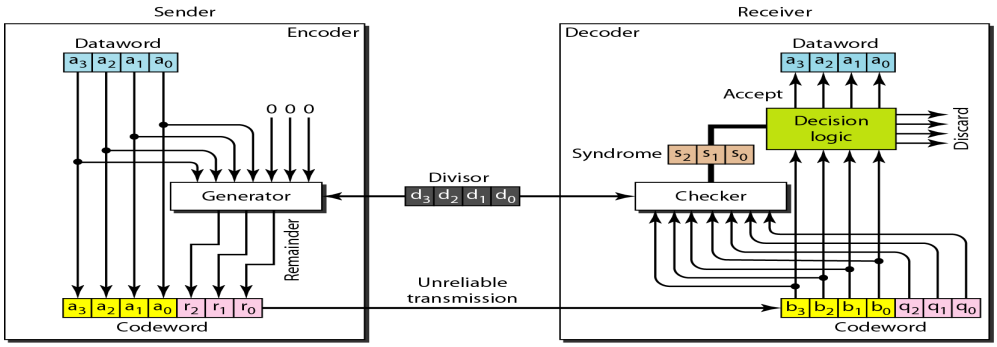


Figure: Sender and receiver

In the encoder, the data word has k bits (4 here); the codeword has n bits (7 here).

The size of the data word is augmented by adding n − k (3 here) 0s to the right-hand side of the word.

Encoder:

The n-bit result is fed into the generator.

The generator uses a divisor of size n − k + 1 (4 here), predefined and agreed upon.

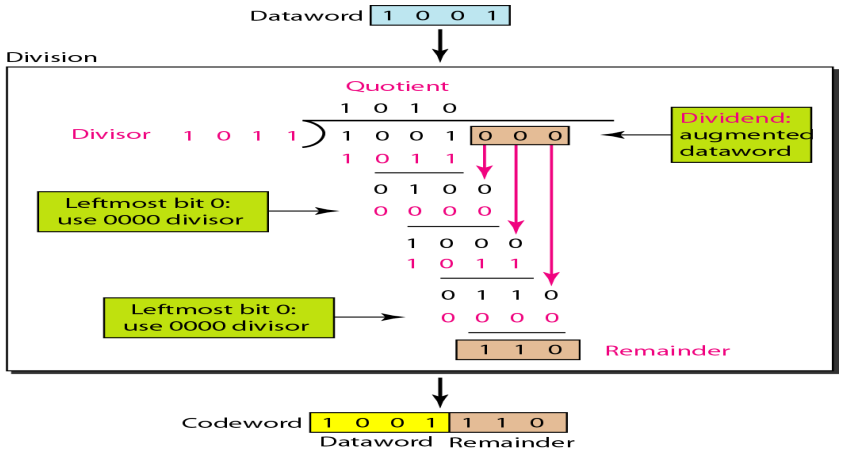
The generator divides (modulo-2 division) the augmented data word by the divisor. The quotient of the division is discarded; the remainder ($r_2r_1r_0$) is appended to the data word to create the codeword.

Decoder:

The decoder receives the codeword. and feeds it to the checker, which is a replica of the generator. The remainder produced by the checker is a syndrome of n − k (3 here) bits,

This remainder is fed to the decision logic analyzer. The analyzer has a simple function. If the syndrome bits are all 0s, the 4 leftmost bits of the codeword are accepted as the data word (interpreted as no error); otherwise, the 4 bits are discarded (error).

Encoder



Division in CRC encoder

Decoder

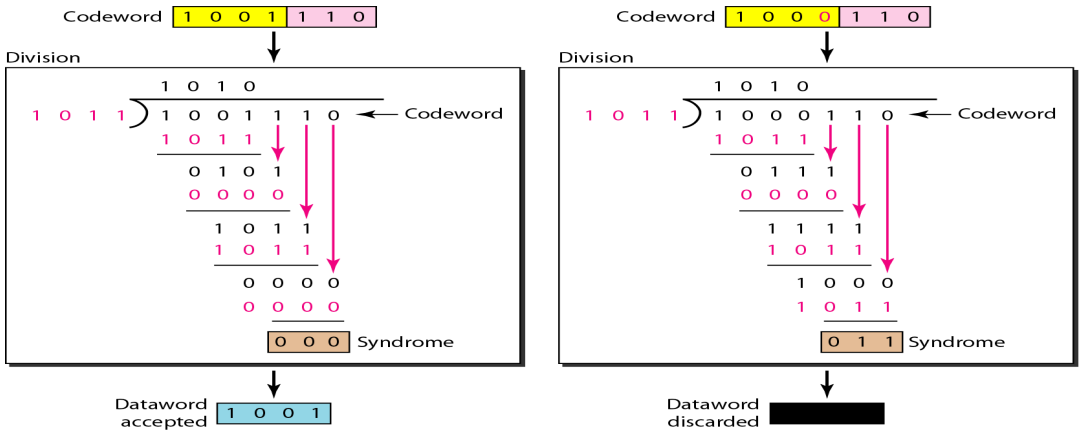


Figure: Division in the CRC decoder for two cases

CHECKSUM

Checksum is an error-detecting technique that can be applied to a message of any length. In the Internet, the checksum technique is mostly used at the network and transport layer rather than the data-link layer.

Checksum is nothing but sum of the transmitting bits.

Example: Suppose we are sending five 4-bit numbers to a destination. In addition to these numbers, we send the sum of the numbers.

Example:

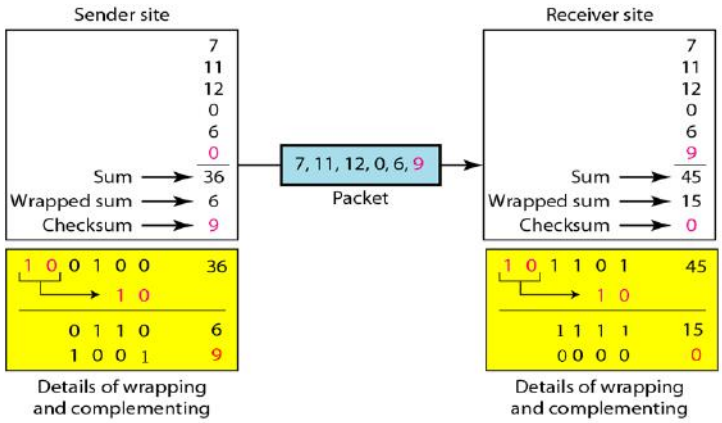
Let the set of numbers is (7, 11, 12, 0, 6). Then we send (7, 11, 12, 0, 6, 36), where 36 is the sum of the original numbers.

The receiver adds the five numbers and compares the result with the sum.

If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum.

Otherwise, there is an error somewhere and the data are not accepted.

Data Link Control



Framing

Frame is a unit of information handled in data link layer. Data is sent in frames. When a message is carried in one very large frame, flow and error control will be very inefficient. Even a single-bit error would require the retransmission of the whole message. When a message is divided into smaller frames, a single-bit error affects only that small frame.

Data-link layer separately adds a sender address and a destination address to each frame in the message. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Frame Size

Frames can be of fixed or variable size.

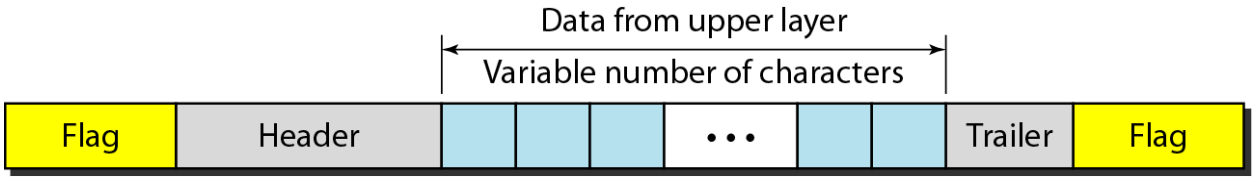
Fixed-size framing: In this, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.

Example: ATM (asynchronous transfer mode) WAN, uses frames of fixed size called cells.

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

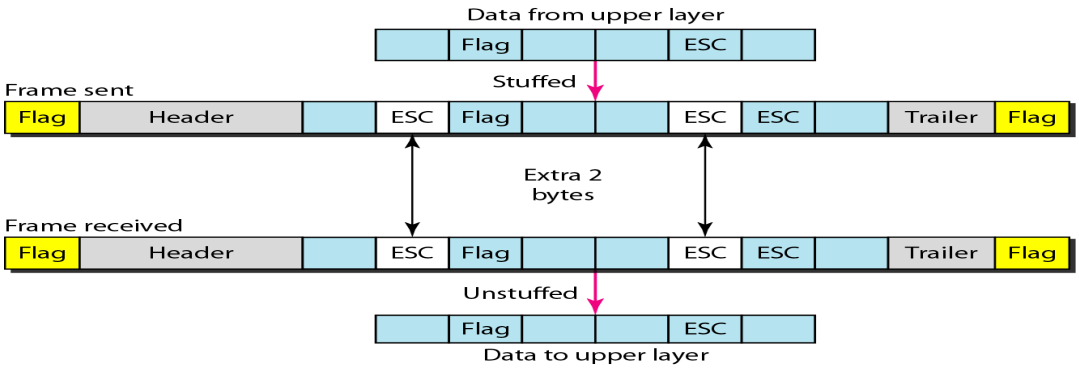
Character-Oriented Framing (or Byte-Oriented) Framing

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



Byte stuffing: In byte stuffing (or character stuffing), the data section is stuffed with an extra byte, i.e., a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. This byte is called “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, but not as a delimiting flag.

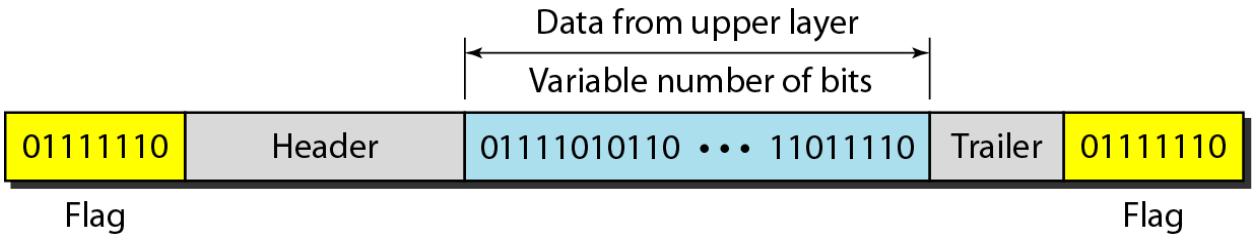
Sometimes a byte may have same pattern as ESC character. Then another ESC character is added before that character.



Thus, Byte stuffing is the process of adding 1 extra byte whenever there is a “flag” or “escape” character in the text.

Bit-Oriented Framing

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



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

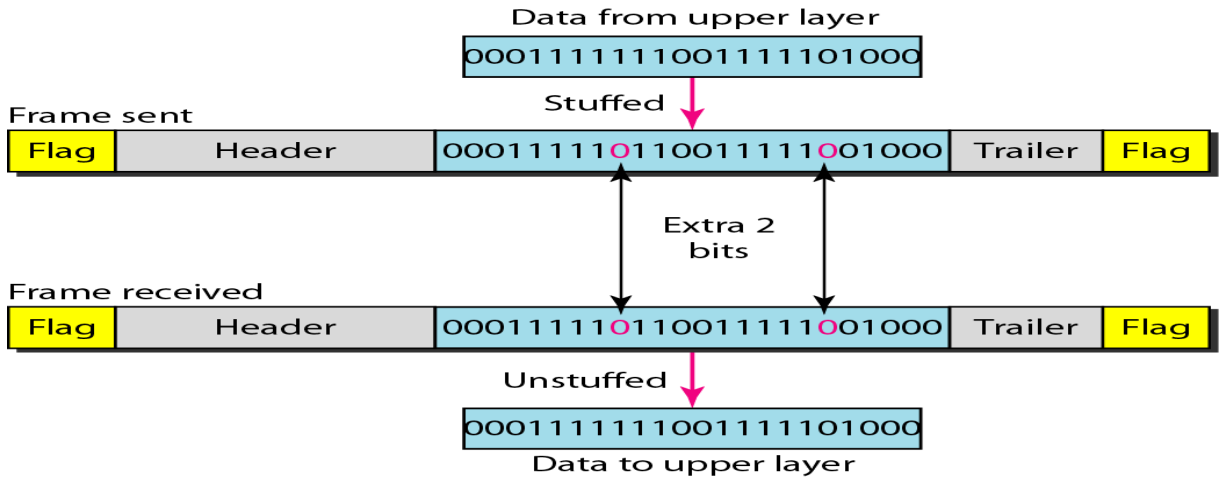


Figure shows bit stuffing at the sender and bit removal at the receiver. Note that even if we have a 0 after five 1s, we still stuff a 0. The 0 will be removed by the receiver. This means that if the flag like pattern 01111110 appears in the data, it will change to 011111010 (stuffed) and is not mistaken for a flag by the receiver. The real flag 01111110 is not stuffed by the sender.

Flow and Error Control

The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control.

Flow Control

Flow control is a set of procedures. It that tells the sender how much data it can transmit and wait for an acknowledgment from the receiver.

Suppose receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.

Then, the receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily.

Error Control

In the data link layer, the term error control refers primarily to methods of error detection and retransmission.

It allows the receiver to inform the sender if any frames lost or damaged in transmission and helps the retransmission of those frames by the sender.

Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

PROTOCOLS

The protocols are normally implemented in software by using one of the common programming languages. To make our discussions language-free, we have written in pseudo code. A pseudo code of each protocol concentrates mostly on the procedure instead of the details of language rules.

Let us consider protocols for noiseless (error-free) channels and then protocols for noisy (error-creating) channels. The protocols for noise-less channels cannot be used in real life, but they serve as a basis for understanding the protocols of noisy channels.

NOISELESS CHANNELS

Let us first assume we have an ideal channel in which no frames are lost, duplicated, or corrupted. We introduce two protocols for this type of channel. The first is a protocol that does not use flow control; the second is the one that does.

1. Simplest Protocol

2. Stop-and-Wait Protocol

1. Simplest Protocol

It is a unidirectional protocol in which data frames are traveling in only one direction-from the sender to receiver. We assume that the receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately.

Design

There is no need for flow control in this scheme. The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it. The data link layer at the receiver site receives a frame from its physical layer, extracts data from the frame, and delivers the data to its network layer. The data link layers of the sender and receiver provide transmission services for their network layers. The data link layers use the services provided by their physical layers (such as signaling, multiplexing, and so on) for the physical transmission of bits. Figure shows a design.

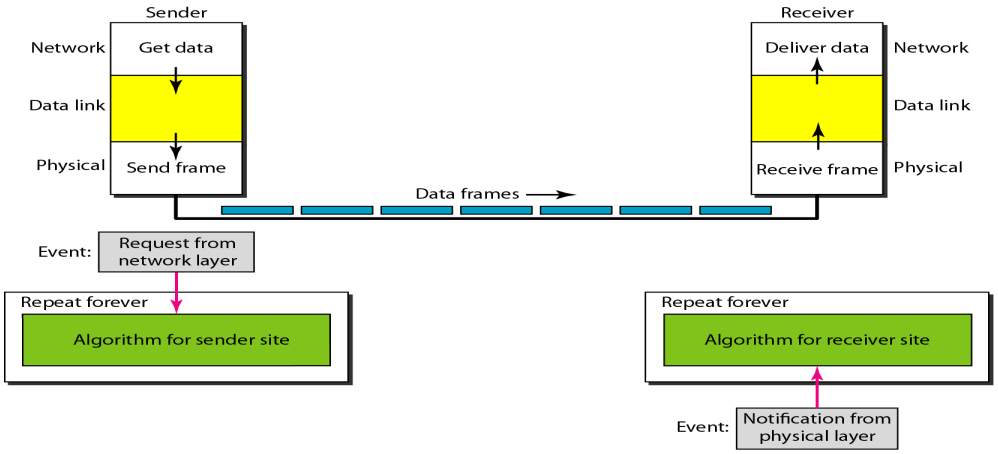
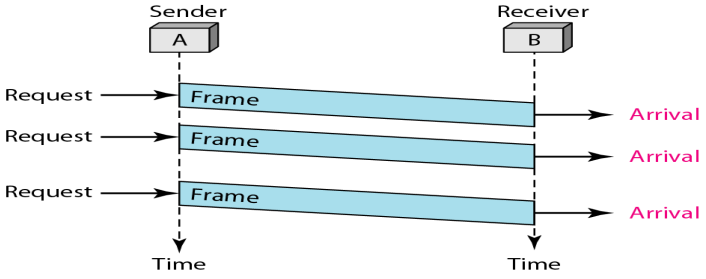


Figure shows an example of communication using this protocol. It is very simple. The sender sends a sequence of frames without even thinking about the receiver. To send three frames, three events occur at the sender site and three events at the receiver site. Note that the data frames are shown by tilted boxes; the height of the box defines the transmission time difference between the first bit and the last bit in the frame.



2. Stop-and-Wait Protocol

The protocol we discuss now is called the Stop-and-Wait Protocol because the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame. We still have unidirectional communication for data frames, but auxiliary ACK frames (simple tokens of acknowledgment) travel from the other direction. We add flow control to our previous protocol.

Design

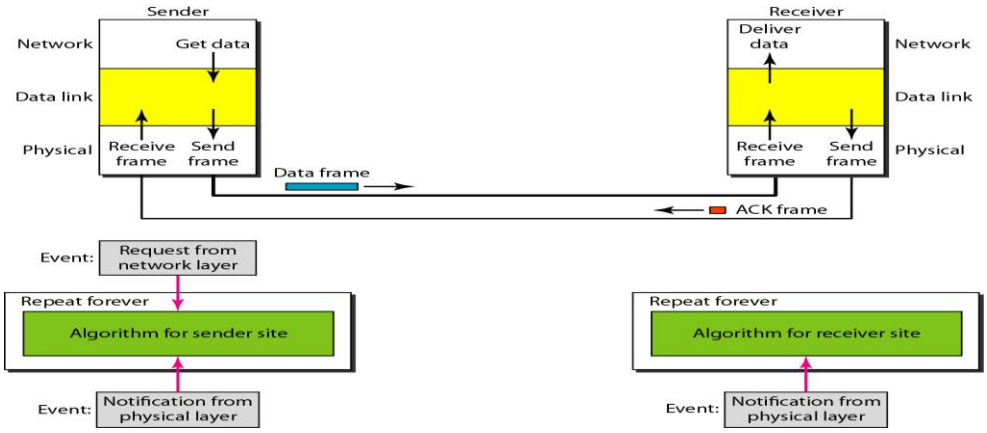
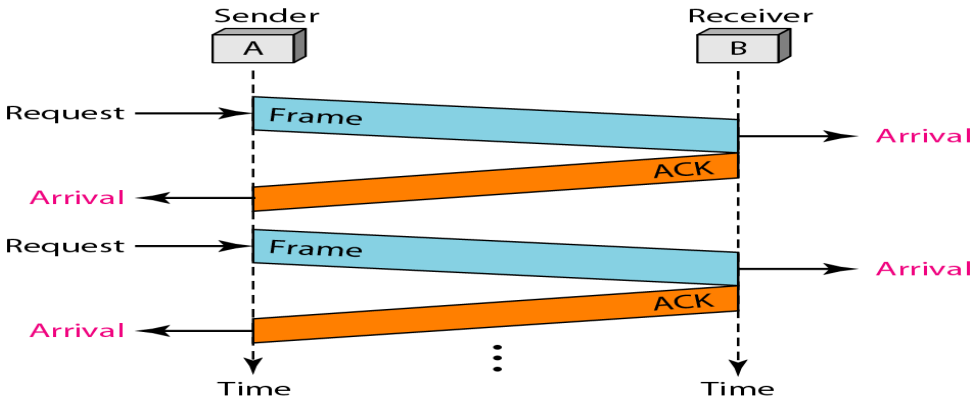


Figure illustrates the mechanism. Comparing this figure with Figure simple protocol, we can see the traffic on the forward channel (from sender to receiver) and the reverse channel. At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel. We therefore need a half-duplex link.

Figure shows an example of communication using this protocol. It is still very simple. The sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame. Note that sending two frames in the protocol involves the sender in four events and the receiver in two events.



NOISY CHANNELS

We discuss three protocols in this section that use error control.

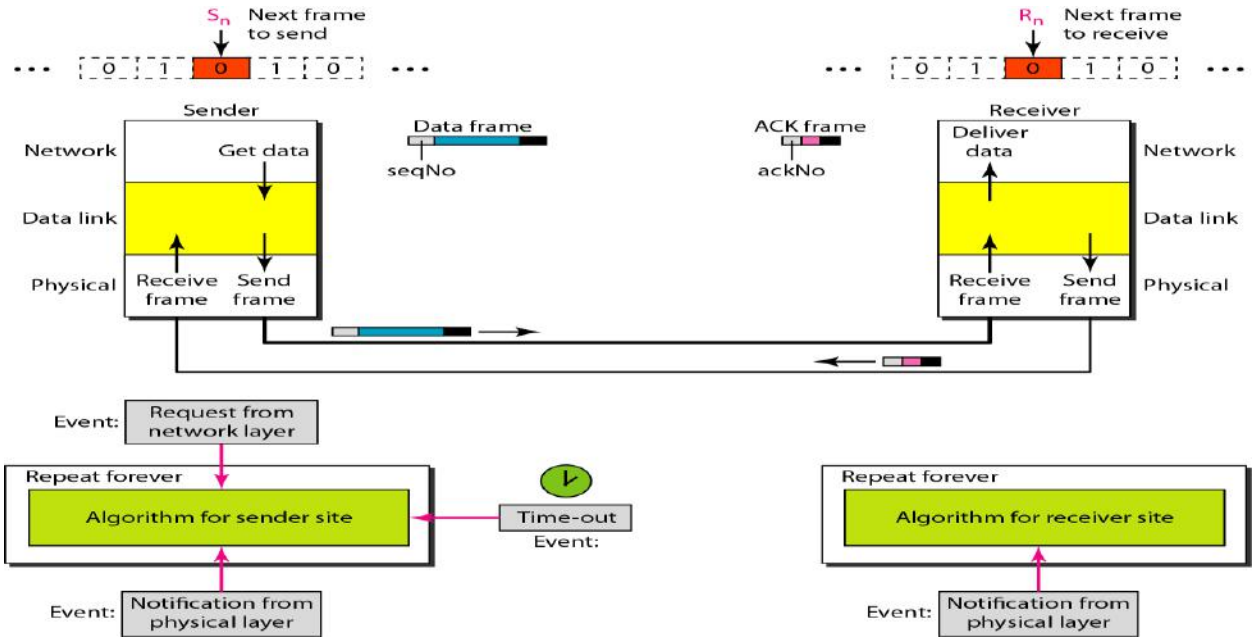
1. Stop-and-Wait Automatic Repeat Request

Our first protocol, called the Stop-and-Wait Automatic Repeat Request (Stop-and Wait ARQ), adds a simple error control mechanism to the Stop-and-Wait Protocol. Let us see how this protocol detects and corrects errors.

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.

Design

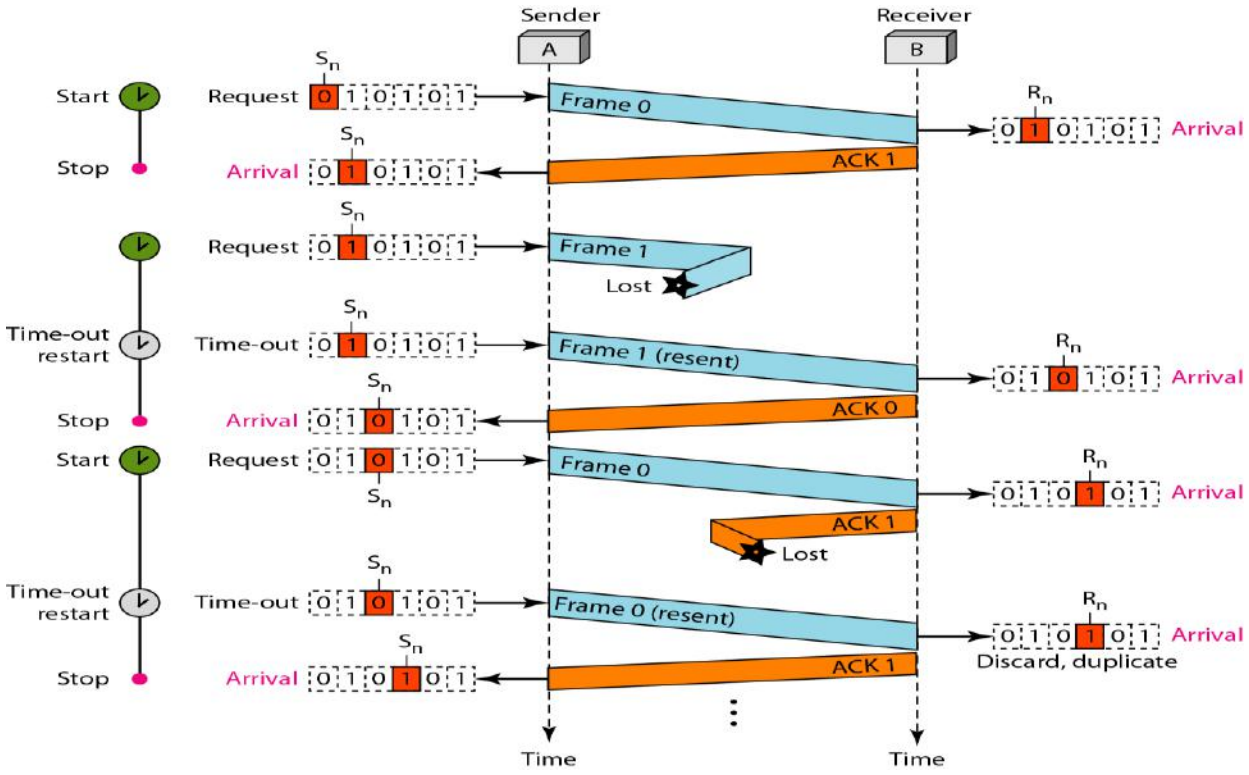
Figure shows the design of the Stop-and-Wait ARQ Protocol. The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame. A data frames uses a seq No (sequence number); an ACK frame uses an ack No (acknowledgment number). The sender has a control variable, which we call S_n (sender, next frame to send), that holds the sequence number for the next frame to be sent (0 or 1).



The receiver has a control variable, which we call Rn (receiver, next frame expected), that holds the number of the next frame expected

Figure shows an example of Stop-and-Wait ARQ. Frame 0 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 ARQ:

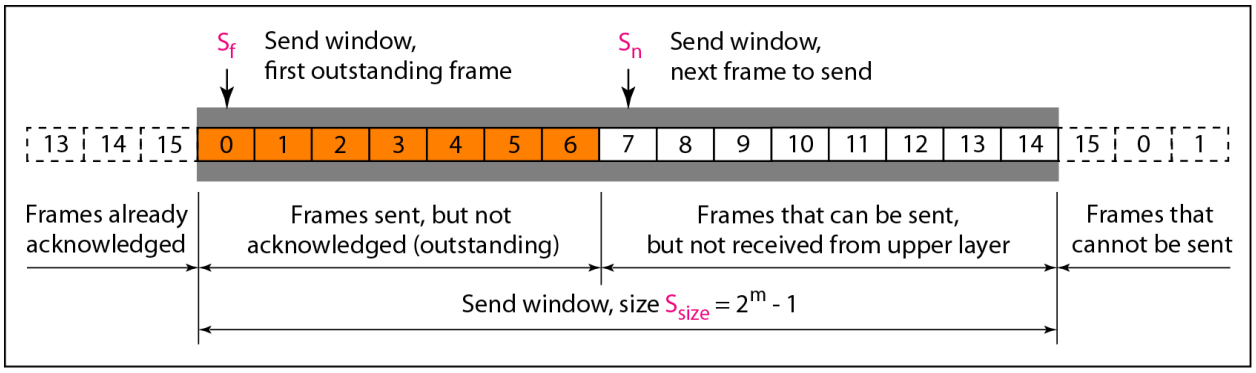
In the Go-Back-N Protocol, the sequence numbers are modulo 2^m, where m is the size of the 'sequence number field' in bits. sequence number is available in the header of the frame.

Sequence Numbers

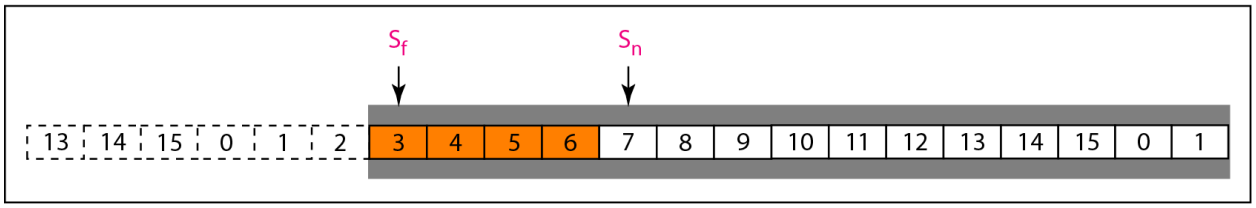
If there are 'm' bits in the sequence number, the sequence numbers range from 0 to $2^m - 1$. For example, if m is 4, the only sequence numbers are 0 through 15 inclusive. However, we can repeat the sequence. So, the sequence numbers are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ...

Send Window: It is a sliding window.

Figure shows a sliding window of size 15 (m =4). Four regions are shown in the figure.



a. Send window before sliding



b. Send window after sliding

The first region: It is from the far left to the left wall of the window. It defines the sequence numbers of frames that are already acknowledged. The sender does not worry about these frames. No need to maintain their copies.

The second region: It is shown colored. It defines the sequence numbers of frames that are sent and status is not known. The sender needs to wait to find out whether these frames were received or lost. These frames are called ‘outstanding frames’.

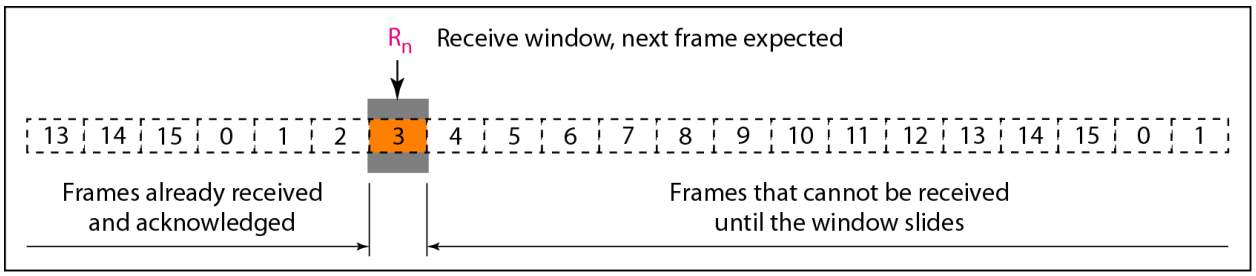
The third range: It is shown white in the figure. It defines the range of sequence numbers for frames that can be sent; however, the corresponding data packets have not yet been received from the network layer.

The fourth region: It defines sequence numbers that cannot be used until the window slides.

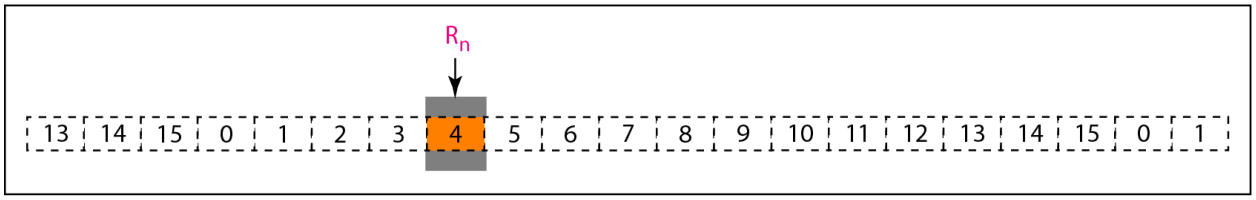
The send window is an abstract concept. It defines an imaginary box of size $2^m - 1$ with three variables: S_f, S_n, and S_{size}.

Send window can slide ‘one or more slots’ when a valid acknowledgment arrives.

Receive window:



a. Receive window



b. Window after sliding

The receive window also slides, but only one slot at a time. When a correct frame is received (and a frame is received only one at a time), the window slides.

The receive window is an abstract concept defining an imaginary box of size 1 with one single variable Rn.

Receive window slides when a correct frame has arrived; sliding occurs one slot at a time

Timers

There can be a timer for each frame that is sent. Here, we use only one in our protocol. The reason is that the timer for the first outstanding frame always expires first and then we send all outstanding frames.

Acknowledgment

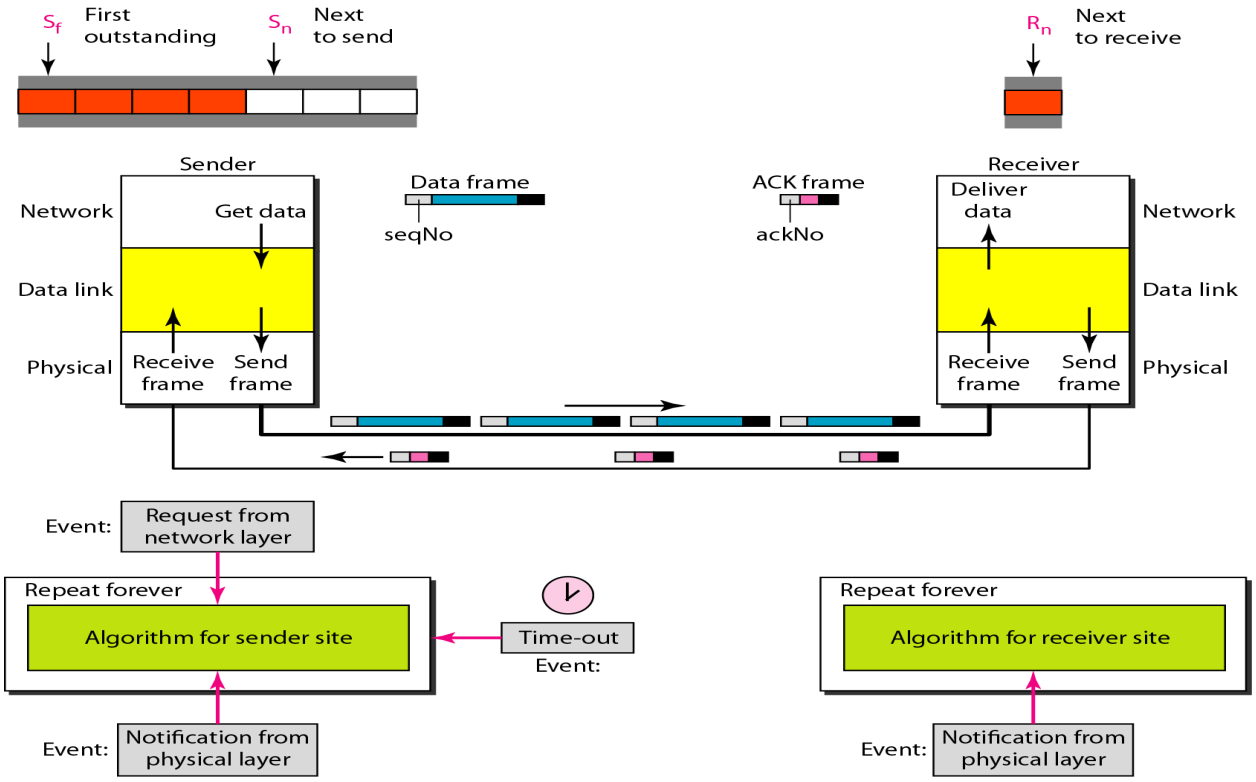
The receiver sends a positive acknowledgment if a frame has arrived safe and in order. If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives the one it is expecting.

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.

Design:

Figure shows the design for this protocol.



As we can see, multiple frames can be in transit (move) in the forward direction, and multiple acknowledgments in the reverse direction. The idea is similar to Stop-and-Wait ARQ; the difference is that the send window allows multiple frames. Their number is equal to the slots in the send window.

3. Selective Repeat ARQ

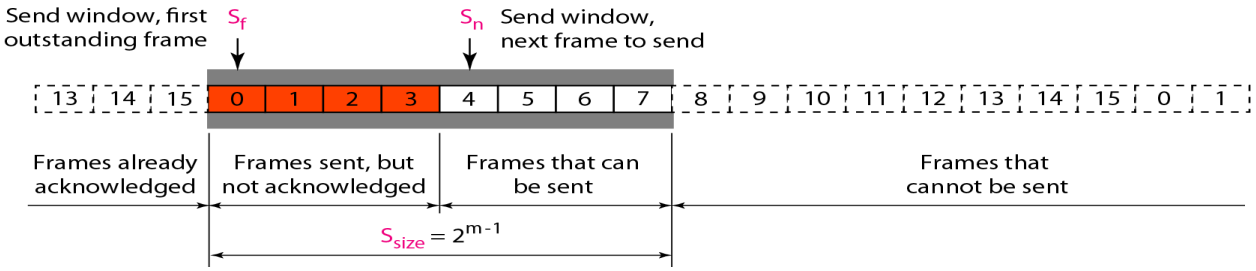
This protocol does not resend N frames when just one frame is damaged; only the damaged frame is resent. This mechanism is called Selective Repeat ARQ. It is more efficient for noisy links, but the processing at the receiver is more complex.

Windows

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

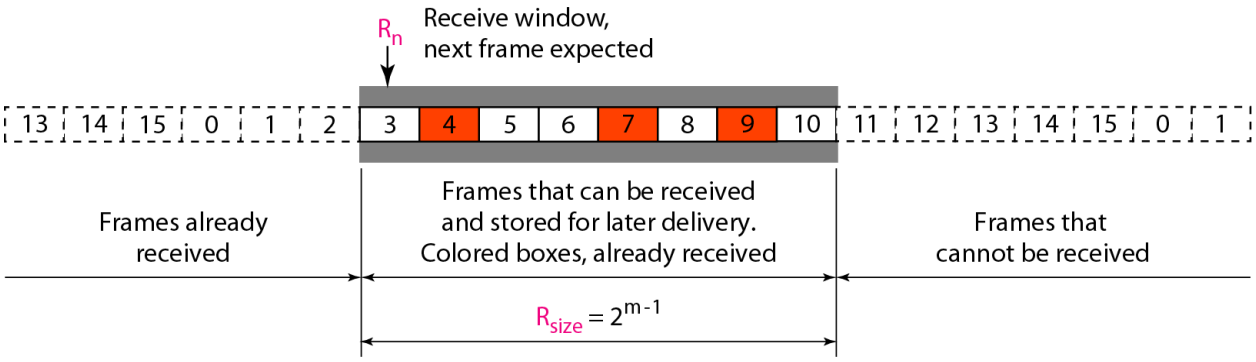
The size of the sender and receiver window are equal. This size must be at most one-half of 2^m. where m is the size of sequence number. For example, if m = 4, the sequence numbers go from 0 to 15, but the size of the window is just 8. The smaller window size means less efficiency in filling the pipe But there are fewer duplicate frames.

Send window:



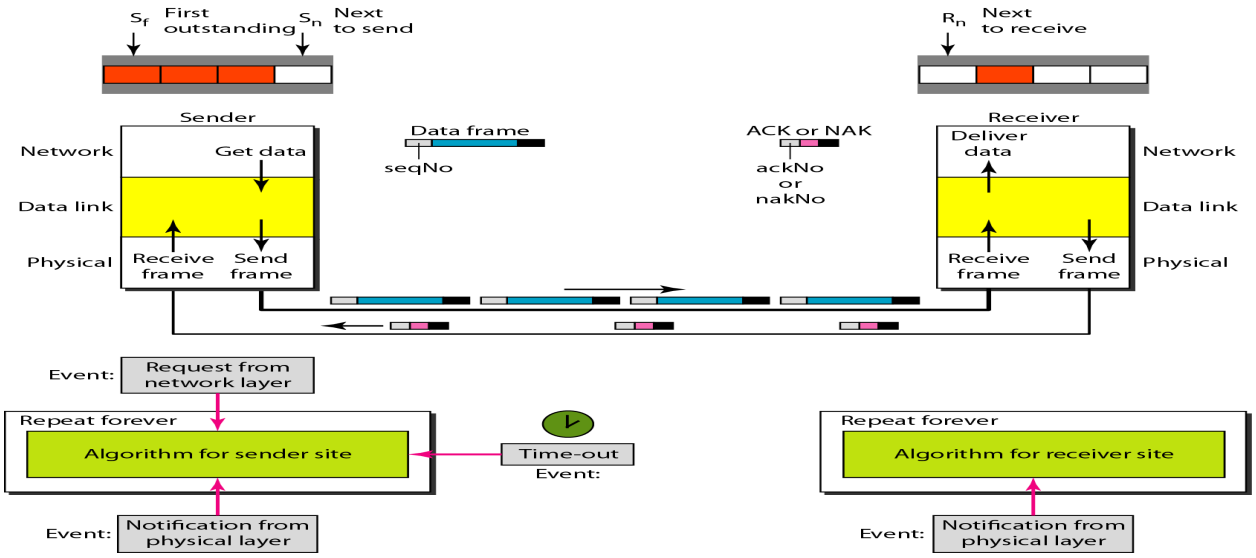
Receive window:

The receive window in Selective Repeat is totally different from the one in Go Back-N. First, the size of the receive window is the same as the size of the send window. The Selective Repeat Protocol allows as many frames as the size of the receive window. It allows them to arrive out of order and be kept until other frames come. Then the frames are delivered in-order to the network layer. Figure shows the receive window in this protocol. Those slots inside the window that are colored define frames that have arrived out of order and are waiting for their neighbors to arrive before delivery to the network layer.



Design

The design in this case is nearly similar to design of Go Back-N, but more complicated, as shown in Figure 11.20.



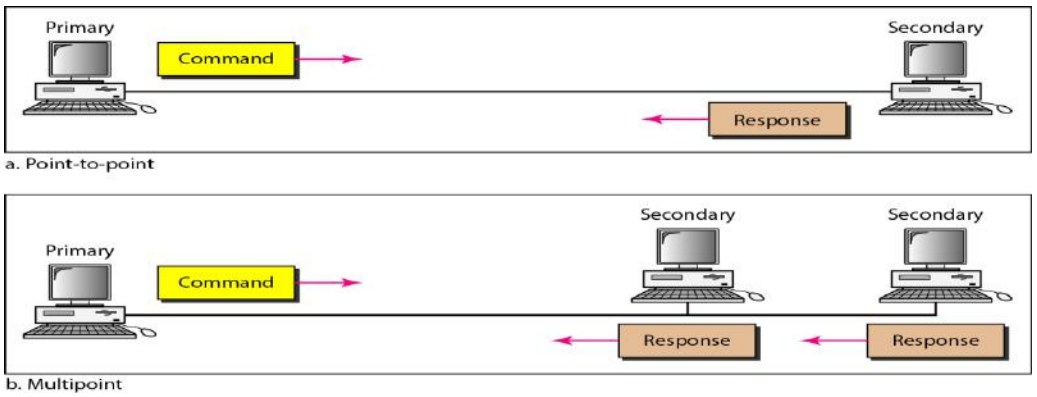
HDLC PROTOCOL

High-level Data Link Control (HDLC) is a bit-oriented protocol used for point-to-point and multipoint configurations. It implements the ARQ mechanism.

Transfer Modes and Configurations:

HDLC provides two common transfer modes: normal response mode (NRM) and asynchronous balanced mode (ABM).

1. Normal response mode (NRM): Here, the station configuration is unbalanced. We have one primary station and multiple secondary stations. A primary station can only send commands; a secondary station can only respond. The NRM is used for both point-to-point and multiple-point links, as shown in Figure.



NORMAL RESPONSE MODE

This is the common mode used today. In this mode, the station configuration is balanced. The link is point-to-point, and each station can function as a primary as well as a secondary (acting as peers), as shown in figure.

Asynchronous Balanced Mode (ABM):

HDLC Frames

HDLC defines three types of frames: information frames (I-frames), supervisory frames (S-frames), and unnumbered frames (U-frames). Each type of frame is used for the transmitting a different type of message.

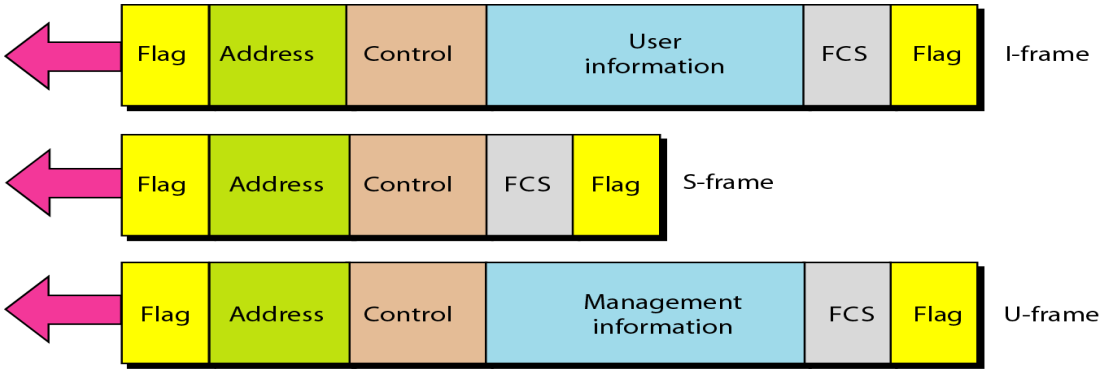
I-frames are used to transport user data and control information related to user data (piggybacking).

S-frames are used only to transport control information.

U-frames are reserved for system management. Information carried by U-frames is intended for managing the link itself.

Frame Format

Each frame in HDLC may contain up to six fields, as shown in Figure.



Flag field: It is an 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame and serves as a synchronization pattern for the receiver. The ending flag of one frame can serve as the beginning flag of the next frame.

Address field: It is 1 byte or several bytes long, depending on the needs of the network. It contains the address of the secondary station.

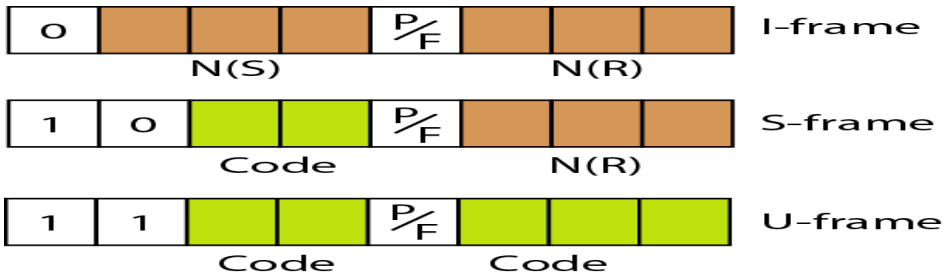
Control field. It is a 1- or 2-byte segment of the frame used for flow and error control. It is further explained in the next section.

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) acts as error detection field. It can contain either a 2-byte or 4-byte ITU-T CRC. (ITU-T stands for International Telecommunication Union-Telecommunication Standardization Sector and CRC stands for cyclic redundancy code.)

Control Field in a HDLC frame

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



1. Control Field for I-Frames

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

The P/F field: It is a single bit with a dual purpose. It has meaning only when it is set (bit = 1) and can mean poll or final.

It means poll when the frame is sent by a primary station to a secondary, i.e., the address field of frame contains the address of the receiver.

It means final when the frame is sent by a secondary to a primary, i.e., when the address field contains the address of the sender.

2. Control Field for S-Frames

S-frames do not have information fields. If the first 2 bits of the control field is 10, this means the frame is an S-frame. The last 3 bits, called N(R), corresponds to the acknowledgment number (ACK) or negative acknowledgment number (NAK) depending on the type of S-frame. The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames as described below.

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

Receive not ready (RNR). If the code subfield is 10, it is an RNR S-frame. It acknowledges the receipt of a frame or group of frames, and it announces that the receiver is busy and cannot receive more frames. It acts as a kind of congestion control mechanism by asking the sender to slow down.

Reject (REJ). If the value of the code subfield is 01, it is a REJ S-frame. This is a NAK (negative acknowledgment or not acknowledged) frame used in Go-Back-N ARQ to improve the efficiency of the process. It informs the sender (before the sender time expires) that the last frame is lost or damaged. The value of N(R) is the negative acknowledgment number.

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

3. Control Field for U-Frames

Unnumbered frames are used to exchange session management and control information between connected devices. U-frames contain an information field that contains system management information. As in S-frames, however, much of the information carried by U-frames is contained in codes included in the control field. 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.

Examples:

Code	Command	Response	Meaning
00 001	SNRM		Set normal response mode
11 000	SABM	DM	Set asynchronous balance mode or disconnect mode
11 001	RSET		Reset
10 001	FRMR	FRMR	Frame Reject

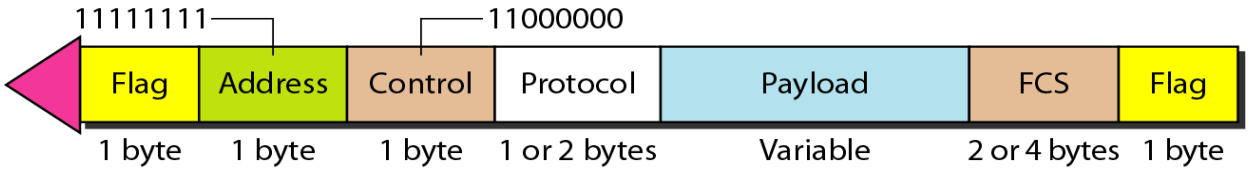
POINT-TO-POINT PROTOCOL (PPP)

HDLC is a general protocol that can be used for both point-to-point and multipoint configurations. Point-to-Point Protocol (PPP) is one of the most common protocols used for point-to-point configuration. PPP is a byte-oriented protocol

Services provided by PPP:

1. PPP defines the format of the frame to be exchanged between devices.
2. It defines how two devices can negotiate the establishment of the link and the exchange of data.
3. It defines how network layer data are encapsulated in the data link frame.
4. It defines how two devices can authenticate each other.
5. It provides multiple network layer services supporting a variety of network layer protocols.
6. It provides connections over multiple links.
7. It provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

Frame Format



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). During negotiation (discussed later), the two parties may agree to omit this byte.

Control. This field is set to the constant value 11000000. PPP does not provide any flow control. Error control is also limited to error detection.

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

Payload field. This field carries either the user data or other information.

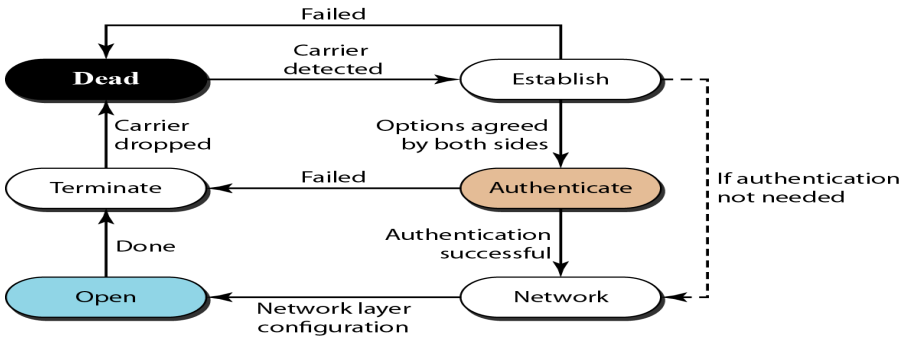
FCS. The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC

Byte Stuffing

PPP is a byte-oriented protocol using byte stuffing with the escape byte 01111101.

Transition Phases

A PPP connection goes through phases which can be shown in a transition phase diagram



Dead: In the dead phase the link is not being used. There is no active carrier (at the physical layer) and the line is quiet.

Establish: When one of the nodes starts the communication, the connection goes into this phase. In this phase, options are negotiated between the two parties. If the negotiation is successful, the system goes to the authentication phase (if authentication is required) or directly to the networking phase.

Authenticate: The authentication phase is optional; the two nodes may decide, during the establishment phase, not to skip this phase. However, if they decide to proceed with authentication, they send several authentication packets. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.

Network: In the network phase, negotiation for the network layer protocols takes place. PPP specifies that two nodes establish a network layer agreement before data at the network layer can be exchanged. The reason is that PPP supports multiple protocols at the network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.

Open: In the open phase, data transfer takes place. When a connection reaches this phase, the exchange of data packets can be started. The connection remains in this phase until one of the endpoints wants to terminate the connection.

Terminate: In the termination phase the connection is terminated. Several packets are exchanged between the two ends for house cleaning and closing the link.

UNIT-III
MULTIPLE ACCESS

Syllabus Contents: Random access and Multiple access, Random access protocols: CSMA, CSMA/CD, CSMA/CA, Controlled Access, Channelization, Wired LANs: IEEE Standards, Standard Ethernet, Fast Ethernet, Gigabit Ethernet, Wireless LAN, IEEE 802.11, Bluetooth IEEE 802.15, WiMAX 802.16

Multiple Access

Multiple access is a method which allows a number of nodes or users to access a shared network channel. In other words, multiple users can access and use the channel simultaneously. A network channel that allows multiple access is called multiple access channel. Multiple access protocols are a set of protocols used to coordinate multiple access. These protocols operate in the Medium access control (MAC) sublayer. multiple access is achieved by using the popular schemes used in multiple access are FDMA, TDMA and CDMA.

Random Access

Random access method is an access method in which any memory location can be accessed directly rather than being accessed sequentially. In a Random-access protocol, all stations have same superiority. Any station can send data at any time, based on medium status (idle or busy). Random access protocols classified as ALOHA, CSMA, CSMA/CD, and CSMA/CA protocols. A random access channel (RACH) is popularly used by GSM mobiles for transmission over cellular networks.

Multiple Access Protocols:

These protocols are categorized into three groups, as shown in Fig.1.

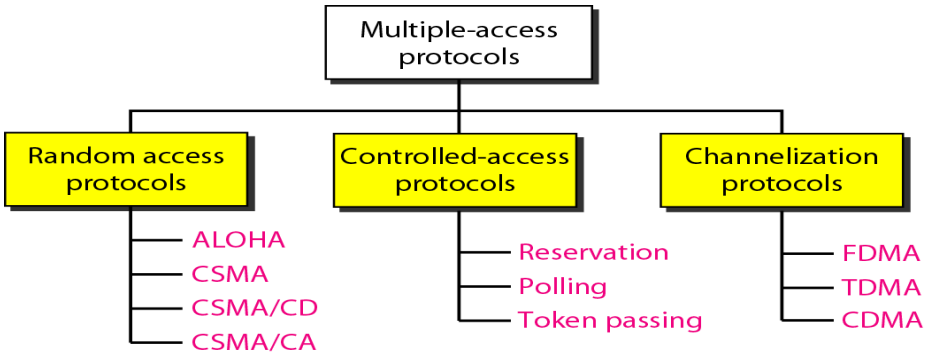


Fig.1: Multiple Access Protocols

1. ALOHA

ALOHA is the protocol developed at the University of Hawaii in 1970s. It is also called ALOHAnet or ALOHA System. It was designed for a radio (wireless) LAN, but it can be used on any shared medium. It uses the multiple access procedure. ALOHA has two versions: Pure ALOHA (original version) and Slotted ALOHA (modified version).

Pure ALOHA

In this, each station can send a frame at any time. It allows multiple access. However, there is only one channel and different stations use this channel to share frames. So, there is the possibility of collision among frames.

Example: Fig.2 shows an example of frame collisions in pure ALOHA.

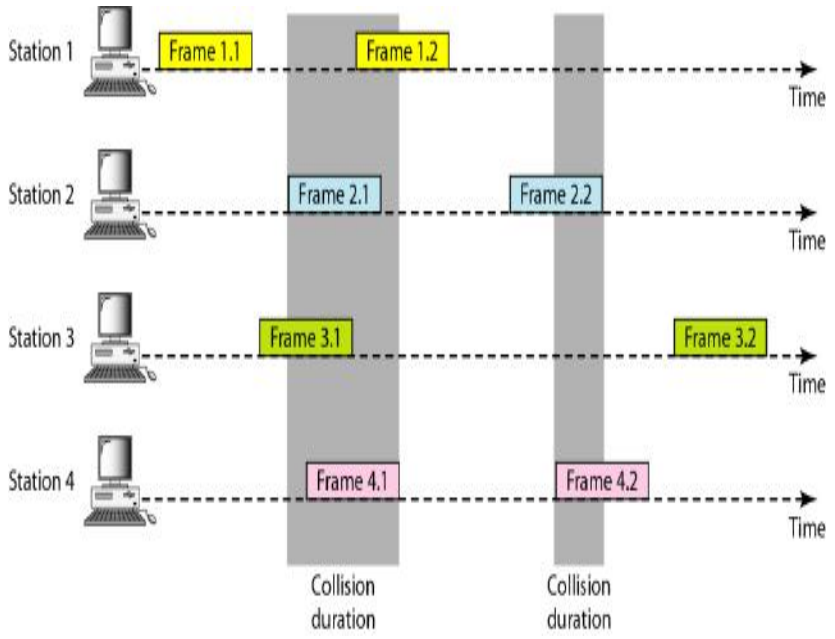


Fig.2: Frame collisions in pure ALOHA

There are four stations with shared channel. Each station sends two frames. Thus, totally there are 8 frames on the channel. Some of these frames collide because multiple frames are in contention for the shared channel. In this example, only two frames survived: one frame from station 1 and one frame from station 3.

When a station sends data it waits for an acknowledgement. If the acknowledgment does not arrive after a time-out period, then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Thus, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the backoff time (T_B). After maximum number of attempts (normally 15), it will terminate.

Vulnerable time

Let us find the vulnerable time is the length of time in which there is a possibility of collision. In other words, it is the time during which no transmission should be done to avoid any collision. Let G be the number of transmission attempts per frame time. Let the stations send fixed-length frames with each frame taking T_{fr} seconds to send. Fig.3 shows collisions in pure ALOHA protocol

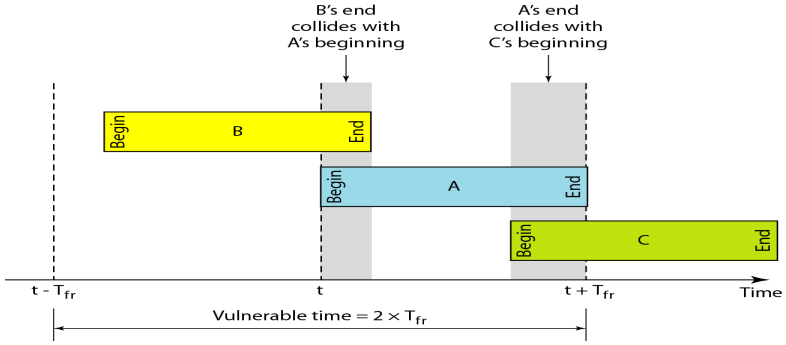


Fig.3: Frame collisions in pure ALOHA

Vulnerable Time in pure ALOHA= 2* T_{fr}

Throughput

Throughput is the average number of successfully transmitted frames. for pure Let G be the average number of frames generated by the system during one frame transmission time. i.e., G is the number of transmission attempts per frame time. Then, throughput 'S' for pure ALOHA is

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

Maximum throughput $S_{max} = 0.184$ for G = 1/2 (i.e., if one frame is sent during two frame transmission times)

Slotted ALOHA

It is similar to pure aloha, except that we divide time into slots of T_{fr} seconds and the transmission is allowed only at the beginning of a time slot. If a station misses this moment. it must wait until the beginning of the next slot. This means that the station which started at the beginning of this slot has already finished sending its frame. This reduces the probability of collision. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half.

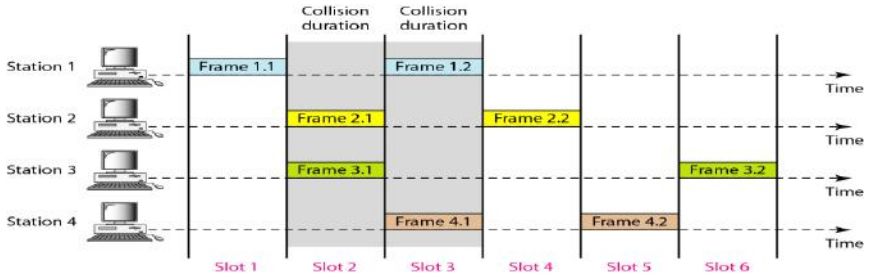


Fig.4: Frame collisions in slotted ALOHA

Vulnerable Time of slotted ALOHA = T_{fr} (where T_{fr} is the frame transmission time)
Throughput for slotted ALOHA is $S = G \times e^{-G}$
The maximum throughput S_{max} is 0.368, when G =1. (i.e., if one frame is sent during one frame transmission times)

2. CSMA (Carrier Sense Multiple Access)

Collision can be reduced if a station senses the medium before using it. CSMA method was developed to minimize the chance of collisions. CSMA is based on the principle "sense before transmit" or "listen before talk." Here, each station first listens to the medium (i.e., check the state of the medium) before trying to use it. Thus, CSMA can reduce the possibility of collision.

Example: At time t1, station B senses the medium and finds it idle, so it sends a frame. At time t2 (t2 > t1), 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.
The vulnerable time for CSMA is the propagation time Tp. 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.
Persistence Methods

Three methods have been devised to answer the questions: What should a station do if the channel is busy? What should a station do if the channel is idle? They are called persistence methods. They are: the 1-persistent method, the non-persistent method, and the p-persistent method.

1-Persistent Method

The 1-persistent method is simple and straightforward. In this method, If the station finds the line idle, it sends its frame immediately (with probability 1). If channel is busy, the station waits until it become idle. This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately. Vulnerable Time

Non persistent Method

In the non-persistent 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.

p-Persistent Method

Here channel has time slots. Duration of each slot is ≥ 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:

With probability p, the station sends its frame.

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.

Fig. shows the behavior of three persistence methods when a station finds a channel busy.

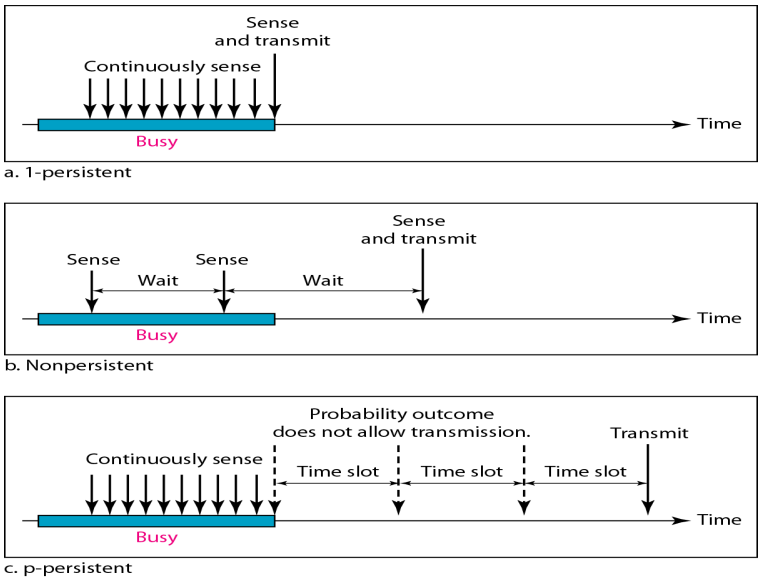


Fig.5: Persistent methods

3. CSMA/CD (Carrier Sense Multiple Access With Collision Detection)

Simple CSMA method does not specify the procedure following a collision. CSMA/CD augments the algorithm to handle the collision. CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.
In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If transmission is not successful (i.e., there is a collision), the frame is sent again.

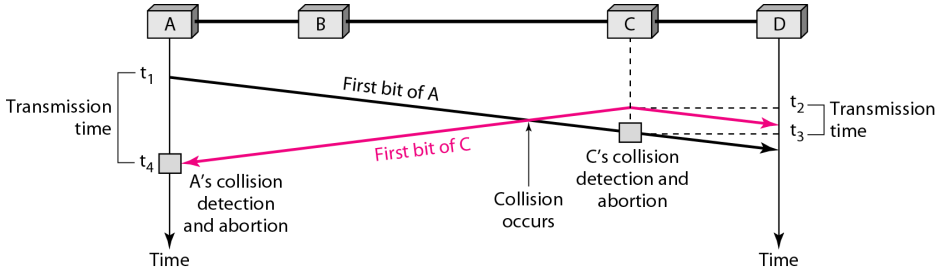


Fig.6: Collision of the first bit in CSMA/CD

At time t1, station A has executed its persistence procedure and starts sending the bits of its frame. At time t2, 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 sometime after time t2. Station C detects a collision at time t3 when it receives the first bit of A's frame. Station C immediately aborts transmission. Station A detects collision at time t4 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 t4 -t1; C transmits for the duration t3 -t2.
To avoid the collision, frame transmission time T_{fr} must be at least two times the maximum propagation time T_P

Energy Level of channel
The level of energy in a channel can have three values: zero, normal, and abnormal. At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame. At the abnormal level, there is a collision and the level of the energy is twice the normal level.
A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode.

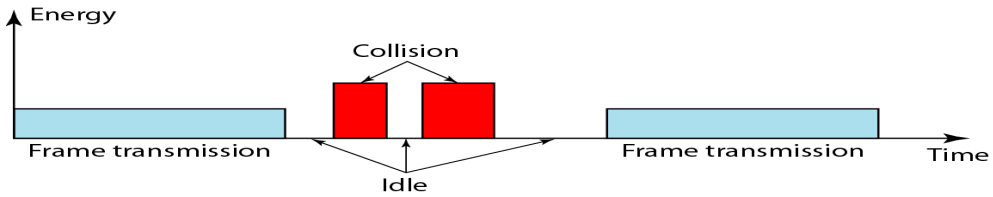


Fig.7: Energy Level of channel

Throughput
The throughput of CSMA/CD is greater than that of pure or slotted ALOHA.
The maximum throughput occurs at a different value of G and is based on the persistence method and the value of p in the p-persistent approach.
For 1-persistent method throughput is 50% when G=1.
For non-persistent method throughput can go up to 90%.

4. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

CSMA/CA was invented for wireless networks. Collisions are avoided through the use of its three strategies: the inter frame space, the contention window, and acknowledgments, as shown in Figure.

Inter frame Space (IFS). First, collisions are avoided by deferring (postponing) transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the inter frame space or IFS.

Contention Window. The contention window is time interval 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 back off strategy.

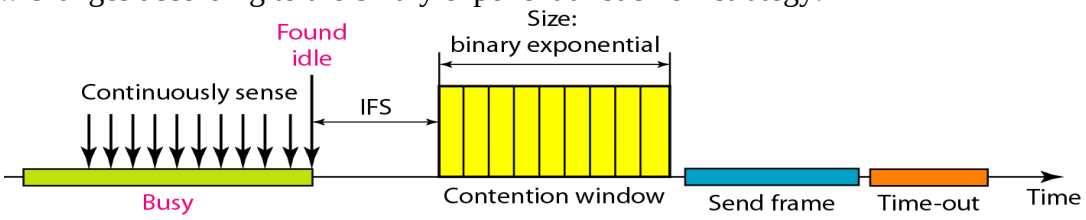


Fig.8: Timing in CSMA/CA

Acknowledgment: Even with all these precautions, a collision may occur resulting in destroyed data. 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.

CSMA/CA Procedure:

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

a. The channel uses a persistence strategy with backoff until the channel is idle.

b. 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). The time interval that a station should wait before it sends its request frame is known as DCF Interframe Spacing (DIFS). DISF is calculated as the sum of SISF and twice the slot time.

2. After receiving the RTS, the destination station waits for a period of time called the short interframe space (SIFS). SIFS is the amount of time required for processing a received frame and to respond with a response frame.

After waiting for SIFS, destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame CTS indicates that the destination station is ready to receive data

3. The source station sends data after waiting an amount of time equal to SIFS.

4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.

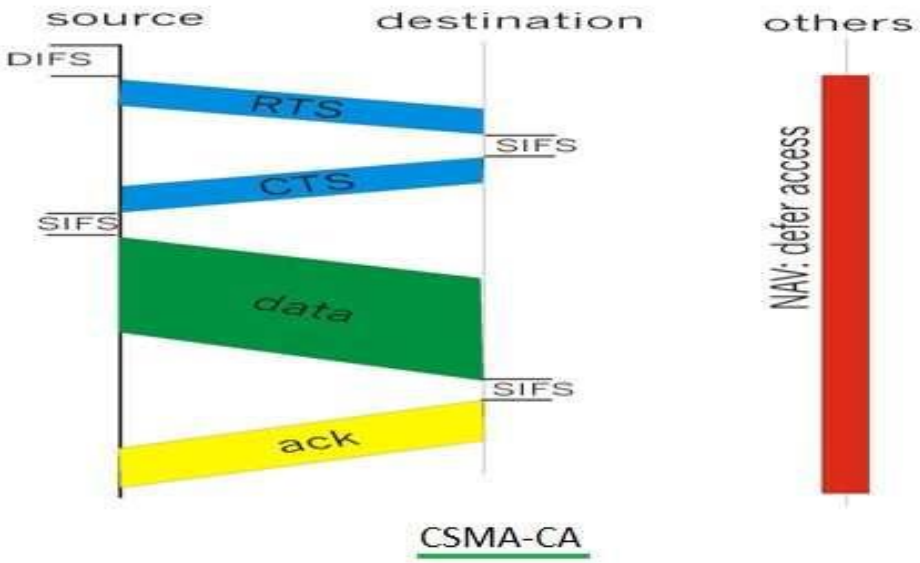


Fig.9: Frames in CSMA/CA

Abbreviations used:
IFS: Inter Frame Space.
SIFS: short interframe space
DIFS: Distributed Coordination Function Inter Frame Space.

Table: 1: Comparison of CSMA/CD and CSMA/CA

S. No.	**CSMA/CD**	**CSMA/CA**
1	CSMA / CD is effective after a collision	CSMA / CA is effective before a collision
2	CSMA / CD is used in wired networks	CSMA / CA is commonly used in wireless networks
3	CSMA / CD reduces the recovery time	Whereas CSMA/ CA minimizes the risk of collision
4	CSMA / CD is used in 802.3 standard	CSMA / CA is used in 802.11 standard
5	More efficient than simple CSMA	similar to simple CSMA

CONTROLLED ACCESS

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. There are 3 popular controlled access methods

1. Reservation

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval. Figure shows a situation with five stations and a five-mini slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

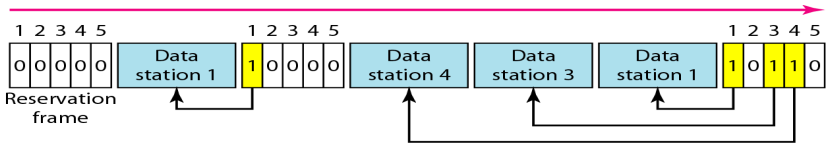


Fig.10: Reservation frames

2. Polling

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges are done through the primary device. The primary device controls the link; the secondary devices follow its instructions. This method uses poll and select functions to prevent collisions.

Select:

The 'select' function is used whenever the primary device has something to send to a secondary device. Before sending data, the primary device creates and transmits a select (SEL) frame. SEL frame has an address field containing address of the intended secondary device.

Poll:

The poll function is used when transmission is from the secondary devices. Here,
the primary asks (polls) each secondary in turn to check if there is data to be sent.
Let the first secondary is approached.
If the secondary has data it responds with the data frame. The primary reads the frame and returns an acknowledgment (ACK frame) to the first secondary.
If the secondary has no data, it responds with NAK frame.
Then the primary polls second secondary device and procedure repeats until last secondary device.

3. Token Passing

Here, the stations in a network are organized in a logical ring. In other words, for each station, there is a 'predecessor' and a 'successor'.
Predecessor: It is the station which is logically before the station in the ring.
Successor: It is the station which is after the station in the ring.
Current station: It is the station that is accessing the channel now.
The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.
A special packet called a token circulates through the ring. This token gives a station the right to access the channel and send its data. When a station has some data to send, it waits to receive token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the token to the next station.
Fig.11 shows four different physical topologies that can create a logical ring.

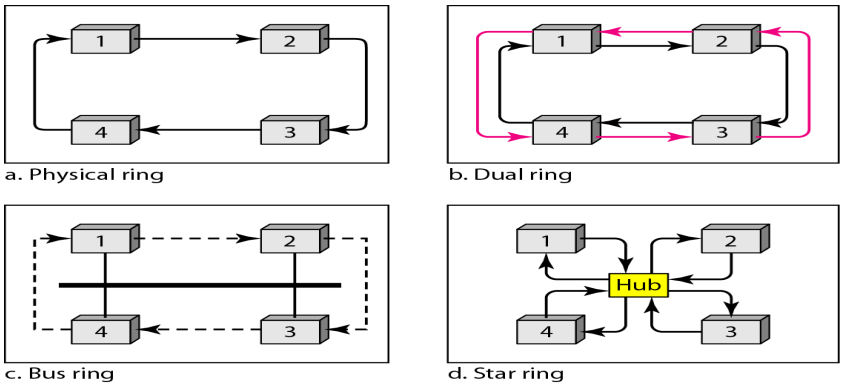


Fig.11: Four physical topologies that can create a logical ring.

Physical ring topology: It does not have successor address. It just treats next station as successor. If one link between two adjacent station fails, the whole system fails.
The dual ring topology: It uses a second (auxiliary) ring for emergency purposes. It operates in the reverse direction compared with the main ring. When normal situation is resumed, the auxiliary ring becomes idle again. Here, each station needs two transmitter ports and two receiver ports.
Bus ring topology (also called a token bus): In this, the stations are connected to a single cable called a bus. They, however, make a logical ring, because each station knows the addresses of its successor predecessor. Suppose a station has finished sending its data. Then it inserts the address of its successor in the token and releases it.
Star ring topology. Here, the stations are connected through a hub in a star fashion. It is less prone to failures. If a link goes down, it will be bypassed by the hub and the rest of the stations can operate. Moreover, adding and removing stations from the ring is easier.

CHANNELIZATION

Channelization (or channel partition) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations. There are three important channelization protocols: FDMA, TDMA, and CDMA.

1. FDMA

In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. In other words, each station is allocated a band to send its data. Each station also uses a bandpass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands. Fig. shows the idea of FDMA.

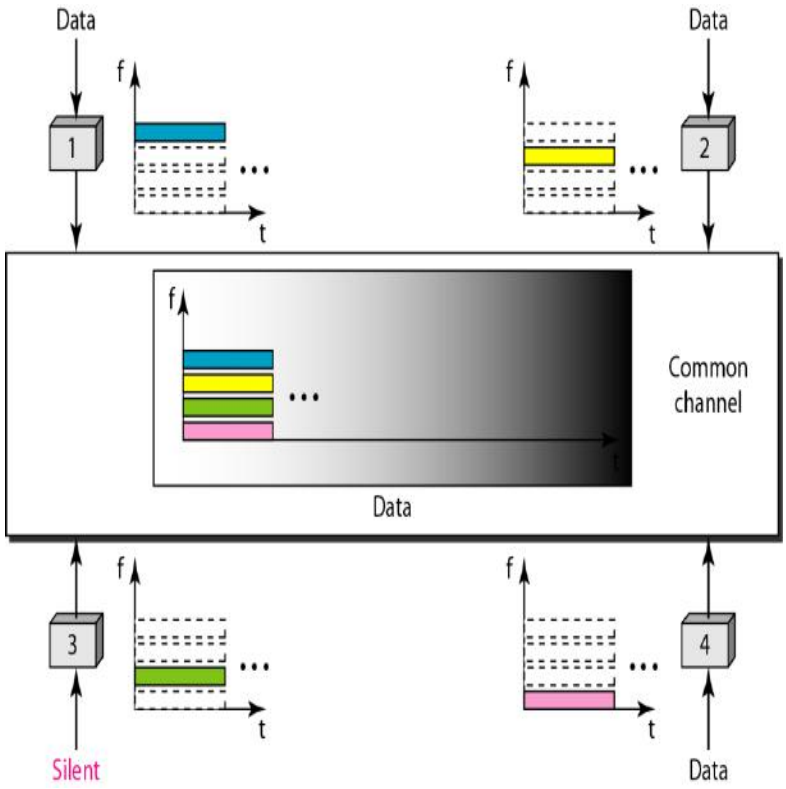


Fig.12: FDMA

FDMA specifies a predetermined frequency band for the entire period of communication. This means that stream data (a continuous flow of data that may not be packetized) can easily be used with FDMA.

FDMA is an access method in the data link layer. The data link layer in each station tells its physical layer to make a bandpass signal from the data passed to it. The signal must be created in the allocated band.

2. TDMA

In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in its assigned time slot. Fig. shows the idea behind TDMA.

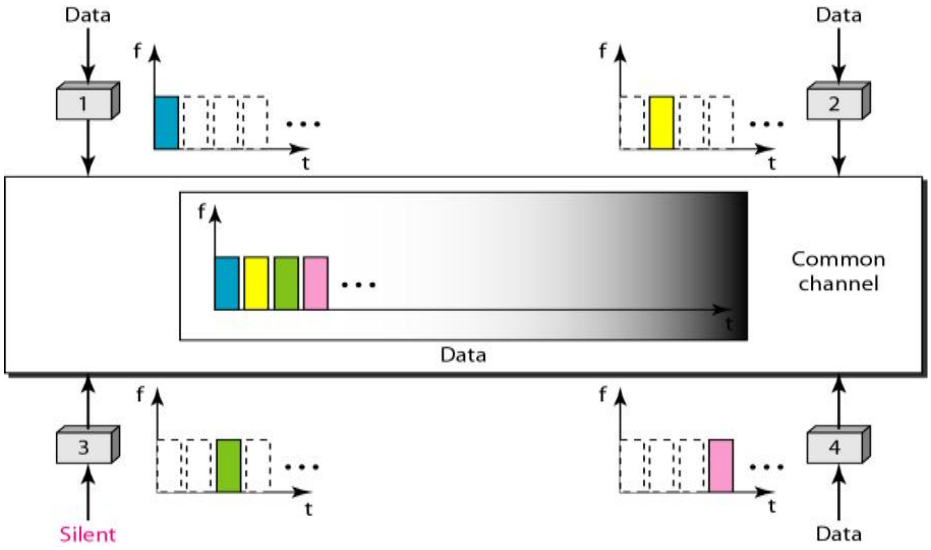


Fig.13: TDMA

The main problem with TDMA lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot. If the stations are spread over a large area, propagation delays are introduced in the system. To compensate for the delays, we can insert guard times. Synchronization is normally accomplished by having some synchronization bits called 'preamble bits' at the beginning of each slot.

TDMA, on the other hand, is an access method in the data link layer. The data link layer in each station tells its physical layer to use the allocated time slot.

3. CDMA

Code-division multiple access (CDMA) was thought of several decades ago. It was implemented later using recent technology. CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link. It differs from TDMA in that all stations can send data simultaneously; there is no timesharing.

CDMA simply means communication with different codes. Let us assume we have four stations, 1, 2, 3, and 4, connected to the same channel. The data from station 1 are d1, from station 2 are d2, and so on. The code assigned to the first station is c1, to the second is c2, and so on. We assume that the assigned codes have two properties.

1. If we multiply each code by another, we get 0.
2. If we multiply each code by itself, we get 4 (the number of stations).

With these two properties in mind, let us see how the above four stations can send data using the same common channel, as shown in Figure. Station 1 multiplies its data by its code to get d1 .c1. Station 2 multiplies its data by its code to get d2 .c2, and so on. The data that go on the channel are the sum of all these terms, as shown in the box.

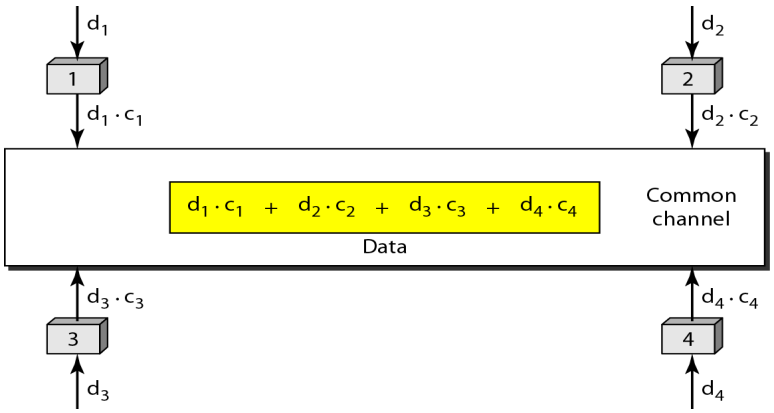


Fig.14: Sharing channel in CDMA

Chips

CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips, as shown in Figure

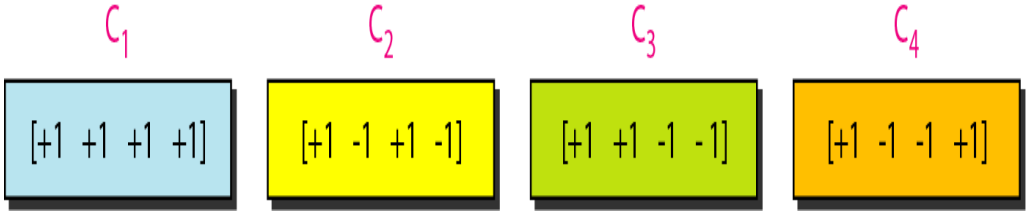


Fig. Chip codes of four stations

Note that these codes are not random. They are properly selected orthogonal sequences with the following properties.

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

If we multiply a sequence by a number, every element in the sequence is multiplied by that element. This is called multiplication of a sequence by a scalar. For example, 2. [+1 +1-1-1] = [+2+2-2-2]

If we multiply two equal sequences, element by element, and add the results, we get N, where N is the number of elements in the sequence. This is called the inner product of two equal sequences. For example, [+1 +1-1 -1] · [+1 +1 -1 -1] = 1 + 1 + 1 + 1 = 4

If we multiply two different sequences, element by element, and add the results, we get 0. This is called inner product of two different sequences. For example, [+1 +1 -1 -1] • [+1 +1 +1 +1] = 1 + 1 - 1 - 1 = 0

Adding two sequences means adding the corresponding elements. The result is another sequence. For example, [+1+1-1-1]+[+1+1+1+1]=[+2 + 2 0 0]

Data Representation

We follow these rules for encoding: If a station needs to send a 0 bit, it encodes it as -1; if it needs to send a 1 bit, it encodes it as +1. When a station is idle, it sends no signal, which is interpreted as a 0. These are shown in Figure

Fig.15: Data representation

Encoding and Decoding

Now imagine that station 3, which we said is silent, is listening to station 2. Then, station 3 multiplies the total data on the channel by the station 2 code, which is [+1 -1 +1 -1] to get

$$[-1\text{-}1\ -3\ +1] \bullet [+1\text{-}1\ +1\ -1] = -4/4 = -1 \quad \text{(Bit 0)}$$

Fig. shows the data transmission in CDMA

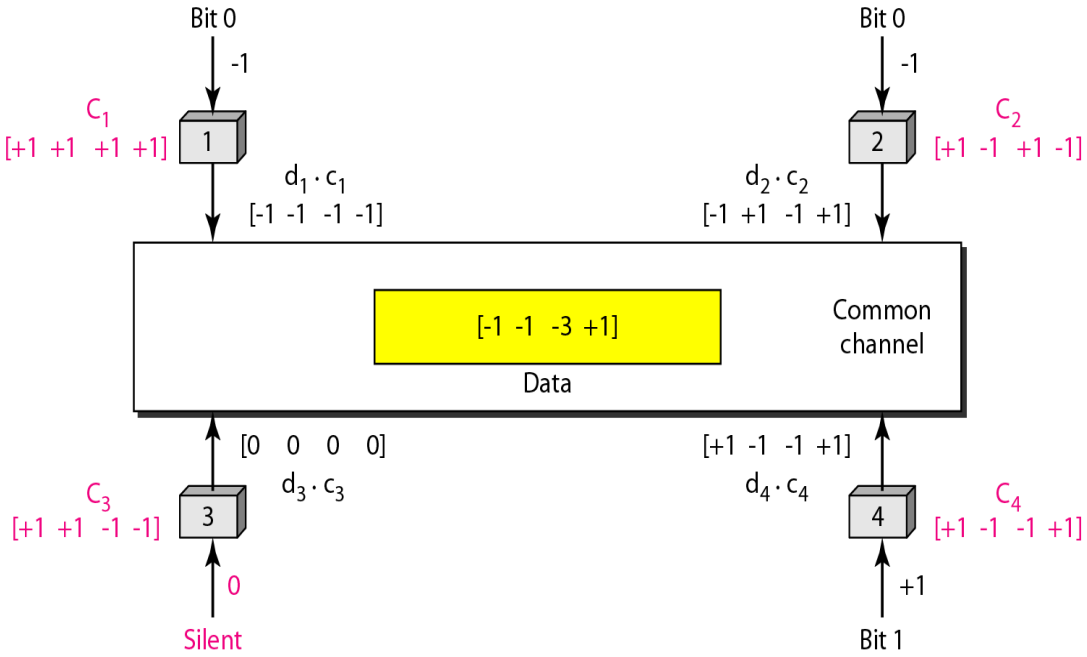


Fig.16: Encoding and data transmission

Signal Level

The figure shows the corresponding signals for each station (using NRZ-L for simplicity) and the signal that is on the common channel.

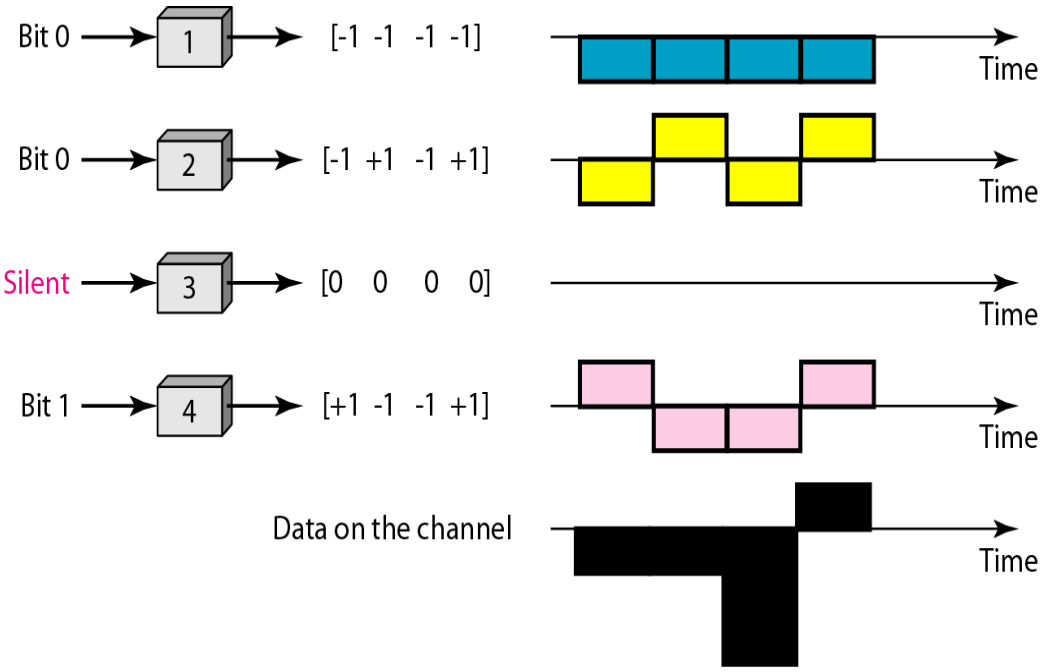


Fig.17: Various signal levels

Figure shows how station 3 can detect the data sent by station 2 by using the code for station 2. The total data on the channel are multiplied (inner product operation) by the signal representing station 2 chip code to get a new signal. The station then integrates and adds the area under the signal, to get the value −4, which is divided by 4 and interpreted as bit 0.

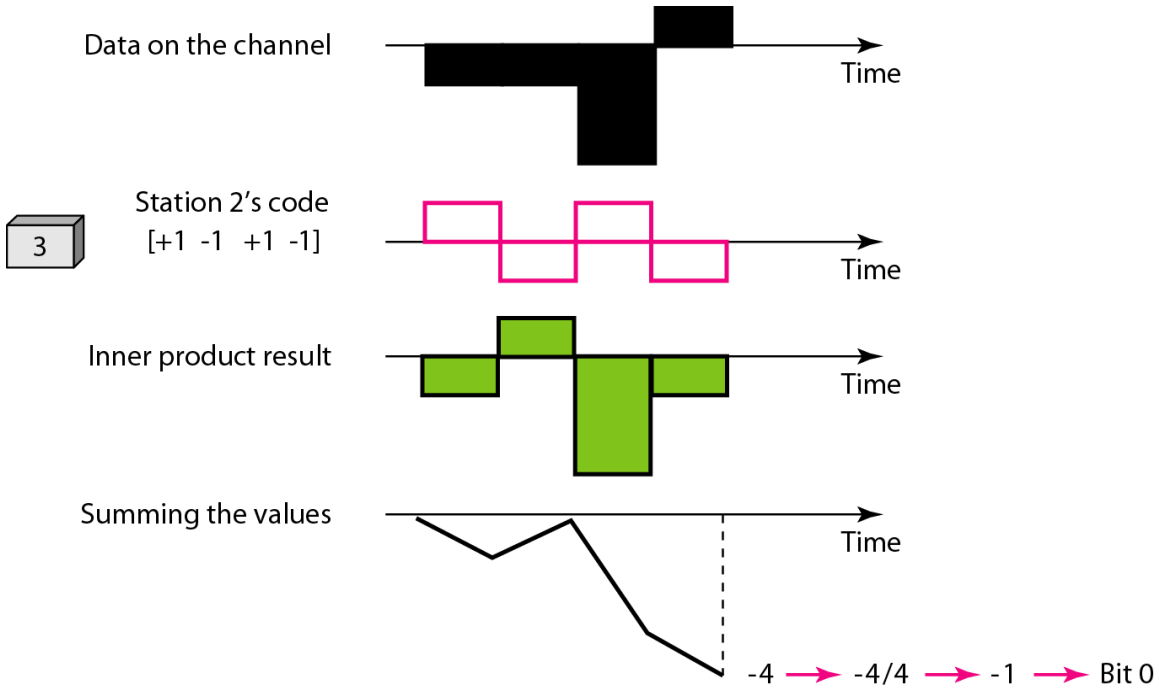
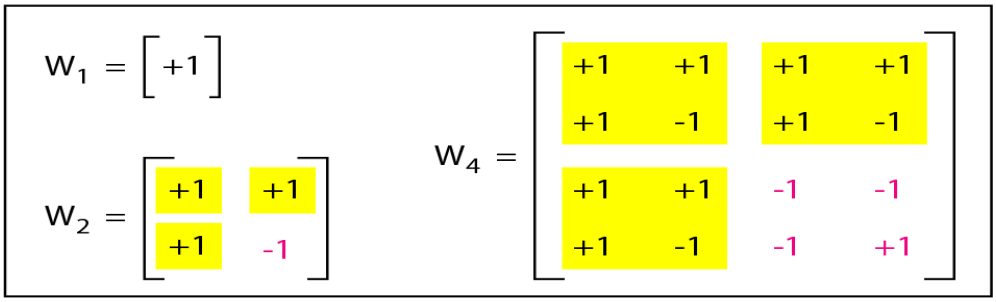


Fig.18: Decoding of the composite signal in CDMA

Sequence Generation

To generate chip sequences, we use a Walsh table, which is a two-dimensional table with an equal number of rows and columns, as shown in Figure

a. Two basic rules



b. Generation of W_1, W_2, and W_4

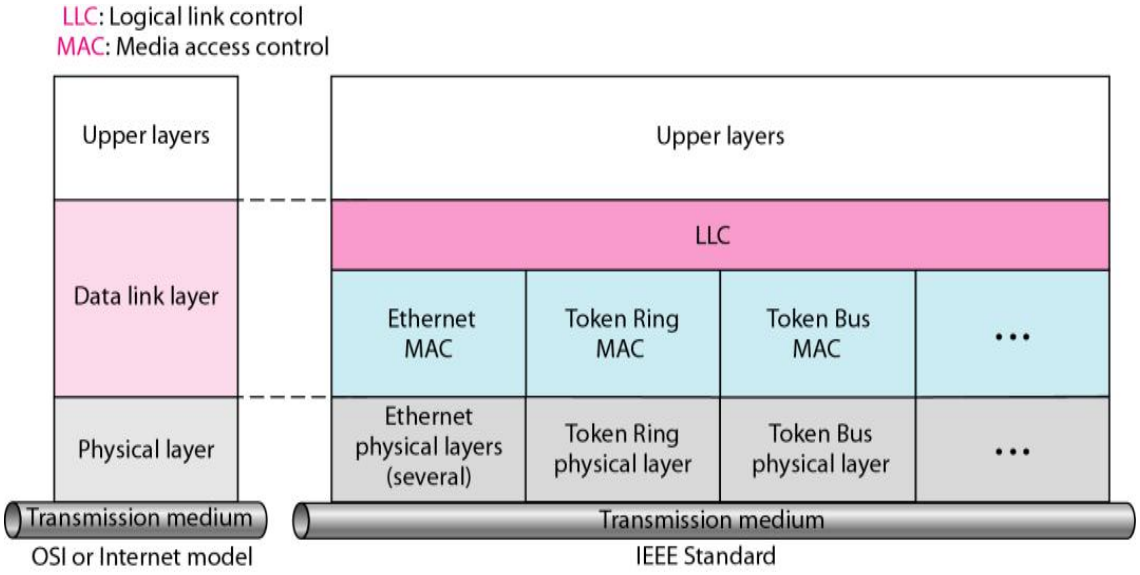
Fig.19: Sequence Generation

WIRED LANS: IEEE STANDARDS

ETHERNET

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set communication standards. Project 802 does not try to replace any part of the OSI model or TCP/IP protocol suite. It specifies functions of the physical layer and the data-link layer of major LAN protocols.

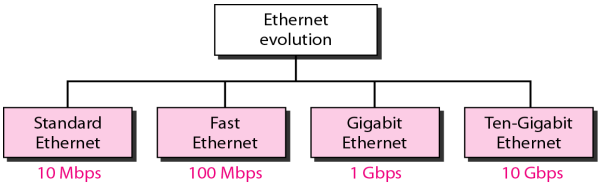
The relationship of the 802 Standard to the TCP/IP protocol suite is shown in Figure. The IEEE has subdivided the data-link layer into two sub layers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical-layer standards for different LAN protocols.



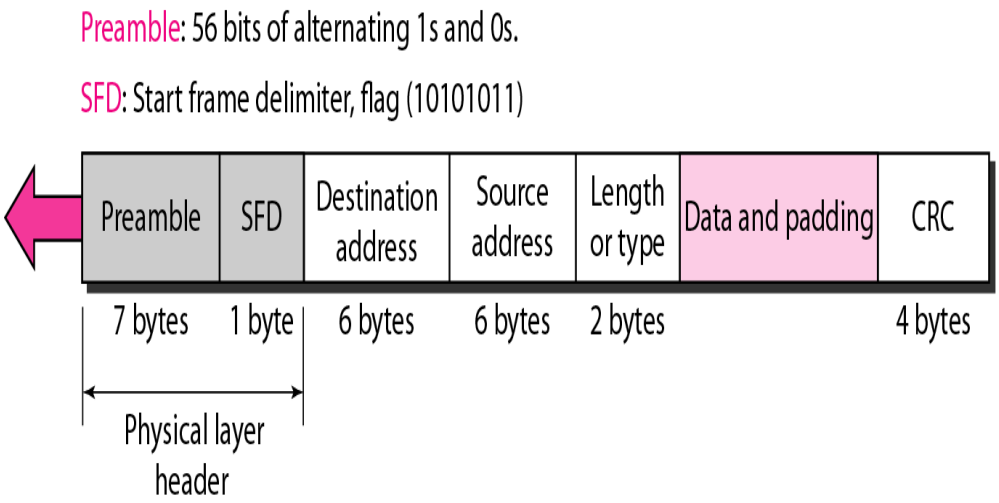
Ethernet Evolution

Ethernet: Ethernet is the traditional technology for connecting devices in a wired LAN or WAN using a protocol. Ethernet describes how network devices format and transmit data. We use Ethernet cable to physically connect computer to the internet. Ethernet connections are almost always faster than Wi-Fi connections, and are usually more stable. Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame

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), as shown in Figure



Frame Format



Preamble: This field contains 7 bytes (56 bits) of alternating 1s and 0s. It alerts the receiving system to the coming frame and enables it to synchronize its clock. The pattern provides only an alert and a timing pulse,

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. and alert the receiver that the next field is the destination address.

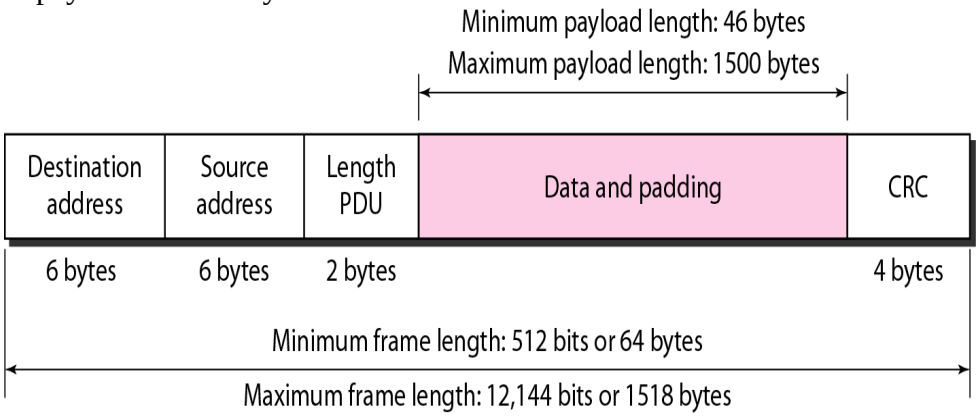
Destination address (DA): This field is six bytes (48 bits) and contains the link layer address of the destination station (s).

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.

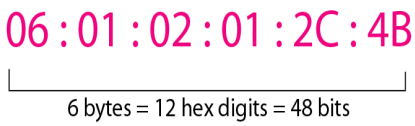
Data: This field carries data from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.

CRC (CRC-32): This last field contains error detection information. The receiver calculates the CRC. If CRC is not zero (corruption in transmission), it discards the frame
Frame Length: Minimum length Ethernet frame is 512 bits or 64 bytes. The minimum length of data from the upper layer is 64 -18 =46 bytes.
The maximum length of a frame (without preamble and SFD field) as 1518 bytes. The maximum length of the payload is 1500 bytes.

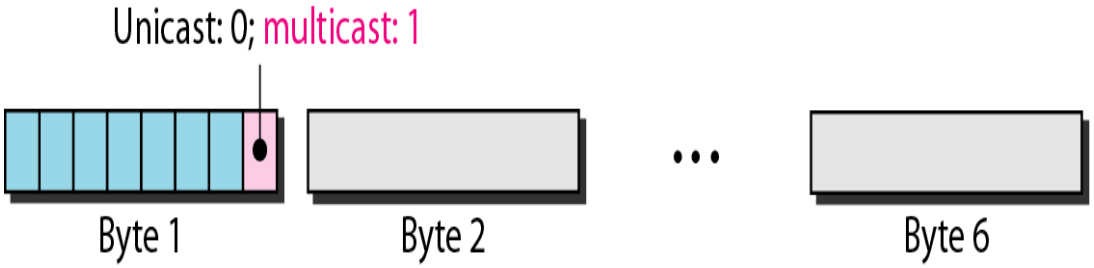


*Padding means adding 0's meet the minimum possible length

Addressing
Each station on an Ethernet network 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:

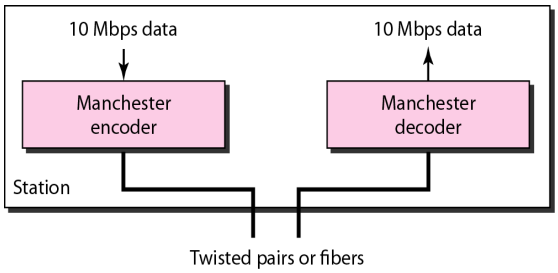


Unicast, Multicast, and Broadcast Addresses
Unicast: from one source to one destination i.e. One-to-One.
Multicast: from one source to multiple destinations, i.e. One-to-Many.
Broadcast address: A special case of the multicast address; the recipients are all stations on the LAN, i.e., One-to-All
If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast. A broadcast destination address is forty-eight 1s; one to all



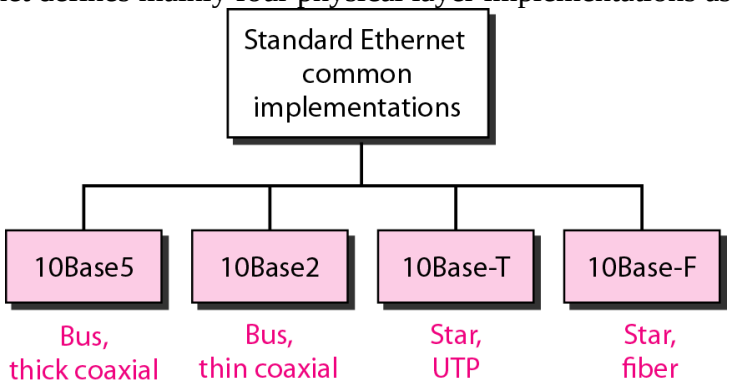
Standard Ethernet

The original Ethernet technology with data rate of 10 Mbps is called Standard Ethernet.
Encoding and Decoding: All standard implementations use digital signaling (baseband) at 10 Mbps. Manchester coding is used in standard Ethernet.

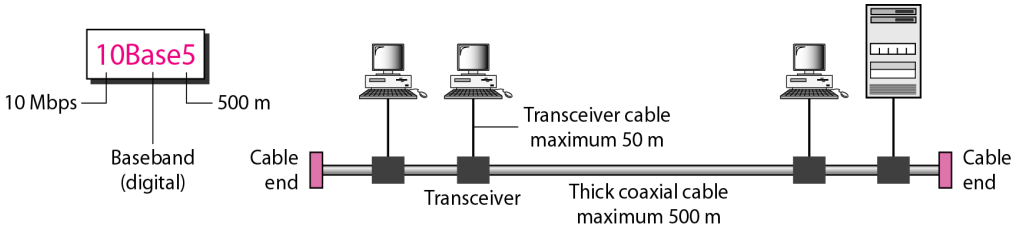


STANDARD ETHERNET IMPLEMENTATIONS:

The Standard Ethernet defines mainly four physical layer implementations as shown below.



10Base5: Thick Ethernet



It was the first Ethernet specification. It is also called "Thick net" because it uses a thick coaxial cable like a hose pipe used in garden. It is too stiff to bend with hands.

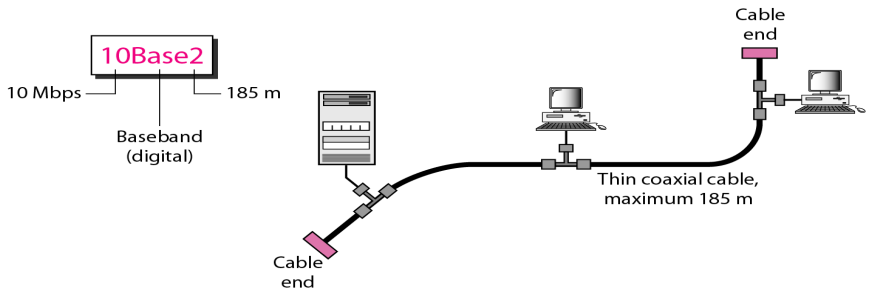
10Base5 means that it operates at 10 Mbps, use baseband signaling, and can support segments of up to 500 meters.

The maximum length of the coaxial cable must not exceed 500 meters to minimize the effect of attenuation. If a length of more than 500 m is needed, repeaters are used for each segment.

It uses a bus topology with an external transceiver (transmitter/receiver) connected to the station via a transceiver cable.

The transceiver is responsible for transmitting, receiving, and detecting collisions. It provides separate paths for sending and receiving. This means that collision can only occur in the coaxial cable.

10Base2: Thin Ethernet

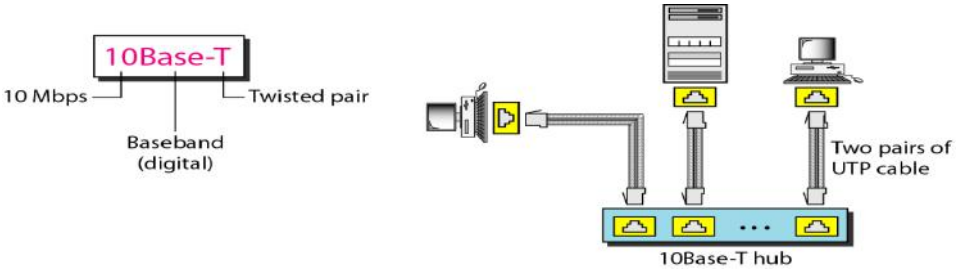


- 10Base2 means that it operates at 10 Mbps, use baseband signaling, and can support segments of up to 185 meters (nearly 200 meters).
- It is also called "Thin Ethernet", because the coaxial cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. Coaxial cable is terminated with BNC connectors, which are relatively less expensive
- Here, implementation is easy and more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial.
- It also uses a bus topology.
- In this, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

Any collision here happens in the coaxial cable.

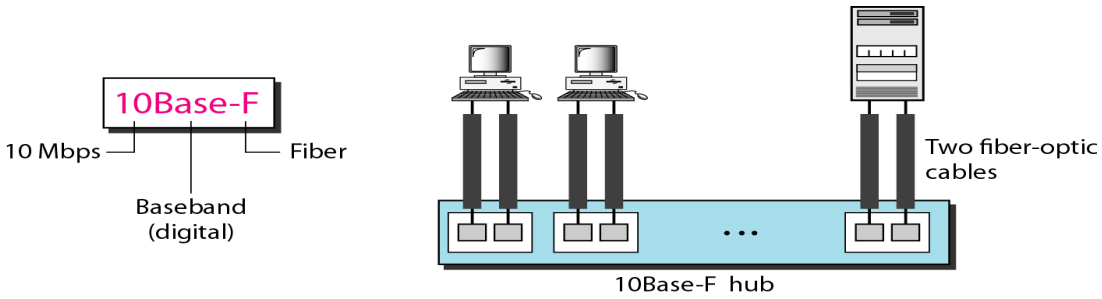
10Base-T: Twisted-Pair Ethernet

The third implementation is called 10Base-T. 10Base-T means that it operates at 10 Mbps, use baseband signaling and Twisted pair cables. The maximum length of the twisted cable is 100 m, to minimize the effect of attenuation in the twisted cable.



- It uses a physical star topology.
- The stations are connected to a hub via two pairs of twisted cable. One pair is used for sending and other for receiving,
- Any collision here happens in the hub.

10Base-F: Fiber Ethernet:



- ✓ 10-Mbps Ethernet is the most common Ethernet used. It uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables
- ✓ It is expensive due to the cost of the connectors and terminators, but it has excellent noise immunity.
- ✓ It is the method of choice when running between buildings or widely-separated hubs. Runs of up to Km are allowed. It also offers food security

Summary of Standard Ethernet implementations

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

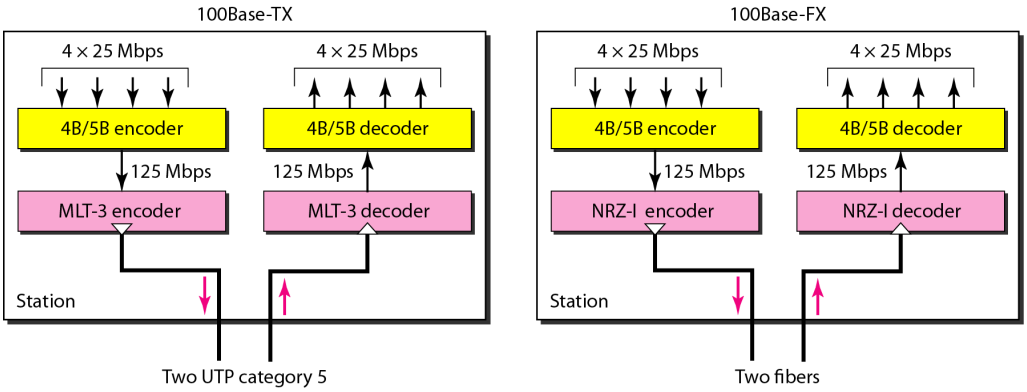
FAST ETHERNET (100 MBPS)

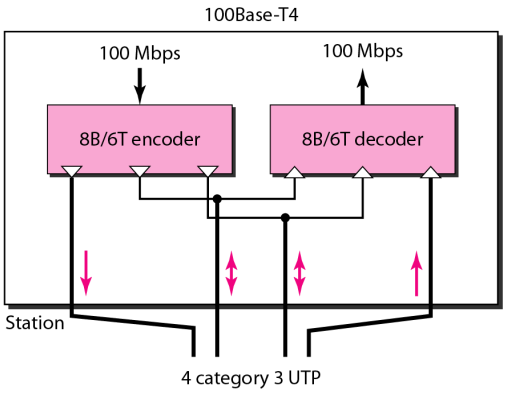
Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible (meaning: compatible with older equipment or previous versions of software) with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.

The goals of Fast Ethernet can be summarized as follows:

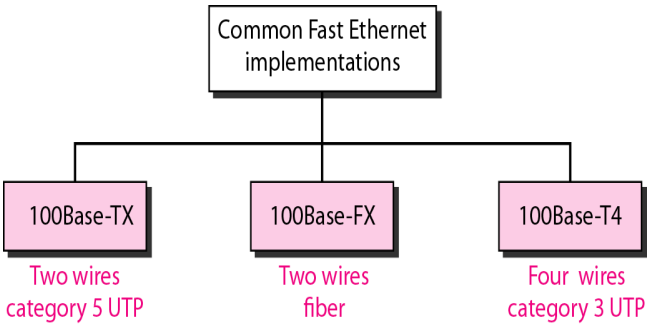
1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format

Encoding for Fast Ethernet implementation





Fast Ethernet Physical layer implementations



100Base-TX uses two pairs of twisted-pair cable (either category 5 UTP or STP). For this implementation, the MLT-3 scheme was selected since it has good bandwidth performance. However, since MLT-3 is not a self-synchronous line coding scheme, 4B/5B block coding is used to provide bit synchronization by preventing the occurrence of a long sequence of 0s and 1s. This creates a data rate of 125 Mbps, which is fed into MLT-3 for encoding.
100Base-FX uses two pairs of fiber-optic cables. Optical fiber can easily handle high bandwidth requirements by using simple encoding schemes. The designers of 100Base-FX selected the NRZ-I encoding scheme for this implementation. However, NRZ-I has a bit synchronization problem for long sequences of 0s (or1s, based on the encoding. To overcome this problem, the designers used 4B/5B block

100Base-T4, was designed to use category 3 or higher UTP. The implementation uses four pairs of UTP for transmitting 100 Mbps. Encoding/decoding in 100Base-T4 is more complicated. 8B/6T satisfies this requirement. In 8B/6T, eight data elements are encoded as six signal elements.

Summary of Fast Ethernet implementations

Characteristics	100Base-TX	100Base-FX	100Base T-4
Media	5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

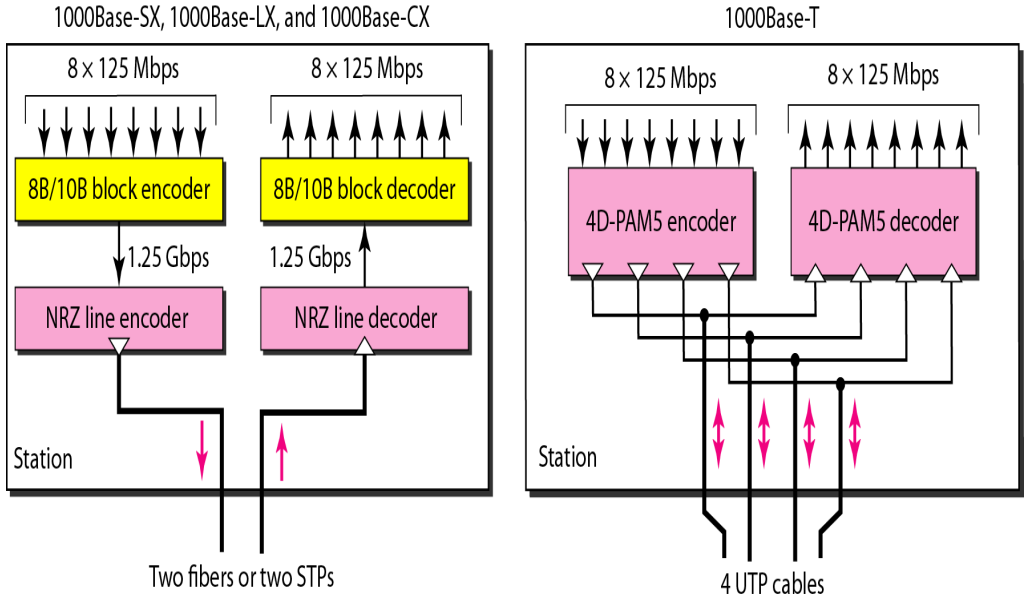
GIGABIT ETHERNET

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the standard 802.3z.

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. Supports auto negotiation as defined in Fast Ethernet.

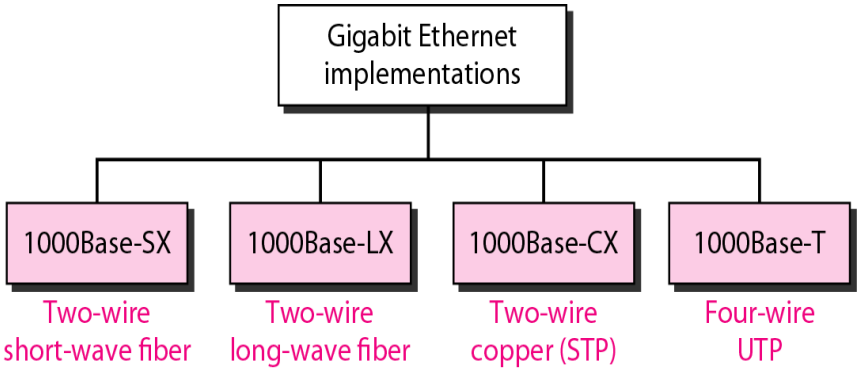
Encoding in Gigabit Ethernet implementations



Gigabit Ethernet cannot use the Manchester encoding scheme because it involves a very high bandwidth (2 GB). The two-wire implementations use an NRZ scheme, but NRZ does not self-

synchronize properly. To synchronize bits, particularly at this high data rate, 8B/10B block encoding is used. This block encoding prevents long sequences of 0s or 1s in the stream, but the resulting stream is 1.25 Gbps. Note that in this implementation, one wire is used for sending and one for receiving.
In the four-wire implementation it is not possible to have 2 wires for input and 2 for output, because each wire would need to carry 500 Mbps, which exceeds the capacity for category 5 UTP. As a solution, 4D-PAM5 encoding, is used to reduce the bandwidth. Thus, all four wires are involved in both input and output; each wire carries 250 Mbps, which is in the range for **category 5 UTP cable.**

Gigabit Ethernet implementations



Summary of Gigabit Ethernet implementations

Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

Comparison of Fast Ethernet and Gigabit Ethernet

Basis For Comparison	Fast Ethernet	Gigabit Ethernet
Basic	Offers 100 Mbps speed.	Provide 1 Gbps speed.

Delay	Generate more delay.	Less comparatively.
Configuration	Simple	Complicated and create more errors.
Coverage	Can cover distance up to 10 km.	Has the limit of 70 km.
Round trip delay	100-500 bit times	4000 bit times

10 GIGABIT ETHERNET (2002)

Enterprises use 10 Gigabit Ethernet switches for very high-speed network applications – mostly in the data center or server room.

It offers data speeds up to 10 gigabits per second.

It operates only in full-duplex mode. So, there is no need for contention;

CSMA/CD is not used in 10 Gigabit Ethernet.

Ten-Gigabit (10Gbe) Ethernet implementations

Most common implementations are: 10GBase-S, 10GBase-L, 10GBase-E. Table shows the summary of the 10 Gigabit Ethernet implementations

Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

WIRE LESS LAN IEEE 802.11

IEEE standard, called IEEE 802.11 covers the physical and data-link layers. It is sometimes called wireless Ethernet. In some countries, including the United States, the public uses the term WiFi as a synonym for wireless LAN.

Architecture

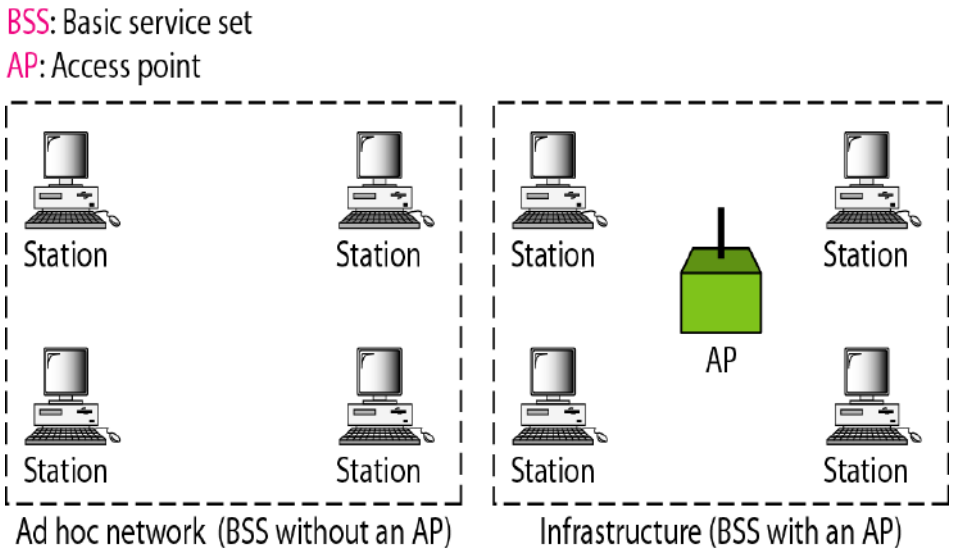
The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

BSS (Basic Service Set)

BSS acts as the building blocks of a wireless LAN. It 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.

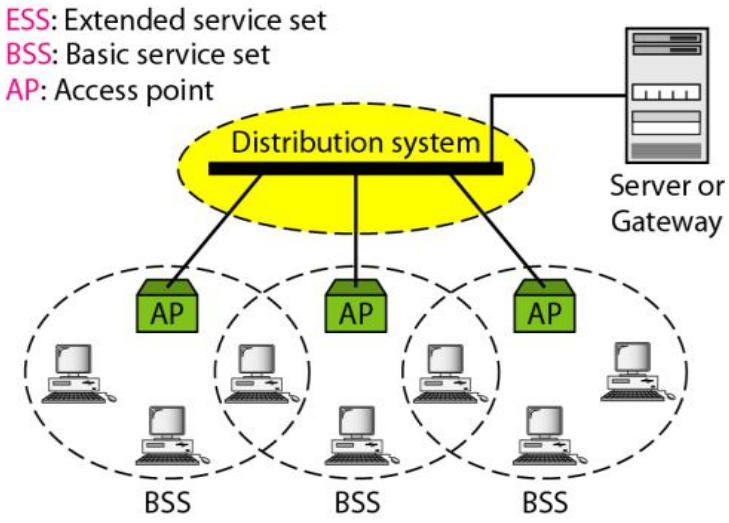
The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP. They can locate one another and agree to be part of a BSS.

A BSS with an AP is sometimes referred to as an infrastructure BSS.



ESS (Extended Service Set)

An extended service set (ESS) is made up of two or more BSSs with APs. A distribution system (which is a wired or a wireless network) is used to connect the APs of the BSSs in the BSSs. It can be any IEEE LAN such as an Ethernet

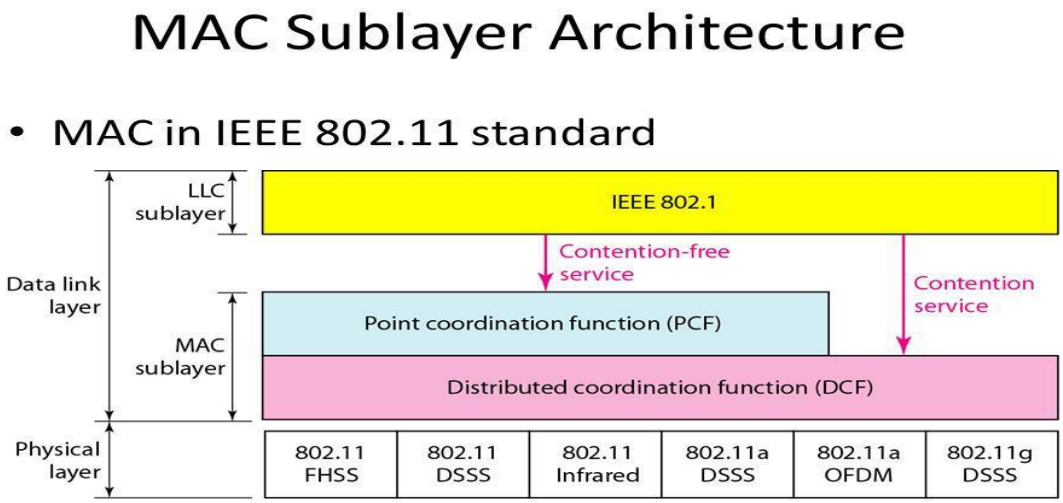


Station Types

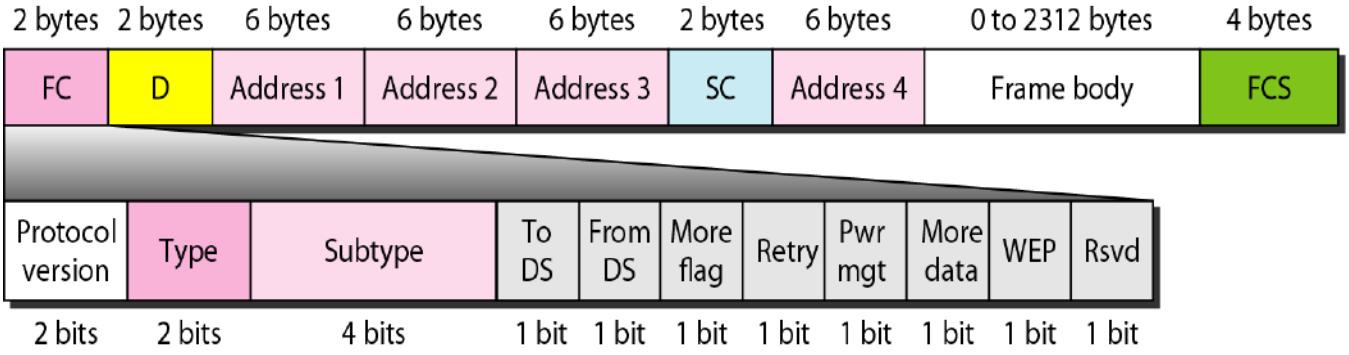
IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition, BSS-transition, and ESS-transition mobility. A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS. A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS. A station with ESS-transition mobility can move from one ESS to another.

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.



DCF:
It uses CSMA/CA as the access method.
Point Coordination Function (PCF)
It is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). It is implemented on top of the DCF and is used mostly for time-sensitive transmission.
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 resend a small frame than a large one.
Frame Format
The MAC layer frame consists of nine fields, as shown in Figure

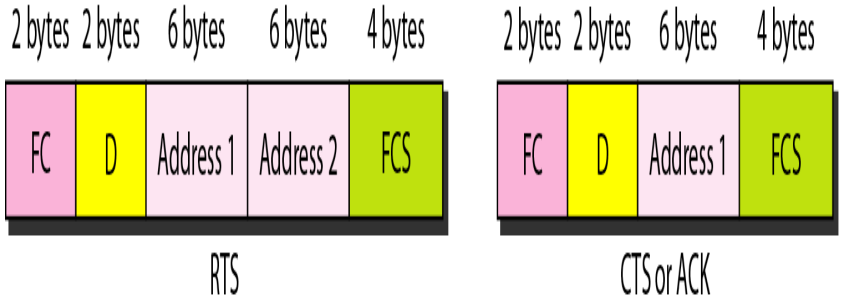


Frame control (FC): The FC field is 2 bytes long and defines the type of frame and some control information. It has 11 subfields.
D: It defines the duration of the transmission that is used to set the value of the network allocation vector (NAV). NAV is a virtual carrier sensing mechanism that forms an important part of the CSMA/CA.
Addresses: There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the 'To DS' and 'From DS' subfields.
Sequence control: This is also called the SC field. It defines a 16-bit value. The first four bits define the fragment number. The last 12 bits define the sequence number, which is the same in all fragments.
Frame body: This field can be between 0 and 2312 bytes. It contains information based on the type and the subtype defined in the FC field.
Frame check sequence (FCS): It is 4 bytes long and contains a CRC-32 error-detection sequence.

Subfields in FC field

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

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. Figure shows the format



For control frames the value of the type field is 01; the values of the subtype fields for frames

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Data Frames

Data frames are used for carrying data and control information.

Addressing Mechanism

The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, 'To DS' and 'From DS'. Each flag can be either 0 or 1, resulting in four different situations.

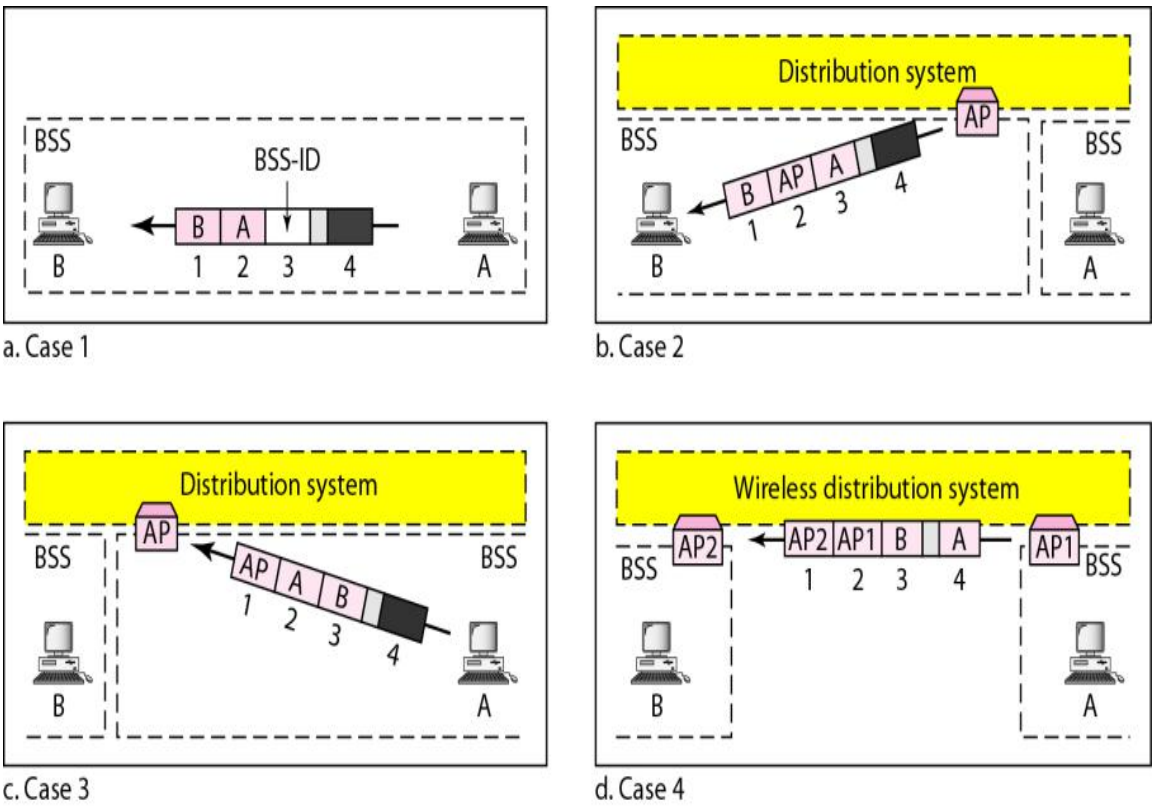
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Case 1: 00 In this case, To DS =0 and From DS =0. This means that the frame is not going to a distribution system (To DS =0) and is not coming from a distribution system (From DS =0).

Case 2: 01 In this case, To DS =0 and From DS =1. This means that the frame is coming from a distribution system (From DS =1).

Case 3: 10 In this case, To DS =1 and From DS =0. This means that the frame is going to a distribution system (To DS =1).

Case 4: 11 In this case, To DS =1 and From DS =1. This is the case in which the distribution system is also wireless. The frame is going from one AP to another AP in a wireless distribution system.



Physical Layer

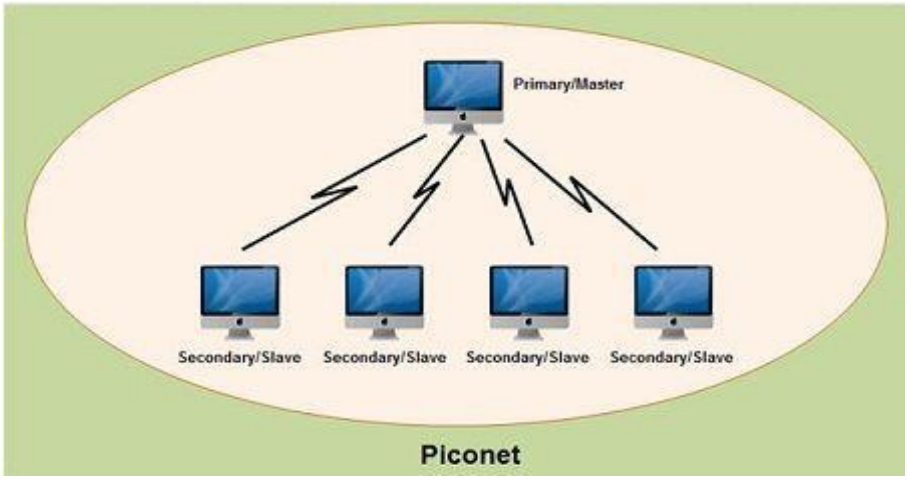
We discuss six specifications, as shown in Table 15.4. All implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines three unlicensed bands in the three ranges 902–928 MHz, 2.400–4.835 GHz, and 5.725–5.850 GHz.

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

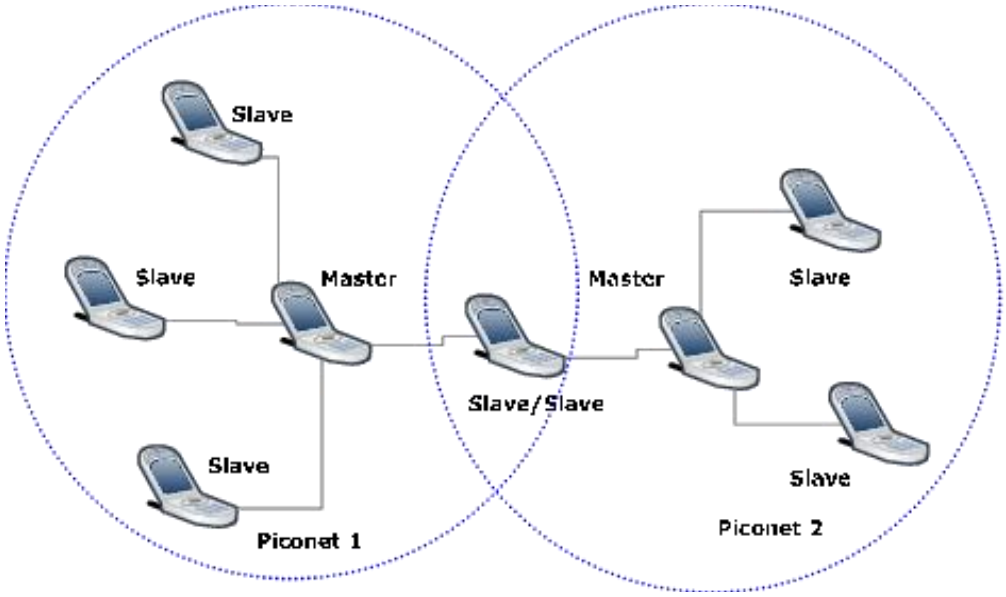
IEEE 802.15 (BLUETOOTH)

Bluetooth:
Bluetooth is a wireless LAN technology designed to connect devices of different functions such as mobile phones, computers (desktop and laptop), cameras, printers, wireless mouse and keyboards, wireless headset, 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 are called gadgets. They find each other and make a network called a 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. Note that 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. Figure shows a piconet.



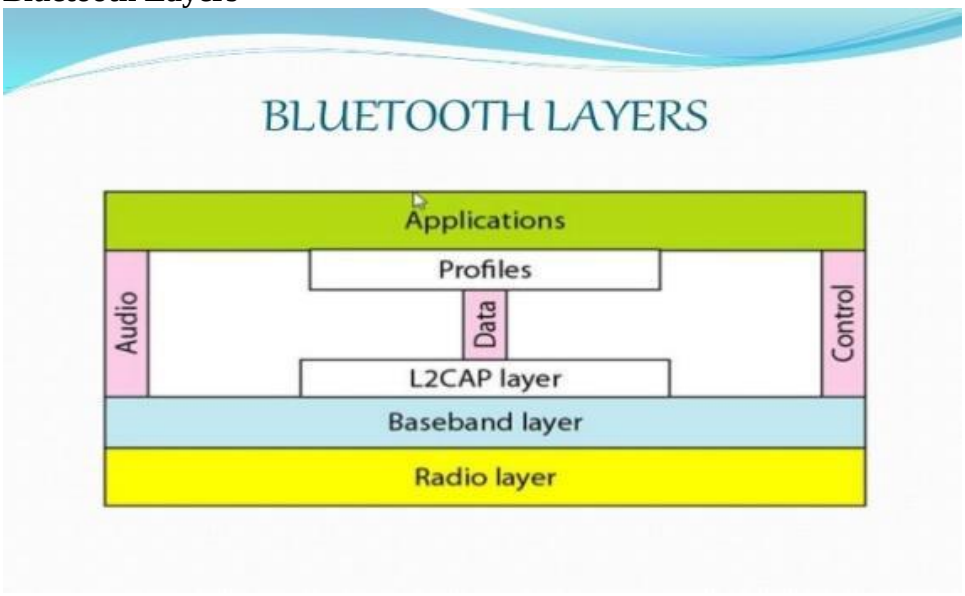
Scatternet
Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.



Bluetooth Devices

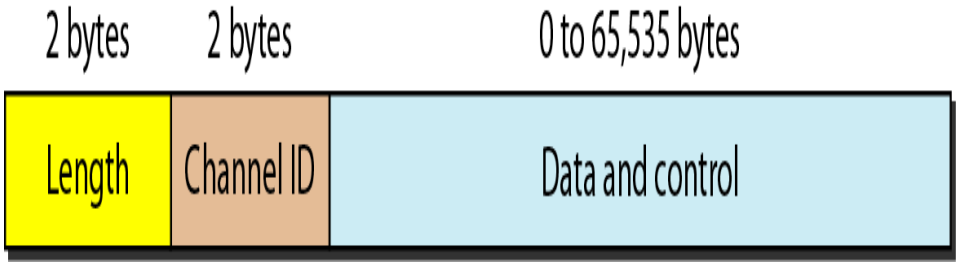
A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth.

Bluetooth Layers



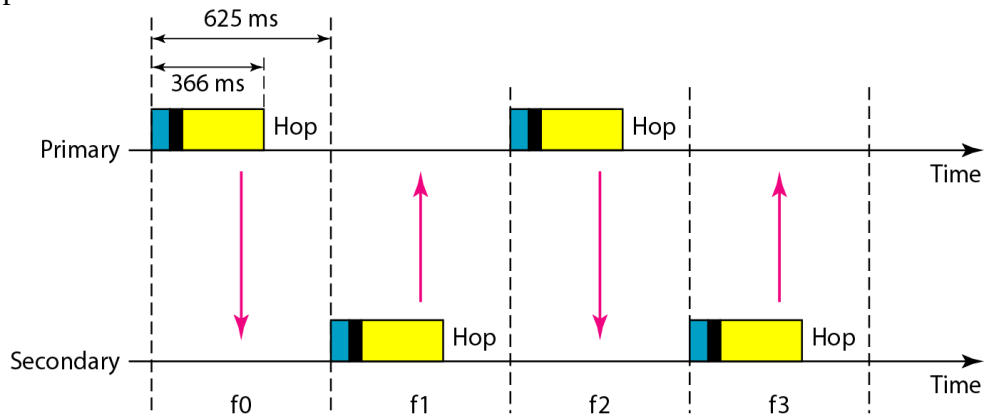
L2CAP

The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs. Figure shows the format of the data packet at this level.



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 created at this level (see below).
The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

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 dwell time (the period during which a data packet gets transmitted). 625 us.
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).
Single-Secondary Communication: If the piconet has only one secondary, the TDMA operation is very simple. The time is divided into slots of 625 us. The primary uses even-numbered slots (0, 2, 4, ….); the secondary uses odd-numbered slots (1, 3, 5, ….). TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode. In slot 0, the primary sends and the secondary receives; in slot 1, the secondary sends and the primary receives. The cycle is repeated.



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.
Let us elaborate on the figure.
1. In slot 0, the primary sends a frame to secondary 1.

2. In slot 1, only secondary 1 sends a frame to the primary because the previous frame was addressed to secondary 1; other secondaries are silent.
3. In slot 2, the primary sends a frame to secondary 2.
4. In slot 3, only secondary 2 sends a frame to the primary because the previous frame was addressed to secondary 2; other secondaries are silent.
5. The cycle continues.
.

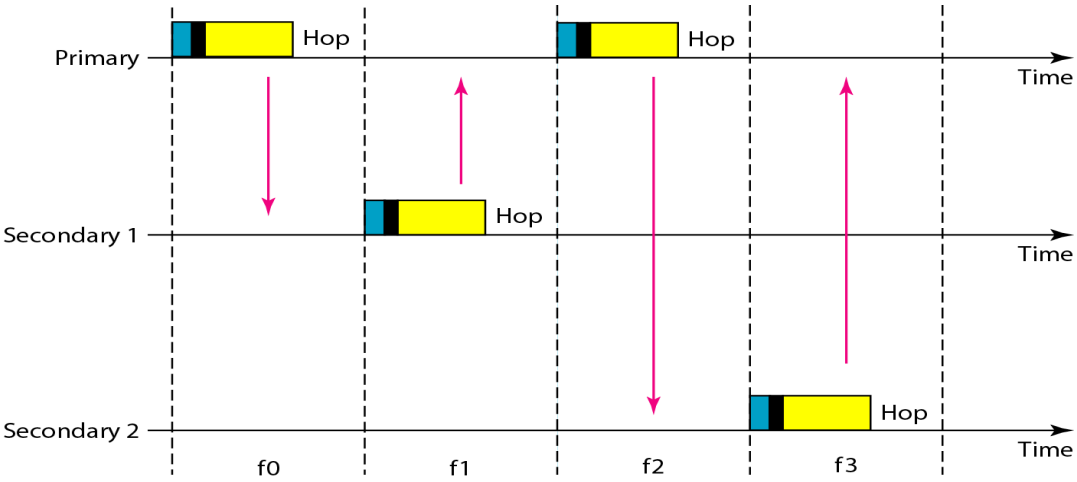
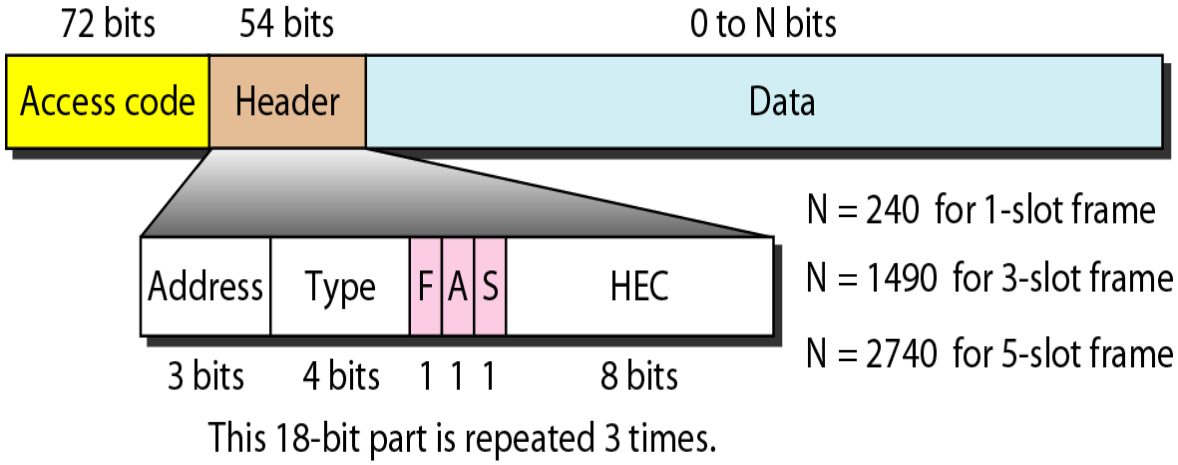


Fig.: Multiple-secondary communication

Frame Format

A frame in the baseband layer can be one of three types: one-slot, three-slot, or five slot-frame. A slot, as we said before, is 625 us. However, in a one-slot frame exchange, 259 us is needed for hopping and control mechanisms. This means that a one-slot frame can last only 625 -259, or 366us. With a 1-MHz bandwidth and 1 bit/Hz, the size of a one-slot frame is 366 bits. A three-slot frame occupies three slots. The length of the frame is 3*625 -259 =1616 us or 1616 bits. A five-slot frame also uses 259 bits for hopping, which means that the length of the frame is 5*625 -259 =2866 bits. Figure shows the format of the three frame types..



Access code: This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.

Header: This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:
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.
HEC (Header error correction): The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.
Payload: This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

Radio Layer

The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band

Bluetooth uses a 2.4-GHz ISM (Industrial, Scientific, and Medical) band divided into 79 channels of 1 MHz each.

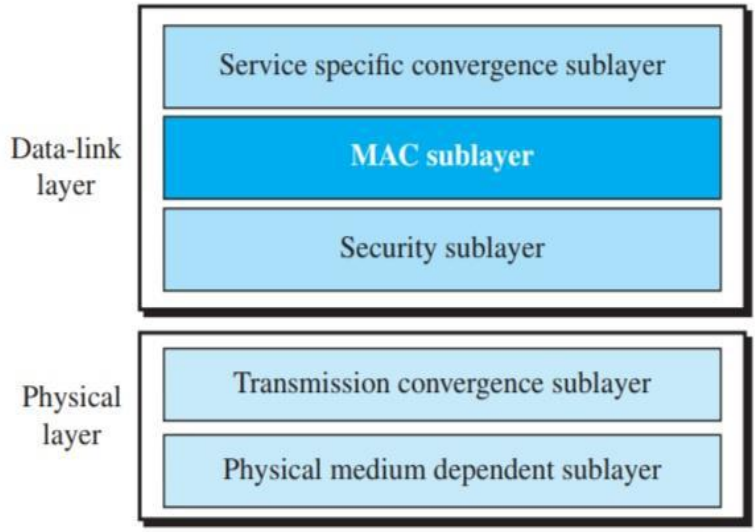
FHSS

Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks. FHSS is a method of transmitting radio signals by rapidly changing the carrier frequency among many distinct frequencies occupying a large spectral band. Bluetooth hops 1600 times per second. (a hop is a portion of a signal's journey from source to receiver)
FHSS:
Modulation
To transform bits to a signal, Bluetooth uses a sophisticated version of FSK (Frequency shift keying), called GFSK (FSK with Gaussian bandwidth filtering).

WiMAX-IEEE 802.16

WiMAX stands for Worldwide Interoperability for Microwave Access. WiMAX is also called ‘wireless local loop’. WiMAX aims provide higher bandwidth and larger coverage than existing wireless technologies such as Wi-Fi and 3G. WiMAX is the outcome of the IEEE 802.16 Project. Its revised versions are called IEEE 802.16d (fixed WiMAX), and IEEE 802.16e (mobile WiMAX)
Layers in Project 802.16:
IEEE has divided the data-link layer into three sublayers and the physical layer into two sublayers. The 5 sublayers are shown in the following figure.

Data-link and physical layers



1. Service Specific Convergence Sublayer

This is sublayer used for broadband wireless communication. It was devised for a connection-oriented service with a specific quality of service (QoS).

Note: QoS is the description or measurement of the overall performance of a service from users' view. It is important for a telephone or computer network.

2. MAC Sublayer

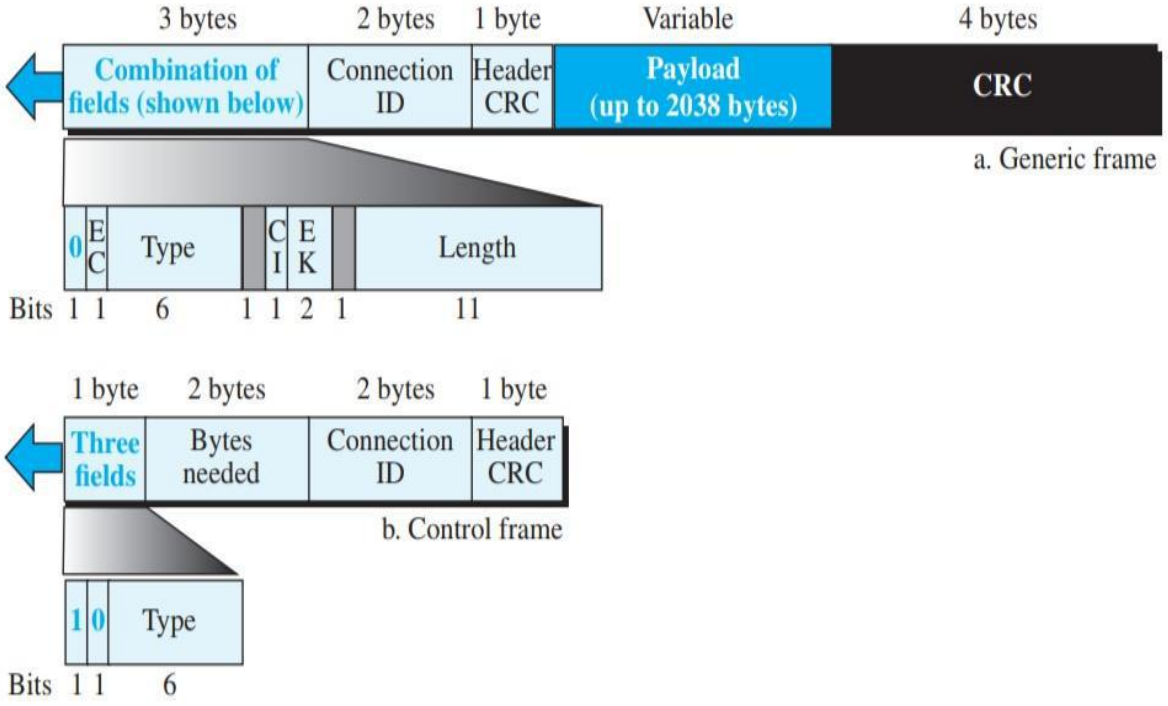
The MAC sublayer defines the access method and frame-format. It is designed for connection-oriented service. WiMAX uses the reservation (scheduling) access method. i.e., a station needs to make a reservation before sending data.

Addressing: Each subscriber and base station typically have a 48-bit MAC address.

Frame Format:

We distinguish two types of frames: generic and control. The first is used to send and receive payload. The second is used only during the connection establishment. Both frame types use a 6-byte generic header.

Figure 16.4 *WiMAX MAC frame format*



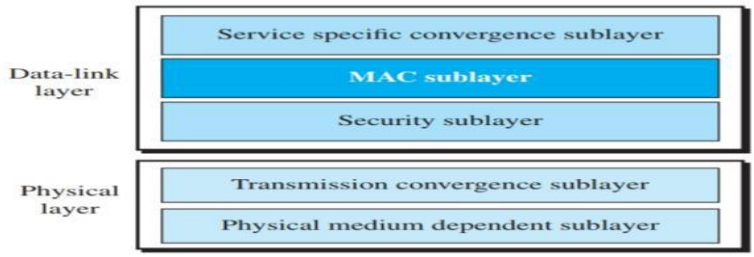
The first bit in a frame is the frame identifier. If it is 0, the frame is a generic frame; if it is 1, it is a control frame.

EC (Encryption control) field: It has one bit. EC = 0 means no encryption. 1 means the frame needs encryption at the security sublayer.

Type: This 6-bit field defines the type of the frame. This field is only present in the generic frame and normally is used to define the type of the payload.

CI (Checksum ID) field: It uses one bit to define whether the frame checksum field is needed or not.

Data-link and physical layers



EK (Encryption key) field: It uses two bits to define one of the four keys for encryption if encryption is required.

Length: The length field uses eleven bits to define the total length of the frame.

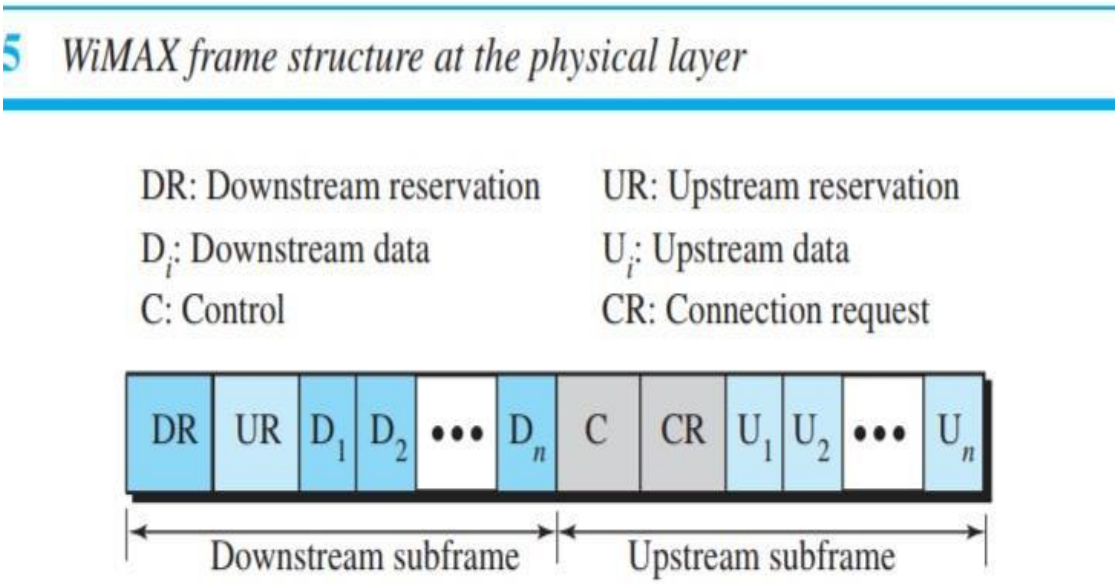
Bytes Needed field: It uses sixteen bits to define the number of bytes needed for allocated slots in the physical layer.
Connection ID: It uses sixteen bits to define the connection identifier for the current connection.
Header CRC field: The header CRC is used to check whether the header itself is corrupted. Both types of frames have an this 8-bit field.
Payload: This variable-length field defines data in the frame from the service specific convergence sub layer.
CRC: If present, it is used for error detection over the whole frame.

3. Security Sub layer

It provides security for communication using WiMAX.

4. Transmission Convergence Sub layer

It uses TDD (time-division duplex), a variation of time-division multiplexing, designed for duplex (bidirectional) communication. It packs the frames received from the data-link layer into two sub frames.



5. Physical Medium Dependent (PMD) Sub layer

PMD sub layer defines the details of transmission and reception of individual bits on a physical medium. This sub layer is in continuous revision. Originally, 802.16 defined the band 10-66 GHz and modulations QPSK. Later IEEE modified it as 802.16d (fixed WiMAX) and 802.16e (mobile WiMAX).
IEEE 802.16d (2-11 GHz) uses Orthogonal frequency-division multiplexing (OFDM). Later IEEE 802.16e added Scalable orthogonal frequency-division multiplexing (SOFDM).

UNIT-IV

NETWORK LAYER

Syllabus Contents: Design Issues, Routing--Algorithms, Congestion control—Algorithms, IPV4 Addresses, Connecting Devices, Virtual LAN, IPV6 Addresses, Internet Protocol, Hardware Addressing versus IP Addressing, IP Data Gram.

Network Layer:

The main function of the network layer is routing packets from source to destination. The routing algorithm a procedure that lays down the route or path to transfer data packets from source to the destination.

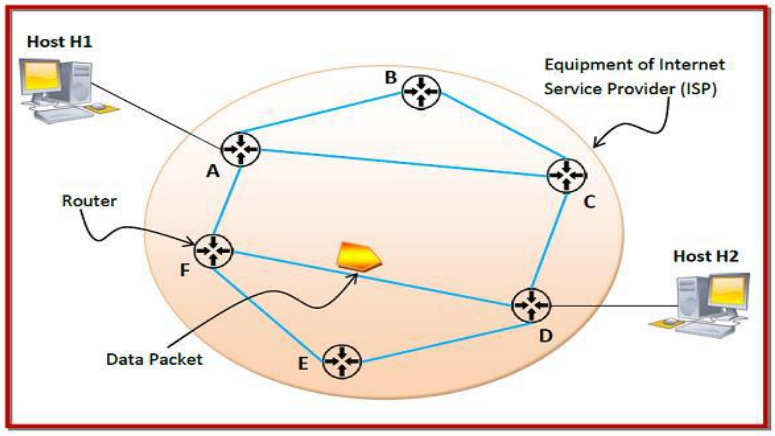
DESIGN ISSUES OF NETWORK LAYER

(i) Storing and forwarding packets.
(ii) Services to upper (Transport) layer.
(iii)Implementing Connectionless Service.
(iv)Implementing Connection-Oriented Service

(i) Store and Forward Packet Switching

Store-and-forward packet switching is a technique where each intermediate node stores the packets and compute CRC. If a packet is error-free (CRC=0), it is transmitted to the next node. If the packet is corrupted, it is discarded.

Example:



In the above diagram, here there are 6 nodes (A to F) connected by transmission lines shown in blue lines. There are two hosts, host H1 is connected to router A, while host H2 is connected to

router D. Suppose that H1 wants to send a data packet to H2. H1 sends the packet to router A. The packet is stored in router A until it has arrived fully. Router A verifies the checksum using CRC (cyclic redundancy check) code. If there is a CRC error, the packet is discarded, otherwise it is transmitted to the next hop (F). The same process is followed by router F which then transmits the packet to router D. Finally, router D delivers the packet to host H2. This method ensures high quality data packet transmission. But it involves more delay because a node has to wait until the packet arrives fully, store it and compute CRC.

(ii) Services Provided to Transport Layer

The services should be independent of the router technology

The number, type and topology of the routers should not affect transport layer.

The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs

(iii) Implementing Connectionless Service (Datagram)

Connectionless Service:

No connection setup.

Message is broken into packets called datagrams

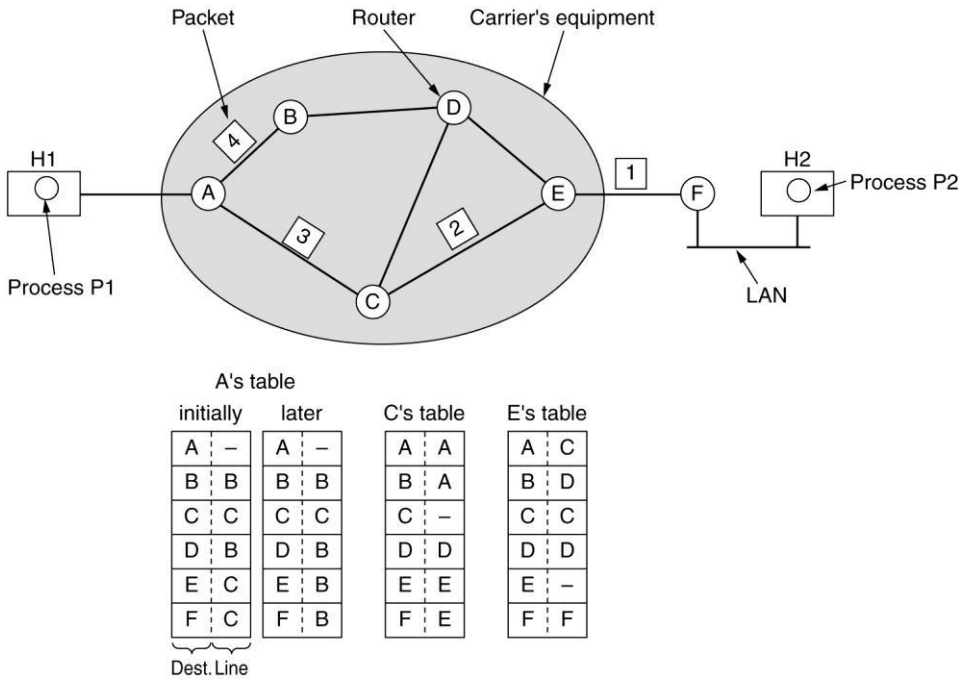
Each packet is individually routed.

Packets may follo w different paths. Routers decide route based on routing table

Packets may not arrive in order.

Analogy: Telegram

Implementation of Connectionless Service (Datagram):



The long message is divided in to 4 packets: 1,2,3, and 4.

Every router has an internal table telling it where to send the packets for each destination (A,

B, C, D, E, or F). Destinations are given in first column. Second column gives the outgoing line to use for that destination.

Initial and final tables for A: for sending packet to say destination E, there are two possibilities B and C. Let A selected C (initial table). But for some reason like traffic jam, it selected B (not C). This is shown in final table of A. See 5th row in initial and final tables. **The algorithm that manages the tables and makes the routing decisions is called routing algorithm**

(iv) Implementation of Connection-Oriented Service (Virtual circuit)

Connection-Oriented Service:

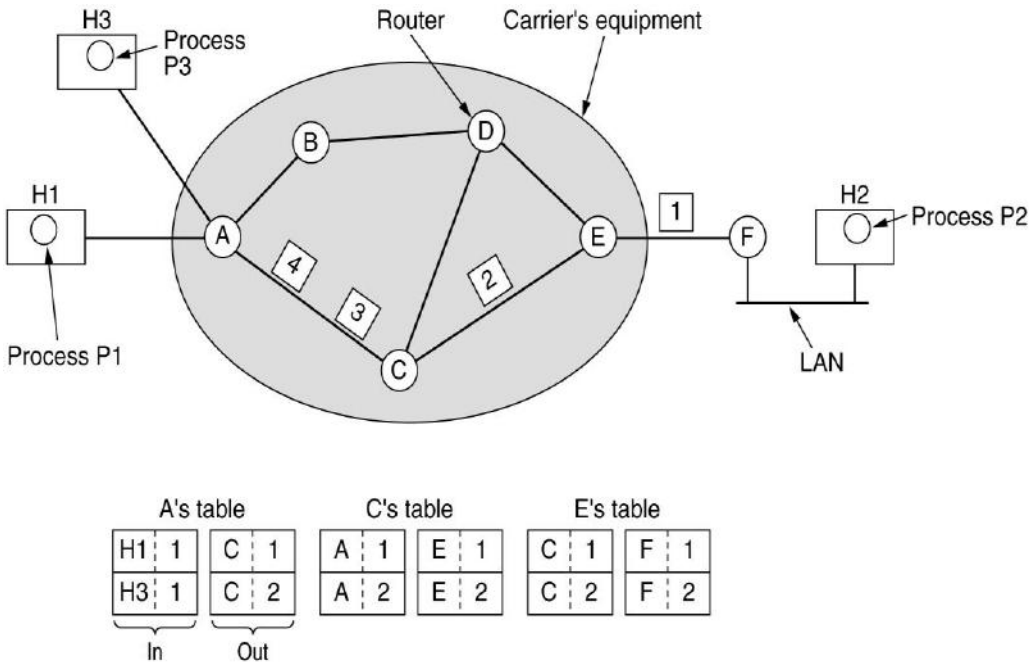
Path from source to destination must be established before sending data.

Same route used for all packets in connection. No need to select new routes.

Each packet has ID called 'VCI'.

Analogy: Physical circuit in phone system

Implementation of Connection-Oriented Service:



The route is selected in setup phase and stored in tables in the router. This route is used for all packet-traffic like telephone. When connection is released, the VC is also terminated. Each packet carries a virtual circuit identifier (VCI) telling which VC it belongs to.

Conflict: Suppose H3 also wants a connection with H2. It chooses connection identifier '1' (It is its only connection) as given in 'in' table for A. Now next node is C. This cannot distinguish packets. It does not know whether packet is coming from H1 or H3. So, A assigns a different identifier '2' to the outgoing traffic (as shown in 'out' table for A). Similarly other 'in' and 'out' tables for C and E can be interpreted.

Comparison of Virtual-Circuit and Datagram circuit

S.No.	Datagram Circuit	Virtual Circuit
1	Connection-less. Less reliable	Connection- oriented. More reliable
2	Each packet contains destination address	Packet contains a a virtual circuit identifier
3	Packets have no fixed paths	All packets follow same path
4	Packets may not reach destination in order	Packets reach destination in order
5	QoS: Difficult	QoS: Easy

Routing: Routing is the process of forwarding the packets from source to the destination. There are 4 types of types of routing: Unicast, Multicast, Broadcast and Anycast routing

(i) Unicast routing: From one source to one destination i.e. One-to-One. It is the simplest form of routing because the destination is clearly known.

(ii) Broadcast address: Here, the recipients are all the nodes on the LAN, i.e., One-to-All. Thus, a broadcast message is destined to all network devices.

(iii) Multicast routing: From one source to multiple destinations, i.e. One-to-Many.

Multicast vs broadcast: *Multicast routing is special case of broadcast routing. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.*

Anycast routing: A single destination IP address is shared by devices in multiple locations.

When a packet sent to this logical address is received, it is sent to the host which is nearest in routing topology. Anycast routing is done with help of DNS server.

ROUTING ALGORITHMS

Routing is the process of forwarding the packets from source to the destination. Routing algorithm is the algorithm that determines the best route to send the packets.

Routing algorithms can be divided into two groups:

1. **Nonadaptive algorithms (Static routing):** Routing decision is not based on the traffic and topology. However, the choice of the route is done in advance.
2. **Adaptive algorithms (Dynamic routing):** Routing decision is based on the traffic and topology. If there are any changes in topology or traffic, the routing decision may also be changed. The main parameters related to this algorithm are hop count, distance and estimated transit time.

STATIC ALGORITHMS

1. Shortest path routing using Dijkstra algorithm:

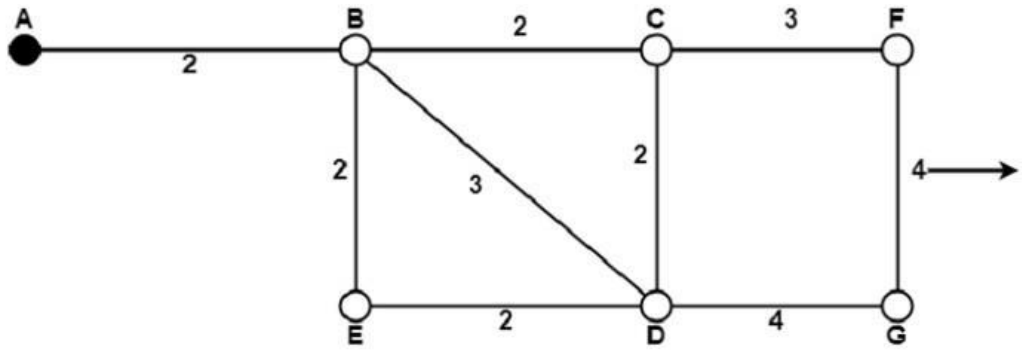
To discover the shortest path between two nodes, one can use a factor like number of hops, geographical distance, bandwidth, throughput, error rate, communication cost, measured delay, etc. Thus, algorithm chooses a cost factor (or simply cost) out of the above.

Each arc and node are labeled using this cost factor. Similarly, each node is labeled using the cost

The communication network is defined using a directed weighted graph. The nodes in the graph define switching components. The directed arcs define the communication path between switching components. Each arc has a positive weight that defines the cost. A path between two nodes can go through various intermediate nodes and arcs.

The goal of shortest path routing is to find a path between two nodes that has the lowest total cost, where the total cost of a path is the sum of arc costs in that path.

For example, Dijkstra Algorithm is considered here. Here, nodes are labelled with its distance from the source node along the better-known route. Initially, all nodes are labeled with infinity, and as the algorithm proceeds, the label may change. The labeling graph is displayed in the figure.



Graphical Representation of Nodes with labeled path

Example; Let us find the shortest path between A and G. It can be done in various passes as follows, with A as the source.

Pass 1: B(2, A), C(∞,−), F(∞,−), E(∞,−), D(∞,−), G(∞,−)

Pass 2: B(2, A), C(4, B), D(5, B), E(4, B), F(∞,−), G(∞,−)

Pass 3: B(2, A), C(4, B), D(5, B), E(4, B), F(7, C), G(9, D)

We can see that there can be two paths between A and G. One follows through ABCFG and the other through ABDG. The first one has a path length of 11, while the second one has 9. Hence, the second one, as G (9, D), is selected.

Suppose we want to find shortest path between A and D. Node D has three paths from A as ABD, ABCD and ABED. The first one has a path length of 5 rest two have 6. So, the first one is selected.

Note: All nodes are searched in various passes, and finally, the routes with the shortest path lengths are made permanent, and the nodes of the path are used as a working node for the next round.

2. Flooding:

In this algorithm every incoming packet is sent out on every outgoing line except the line on which it has arrived.

The disadvantage here is that very large number of duplicate packets are produced. Therefore, we use **selective flooding**.

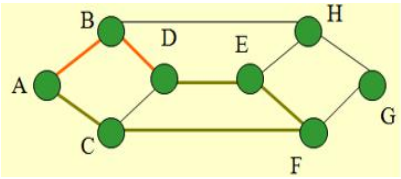
In selective flooding every incoming packet is not sent out on every output line.

Instead, packet is sent only on those lines which are approximately going in the right direction.

3. Flow Based Routing

Flow-based routing uses network topology, traffic matrices, and capacity matrices to determine static routes.

For example, in figure below, there is always a huge traffic from A to B and/or B to D.



Then the traffic from A to D should not be routed through B.

Instead route it through ACFED even though it is a longer path than ABD. This is called flow-based routing.

DYNAMIC ROUTING ALGORITHMS

Static algorithms do not take the current network load into account. So, modern computers use dynamic algorithm like distant vector routing and link state routing

1. Distance vector Routing Algorithm (Bellman-Ford routing algorithm or ford-Fulkerson algorithm).

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop in routing).

We can think of nodes as the cities in an area and the lines as the roads connecting them. A table can show a tourist the minimum distance between cities. In the figure, we show a system of five nodes with their corresponding tables.

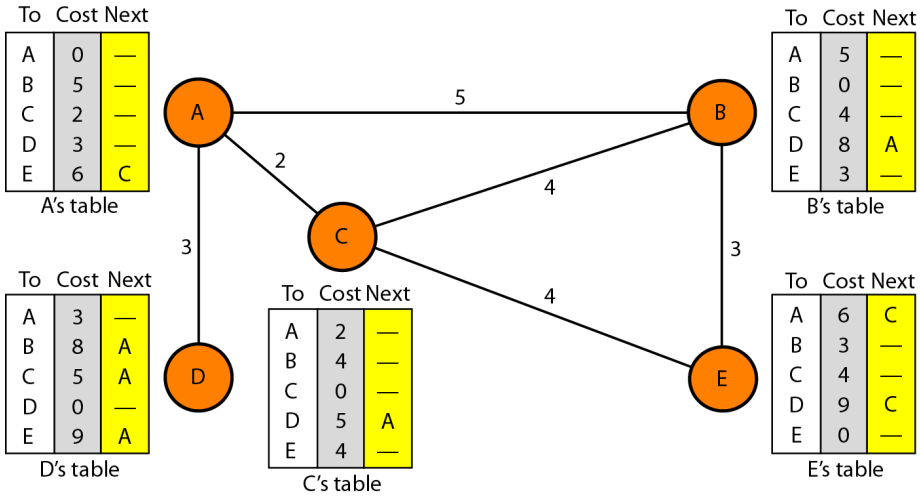


Fig. A system with 5 nodes with corresponding tables

For example, table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.

Sharing

The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So, if node C shares its routing table with A, node A can also know how to reach node E.

On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D.

In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.

There is only one problem. How much of the table must be shared with each neighbor? A node is not aware of a neighbor's table. The best solution for each node is to send its entire table to the neighbor and let the neighbor decide.

Updating

When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is *x* mi, and the distance between A and C is *y* mi, then the distance between A and that destination, via C, is $x + y$ mi.

2. The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.

3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

a. If the next-node entry is different, the receiving node chooses the row with the smaller cost.

b. If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3. Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity. Node A must not ignore this value even though its old entry is smaller. The old route does not exist anymore. The new route has a distance of infinity.

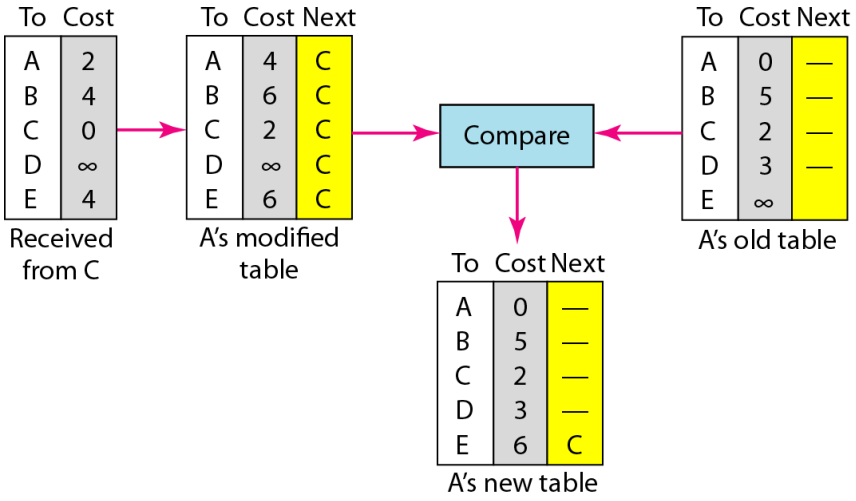


Fig. Updating of A's table

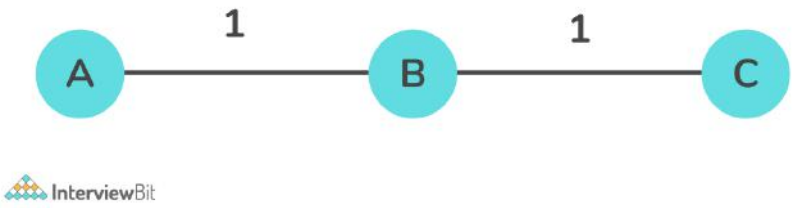
Figure shows how node A updates its routing table after receiving the partial table from node C.

There are several points we need to emphasize here. First, as we know from mathematics, when we add any number to infinity, the result is still infinity. Second, the modified table shows how to reach A from A via C. If A needs to reach itself via C, it needs to go to C and come back, a distance of 4. Third, the only benefit from this updating of node A is the last entry, how to reach E. Previously, node A did not know how to reach E (distance of infinity); now it knows that the

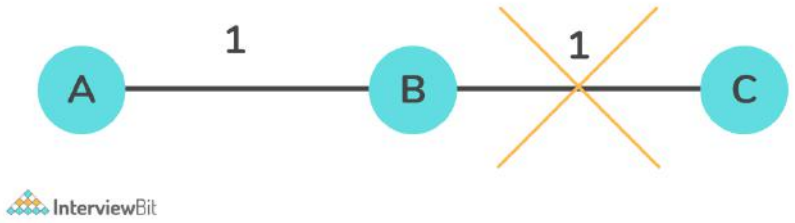
cost is 6 via C. Each node can update its table by using the tables received from other nodes. In a short time, if there is no change in the network itself, such as a failure in a link, each node reaches a stable condition in which the contents of its table remain the same.

The Count to Infinity Problem in this algorithm:

The typical situation in 'Count to Infinity' problem is that if node A tells node B that it has a path somewhere, there is no way for node B to know if the path has node B as a part of it.



Consider the above diagram, for this setup, for each router, entries are made for each other. Router A will infer that it can reach B at a cost of 2 units, and B will infer that it can reach C at a cost of 1 unit.



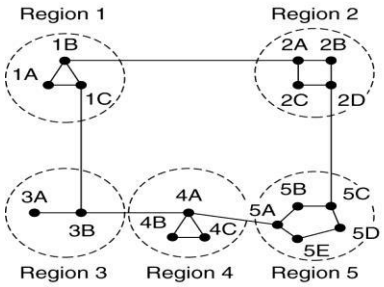
Consider the case in the above diagram, where the connection between B and C gets disconnected. In this case, B will know that it cannot get to C at a cost of 1 anymore and update its table accordingly. However, it can be possible that A sends some information to B that it is possible to reach C from A at a cost of 2. Then, since B can reach A at a cost of 1, B will erroneously update its table that it can reach C via A at a cost of 1 + 2 = 3 units. A will then receive updates from B and update its costs to 4, and so on. Thus, the process enters into a loop of bad feedback and the cost shoots towards infinity. This entire situation is called the Count to Infinity problem.

2. Link State Routing

- The link state routing is simple. Here, each router has to perform the following operations
- Each router discovers its neighbors and obtain their network addresses.
- Then it measures the delay or cost to each of these neighbors.
- It constructs a packet with these details and sends this packet to all other routers.
- Computes the shortest path to every other router.

3. Hierarchical Routing

When the network size grows, the number of routers in the network increases. Consequently, the size of routing tables increases, and routers can't handle network traffic as efficiently. We use hierarchical routing to overcome this problem. In hierarchical routing, routers are classified in groups known as '**regions'**. Each router has only the information about the routers in its own region and has no information about routers in other regions. So, routers just save one record in their table for every other region. In this example, we have classified our network into five regions.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

If 1A wants to send packets to any router in region 2 (A, B, C or D), it sends them to 1B, and so on. In this type of routing, the tables can be summarized, so network efficiency improves.

CONGESTION CONTROL TECHNIQUES

Network congestion occurs when the network is carrying more data than it can comfortably handle. It may deteriorate network service quality, resulting in queuing (waiting for transmission) delay, frame or data packet loss and the blocking of new connections.

Congestion control refers to the mechanisms and techniques used to control congestion and keep the traffic below the capacity of the network. The congestion control techniques can be broadly classified two categories:

Open loop: Protocols try to prevent or avoid congestion.

Close loop: After congestion, protocols detect it, and remove it.

Factors that Cause Congestion

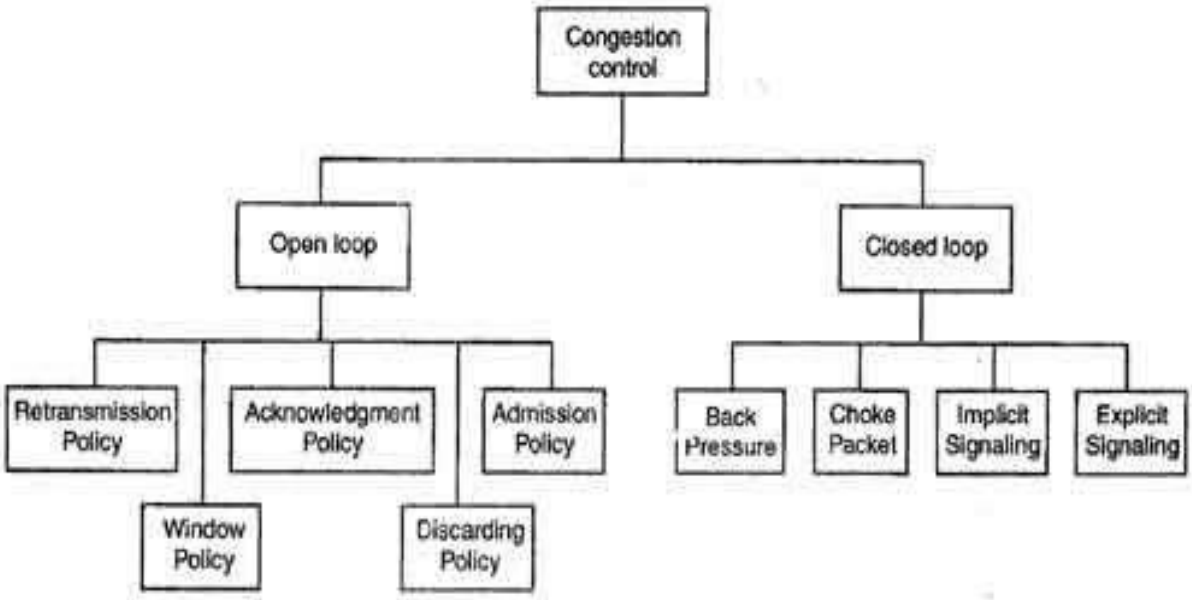
Packet arrival rate exceeds the outgoing link capacity.

Insufficient memory to store arriving packets

Bursty traffic (Unexpected or sudden network traffic)

Slow processor.

Types of congestion control methods:



Types of Congestion Control Methods

Methods used for open loop congestion control

1. Retransmission Policy

The sender retransmits a packet, if it feels that the packet sent by it is lost or corrupted.

In retransmission policy, retransmission timers are used to optimize efficiency and at the same time prevent the congestion.

2. Window Policy

To implement window policy, ‘selective reject window’ method is used for congestion control. Here, the specific lost or damaged packets are sent again. (Not all packets)

3. Acknowledgement Policy

If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

4. Discarding Policy

A router discards less-sensitive packets when congestion is likely to happen. This may prevent congestion. At the same time this may not harm the integrity of the transmission.

5. Admission Policy

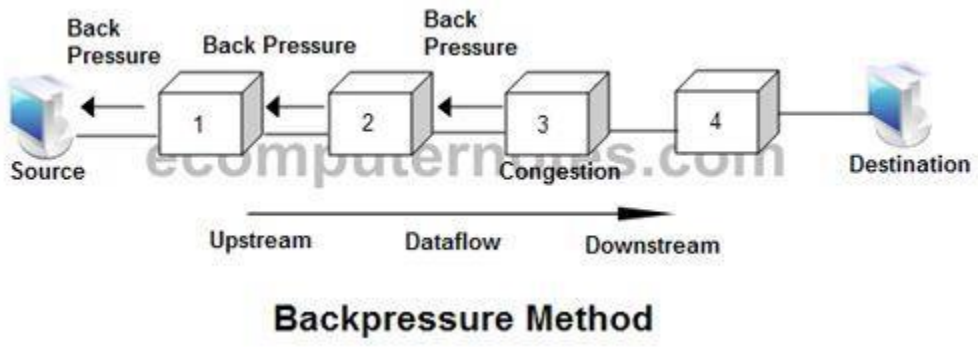
It is a quality-of-service (QoS) mechanism. It can prevent congestion in virtual circuit networks.

Here, switches in a flow should first check the resource requirement of a network flow before admitting it to the network. For example, a router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion.

Methods used for Closed Loop Congestion Control

1. Backpressure Method

Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.



Backpressure Method

In this method, the congested node stops receiving data from the immediate upstream node or nodes.

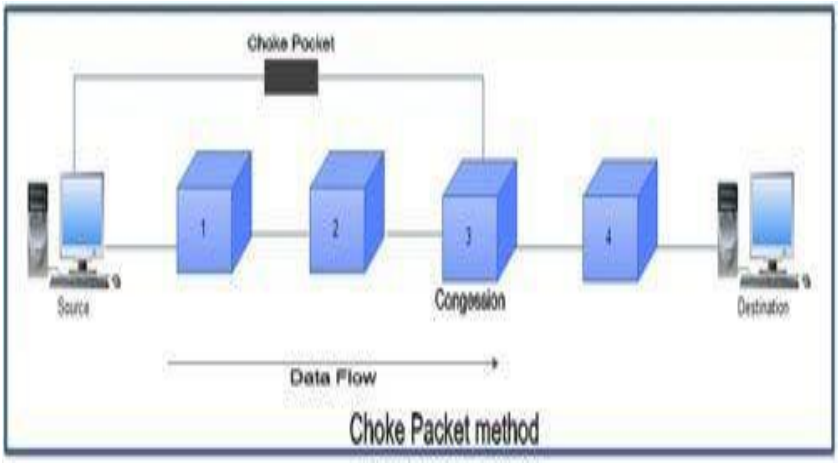
This may cause the upstream node on nodes to become congested, and they, in turn, reject data from their upstream node or nodes.

Example: As shown in fig node 3 is congested and it stops receiving packets and informs its upstream node 2 to slow down. Node 2 in turns may be congested and informs node 1 to slow down. Now node 1 may create congestion and informs the source node to slow down. In this way the congestion is reduced. Thus, the pressure on node 3 is moved backward to the source to remove the congestion.

2. Choke Packet

Here, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.

In this method, congested node does not inform its upstream node about the congestion as in backpressure method. It sends a warning directly to the source station



3. Implicit Signaling

In implicit signaling, there is no communication between the congested node (or nodes) and the source.

The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. The delay in receiving an acknowledgment is interpreted as congestion in the network. On sensing this congestion, the source slows down. This type of congestion control policy is used by TCP.

4. Explicit Signaling

• In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.

• Explicit signaling can occur in either the forward direction or the backward direction.

• In forward signaling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion.

• In backward signaling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow down.

• Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data.

CONGESTION CONTROL ALGORITHMS

1. Leaky Bucket Algorithm

Consider a Bucket with a small hole at the bottom. Then, whatever may be the rate of water pouring into the bucket, the rate at which water comes out from that small hole is constant. This scenario is depicted in figure. Once the bucket is full, any additional water entering it spills over the sides and is lost. The same idea of leaky bucket can be applied to packets, as shown in Figure. Conceptually each network interface contains a leaky bucket. And the following steps are performed:

When the host has to send a packet, the packet is thrown into the bucket.

The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.

Bursty traffic is converted to a uniform traffic by the leaky bucket.

In practice the bucket is a finite queue that outputs at a finite rate.

Whenever a packet arrives, if there is room in the queue it is queued up and if there is no room then the packet is discarded.

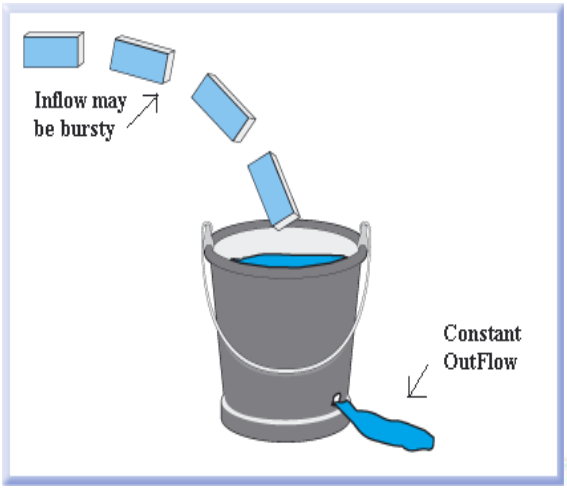


Fig (a)

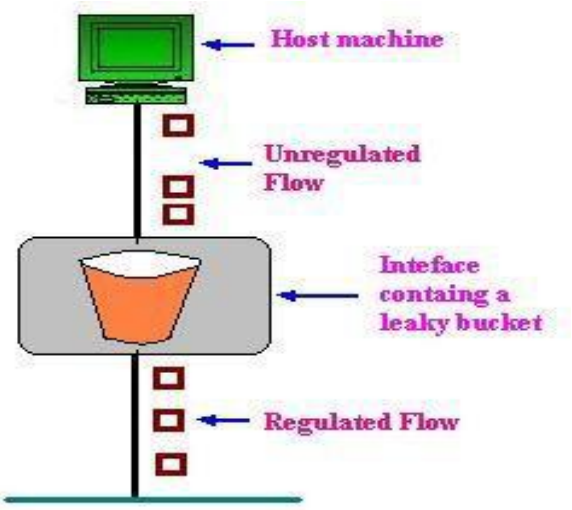


Fig (b)

Token Bucket Algorithm

The leaky bucket algorithm described above, enforces a rigid pattern at the output stream, irrespective of the pattern of the input. For many applications, when a larger burst arrives, it is better to allow the output to speed up than to lose the data. Token Bucket algorithm provides such a solution. In this algorithm leaky bucket holds token, generated at regular intervals. Main steps of this algorithm can be described as follows:

In regular intervals tokens are thrown into the bucket.

The bucket has a maximum capacity.

If there is a ready packet, a token is removed from the bucket, and the packet is sent.

If there is no token in the bucket, the packet cannot be sent.

Figure shows the two scenarios before and after the tokens present in the bucket have been consumed. In Fig. (a) the bucket holds two tokens, and three packets are waiting to be sent out of the interface, in Fig.(b) two packets have been sent out by consuming two tokens, and 1 packet is still left.

The implementation of basic token bucket algorithm is simple; a variable is used just to count the tokens. This counter is incremented every ‘t’ seconds and is decremented whenever a packet is sent. Whenever this counter reaches zero, no further packet is sent out.

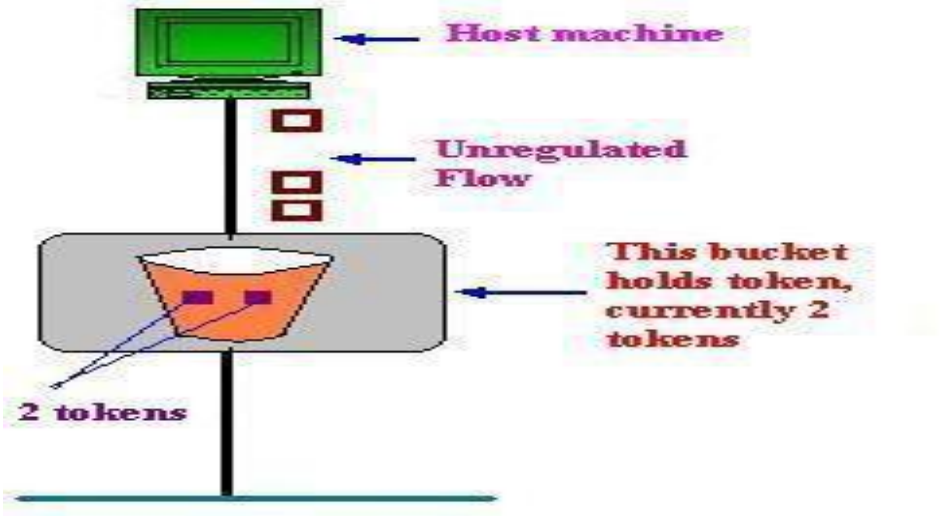


Fig (c)

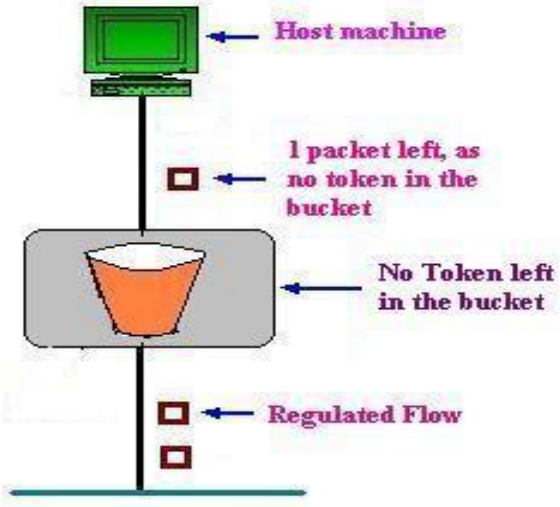


Fig (d)

Fig. (c) Token bucket holding two tokens, before packets are send out Fig (d) Token bucket after two packets are send, one packet still remains as no token is left.

IPv4 ADDRESSES

IPv4: Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). An IPv4 address is a 32-bit address. It is a unique address that universally defines the connection of a device (e.g.: a computer or a router).

Address Space: An address space is the total number of addresses used by the protocol. IPv4 protocol uses 32 bits. So, its address space is 2^{32} unique addresses. This is theoretical figure. The actual number is much less because of the restrictions imposed on the addresses.

Addressing notations:

There are two general notations to represent an 4 address: binary notation and dotted decimal notation.

Binary Notation: In binary notation, the IPv4 address is displayed as 32 bits (4 byes).

Example: 10000000 00001011 00000011 00011111

Dotted-Decimal Notation: It consists of a decimal numbers, usin full stop (dot) as separation character It is more compact and easier to read. Note that because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255

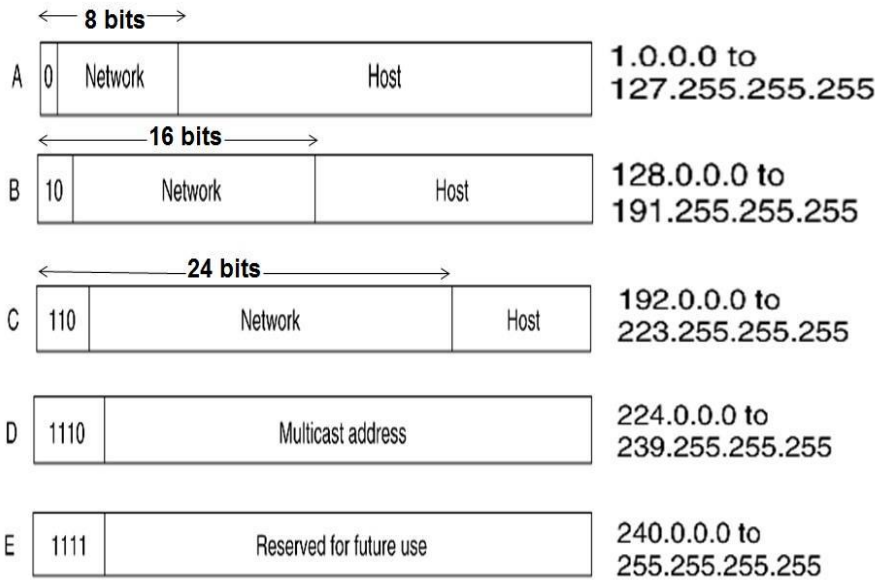
Example: 128.11.3.31

Types of Addressing: There are two types of addressing: Classful Addressing and Classless Addressing

1. Classful Addressing:

In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.

We can find the class of an address when given address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few ‘bit’s can immediately tell us the class of the address. If the address is given in decimal-dotted notation, the first byte defines the class. It is illustrated in the following figure.



Blocks: Here, each class is divided into a fixed number of blocks with each block having a fixed size. For example, in Class A **nt features of Classful addressing:**

Class A addresses were designed for large organizations. Class B addresses were designed for midsize organizations. Class C addresses were designed for small organizations.

Class A, B and C are used for unicast. Class D is used for multicasting. Class E is used for research This concept does not apply to class D and E.

Example-

Class	**Network ID**	**Host ID**
A	First byte	Last 3 bytes
B	First 2 bytes	Last 2 bytes
C	First 3 bytes	Last byte

Classful addressing is used by RIP (Routing Information Protocol) protocol.

Drawback: A block in class A address or class B address is too large for many organizations. This means most of the addresses in class A and B were wasted and were not used. A block in class C is probably too small for many organizations.

Classful addressing is almost obsolete now. It is replaced with classless addressing

2. Classless Addressing:

Classless Addressing is also known as CIDR (classless interdomain routing). In this scheme, there are no classes, but the addresses are still granted in blocks.

Important features of Classless addressing:

1. Address Blocks

In classless addressing, when an entity is to be connected to the Internet, it is given a block (range) of addresses. The size of the block (the number of addresses) depends on the nature and size of the entity. The Internet authorities impose three restrictions on classless address blocks:

The addresses in a block must be contiguous, i.e., one after another.

The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ...).

The first address must be evenly divisible by the number of addresses.

Subnet masks: A subnet mask is used to show which part of the IP address is the network portion and which part is the host portion. It is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s.

The **default mask** in IPv4 is 255.255. 0.0. Net mask and subnet mask are similar**.** But subnet masks are mostly used in network configurations, while netmasks often refer to classes of IP addresses.

The three default subnet masks are 255.0. 0.0 for Class A, 255.255. 0.0 for class B, and 255.255. 255.0 for Class C. There is no default subnet mask in classless addressing. Subnet masks used in classless addressing are described by CIDR (Classless Inter Domain Routing) notation.

Subnetting vs Supernetting:

In subnetting, a single big network is logically divided into multiple smaller subnetworks. Supernetting is the opposite of subnetting. In supernetting, multiple networks are combined into a bigger network called a supernet. A supernet consumes less address space and has smaller routing tables.

Classless addressing allows us to use Variable Length Subnet Mask (VLSM)

Different subnet masks are used in same network.

In this, there is no boundary on host id and network id

There is no default subnet mask in classless routing.

IPV4 HEADER

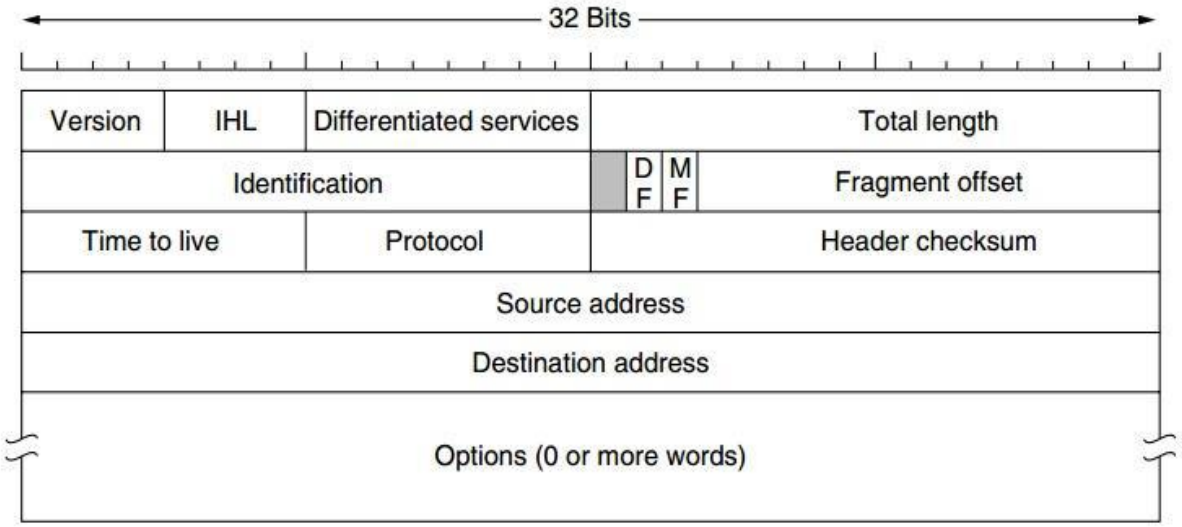


Figure 5-46. The IPv4 (Internet Protocol) header.

Version: Version no. of Internet Protocol used (e.g., IPv4).

IHL (Internet Header Length); Length of entire IP header.

DSCP (Differentiated Services Code Point): This is Type of Service. It defines the level of service received by a packet in the network.

ECN (Explicit Congestion Notification): It carries information about the congestion seen in the route.

Total Length: Length of entire IP Packet (including IP header and IP Payload).

Identification: If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.

DF and MF fields: The first bit is always set to 0. The second bit is called the DF (Don't Fragment) bit and indicates that this packet should not be fragmented. The third bit is called the MF (More Fragments) bit and is set on all fragmented packets except the last one.

Flags: If IP Packet is too large to handle, these 'flags' tell us if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.

Fragment Offset: This offset tells the exact position of the fragment in the original IP Packet.

Time to Live (TTL): It tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded. To avoid looping in the network, every packet is sent with some TTL value set,

Note: A network loop occurs when a network has more than one active path carrying information from the same source to the same destination. The information loops and amplifies itself using the additional path instead of stopping when it reaches its destination.

Protocol: It tells the Network layer at the destination host, to which protocol this packet belongs to (i.e., the next level Protocol). For example, protocol number of ICMP is 1, TCP is 6 and UDP is 17.

Header Checksum: This field is used to keep checksum value of entire header.

Source Address: 32-bit address of the sender (or source) of the packet.

Destination Address: 32-bit address of the receiver (or destination) of the packet.

Options: If the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc. This is optional field.

IPv6 ADDRESSES

IPv6 addresses consist of 128 bits, instead of 32 bits, and include a scope field that identifies the type of application suitable for the address. IPv6 does not support broadcast addresses. But it uses multicast addresses for broadcast. In addition, IPv6 defines a new type of address called anycast address.

Structure

An IPv6 address consists of 16 bytes (128 bits).

Hexadecimal Colon Notation

IPv6 is specified hexadecimal colon notation. In this notation, 128 bits are divided into eight groups, each of 16 bits. Each group is expressed as four hexadecimal digits. Every four hexadecimal digits are separated by a colon.

Example IPv6 address:

Original form:

FDEC:0074:0000:0000:0000:B0FF:0000:FFF0

Abbreviated form: Here, the leading zeros in a byte can be omitted. So we write

FDEC: 74:0:0:0:B0FF:0:FFF0

More abbreviated form: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign :: (See 3rd, 4th, and 5th blocks). So, we write

FDEC:74::B0FF:0:FFF0

Address Space

IPv6 has a much larger address space; 2^{128} addresses are available. The designers of IPv6 divided the address into several categories. A few leftmost bits, called the type prefix, in each address define its category.

Unicast address: A **unicast address** refers to a single computer. IPv6 defines two types of unicast addresses: geographically based and provider-based.

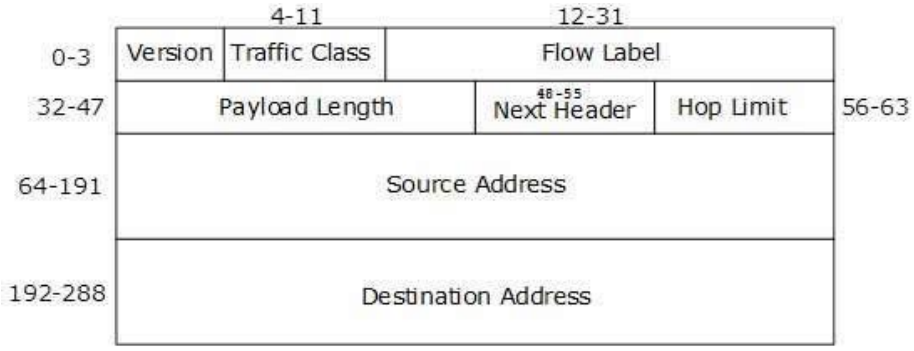
Multicast Addresses: Multicast addresses are used to define a group of hosts instead of just one.

Anycast Addresses: Here multiple computers have same IP address. However, a packet destined for an anycast address is delivered to only one of such computers. It is the nearest one (the one with the shortest route).

Reserved Addresses: Another category in the address space is the reserved address. These addresses start with eight 0s (type prefix is 00000000).

Local Addresses: These addresses are used when an organization wants to use IPv6 protocol without Internet. In other words, they provide addressing for private networks.

IPv6 header:



Version: 4-bit version number of Internet Protocol = 6.

Traffic class: 8-bit traffic class field. It helps routers to handle the traffic based on priority of the packet. If congestion occurs on router, then packets with least priority will be discarded.

Flow label: 20-bit field. Flow Label field is used by source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers

Payload length: It is a 16-bit (unsigned integer) field, indicates total size of the payload. It tells routers about amount of information a particular packet contains in its payload.

Next header: Next Header indicates type of extension header (if present) immediately following the IPv6 header.

Code	*Next Header*
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no next header)
60	Destination option

Hop limit: Hop Limit field is same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and packet is discarded if value decrements to 0..

Source address: 128 bits. The address of the initial sender of the packet.

Destination address: 128 bits. The address of the intended recipient of the packet.

External Headers: IPv6 introduces the concept of (optional) **extension headers**. These headers provide extra information, and encoded in an efficient way. Six kinds of extension headers are defined at present, as listed in table

External Header	**Description**
Hop-by-hop options	Examined by all devices on the path
Destination options (with routing options)	Examined by destination of the packet

Routing Header	Methods to take routing decisions
Fragment Header	Contains parameters of fragmented datagram done by source
Authentication header	Verify authenticity
Encapsulating Security Payload	Carries encrypted data

Comparison of IPv6 over IPv4

S.No.	Characteristic	IPv4	IPv6
1	Address length	32-bits	128-bits
2	Address space	2^{32}	2^{128}
3	Address representation	Binary or dotted decimal notation	Hexadecimal notation
4	Header length	Variable (20 to 40 bytes)	Fixed (40 bytes)
5	Flow label field	**No**	**Yes**
6	Checksum field	**Yes**	**No**
7	Transmission Scheme	Broadcast	Multicast and Anycast
8	Encryption & Authentication	**No**	**Yes**

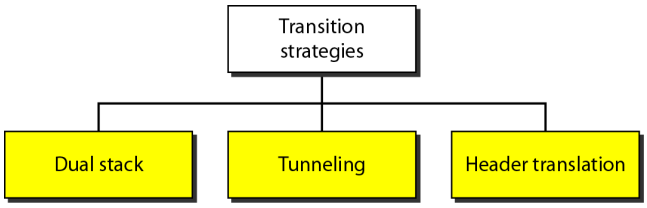
Fields present in IPv4 and eliminated in IPv6:

Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

Advantages of IPv6 over IPv4

- Larger address space
- Simple header format
- Flexible options and extensions
- More security
- Easier administration
- Routing more efficient and hierarchical, because of smaller routing tables

Transition from IPv4 to IPv6:



Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6.

Transition strategies: Dual Stack, Tunneling, and Header Translation

(i) Dual stack

Dual stack means that devices are able to run IPv4 and IPv6 in parallel. Here, every networking device, server, switch, router, and firewall in an ISP's network will be configured with both IPv4 and IPv6 connectivity capabilities. This allows hosts to simultaneously reach IPv4 and IPv6 content. It offers a very flexible coexistence strategy.

(ii) Tunnelling

Tunnelling provides a way to use an existing IPv4 routing infrastructure to carry IPv6 traffic. i.e., routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves.

(iii) Header Translation by using NAT Protocol :

Suppose a host with IPv4 address sends a request to an IPv6 enabled server on Internet. Then it does not understand IPv4 address. In this scenario, a NAT-PT (Network Address Translation – Protocol Translation) enabled device can help them communicate.

When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa.

Header Translation Procedure
1. The IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32 bits.
2. The value of the IPv6 priority field is discarded.
3. The type of service field in IPv4 is set to zero.
4. The checksum for IPv4 is calculated and inserted in the corresponding field.
5. The IPv6 flow label is ignored.
6. Compatible extension headers are converted to options and inserted in the IPv4 header. Some may have to be dropped.
7. The length of IPv4 header is calculated and inserted into the corresponding field.
8. The total length of the IPv4 packet is calculated and inserted in the corresponding field.

CONNECTING DEVICES

1. Repeater:

A repeater is a network device that operates at **physical layer**. It is also called signal booster. During long distance transmission, the signals get weaker. Repeaters are used to receive, amplify and retransmit such weak signals.

Advantages: 1. Repeaters are cost-effective and easy to use. 2. They don't affect the network performance.

Disadvantage: While amplifying the signals, the repeaters also amplify the noise level in those signals.

2. Hub:

A hub is a multi-port network device that operates at **physical layer**. It is used to connect multiple devices in a network. It uses star topology. Hubs cannot filter data, so data packets are sent to all connected devices (broadcasting). It uses **half duplex transmission mode.** There are 3 types of hubs.

Active Hubs: Active hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serve both as a repeater as well as connecting center.

Passive Hubs: These are the hubs which collect wiring from nodes and power supply from active hub. They transmit signals without amplifying or regenerating them.

Intelligent Hubs: They are active hubs that provide additional functions like network management, switching. They provide flexible data rates.

3 Switch:

A switch is a multi-port hardware network used to connect various nodes (devices) in a computer network. It operates at **data link layer.**

When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s) using MAC addresses and packet switching technique. It supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.

It can perform error checking before forwarding data

4. Router:

A router is a device like a switch that routes data packets from source to destination, based on their IP addresses. Router is mainly a **network layer** device. Routers normally connect LANs and WANs together. They build a routing table based on ARP requests and determine the best path to send packets.

Routers are generally a mixture of hardware and software. The hardware includes physical interfaces to various networks, while the software consists of operating system and routing protocol.

5. Bridge:

A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. A bridge operates at **data link layer**. It uses the MAC addresses of source and destination. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects.

6. Gateway:

A gateway is a network node that connects two networks. It converts data from one protocol or format to another. In other words, it can link two dissimilar LANs. So, gateways are also called protocol converters.

Gateways can operate at **any network layer.**

A Gateway serves as an entry and exit point for a network.

Gateways are generally more complex than switches or routers.

7. Brouter (Bridge Router):

A brouter is a network device that functions both as a bridge and a router. Working as router, it is capable of routing packets across networks. Working as bridge, It can forward data between networks.

It can work either at **data link layer or** at **network layer.**

It has better security over any other network relating device

The main disadvantage of the gateway is that gateways are slow because they need to perform intensive conversions.

VIRTUAL LAN (VLAN)

A VLAN is roughly defined as a LAN configured by software, not by physical wiring.

Switched LAN:

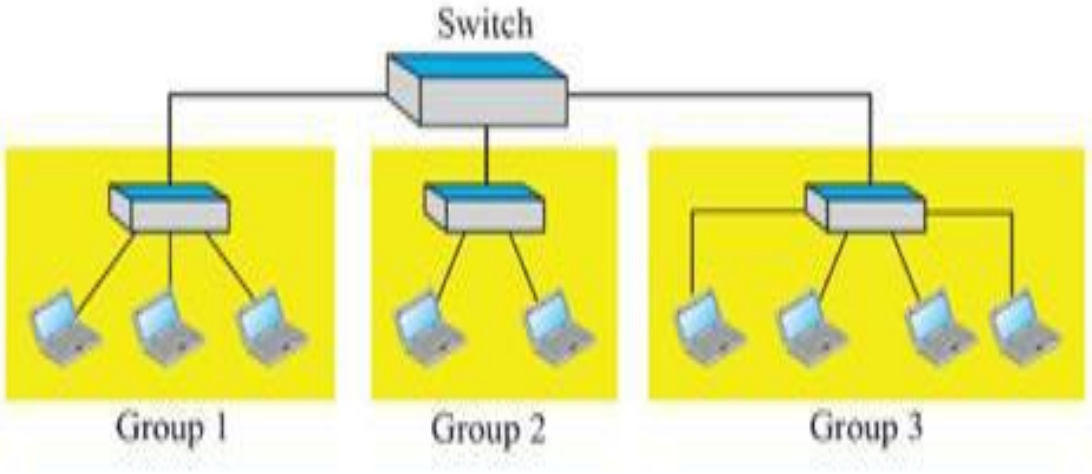


Fig.: A switch connecting three LANs

Figure shows a switched LAN in an engineering firm. Here, 9 stations are grouped into three LANs and are connected by a switch. The first 3 engineers work together as the first group, the next 2 engineers work together as the second group, and the last 4 engineers work together as the third group. The LAN is configured to allow this arrangement.

What would happen if the administrators needed to move engineers from one group to other?

The LAN configuration has to be changed.

The network technician must rewire.

Thus, in a switched LAN, changes in the work group means physical changes in the network configuration.

VLAN:

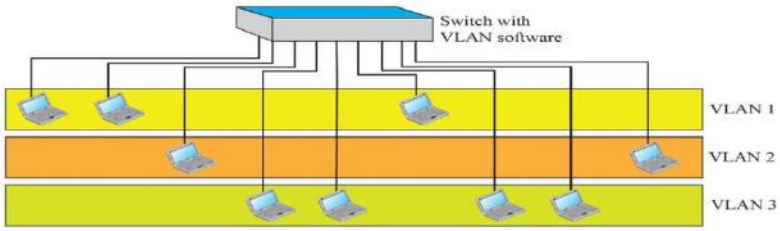


Fig.: The same switched LAN divided into VLANs.

A LAN can be divided into several logical LANs called VLANs. Each VLAN is a work group in the organization.

If a person moves from one group to another, there is no need to change the physical configuration. The group membership in VLANs is defined by software, not hardware.

Any station can be logically moved to another VLAN. All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN.

Grouping of stations connected to different switches in VLAN:

Figure shows a backbone local area network with two switches and three VLANs. Stations from switches A and B belong to each VLAN.

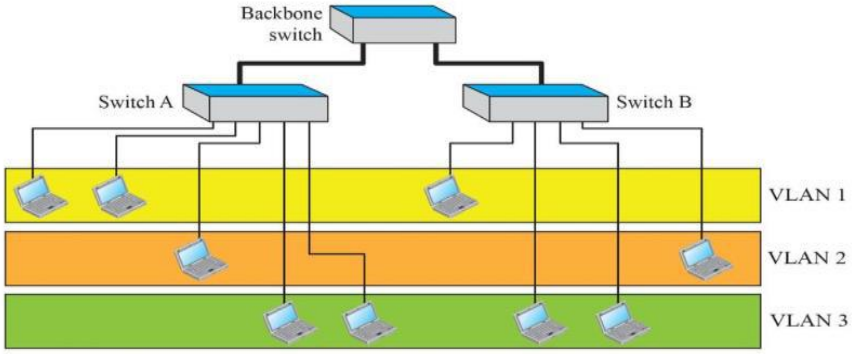


Fig.: Two switches with a backbone using VLAN software

Important features:

1. Membership characteristics:

Vendors use different characteristics such as port numbers, 48-bit MAC addresses, 32-bit IP addresses, IP multicast addresses, or a combination of two or more of these, as membership characteristics. Recently a new software is available from some vendors. It allows all these characteristics to be combined.

2. Assigning stations to LANS to VLAN (Configuration):

Manual Configuration

The administrator types the port numbers, the IP addresses, or other characteristics, using the VLAN software, to assign the stations into different VLANs.

Automatic Configuration

The stations are automatically connected or disconnected from a VLAN using criteria defined by the administrator.

Semiautomatic Configuration

Initializing is done manually, with migrations done automatically.

3. Communication Between Switches: Table maintenance, frame tagging, and time-division multiplexing are used for this purpose.

Advantages of VLANs:

- Cost and time reduction
- Creating virtual work groups
- Security

HARDWARE ADDRESSING VERSUS IP ADDRESSING

Hardware Addressing:

The hardware address is also called a physical address, Ethernet address, or media access control (MAC) address. It's a unique identifier for your hardware. it can be easily identified by your local area network or any network.

MAC address formats:

MAC-48: Format form is in six groups, and each group consists of two hexadecimal digits and is separated by hyphens. (01-02-03-04-ab-a1)

EUI-48: Format form is in six groups, and each group consists of two hexadecimal digits but is separated by colons. (01:02:03:04:ab:a1)

EUI-64: Format form is in three groups, and each group consists of four hexadecimal digits and is separated by dots. (0102. 0304.aba1)

IP Addressing:

IP Address means Internet Protocol address. It is an identifier (a numerically label) for your computer network. It has two principal functions: your network interface identification and

location addressing. It is responsible for connecting you with your private or public network through network interface. There are two types of address assignment:

Static IP address: It is an IP address manually assigned to a computer by an administrator or ISP (Internet service provider). This IP address does not change.

Dynamic IP address: It is an IP address usually assigned dynamically on LANs and broadband networks by DHCP (Dynamic Host Configuration Protocol). This IP address changes constantly.

IP address formats:

IPv4 uses 32-bit IP addresses, whereas IPv6 uses 128-bit IP addresses

Example:

IPv4: 192.168.1.1

IPv6: F232:F200:3204:0B00

Comparison

S.No.	MAC Layer	IP Address
1	MAC Address stands for Media Access Control Address	IP Address stands for Internet Protocol Address
2	It is physical address	It is logical address
3	NIC Card's Manufacturer provides the MAC Address.	DHCP, Network administrator or Internet Service Provider provides IP Address
4	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network
5	ARP protocol can find MAC address using IP address	RARP protocol can find IP address using MAC address
6	MAC Address is implemented in the data link layer	IP Address is implemented in the network layer

UNIT-V

TRANSPORT LAYER

Syllabus contents: Transport Layer Protocols: UDP and TCP, ATM, Cryptography, Network Security.

TRANSPORT LAYER

Main function of Transport Layer is **Process to process delivery.** Transport Layer uses TCP (Transmission Control Protocol), UDP (User Datagram Protocol), DCCP (Datagram Congestion Control Protocol), etc.

Basic unit of data in the Transport Layer is called 'segment'. It is also called Transport Protocol Data Unit (TPDU) for messages.

Responsibilities/Services of Transport Layer:

- **Process to process delivery:**
  Many processes (programs) run on the host. Hence host to host delivery is not enough. Process-to-process delivery is essential. For this, each process is assigned a 16-bit address called port number. It is used to identify any client-server program uniquely.
- **Multiplexing and Demultiplexing:**
  Multiplexing: The transport layer sends packet streams from various applications simultaneously over a network using port numbers.
  Demultiplexing: The sent packets are recovered and delivered to the appropriate process running on the receiver.
- **Congestion Control:**
  Network congestion occurs when the network is carrying more data than it can handle. It results in waiting delay and loss of packets. So, some packets have to be retransmitted. This further increases the congestion. Transport layer uses **open loop** congestion control to prevent the congestion and **closed loop** congestion control to remove the congestion in a network.
- **Flow control:**

Flow control is the process of managing the rate at which data is transmitted. Using flow control, a receiver can signal that it is not ready to receive data. Transport layer provides flow control using sliding window protocol.

- **Error Control and data integrity:**
  The transport layer performs error checking in the messages by using error detection codes and computing checksums. This ensures **integrity (accuracy) of data**.

Transport Layer Primitives (operations or activities):

1. Listen: When server is ready to accept a connection request from a client, it puts (executes) this primitive into action and waits for the request.

2. Connect: This primitive is used to establish connection with the waiting peer. When a client wants to talk to the server, it executes a CONNECT primitive. Then--
A '**Connection Request TPDU'** is sent to the server. On receiving it server sends a **'Connection Accepted TPDU'** back to the client. Thus, the connection is established.

3. Receive: Receive primitive simply waits for incoming message. Client transmits its request and puts receive primitive into action to get the reply.

4. Send: client puts this primitive into action. Send primitive simply sends or transfers the message to the peer.

5. Disconnect: This primitive is simply used to terminate or end the connection. 'Disconnection' has two variants:

(i) Asymmetric variant: Either of the transport user can issue a DISCONNECT primitive. Then a Disconnect TPDU being sent and the connection is released.
(ii) Symmetric variant: Connection is released when both sides have done a DISCONNECT.

Quality of service (QoS) parameters:

Quality of service (**QoS**) is the description or measurement of the overall performance of a service (Examples: Telephone network or computer network). It is particularly the performance seen by the users of the network. QoS can be quantitatively measured using parameters described below.

- **Packet loss** Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is commonly caused by

network congestion, hardware issues, software bugs, and other factors. 1 to 2.5% t packet loss is acceptable.

- **Latency** is the time it takes a packet to travel from its source to its destination. Latency should be as close to zero as possible. If a voice over IP call has a high amount of latency, it can experience echo and overlapping audio.
- **Jitter**: Jitter is the amount of inconsistency in latency across the network. Jitter is the result of network congestion and sometimes route changes. Too much jitter can degrade the quality of voice and video communication. It can cause flickering in display monitors and delayed data transmission.
- **Bandwidth (throughput):** Bandwidth is the capacity of a network link to transmit the data from one point to another in a given amount of time. QoS optimizes the network by managing bandwidth and setting priorities for applications that require more resources than others.
- **Availability:** Availability refers to the operational status of a computer network and its ability to quickly make connections, process traffic, and respond to user requests. It is measured as the average percentage of time during which the network is performing its intended function.
- **Minimum and average arrival times** in case of connectionless protocols like UDP.

UDP (USER DATAGRAM PROTOCOL)

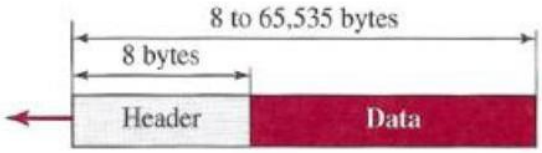
UDP is a connectionless, datagram service. Connectionless means delivery of message is not guaranteed. So, it is unreliable. It works on the top of IP.

UDP is a much simpler protocol without connection setup delays, flow control, and retransmission. An application program uses UDP if the simplicity and speed are more important than reliability. In other words, UDP is suitable for time-sensitive applications.

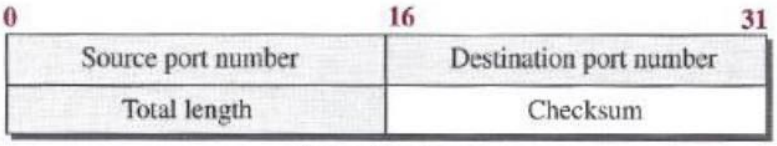
User Datagram

UDP packet is called datagram. It has a fixed-size **header** of 8 bytes made of four fields. Length of each field is 2 bytes.

User datagram packet format



a. UDP user datagram



b. Header format

'Source port number' and 'destination port number' define application numbers (16 bits) of source and destination respectively. 'Total length' field has 16 bits. It can indicate 0 to 65,535 bytes. However, the total length needs to be less because a UDP user datagram is stored in an IP datagram with the total length of 65,535 bytes. The last field can carry the optional checksum.

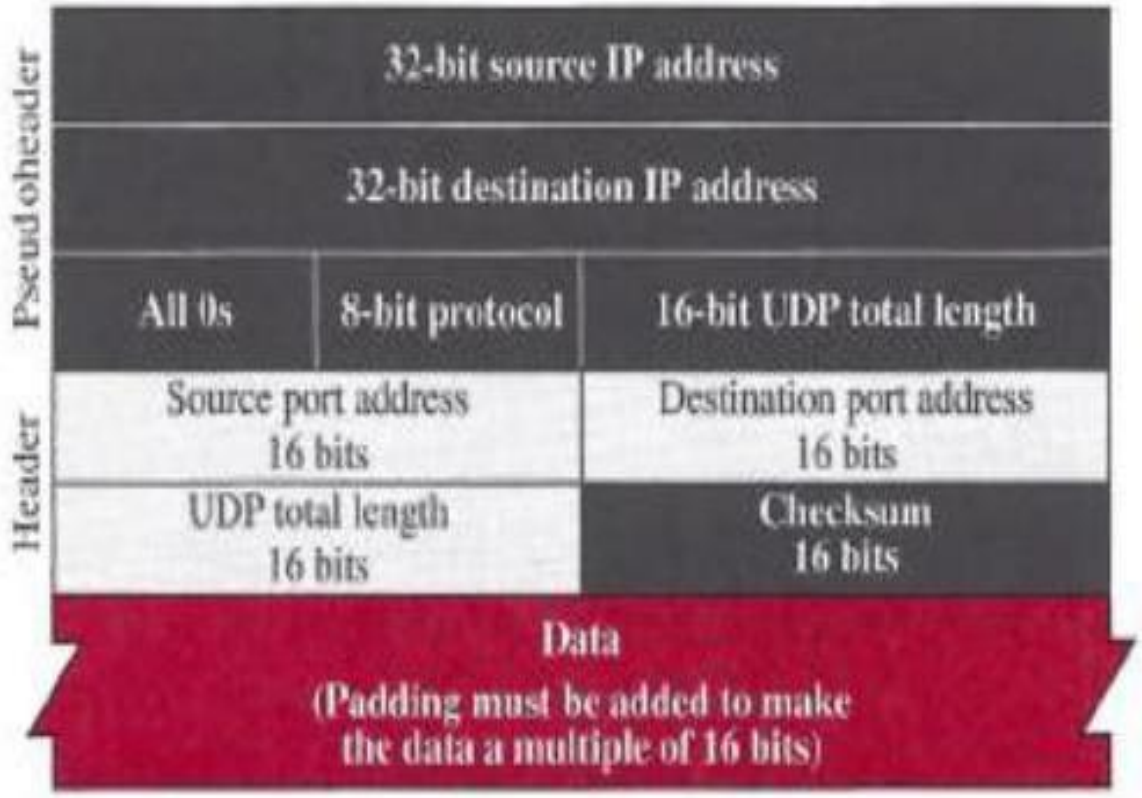
UDP Services

- Process-to-Process Communication.
- Connectionless Services.
- Flow Control; There is **no flow control**
- Error Control: Error control is only provided by using checksum

UDP checksum calculation:

It includes three sections: a pseudo header, the UDP header, and the data coming from the application layer. The pseudo header is the part of the header of the IP packet in which the user datagram is to be encapsulated with some fields filled with 0s

Pseudoheader for checksum calculation



Typical UDP Applications

- Used when speed is more important and flow and error control are not important

  Example: Voice over IP (VoIP)
- Used for a process with internal flow-and error-control mechanisms

  Example: such as TFIP (Trivial File Transfer Protocol)
- Used for multicasting.

  Example: Videoconferencing
- Used for management processes

  Example: Simple Network Management Protocol (SNMP)
- It is used for some route updating protocols

  Example: RIP (Routing Information Protocol)

TCP (TRANSMISSION CONTROL PROTOCOL)

Transmission Control Protocol (TCP) is a connection-oriented protocol. TCP explicitly defines connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service. It is a reliable protocol, since delivery of message is guaranteed.

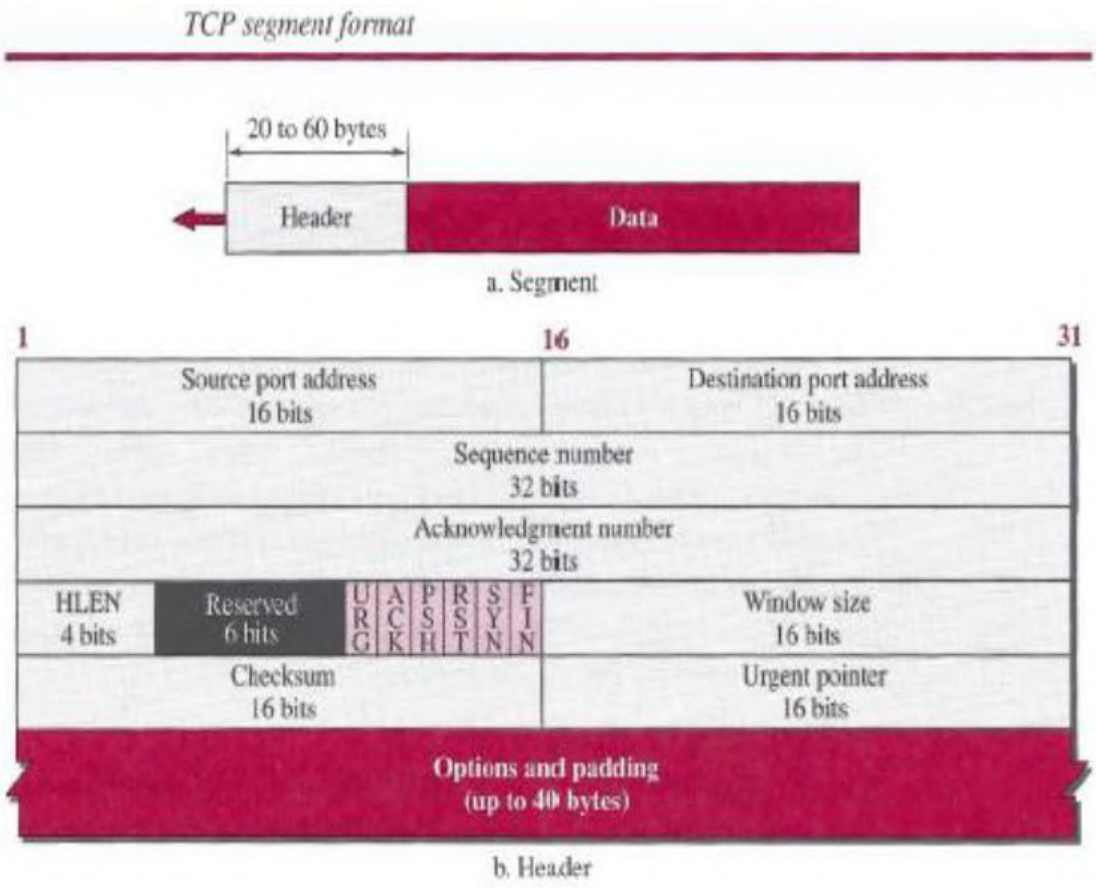
TCP is used extensively by many **Internet applications**, including the World Wide Web (WWW), email, File Transfer Protocol, Secure Shell, peer-to-peer file sharing, and streaming media.

TCP Services:

- Process-to-Process Communication
- Stream Delivery Service (data stream means data that is generated continuously by many data sources)
- Segmentation
- Full-Duplex Communication
- Reliable Service

Format:

The segment consists of a header of 20 to 60 bytes, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options.



Source port address This is a 16-bit field that defines the port number of the application program in the host that is sending the segment.

Destination port address This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment.

Sequence number This 32-bit field defines the number assigned to the first byte of data contained in this segment.

Acknowledgment number This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party.

HLEN (Header length): This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes.

Reserved. This is a 6-bit field reserved for future use.

Control. This field defines 6 different control bits or flags as shown in Figure. One or more of these bits can be set at a time.

URG: URG flag is used to inform a receiving station that certain data within a

segment should be processed immediately. If the URG flag is set, the receiving station evaluates the urgent pointer, a 16-bit field in the TCP header.

ACK: Acknowledgment is valid.

PSH: Request for push. It informs the receiver that the data should be pushed up to the receiving application immediately.

RST: Reset the connection

SYN: Synchronize sequence numbers.

FIN: Finish (Terminate) the connection.

Window size: Window size is how much data (in bytes) the receiving device is willing to receive at any point in time. The length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes.

Checksum: This 16-bit field contains the checksum. The calculation of the checksum for TCP is similar to that for UDP.It

Urgent pointer: This l6-bit field, which is valid only if the urgent flag is set. It is used when the segment contains urgent data.

Options. There can be up to 40 bytes of optional information in the TCP header.

Important Features of TCP

1. Re-transmission

The heart of the error control mechanism is the retransmission of segments. When a segment is corrupted, lost, or delayed, it is retransmitted. In modern implementations, a segment is retransmitted on two occasions:

- When a retransmission timer expires, it retransmits.
- TCP detects a packet loss through the receipt of a number of duplicates. When the sender receives three duplicate ACKs, it retransmits.

Note that no retransmission occurs for segments that do not consume sequence numbers. In particular, there is no retransmission for an ACK segment.

2. Congestion Control and Flow Control

Congestion Control: Network congestion occurs when the network is carrying more data than it can handle. It results in waiting delay and loss of packets. Hence, some packets have to be retransmitted. This further increases the congestion. Transport layer uses **open loop** congestion control to prevent the congestion and closed loop congestion

control to remove the congestion in a network. Here, receiver sends signals to slow down the process or delay the transmission. Thus, right amount of data is being transmitted.

Flow Control: Flow control is the process of managing the rate at which data is transmitted. Using flow control, a computer receiving data can signal that it is not ready to receive data. It is essential when receiver is slower than sender. TCP provides a flow control mechanism using acknowledgements of TCP sequence numbers.

5. Error Control

To provide reliable service, TCP implements an error control mechanism.

Error detection using the checksum, retransmission and acknowledgements are used in error control.

3. Unique Identification

In TCP each computer on the network has been assigned with a unique IP address over the network. Besides that, each domain is assigned with a name. Therefore, ultimately TCP provides benefits of name and address resolution services.

4. In Order Delivery

In computer networking, out-of-order delivery is the delivery of data packets in a different order from which they were sent. One of the functions of TCP is to prevent the out-of-order delivery of data, either by reassembling packets in order or requesting retransmission of out-of-order packets. Finally, the packets reach destination in order

Disadvantages of TCP

1. Slow Start: The process of TCP is always slow at the beginning. TCP is comparatively slower than UDP. Whenever there is a data congestion, TCP will be slowing down so that it can send traffic in a steady rate.

2. Image Blockings: Suppose a webpage has many images. If one image Is lost, other images can't be loaded.

3. Slow Handshake process.

4. Originally a TCP connection is optimized only for WAN, but not for LAN or PAN (Personal Area Network) .

TCP Connection Management:

Handshaking: Handshaking is the process of establishing communication between two networking devices. It determines which protocols, speeds, compression, and error-

correction schemes will be used during the communication session. The type of handshaking used in setting up TCP connection is called 3-way handshaking, because it involves 3 messages.

(i) Connection establishment

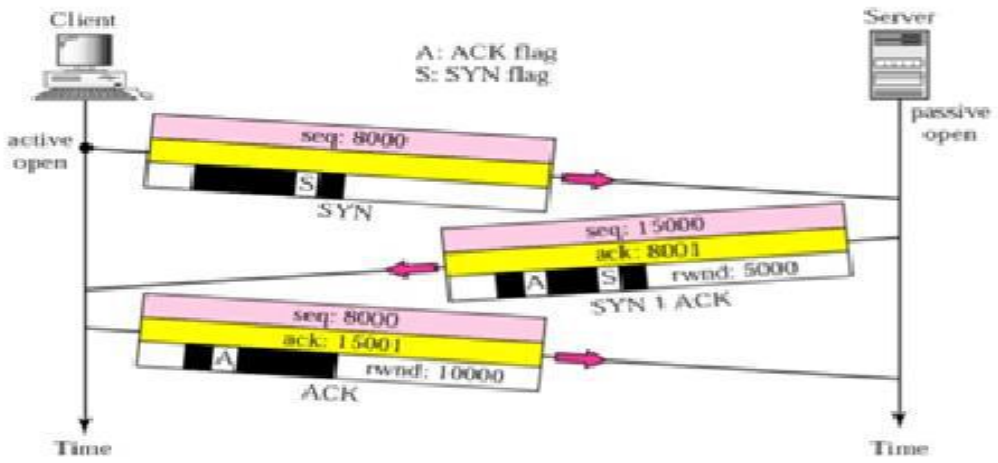


Fig. Connection establishment

- Client sends a 'SYN' segment, with SYN flag set, but no data. It is for synchronization of sequence numbers. It consumes one sequence number.
- Then server sends a 'SYN + ACK' segment, with 2 flag bits set: SYN and ACK. This segment has a dual purpose. It acts as a SYN segment for communication in the other direction. It also serves as acknowledgment for the first SYN segment. It cannot carry data. But it consumes one sequence number.
- Client sends an 'ACK' segment for the above segment, which has ACK flag and acknowledgment number fields. Note that the sequence number in this segment is the same as the one in the first SYN segment. i.e., it does not consume any sequence numbers.

Active Open, Passive Open and Simultaneous Open

- **Active Open:** client process initiates the connection by sending a SYN message to start the connection.
- P**assive OPEN:** It specifies that server process is waiting for an active OPEN

from a specific client.

- **Simultaneous Open** (it is rare): Both processes issue an active open, both TCPs transmit a SYN + ACK segment to each other. One single connection is established between them.

(ii) Data Transfer

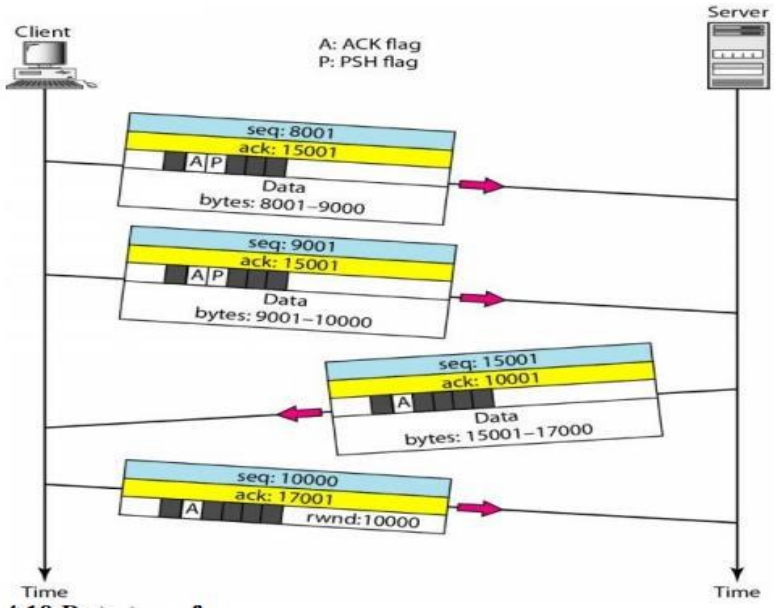


Fig. Data transfer

After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgments.

A variable field called 'Receiver Window (rwnd)' is used to indicate amount of data that the destination can receive. Its purpose is to regulate data flow and minimize congestion, and improve network performance.

(iii) Connection Termination

Client or server can close the connection, although it is usually initiated by the client.

1. When client issues close command, its TCP sends a 'Finish (FIN)' segment with FIN flag set.

   It may have the last chunk of data sent by the client. If it does not carry data, it consumes only one sequence number

2. Second segment: It sends the a 'FIN + ACK' segment, to confirm the receipt of the FIN segment from the client. It also announces the closing of the connection in the other direction.

   This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number
3. Third segment: The client TCP sends an 'ACK' segment where acknowledgement number = sequence number in Fin segment from server + 1. Thus, it confirms the receipt of the FIN segment from the TCP server.

   This segment cannot carry data and consumes no sequence numbers.

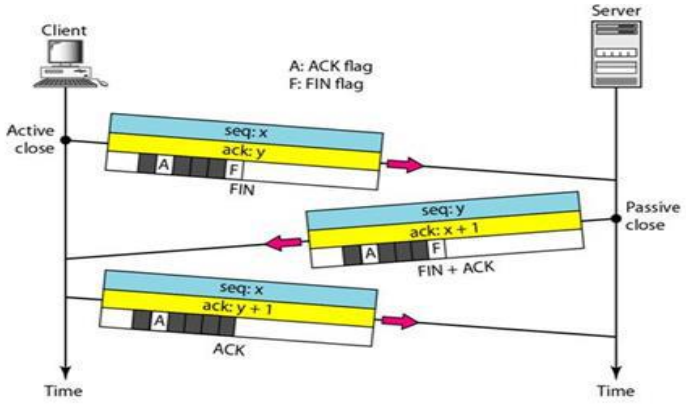


Fig. Connection Termination

ATM (ASYNCHRONOUS TRANSFER MODE)

Asynchronous Transfer Mode (ATM) is an ITU-T standard that is based on cell-switching) technology. *ITU-T stands for International Telecommunication Union-Telecommunications Standards Section.* ATM is called cell-switching (or cell relay) technology because it uses fixed length packets. In packet switching technology, the packets are of variable lengths, but in cell switching, packets have a fixed length of 53 bytes with a 5-byte header.

Important features of ATM:

- It is a connection-oriented technology.
- It involves dedicated full duplex communication between network and end points.

- An ATM network consists of a set of ATM switches interconnected by point-to-point ATM links or interfaces.
- QoS is an important feature of the network.
- It is more efficient than circuit switching

Benefits of ATM:

- It provides dynamic bandwidth that is particularly suited for bursty traffic.
- Small sized header reduces packet overload, thus ensuring effective use of bandwidth.
- Small and fixed cells ensure simple data transmission.
- Mixed traffic is handled efficiently.
- Supports multiservice traffic: It allows multimedia data. i.e., Text, audio data, video data, graphics and animations (e.g.: cartoon images) in one network. It also supports internetworking.
- Scalability in speed and network size.
- Suitable to LAN and WAN

Types of ATM Networks:

1. Public ATM Network:

- It is provided by public telecommunications carriers (BSNL, Airtel, Reliance Communications, etc., in India)
- It interconnects
  - Private ATM networks.
  - Remote non-ATM LANs.
  - Individual users.

2. Private ATM Network:

- It is owned by private organizations.
- Interconnects low speed, shared medium LANs.
  Examples: Ethernet, Token Ring.
- Interconnects individual users as the front-end LAN for high performance or multimedia applications

ATM Cell Format ATM switches support two primary types of interfaces: (UNI) and

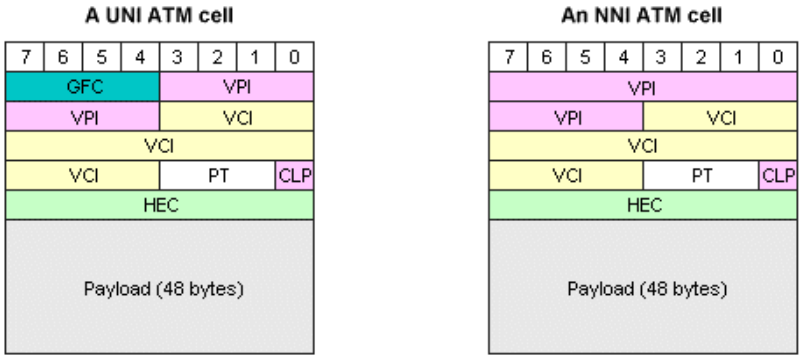
(NNI). UNI is used to connect ATM end systems (such as hosts and routers) to an ATM switch. NNI connects two ATM switches. UNI and NNI can be further subdivided into public and private UNIs and NNIs.

ATM transfers information in fixed-size units called cells. Each cell consists of 53 bytes as shown in Fig. The first 5 bytes contain cell-header information, and the remaining 48 contain the payload (user information).

Header **5 bytes**	**Payload** **48 bytes**

Figure: ATM cell Format

An ATM cell header can be one of two formats: User-Network Interface (UNI) and Network-Network Interface (NNI). The UNI header is used for communication between ATM endpoints and ATM switches in private ATM networks. The NNI header is used for communication between ATM switches. Both headers are shown in figure.



- **Generic Flow Control (GFC):** Provides local functions. (e.g.:identifying multiple stations that share a single ATM interface). This field is typically not used and is set to 0000.
- **VPI (Virtual Path Identifier) and VCI (**Virtual Connection Identifier)**: VPI** is an 8- or 12-bit field used to identify paths between sites on the ATM

network. **VCI** is a 16-bit field used to identify connection between individual devices on the ATM network. "VCI + VPI' is used to identify the next destination of a cell.

- **Payload Type (PT):** Its first bit indicates type of data- user data or control data.
- **Cell Loss Priority (CLP):** It Indicates whether the cell should be discarded if network is congested. If the CLP bit=1, the cell will be discarded.
- **Header Error Control (HEC):** Calculates checksum only on the first 4 bytes of the header. HEC can correct a single bit error in these bytes, thereby preserving the cell rather than discarding it.
- **Payload:** 48 bytes data

Basic operation of ATM Switch

The cell is received across a link with a known VPI/VCI value. The switch looks up the connection value in a local translation table to determine the outgoing port (or ports) of the connection and the new VPI/VCI value of the connection on that link.

ATM Reference Model

The ATM architecture uses a logical model to describe the functionality that it supports. ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model. The ATM reference model is shown in figure. It consists of the 3 planes, which span all layers:

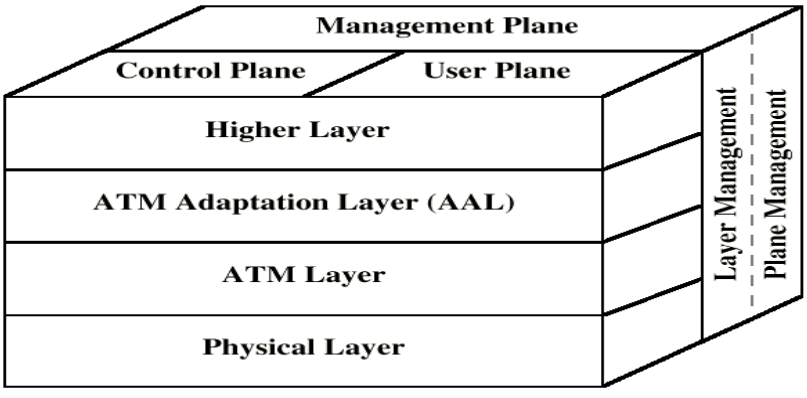


Figure 4.6.9 ATM reference model

Planes in ATM model and their responsibilities:

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

Layers in the ATM reference model

- **Physical Layer:** Its role is similar to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD (Physical Medium Dependent) sub layer and TC (Transmission Convergence) sub layer.
- **ATM Layer:** It works in conjunction with the ATM adaptation layer. As in data link layer of OSI model, it accepts the 48-byte segments from the upper layer, adds a 5-byte header to each segment and converts into 53-byte cells.
  Its responsibilities: Routing of each cell, traffic management, multiplexing and switching.
- **ATM Adaptation Layer (AAL**): Combined with the ATM layer, it is roughly analogous to the data link layer of the OSI model.
  - It facilitates connection between packet switching networks and ATM.
  - It accepts the data and converts them into fixed sized segments.
  - The transmissions data rate can be fixed or variable.
  - This layer has two sub layers: Convergence sub layer and Segmentation & Reassembly sub layer.
- **Higher Layer**: It resides above the AAL. It accepts user data, arrange it into packets, and gives it to the AAL.

ATM end points and ATM switch:

- ✓ **ATM endpoints:** An ATM endpoint (or end system) contains an ATM network interface adapter. Examples of endpoints are workstations, routers, LAN switches,

video coder-decoders (CODECs), etc.

- ✓ **ATM switches**: ATM switches are high-speed packet switches used to process and forward ATM cells through the ATM networks. An ATM switch--
  - ➢ Accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI)
  - ➢ Updates cell headers.
  - ➢ Retransmits cells towards destination.

ATM Applications

- In both LANs and WANs.
- In Multimedia virtual private networks and managed services.
- In Frame-relay backbones.
- In Internet backbones.
- In Carrier infrastructures for the telephone and private-line networks.

CRYPTOGRAPHY

(Greek words 'kryptos" meaning "hidden," and 'graphein' meaning 'to write')

Cryptography

Cryptography is a method of secret writing. In the present-day context, it refers to the tools and techniques used to protect messages from the attacks by hackers. In other words, only the sender and intended recipient of a message can view contents in message. Hackers, advertisers, or any other third party cannot view it. At the sender side, original message is coded and sent. At the receiver side, it is recovered back to its original form.

Terminology:

- Plaintext: The original message
- Ciphertext. Encrypted (coded) message
- Encryption: Process of converting plain text to cypher text.
- Decryption: It is the reverse of encryption. It is the process of converting cypher text into plain text.
- Encryption algorithm (or Cipher): Algorithm used for encryption.
- Decryption algorithm: Algorithm used for encryption

Types of Cryptography

Cryptography is broadly classified into two categories: Symmetric key Cryptography and Asymmetric key Cryptography.

1. Symmetric key cryptography (Private key encryption)

Here, both the sender and receiver use a single key during the communication. This private key is known only to sender and receiver. Sender uses this key for encrypting plain text and sends the ciphered text to the receiver. The receiver uses the same key for decrypting the ciphered text and recovering the plain text back.

Applications of Private key encryption:

- Home Wi-Fi networks
- Mobile telephones.
- ATM machines.

2. Asymmetric key cryptography (Public-key encryption):

Here, we use two keys known as private key and public key. These two keys are related to each other by mathematical process. Sender uses the public key for encryption. This public key is known by everyone. Private key is known only to sender and receiver. Receiver uses private key for decryption.

Applications of Public key encryption:

- Emails.
- In Secure socket layer (SSL) protocol used to make secure connections to websites.
- Digital signature.

Comparison of Symmetric Key Encryption and Asymmetric Key Encryption

Feature	Private key Cryptography	Public key Cryptography
Definition	It uses a single shared key (secret key) for encryption and decryption	It uses two different keys for encryption and decryption
Another name	It is also called Symmetric key encryption	It is also called Asymmetric key encryption
Efficiency	This technique is less efficient; used only for short messages.	This technique is more efficient; used for large amounts of text.
Speed	It is faster as it uses a single key for encryption and decryption.	It is slower as it uses two different keys related through complicated mathematical process.
Sharing	Private key is shared between sender and receiver.	Anyone can use the public key. But they will need a private key during decryption.

RSA Algorithm

The most popular public-key algorithm is the RSA (named after their inventors Rivest, Shamir and Adleman).

Key features of the RSA algorithm:

- RSA is a public key algorithm that performs encryption as well as decryption

based on number theory.

- Key is long for enhanced security and short key is used for efficiency. Typical key length 512 bytes.
- Block size (the number of bytes of the RSA modulus) is variable in size. It is smaller than the key length.
- The private key is a pair of numbers (d, n) and the public key is also a pair of numbers (e, n)

Algorithm:

- Choose two large primes p and q (typically around 256 bits)
- Compute n = p x q and z = (p-1) x (q-1)
- Choose a number e
- Find d such that e x d =1 mod (p-1) x (q-1)
- e and n are known to public; z and d are kept secret.
- For encryption: $C = P^e \pmod n$ For decryption: $P = C^d \pmod i$

Note: A mod B means reminder we get when we divide A by B. (e.g.: 7 mod 4 = 3)

NETWORK SECURITY

Network security refers to the policies, processes and practices adopted to protect network and data from unauthorized access and damage. With so many network security threats, protection of network is vital.

Note: Some common network security threats like Worms, Viruses, Spyware, Adware and Malware (e.g.: Trojan horses) are taken care by using antivirus software, firewalls, etc.

Network security Services:

- Message Confidentiality
- Message Integrity
- Message Authentication (MAC algorithm and Digital Signature)
- Message Nonrepudiation.
- Entity Authentication.

1. Message Confidentiality

Message confidentiality means privacy of messages against unauthorized viewing. In other words, the transmitted message must only be accessible to the intended recipient. Sender and the receiver always expect confidentiality. For example, when a customer communicates with his bank, he expects that the communication is totally confidential. Confidentiality can be achieved using private key encryption or public key encryption.

In former case, a single secret key is used by sender in encryption and the receiver in decryption. In later case, two keys known as private and public key are used. Public key is known to all. But private key is kept secret between sender and receiver.

2. Message Integrity

Message integrity means the accuracy, consistency and reliability of received data. In other words, data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. Integrity is crucial in monetary transactions over the Internet.

Example: It would be disastrous if a request for transferring Rs.100 is changed to a request for Rs.10,000.

Traditionally integrity of a document can be preserved through the use of a **fingerprint**. In modern communications, we use a hash function algorithm. A hash function is a function that is used to map data of arbitrary size to fixed-size values. Output of this function is called message digest or **digital fingerprint**. Thus, compressed image of the message is used like a fingerprint.

The message digest is created at the sender site and is sent with the message to the receiver. The receiver creates the hash function again and compares the new message digest with the one received. If both are the same, the receiver is sure that the original message has not been changed. A message digest, however, does not authenticate the sender of the message.

Availability: Message integrity should be accompanied by Availability. i.e., the authorized users should have access to the systems and the resources they need and get quick response.

3. Message authentication: (Using MAC algorithm and digital signature)

Message authentication is a service beyond message integrity. In message authentication the receiver needs to be sure of the sender's identity and that an imposter (fake person) has not sent the message. There are mainly two ways of achieving it,

(a) Message authentication code (MAC)

A hash function is any function that can be used to map data of arbitrary size to fixed-size values. output of a hash function is called a **message digest or digital fingerprint.**

A message digest guarantees the integrity of a message. i.e., it guarantees that the message has not been changed. However, it does not authenticate the sender of the message. What we need for message authentication is an algorithm to find Message authentication code (MAC).

(i) MAC (Message Authentication Code) algorithm:

MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.

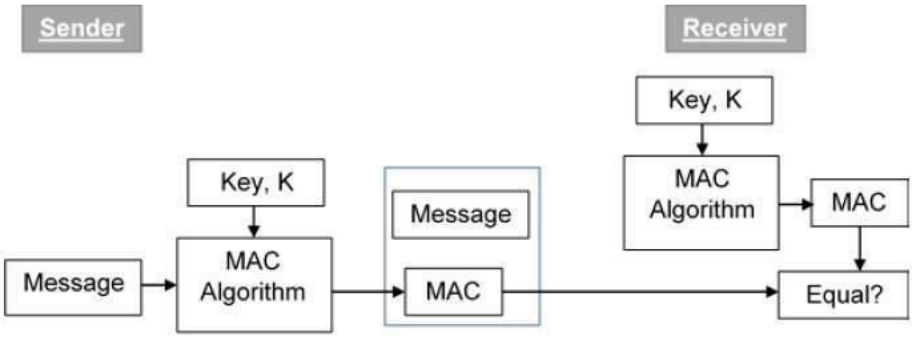


Fig. MAC processd

Steps in MAC Process:

- The sender inputs the message and the secret key K to the MAC algorithm and produces a MAC value. Then sender forwards the message along with the MAC.
- Receiver receives the message and the MAC. Then it feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.
- The receiver now compares the freshly computed MAC with the MAC received from the sender.
- If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.
- If the two MACs do not match, the receiver assumes that the message is not genuine. (i.e., Message is altered or it is sent by some other person)

Main limitations of MAC:

(i) The users are at the risk of using insecure communication channels to establish or share the secret key.

(ii) If the sender and receiver get involved in a dispute over message origination, MAC cannot provide a proof that a message was indeed sent by the sender.

(b) Digital signature

MAC algorithm uses private keys for message authentication. Digital signature uses a private/public key pair. The digit signature resolves the two limitations of MAC, which are mentioned above.

Traditionally, we sign a document to show that it originated from us or was approved by us. The receiver verifies the signature with that in files to assure that document comes from the correct entity (e.g.: (i) customer signature on a bank check (ii) Artist signature on his painting)).

When sender signs a document digitally, the sender uses a signing algorithm to sign the message. The message and the signature are sent to the recipient as two separate documents. The recipient receives the two documents (message and the signature) and applies the verifying algorithm to the combination. If the result is true, the message is accepted, otherwise it is rejected.

Figure shows the digital signature process.

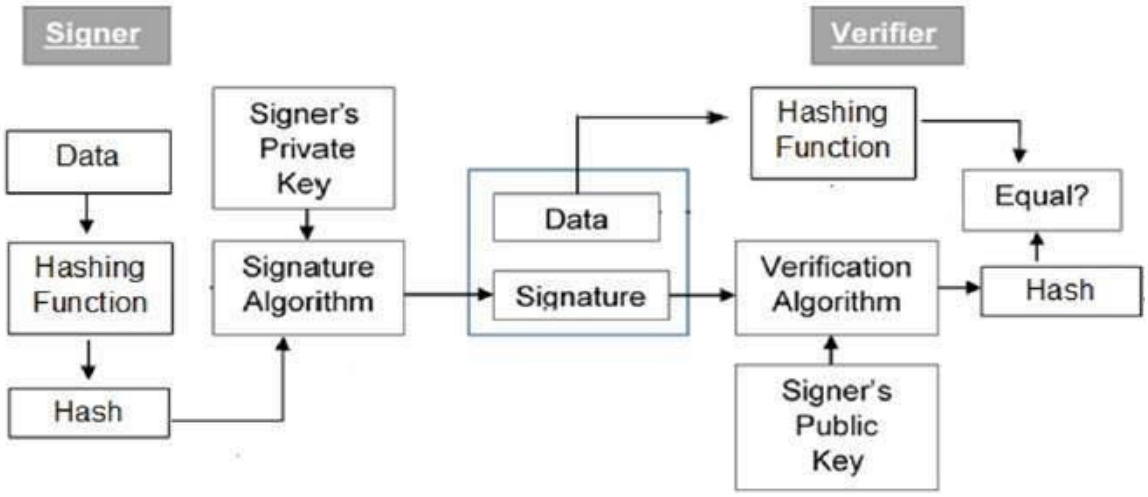


Fig. Digital Signature Process

4. Message Nonrepudiation

Repudiation means denial (rejecting) of the truth or validity of something. Message nonrepudiation means that a sender must not be able to deny sending a message that he has sent. The burden of proof falls on the receiver.

Example: When a customer sends a message to transfer money from one account to another, the bank must have proof that it is the right customer who requested this transaction.

Process: Let 'A' be the sender and 'B' be the recipient of the message. Then they take the help of a trusted third party; and message is sent and received as explained below.

- A creates a signature from his message.
- Then A sends the message, A's identity, B's identity, and the A's signature to the center (trusted third party).
- The center checks A's public key to identify A.
- Then the center saves a copy of the message with the sender identity, recipient identity, and a timestamp in its archive.
- Then center uses its private key to create another signature from the message.
- The center then sends the message, the new signature, A's identity, and B's identity to the receiver.
- The receiver verifies the message using the public key of the trusted center.
- If, in the future, A denies that he has sent the message, the center can show a copy of the saved message.
- To make everything confidential, encryption and decryption are used.

5. Entity Authentication

Entity authentication means identification of user. An entity can be a person, a process, a client or a server. The entity or user is verified before accessing the system resources like files.

Example: A student who needs to access his university resources needs to be authenticated during the logging process. This is to protect the interests of the university and also the student.

In entity authentication, the claimant must identify himself to the verifier. This can be done with one of the following proofs.

- **Something known:** Verifier checks something known only by the claimant
  Examples: Password, PIN, a secret key
- **Something possessed:** This is something that the claimant possess.

Examples: Passport, Driver’s license, a credit card

- **Something inherent**: This is an inherent characteristic of the claimant.
  Examples: Conventional signatures, fingerprints, voice, facial characteristics, retinal pattern.