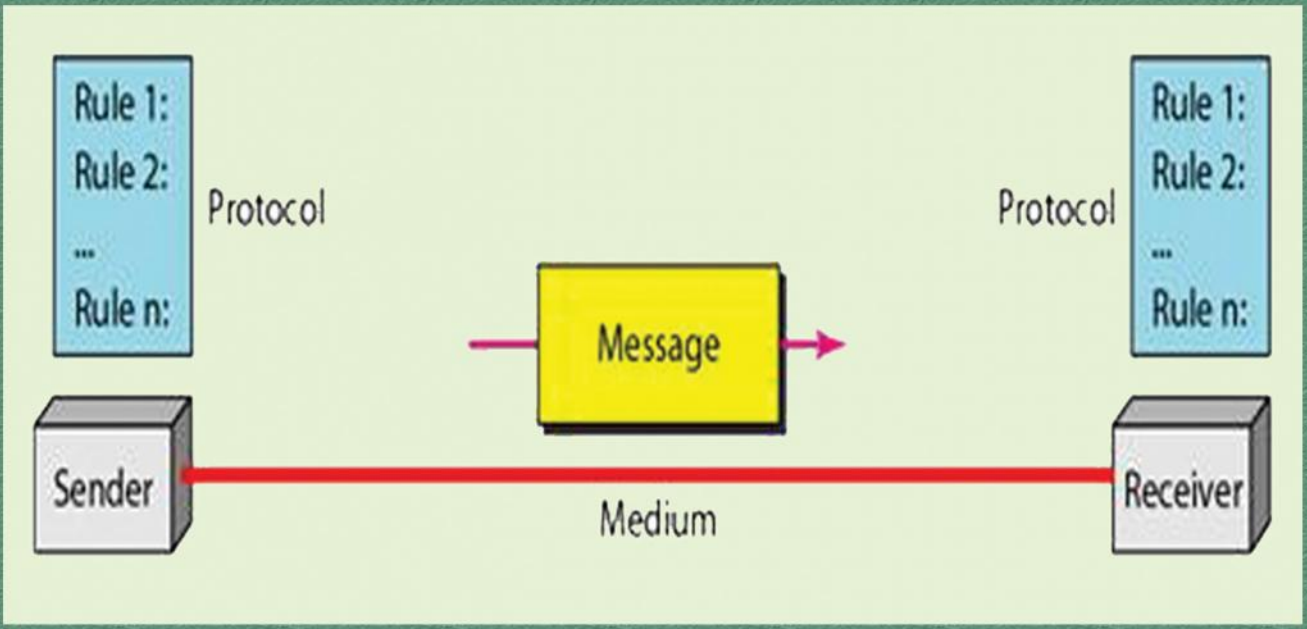
इरिसेट IRISET

TA2

DATA COMMUNICATION & NETWORKING



Indian Railways Institute of
Signal Engineering and Telecommunications
SECUNDERABAD - 500 017

TA2

DATA COMMUNICATION & NETWORKING

The Material Presented in this IRISET Notes is for guidance only. It does not over rule or alter any of the Provisions contained in Manuals or Railway Board's directives.

INDIAN RAILWAYS INSTITUTE OF SIGNAL ENGINEERING & TELECOMMUNICATIONS, SECUNDERABAD - 500 017

Issued in January 2014

TA2

DATA COMMUNICATION & NETWORKING

Contents

Prepared by	V.Radha Krishnan, LT-2
	S.S. Muralidharan, IMP-3
Approved By	P.V. Sreekanth, PT
DTP and Drawings	K.Srinivas, JE (D)
No. of Pages	185
No.of Sheets	94
Revision By	J. Vijay Kumar, INW-2
	D. Anandam, INW-1
Revision Approved by	K.V. Reddy, P(IT)

CHAPTER 1
INTRODUCTION

This chapter introduces the basic concepts of data communication. Data Communication refers to a System for transmitting a message (data) in Digital form; Basic concepts, which are prerequisites, are dealt in this chapter to enable the reader to have a broader spectrum of Data Communication.

1.0 DATA COMMUNICATION

Data communication has become an important aspect of modern world. In the simplest form, data communication involves the exchange of data between two computers. Computers work with a binary language consisting of zeros and ones. Therefore, a computer generates a stream of zeros and ones and sends it to another computer to which it is connected. The connection can be either a simple wire or it can be through wireless media. For data communications to occur, the communicating devices must be part of communication system made up of a combination of hardware (physical equipment) and software (programs).

1.1 Data Representation

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

a. **Text:** In data communications, text is represented as a bit pattern, a sequence of bits (0's or 1's). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Earlier we were using ASCII (American Standard Code for Information Interchange) coding system, but today the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.

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

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

d. **Audio:** Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, number or images. It is continuous, not discrete.

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

1.2 Data Components

A data communications system has five components (see figure 1.1)

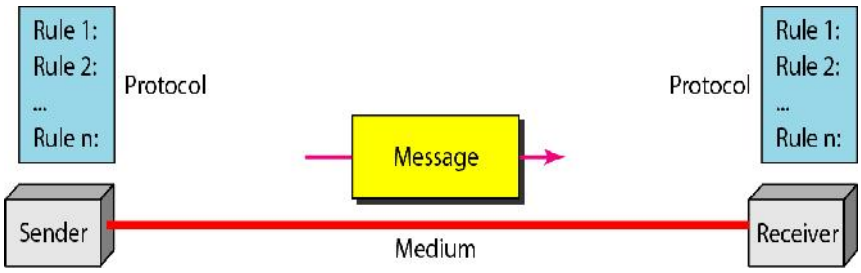


Fig. 1.1 Data communications system

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

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

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

d. **Transmission medium**: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wires, coaxial cable, fiber optic cable and radio waves.

e. **Protocol**: A protocol is a set of rules which is used by computers to communicate with each other across a network. A protocol is a convention or standard or software that controls or enables the connection, communication, and data transfer between computing endpoints.

The purpose of protocols specifies one or more of the following properties.

- Detection of the underlying physical connection (wired or wireless), or the existence of the other endpoint or node
- Handshaking
- Negotiation of various connection characteristics
- How to start and end a message
- Procedures on formatting a message
- What to do with corrupted or improperly formatted messages (error correction)
- How to detect unexpected loss of the connection, and what to do next
- Termination of the session or connection.

In data communications, there are widely accepted protocols for sending & receiving data. Both the sender and receiver must use the same protocol when communicating.

Protocols can be broadly classified as
1. Proprietary Protocols (works on a specific make or brand or model device)
2. Open Source Protocols (works on any make or brand or model device)

1.3 Fundamental Characteristics of Data Communication

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

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

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

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

d. **Jitter:** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets, which results in degradation of the quality. Hence jitter is required to be eliminated.

1.4 Data Flow

Communication between two devices can be simplex, half duplex, or full duplex as shown in figure 1.2.

a. Simplex

In simplex mode, the communication is unidirectional, only one of the two devices on a link can transmit; the other can only receive (see figure1.2a).

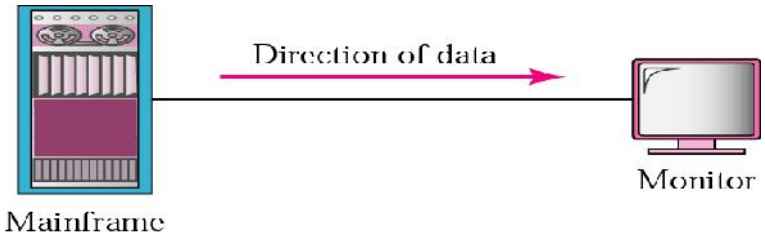


Fig. 1.2a Simplex mode

Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

b. Half-Duplex

In half duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (see fig. 1.2b). In a half duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at a time.

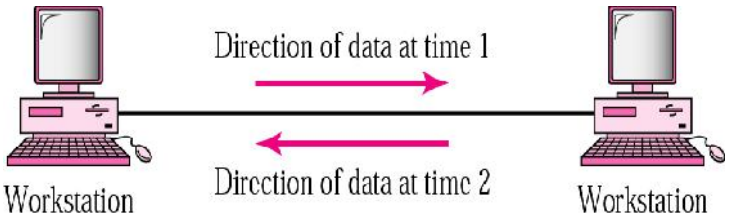


Fig. 1.2b Half Duplex mode

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

c. Full-Duplex

In full duplex mode (also called duplex), both stations can transmit and receive simultaneously (see fig. 1.2c).

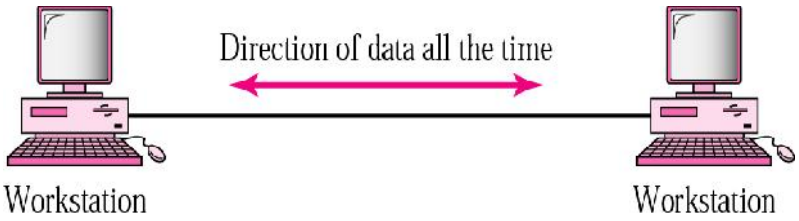


Fig.1.2c Full duplex mode

In full duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This sharing can occur in two ways: either the link must contain two physically separate transmission paths, one for sending or other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

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

The full duplex mode is used when communication in both directions is required all the time. The capacity of the channel however must be divided between the two directions.

1.5 DATA TRANSMISSION

The transmission of binary data across a link can be accomplished in either parallel or serial mode as shown in fig. 1.3a. In parallel mode, multiple bits are sent with each clock tick. In serial mode, 1 bit is sent with each clock tick. While there are no sub classes in parallel data, there are two subclasses of Serial transmission:

1. Asynchronous
2. Synchronous.

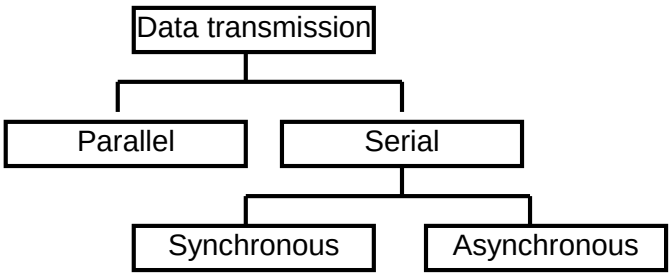


Fig 1.3a Data transmission methods

1.5.1 SERIAL, PARALLEL COMMUNICATION

a. Serial Data Communication

The physical connection determines how many bits (1's or 0's) can be transmitted at a single instance of time. If only 1 bit of information can be transmitted over the data transmission medium at a time then it is considered a Serial Communication. (Refer Fig. 1.3b)

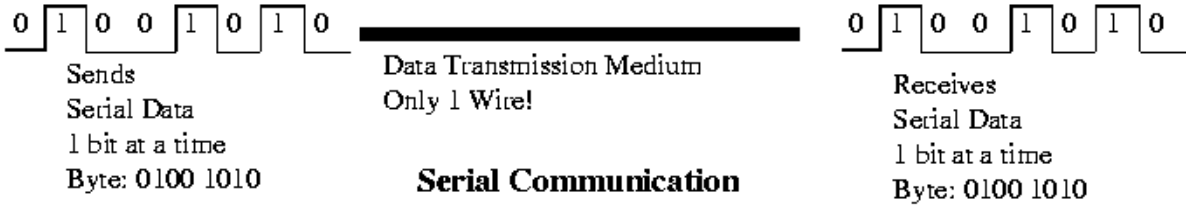


Fig.1.3b Serial communication

b. Parallel Data Communication

If more than 1 bit of information is transmitted over the data transmission medium at a time then it is considered a Parallel Communication. (Refer Fig. 1.3c)

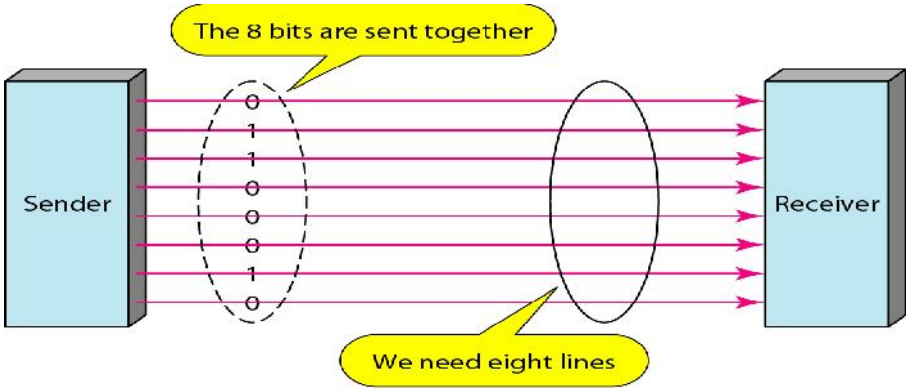


Fig.1.3c Parallel communication

Communications	Advantages	Disadvantages
Parallel	Fast Transfer Rates	Short distances only
Serial	Long Distances	Slow transfer rates

The transfer rate comparison is relative to serial versus parallel. Data can be transferred at much faster rates over long distances using serial methods than using parallel data transfer. At shorter distances, typically less than 15 feet, parallel data transfers are used.

Serial data communication transfers one bit at a time and does not have the timing problems (race conditions) as that of parallel data communications.

1.5.2 ASYNCHRONOUS / SYNCHRONOUS COMMUNICATION

a. Asynchronous Transmission

In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte. There may be a gap between each byte.

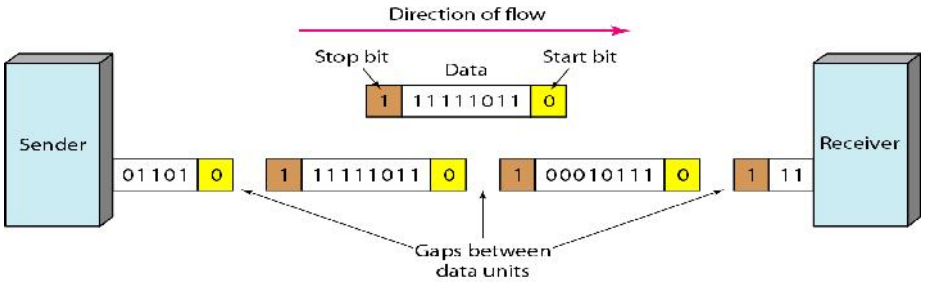


Fig. 1.4a Asynchronous system of sending data

The asynchronous protocol evolved early in the history of telecommunications. It became popular with the invention of the early tele-typewriters that were used to send telegrams around the world.

Asynchronous systems send data bytes between the sender and receiver by packaging the data in an envelope as shown in Fig.1.4a this envelope helps transport the character across the transmission line that separates the sender and receiver. The transmitter creates the envelope, and the receiver uses the envelope to extract the data. Each character (data byte) the sender transmits is preceded with a start bit, and suffixed with a stop bit. These extra bits serve to synchronize the receiver with the sender.

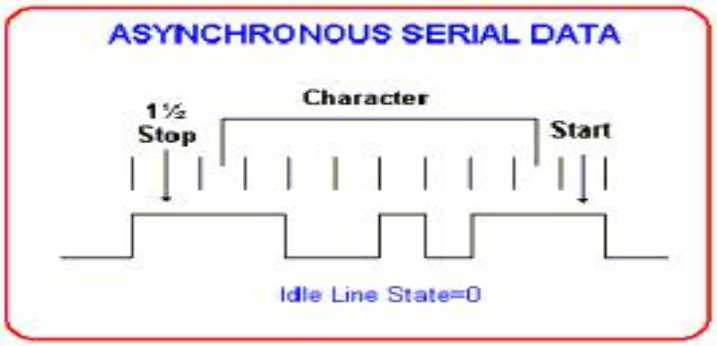


Fig. 1.4b Asynchronous system of sending data

This method of transmission is suitable for slow speeds less than about 32000 bits per second. In addition, notice that, the signal that is sent does not contain any information that can be used to validate if it was received without modification. This means that this method does not contain error detection information, and is susceptible to errors.

In addition, for every character that is sent, additional two bits are also sent as shown in fig 1.4b. Consider the sending of a text document which contains 1000 characters. Each character is eight bits, thus the total number of bits sent are 10000 (8 bits per character plus a start and stop bit for each character). These 10000 bits are actually 1250 characters, meaning that an additional 250 equivalent characters are sent due to the start and stop bits. This represents a large overhead in sending data, clearly making this method an inefficient means of sending large amounts of data.

b. Synchronous Transmission

In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits. (Refer fig.1.5a).

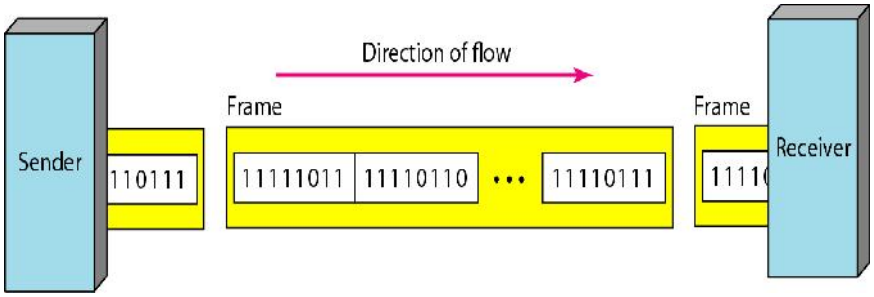


Fig 1.5a Synchronous Transmission

In synchronous transmission, greater efficiency is achieved by grouping characters together, and doing away with the start and stop bits for each character. We still envelop the information in a similar way as before, but this time we send more characters between the start and end sequences. In addition, the start and stop bits are replaced with a new format that permits greater flexibility. An extra ending sequence is added to perform error checking.

In asynchronous transmission, if there was no data to transmit, nothing was sent. We relied on the start bit to start the CLOCK on receiving device and thus begin the preparation to decode the incoming character. However, in synchronous transmission, because the start bit has been dropped, the receiver must be kept in a state of readiness. This is achieved by sending a special code by the transmitter whenever it has no data to send.

In bit orientated protocols, the line idle state is changed to 7E, which synchronizes the receiver to the sender. The start and stop bits are removed, and each character is combined with others into a data packet. User data is prefixed with a header field, and suffixed with a trailer field which includes a checksum value (used by the receiver to check for errors in sending) as shown in Fig. 1.5b.

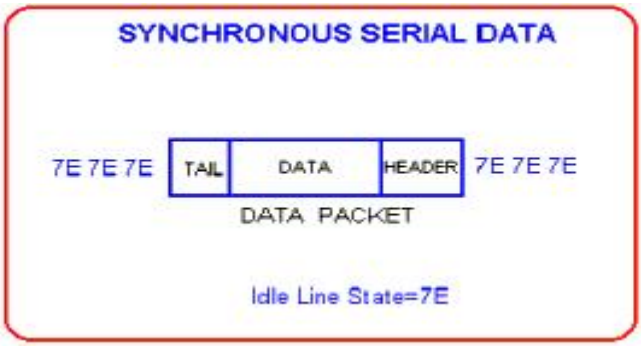


Fig. 1.5b Synchronous serial data

The *header field* is used to convey address information (sender and receiver), packet type and control data. The *data field* contains the users' data (if it can't fit in a single packet, then use multiple packets and number them). Generally, it has a fixed size. The *tail* field contains checksum information which the receiver uses to check whether the packet was corrupted during transmission.

1.6 NETWORK

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer or other device of capable of sending and receiving data generated by other nodes on the network. The main advantage of network is sharing of resources; the resources can be hardware or software.

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

Network criteria

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

a. Performance

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.

The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware and the efficiency of the software.

b. Reliability

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

c. Security

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

1.6.1 Categories of Networks

Networks are categorized in three different categories as (Ref fig no. 1.6)

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

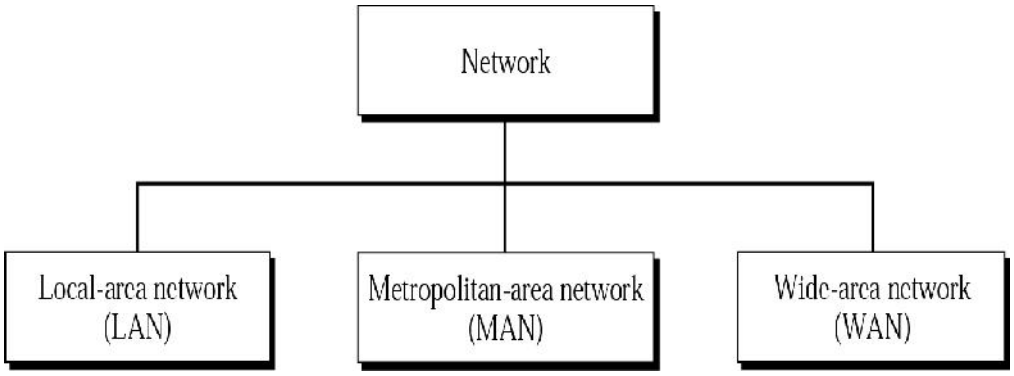


Fig. 1.6 Categories of Networks

1.6.2 LAN (Local Area Network)

Local Area Networks (LANs) are networks that connect computers and resources together in a building or buildings close together as shown in fig 1.7. The computers share resources such as hard-drives, printers, data, CPU power, fax/modem, applications, etc... They usually have distributed processing - means that there are many desktop computers distributed around the network and that there is no central processor machine (mainframe).

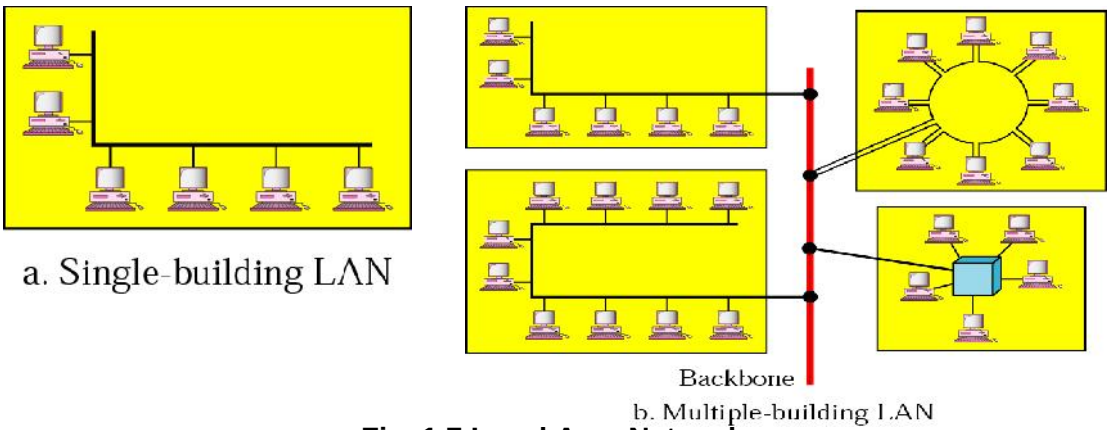


Fig. 1.7 Local Area Network

Location: In a building or individual rooms or floors of buildings or connecting nearby buildings together like a campus wide network like a college or university

1.6.3 Metropolitan Area Networks (MAN)

Metropolitan Area Networks (MANs) are networks that connect LANs together within a city. Fig. 1.8 shows telecommunication services provide the connection (storm clouds) between networks. A local telecommunication service provides the external connection for joining networks across cities.

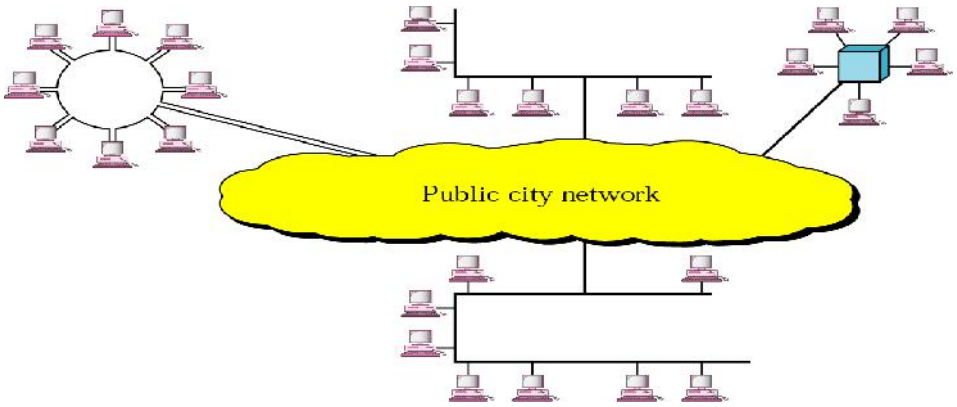


Fig. 1.8 Metro Area networks

Location: Separate buildings distributed throughout a city.

Examples of companies that use MANs are universities, colleges, grocery chains, gas stations, department stores and banks.

1.6.4 WAN (Wide Area Network)

Wide Area Networks (WAN) are a communication system linking LANs between cities, countries and continents as shown in fig 1.9. The main difference between a MAN and a WAN is that the WAN uses Long Distance Carriers rather than Local Exchange carriers. Otherwise the same protocols and equipment are used as a MAN.

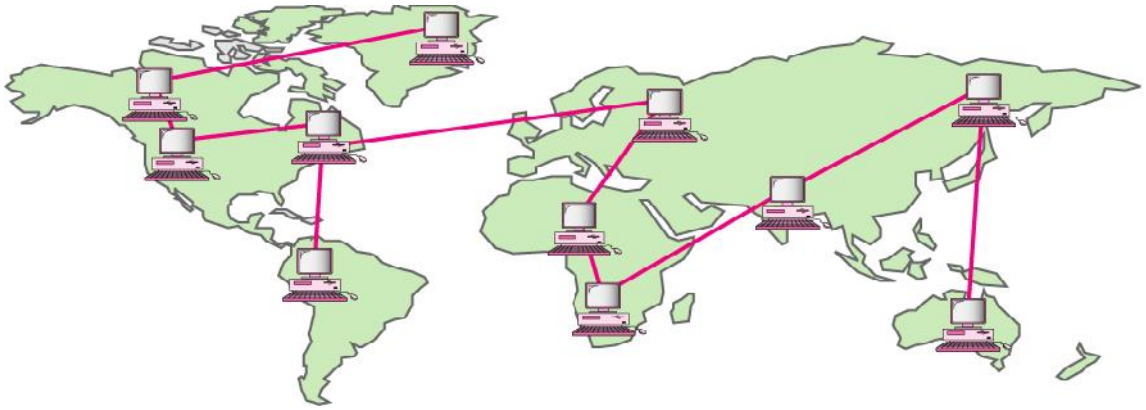


Fig. 1.9 Wide area network

1.7 TOPOLOGY

The networks in which the terminals are interconnected with each other for inter communication within and outside the network is called as Topology.

Basically the Topology is categorized in following four types of designs. (Ref fig no. 1.7a)

1. Mesh topology
2. Star Topology
3. Bus Topology.
4. Ring Topology

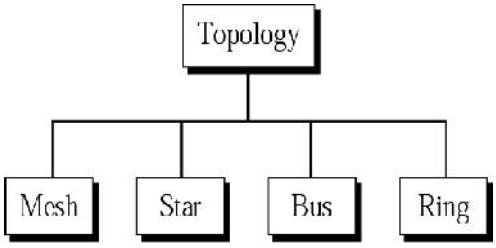


Fig. 1.7a categories of topology

1.7.1 Mesh Topology

In mesh topology every device has a dedicated point to point to every other device. Every device must have (n-1) I/O ports. All WAN is mesh topology. (Ref fig no. 1.10c)

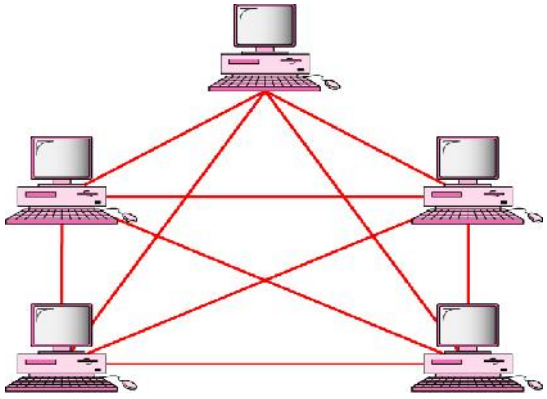


Fig. 1.10c Mesh topology (for five devices)

Advantages

- It is robust.
- Each link can carry its own data load.
- It has privacy or secrecy.
- Fault identification is easy

Mesh **disadvantages** are larger number of cables & I/O ports are required for each device. Also the bulk of the wires can be greater than the available space.

1.7.2 Star Topology

In star topology each device has a dedicated point to point link only to central controller called as HUB as shown in fig no. 1.10d. If one device wants to send data to another device, it sends through the HUB. Generally used in LAN networks

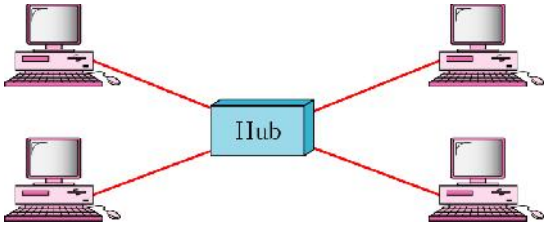


Fig. 1.10d Star topology

Advantages

- It is easy to install and reconfigure.
- Each device needs only one link. Hence it is less expensive.
- If a link fails, only that link has to be attended. All other links remain active.
- It is easy to identify fault.
- It is also robust.

1.7.3 Bus topology

A BUS topology is multipoint. One long cable acts as a backbone to link all devices in a network. The advantage is the installation is easy. Generally used in LAN networks (Ref fig no. 1.10e)

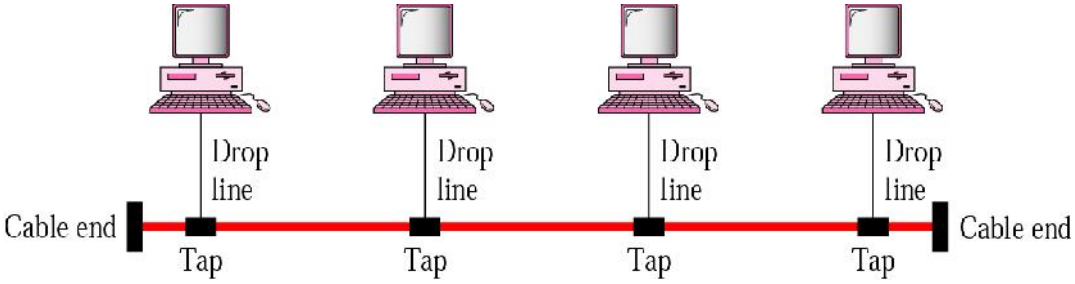


Fig. 1.10e Bus topology

Disadvantages

- Difficult in fault isolation and reconnection.
- Difficult to add device to an existing system.
- A fault or break in bus cable stops all transmission.

1.7.4 Ring Topology

In a ring topology, each has a dedicated point to point connection only with two devices on either side of it. A data is passed along the ring in one direction, from device to device until it reaches its destination. Each device in a ring incorporates a repeater. Generally used in LAN networks (Ref fig no. 1.10f)

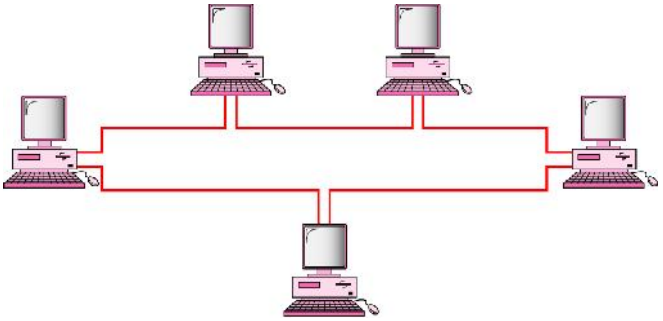


Fig. 1.10f Ring topology

Advantages

- It is easy to install & configure.
- To add or delete a device requires only changing two connections.
- The disadvantages are unidirectional traffic and a break in the ring can disable entire network.

1.8 STANDARD ORGANISATIONS

Because of the wide number of hardware manufacturers, a standard is essential in order to connect one computer to another computer if a different type. There are recognized and widely accepted standards governing how data is to be transmitted, whether asynchronously, parallely, or synchronously. Standards govern the format of the data, and also specify the hardware details like voltages to use, bit durations, speeds etc..The major organizations responsible for standards are

ISO (International Organization for Standards):

It is a nongovernmental organization based in Geneva. ISO has standards covering a wide range of computer related topics and it maintains standard for quality assurance. The most significant activities are its work on open systems, which defines the protocols that would allow any two computers to communicate independent of their architecture.

http://www.iso.org

ITUT (International Telecommunication Union):

Formerly known as CCITT It is an agency of United Nations, it sets standards for modems (V-Series / Which defines data transmission over phone lines) & switching networks (X-Series / Which defines data transmission over switching digital networks) The ITU co-ordinates international communications and recommend standard interfaces and policies for the interconnection of national networks.

http://www.itu.int

ANSI (American National Standard Institute):

Represents a number of US standards organizations. It is a private agency, it sets up the standards for FDDI (which is one of the LAN interface) & ASCII (which is used by many computers for storing information.

http://www.ansi.org

IEEE (Institute of Electrical and Electronic Engineers):

Largest Professional organization of engineers, developing standards for LAN called as IEEE802

http://www.ieee.org

EIA/TIA (Electronic Industries Association/Telecommunication Industries Association):

Defines physical connection interfaces and Electronic signaling specifications for data communications. Their most well known standard is the RS-232(EIA-232); EIA-449 & EIA-530 defines serial transmission between two digital devices (i.e. computer to modem)

http://www.tiaonline.org **,** http://www.eciaonline.org

IEC (International Electro Technical Commission):

It is a non governmental agency devising standards for data processing and safety in office equipments. It has devised a compression standard for images like JPEG.

http://www.iec.ch

ISOC & IETF (Internet Society & Internet Engineering Task Force):

Internet Society concentrates on user issues Including enhancement to the TCP/IP protocol IETF focuses on technical Internet issues(hardware & software) it Developed SNMP(Simple Network Management Protocol)

http://www.ietf.org, http://www.isoc.org

1.9 THE OSI MODEL

OSI MODEL - History, Origin, Purpose

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the open systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperable. The OSI model is a seven-layer framework that allows communication between all types of computer systems.

1.9.1 OSI (Open System Interconnection) MODEL

What is the OSI Model?

- The OSI Model is a way of thinking about how networks 'work'.
- The OSI Model is a *theoretical model*--it is not a technology, it is not a protocol, it is not a program or software.
- The OSI Model sorts network communication functions into *layers*
- The OSI Model *does not* specify how a layer will work internally--that is a matter left to the programmers.
- The OSI Model specifies how layers should talk to each other.
- The OSI Model specifies that any layer's processes should be invisible to the layer above it, and below it.
- The OSI Model defines how information should be handled when being transported over a network.
- The OSI Model defines how software should interact with the network.

1.9.2 Why Should We Learn the OSI model?

- Learning the OSI Model helps us to understand what functions occur where and when
- The OSI Model helps us to understand how a Web browser works
- The OSI Model helps us to understand what Internet Protocol does and how it works
- The OSI Model helps us to understand why we need ARP
- The OSI Model helps us to understand what is MAC address

- Learning the OSI Model makes it easier to learn.
- Learning the OSI Model makes it easier to perform troubleshooting.
- Learning the OSI Model makes it easier to troubleshoot any problem, including computer problems.
- Learning the OSI Model makes it easier to communicate with other technical people and discuss technical issues.

1.9.3 OSI model

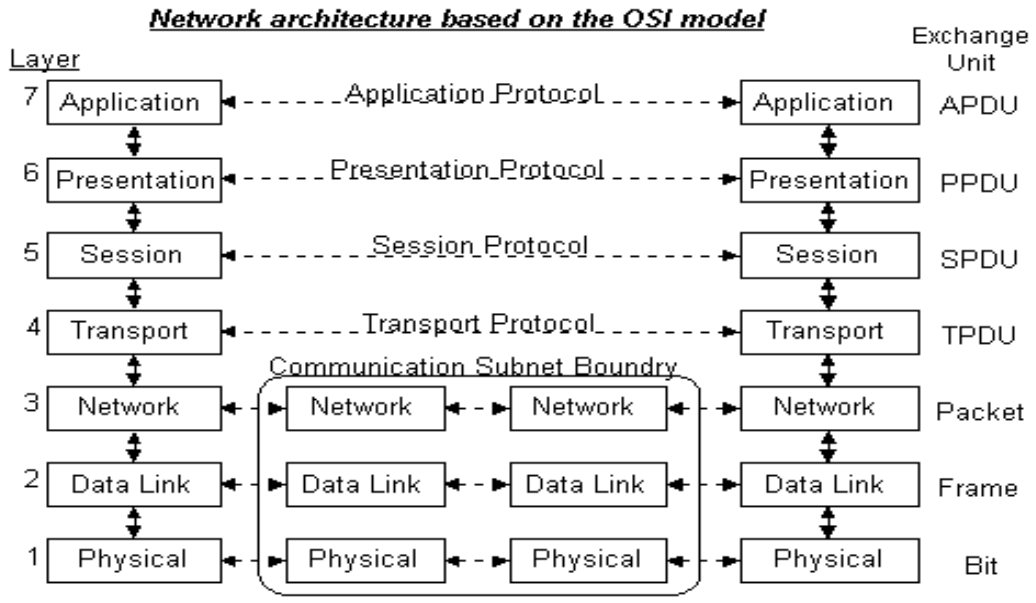


Fig 1.11 OSI model

Network architecture based on OSI model is shown in fig 1.11 (above) & its functional description is given below.

APPLICATION LAYER (Layer 7)

The OSI model defines the **application** layer as being the user interface. The OSI application layer is responsible for displaying data and images to the user in a human-recognizable format and to interface with the **presentation** layer below it.

Examples of applications that utilize the network are:

- Telnet
- FTP
- Instant Message software
- Microsoft Windows File Shares
- Microsoft Internet Explorer (a Web browser)

PRESENTATION LAYER (Layer 6)

The **presentation** layer handles the conversion of data between a System-based or platform independent formats to a format understood by the local machine. This allows for data to be transported between devices and still be understood.

The presentation layer performs the following functions :

- Communication with the **application** layer above.
- Translation of data conforming to cross-platform system into formats understood by the local machine.
- Communication with the **session** layer below.

Examples of Presentation Layer Functions

- Conversion of a Sun .RAS raster graphic to JPG.
- Conversion of ASCII to IBM EBCDIC
- Conversion of .PICT on a MAC to .jpg
- Conversion of .wav to .mp3

SESSION LAYER (Layer 5)

The **session** layer tracks connections, also called sessions.

The **session** layer should keep track of multiple file downloads requested by a particular FTP application, or multiple telnet connections from a single terminal client, or Web page retrievals from a Web server. With TCP/IP this functionality is handled by application software addressing a connection to a remote machine and using a different local port number for each connection.

The **session** layer performs the following functions:

- Communication with the Presentation layer above.
- Organize and manage one or more connections per application, between hosts.
- Communication with the Transport layer below.

Examples

Sessions are used to keep track of individual connections to remote servers. Web browser is an excellent example of the use of **sessions**.

Web browser (an **application** layer object) opens a Web page. That page contains text, graphics, Macromedia Flash objects and perhaps a Java applet. These are all stored as separate files on the Web server. To access them, a separate download must be started. Web browser opens a separate *session* to the Web server to download each of the individual files. The *session* layer keeps track of which packets and data belong to which file and keeps track of where they go (in this case, to Web browser).

In most modern Internet applications, the **session, presentation** and **application** layers are usually rolled together inside the application itself, thus, Web browser performs all functions of the **session, presentation** and **application** layers.

TRANSPORT LAYER (Layer 4)

If networking software performs reliable data transfer functions, then the detection of errors and retransmission of data to recover those errors or lost data will occur in software managing this layer. The *transport* layer may use a variety of techniques such as a Cyclic Redundancy Check, Windowing and acknowledgements. If data is lost or damaged it is the *transport* layer's responsibility to recover from that error.

The **transport** layer is concerned with the following primary functions:

- Communicate with the Session layer above.
- Reassemble *transport* Protocol Data Units into data streams
- Reliable protocols operating at this layer.
- Detect errors and lost data
- Recover lost data
- Manage retransmission of data.
- Segmentation of data streams into *transport* Protocol Data Units.
- Communicate with the Network layer below.

Examples of transport Layer protocol include

- Transmission Control Protocol (Reliable)
- User Datagram Protocol (Unreliable)

NETWORK LAYER (Layer 3)

- It is the **network** layer's job to figure out the **network** topology, handle routing and to prepare data for transmission.
- The **network** layer is concerned with the following primary functions:
- Communication with the Transport layer above.
- Encapsulation of Transport data into **Network** layer Protocol Data Units.
- Management of connectivity and routing between hosts or networks.
- Communication with the **data link** layer below.

Examples of network Layer protocol include

- Internet Protocol
- Internet Control Message Protocol (ICMP or "ping")
- Internet Gateway Management Protocol (IGMP)
- IPX/SPX

DATA LINK LAYER (Layer 2)

The **data link** Layer is the second layer of the OSI model. The **data link** layer performs various functions depending upon the hardware protocol used, but has four primary functions:

- COMMUNICATION with the Network layer above.
- SEGMENTATION of upper layer data grams (also called packets) into frames in sizes that can be handled by the communications hardware.
- BIT ORDERING. The data link layer organizes the pattern of data bits into frames before transmission. The frame formatting issues such as stop and start bits, bit order, parity and other functions are handled here. Management of big-endian / little-endian issues is also managed at this layer.
- COMMUNICATION with the Physical layer below

This layer provides reliable transit of data across a physical link. The *data link* layer is concerned with physical addressing, network topology, physical link management, error notification, ordered delivery of frames, and flow control.

It should be noted that in most modern network interface adaptors, the Physical and Data link functions are performed by the network interface adaptor.

PHYSICAL LAYER (Layer 1)

The physical layer provides for physical connectivity between networked devices. Transmission and receipt of data from the physical medium (copper wire, fiber, radio frequencies, barbed wire, string etc.) is managed at this layer.

The physical layer receives data from the data link Layer, and transmits it to the wire. The physical layer controls the electrical and mechanical functions related to the transmission and receipt of a communications signal. It also manages the encoding and decoding of data contained within the modulated signal.

Note that for two devices to communicate, they must be connected to the same type of physical medium (wiring). 802.3 Ethernet to 802.3 Ethernet, FDDI to FDDI, serial to serial etc. Two end stations using different protocols can only communicate through a multi-protocol bridge or a router.

The physical layer is responsible for following jobs:

- Communication with the **data link** layer above it.
- Fragmentation of data into frames
- Reassembly of frames into **data link** Protocol Data Units.
- Transmission and reception of data.

It should be noted that in most modern network interface adaptors, the physical and data link functions are performed by the adaptor.

Example Physical Protocols

- CSMA/CD
- CSMA/CA
- B8ZS
- 2B1Q
- PCM
- QAM

1.9.4 OSI MODEL - Basic Operation

Network-capable Applications produce **DATA**. Each layer in the OSI Model adds its own information to the front of the data it receives from the layer above it. This information in front of the data is called a **`Header`** and contains information specific to the protocol operating at that layer. The process of adding the header is called **encapsulation.** Encapsulated data is transmitted in **Protocol Data Units** (PDUs). There are **Presentation** PDU's, **Session** PDU's, **Transport** PDU's etc. Thus, PDU's from an upper layer are encapsulated inside the PDU of the layer below it. PDU's are passed down through the stack of layers (called 'the stack' for short) optionally repeating the encapsulation process until they can be transmitted over the **Physical** layer. The physical layer is the wire connecting all the computers on the network.

The OSI system specify that a layer on host #1 speaks the same language as the same layer on host #2 or any other host on the network. Thus, all hosts can communicate via the **`Physical`** layer. This communication between layers is represented by the ⟷ symbols in the diagram above. For example, the **`Transport`** layer on Host 1 should speak the same language as the **Transport** layer on Host 2.

DATA passed upwards is un-encapsulated before being passed farther

All information is passed down through all layers until it reaches the **`Physical`** layer.

The **Physical** layer chops up the PDU's and transmits the PDU's over the physical connection (copper wire, fiber optic cable, radio link etc.). The **`Physical`** layer provides the real physical connectivity between hosts over which all communication occurs.

a. Need for Layered Model

The division of layers is mainly to establish communication crossing three different boundaries

- "Hop-by-Hop"
- "Network-wide" and
- "End-to-End"

The two lowest layers operate between adjacent systems connected via the physical link and are said to work "**hop by hop**". The protocol control information is removed after each "hop" across a link (i.e. by each System) and a suitable new header added each time the information is sent on a subsequent hop.

The network layer (layer 3) operates **"network-wide"** and is present in all systems and responsible for overall co-ordination of all systems along the communications path.

The Layer 4 - 7 protocol control information is therefore unchanged by the IS (Intermediate System) in the network and is delivered to the corresponding ES (End system) in its original form. Layers 4-7 if present in IS play no part in the ES.

Data from an upper layer is supposed to be passed down and inserted into the payload of a PDU in the layer below it. In the real world, the process of *`ENCAPSULATION`* (adding a header) doesn't always occur at all layers and sometimes things get chopped into smaller pieces so they will be easier to send and receive.

Data passed over the Internet gets the first header from the application, then from Transmission Control Protocol (TCP), and then Internet Protocol (IP) adds a header and passes it down to a physical connection. After that point, the hardware (Ethernet on LANs) chops the IP data into pieces and slaps its own header on it. Ethernet and other 802.x protocols also place a CRC at the end of the frame in the form of a frame check sequence. Although IP doesn't conform exactly to the model above, the model is still a good reference point for discussing Internet based network technologies and protocols.

b. An Operational Example of the OSI Model

This example assumes that we are on a local area network and that we are using an Ethernet card to communicate with the network. If we are on a dial-up modem, it will work a little differently from the data link layer down. Modem communication is a bit more different.

LAYER	EXAMPLE	FUNCTION/ACTIVITY
APPLICATION	**Web Browser**	A Web browser such as Internet Explorer or Netscape provides the means for computer to contact a Web server and download several files that go together to produce a single Web page. We can request a Web page by typing in a Web address or by clicking a link in an open Web page. The Web browser is an **APPLICATION**. The Web browser **application** gives the means to select a Web server, contact the server and request a Web page. The Web browser handles the process of finding the Web server, requesting the desired file and displaying all the files contained in the Web page.
PRESENTATION	**HTTP**	Web browser supports various image file formats, audio files and HTML. The Web browser handles **PRESENTATION** of the Web page to the user by converting the files stored at the Web server into formats used to display them on computer. Conversion of data from one format to another is the job of the **PRESENTATION** layer. A Web browser can convert these file formats into the local formats used on the local computer for displaying images, playing sounds and displaying text; if it cannot, it often can launch an application which does understand the format. Much of the **PRESENTATION** layer conversions are handled in the program we are running.
SESSION		When we request a Web page, the Web browser opens a TCP connection to the Web server. The Web server sends back the Web page and closes the connection. Web browser then opens the Web page. Within the Web page instructions are written in HTML tags which tell the browser where to find additional files to be displayed within the Web page such as style sheets, sound files, images, movies, Flash files and applets. Web browser automatically opens additional TCP connections to the Web server. Each TCP connection is a **SESSION**.
TRANSPORT	**TCP**	To communicate with a Web server computer must open a TCP connection to the Web server and request a Web page. The TCP connection breaks up the Web page into manageable chunks, labels them with numbers so they can be reassembled in the correct order and **TRANSPORTS** the pieces across the correct **SESSION**.

NETWORK	**IP** **ARP**		Internet Protocol (IP) is a **NETWORK** layer protocol that uses unique addresses for the Web server and for computer. IP provides the means for computer to determine whether the Web server is a local computer or a computer located somewhere on the Internet. To reach a Web server on the Internet, IP protocol also allows computer to figure out how to reach the Internet Web server via default gateway. Computer creates a message addressed to the Web server with computer's return IP address. Computer uses ARP to figure out the physical MAC address of the default gateway and then passes the data to the **NETWORK** layer.
DATA LINK	**ETHERNET**	**LLC**	Once the request from Web browser has been created it is sent to the network card. Once it reaches network card it must be converted into a message that is sent from computer to the default gateway which will forward the message to the Internet. At the **DATA LINK** layer, the Web request is inserted inside a network request to the default gateway.
		MAC	
PHYSICAL		**CSMA/CD**	The **physical** layer provides the means to transmit the Web page request to the default gateway.

Review Questions:

Subjective:

1. What are the factors that make data communication effective?
2. What are the five (5) components of data communication?
3. Mention the modes of data flow between sender & receiver?
4. What are factors that effect network?
5. What is OSI model and why it should be learnt?
6. Discuss OSI layers, its relevance with Network, functions and associated protocols for data communication?
7. What are data transmission modes?
    a. Describe Serial / Parallel
    b. Describe Synchronous / Asynchronous?
8. What is topology? What are different topologies of networking?
9. What are the categories of network? Discuss?
10. What are protocols? What are the factors that establish protocols? Discuss the relevance of protocols in Networking?

Objective:

1) The _____ is the physical path over which a message travels.
   a) Protocol b) Medium c) Signal d) All the above

2) Frequency of failure and network recovery time after a failure are measured as
   a) Performance b) Reliability c) Security d) Feasibility

3) Which topology requires a multipoint connection?
   a) Mesh b) Star c) Bus d) Ring

4) _____ refers to the structure or format of the data, meaning the order in which they are presented.
   a) Semantics b) Syntax c) Timing d) All of the above

5) Data flow between two devices can occur in a _____ way.
   a) simplex b) half-duplex c) full-duplex d) all of above

6) _____ refers to the physical or logical arrangement of a network.
   a) Data flow b) Mode of operation c) Topology d) None of the above

7) _____ is a collection of many separate networks.
   a) WAN b) An internet c) a LAN d) None of the above

8) The process-to-process delivery of the entire message is the responsibility of the _____ layer.
   a) Network b) Transport c) Application d) Physical

9) Mail services are available to network users through the _____ layer.
   a) Data link b) Physical c) Transport d) Application

10) As the data packet moves from the upper to the lower layers, headers are _____.
   a) Added b) Removed c) Rearranged d) Modified

11) When a host on network A, sends a message to a host on network B, which address does the router look at?
   a) Port b) Logical c) Physical d) None of the above

12) The _____ layer is responsible for moving frames from one hop (node) to the next.
   a) Physical b) Data link c) Transport d) None of the above

CHAPTER-2

DATA TRANSMISSION ON PHYSICAL MEDIA

In this chapter, topics which are most essential for "Data Transmission on a Physical media" are covered.

Topics are

- Data & Signal
- Line coding & Block Coding
- Transmission Media
- Cables & Connectors
- RS - 232 standard explained

2.0 DATA & SIGNAL

Data can be analog or digital. Analog data are continuous and take continuous values. Digital data have discrete states and take discrete values.

Signals can be analog or digital. Analog signals can have an infinite number of values in a range; digital signals can have only a limited number of values.

In data communications, we commonly use periodic analog signals and non-periodic (a periodic) digital signals.

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite Periodic analog signal is composed of multiple sine waves.

The bandwidth of a composite signal is the difference between the Highest and the lowest frequencies contained in that signal.

A digital signal can have more than two levels, we can send more than 1 bit for each level. Figure 2.1 shows two signals, one with two levels and the other with four.

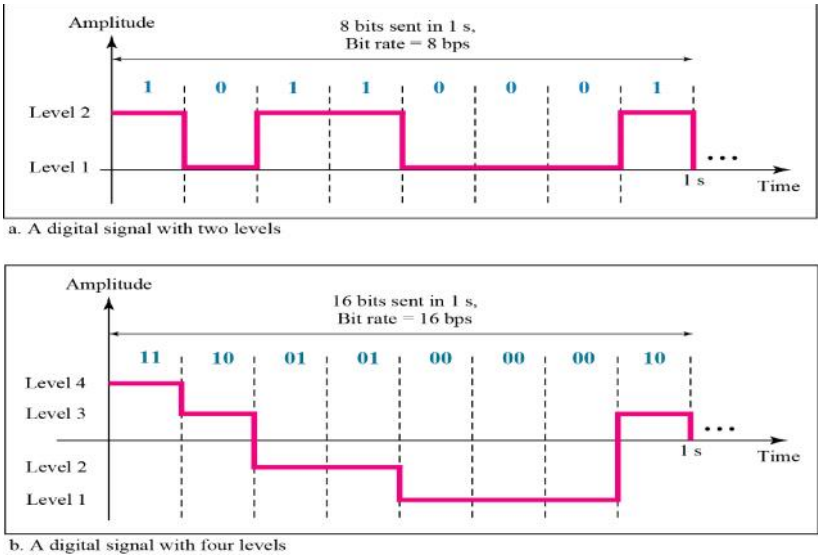


Fig. 2.1 Encoded digital signal

We send 1 bit per level in **part-a** of the figure & 2 bits per level in **part-b** of the figure. In general, if a signal has **L** levels, each level needs **$\log_2$ L** bits.

e.g. If a digital has eight (8) levels, we need three (3) bits per level

Number of bits per level= $\log_2 8 = 3$

Digital signal (whether periodic or non-periodic) is a composite analog signal with frequencies between zero and infinity. Digital signal is transmitted either baseband or broadband transmission method.

Baseband Transmission:

In Baseband, data is sent as digital signals through the media as a single channel that uses the entire bandwidth of the media. The signal is delivered as a pulse of electricity or light depending on the type of cabling being used. Baseband communication is also bi-directional, which means that the same channel can be used to send and receive signals. In Baseband frequency-division multiplexing is not possible.

In baseband transmission, the required bandwidth is proportional to the bit rate, if we need to send bits faster, we need more bandwidth.

Broadband Transmission:

In Broadband sends information in the form of an analog signal, which flows as electromagnetic waves or optical waves. Each transmission is assigned to a portion of the bandwidth; hence multiple transmissions are possible at the same time. Broadband communication is unidirectional, so in order to send and receive, two pathways are needed. This can be accomplished either by assigning a frequency for sending and assigning a frequency for receiving along the same cable or by using two cables, one for sending and one for receiving. In broadband frequency-division multiplexing is possible

Transmission Impairment

Signals travel through transmission media is not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise. Ref fig 2.2

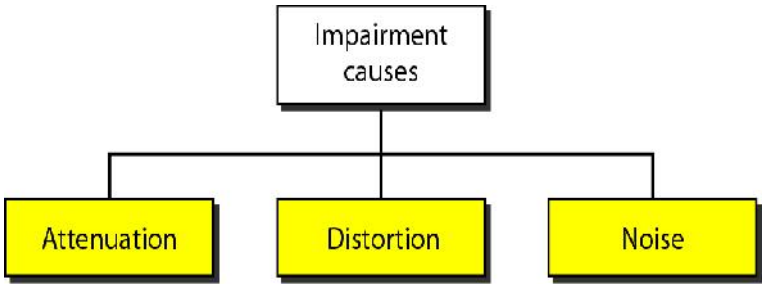


Fig. 2.2 signal impairment.

Attenuation:

Attenuation means loss of energy. When a simple or composite signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. To compensate this loss amplifiers are used to amplify the signal.

The **decibel (dB)** measures the relative strengths of two signals or one signal at two different points. The decibel value is negative if a signal is attenuated & positive if a signal is amplified.

$$dB = 10 \log_{10} P2 / P1$$

Distortion:

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed; own delay in arriving at the destination causes phase difference at the receiver.

Noise:

Noise causes signal impairment. Several types of noise, like thermal noise, induces noise, crosstalk noise & impulse noise corrupts the signal

Signal-to-Noise Ration (SNR):

It is ratio of what is wanted (Signal) to what is not wanted (noise). A high SNR means the signal is less corrupted by noise; a low SNR means the signal is more corrupted by noise.

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

Because SNR is the ratio of powers, it is often described in decibel units called SNR_{dB}

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

Data rate:

In data communications it is very important how fast we send data in bits per second (bps) over a channel. This data rate depends on

1. The bandwidth available
2. The level of the signal we use
3. The quality of the channel (the level of the noise)

Data rate is calculated in two methods

1. Nyquist bit rate (noiseless channel)
2. Shannon capacity (noisy channel)

Nyquist bit rate (noiseless channel):

For a noiseless channel, the nyquist bit rate defines the theoretical maximum bit rate is

$$\text{Bit Rate} = 2 \times \text{bandwidth} \times \log_2 L$$

'bandwidth' is the bandwidth of the channel

'L' is the number of signal levels used to represent data

On a given specific bandwidth we can increase the bit rate by increasing the number of signal levels. But practically there is a limit, it will burden the receiver. Hence increasing the levels of a signal may reduce the reliability of the system.

Shannon capacity (noisy channel):

Practically we cannot have a noiseless channel, hence as per the Shannon capacity the theoretical maximum bit rate of a noisy channel is

$$\text{Bit Rate} = \text{bandwidth} \times \log_2 (1 + SNR)$$

'bandwidth' is the bandwidth of the channel

'SNR' is the signal-to-noise ratio

Whatever may be the no. of signal levels, we cannot achieve a data rate higher than the capacity of the channel and it defines the characteristics of the channel, not the method of transmission.

Bandwidth:

In networking, we use the term bandwidth in two contexts.

- The first, bandwidth in hertz, refers to the range of frequencies in a composite signal or the range of frequencies that a channel can pass.
- The second, bandwidth in bits per second, refers to the speed of bit transmission in a channel or link.

An increase in bandwidth in hertz means an increase in bandwidth in bits per second. This relationship depends on whether baseband transmission or broadband (modulation) transmission.

Baud Rate:

Baud rate refers to the signal (symbol) rate, how many signal changes are transmitted per second. One goal of the data communications is to increase the data rate while decreasing the signal rate. Increasing the data rate increases the speed of transmission; decreasing the signal rate decreases the bandwidth requirement.

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

BPS = Baud per second x the number of Bits per Baud

The relationship between the data rate (bit rate) and the signal rate (baud rate) is

$$S = N \times 1 / r \text{ baud}$$

Where ‘S’ is the baud rate, ‘N’ is the bit rate and ‘r’ is the ratio of number of data elements carried in one signal element.

$$r = \log_2 L$$

Where ‘L’ is the no. of signal elements.

Throughput:

It is a measure of how fast we can actually send data through a network; throughput is also measured as bits per second (bps) as that of bandwidth. But both are not same, throughput is always less than the bandwidth. Bandwidth is a potential measurement of a link; the throughput is an actual measurement of a link.

2.1 ENCODING

Data (or) Signal encoding can be of four types:

a. DIGITAL-TO-ANALOG CONVERSION
b. ANALOG TO ANALOG CONVERSION
c. ANALOG-TO-DIGITAL CONVERSION
d. DIGITAL-TO-DIGITAL CONVERSION

2.1.1 DIGITAL-TO-ANALOG CONVERSION

Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data. (Refer Fig. 2.3)

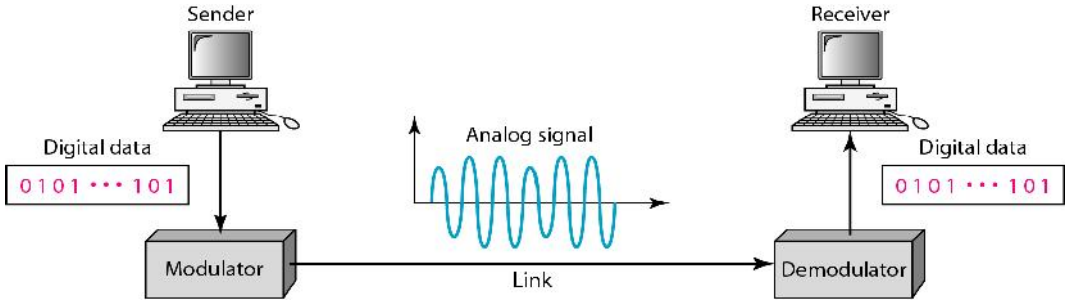


Fig. 2.3 Digital-to-Analog conversion

There can be different types of DIGITAL TO ANALOG conversion techniques as shown below fig 2.4

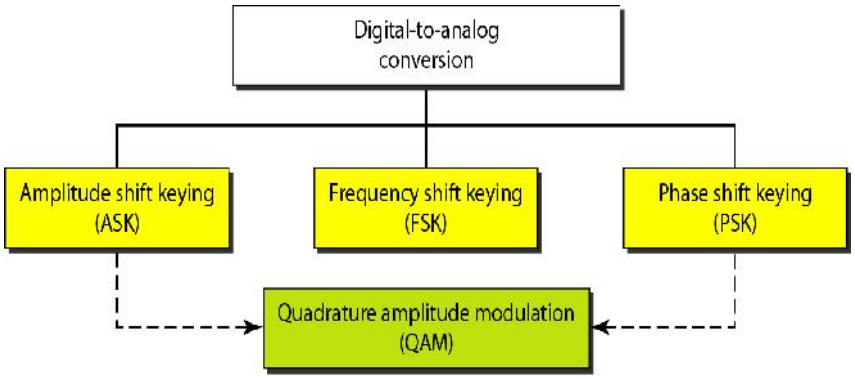


Fig. 2.4 Types of Digital-to-Analog conversion techniques

This sort of conversion will enable digital data to be carried over a 'Long Distance Communication Link'.

Example. Modem is one such device that employs this conversion technique to interface a Digital source and an Analog Media.

2.1.2 ANALOG TO ANALOG CONVERSION

Analog-to-analog conversion is the representation of analog information by an analog signal. One may ask why we need to modulate an analog signal; it is already analog. Modulation is needed if the medium is band pass in nature or if only a band pass channel is available to us.

There can be different types of ANALOG TO ANALOG conversion techniques as shown below fig 2.5

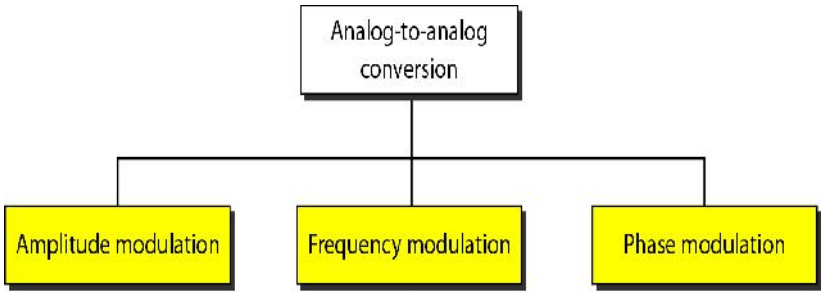


Fig. 2.5 Types of Analog-to-Analog conversion techniques

2.1.3 ANALOG-TO-DIGITAL CONVERSION

A Digital signal is superior to an analog signal. The tendency today is to change an analog signal to digital data before transmission. One such technique is Pulse Code Modulation, is shown (Fig. 2.6), schematically, below.

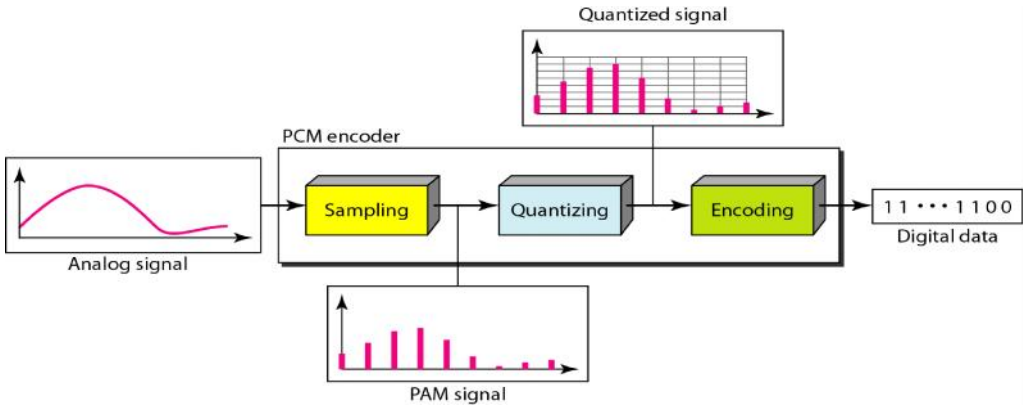


Fig. 2.6 Analog to Digital conversion

Example: Transmission of Voice, Video, Telemetry

2.1.4 DIGITAL-TO-DIGITAL CONVERSION

In this section, we see how we can represent digital data by using digital signals (Fig 2.7) The conversion involves three techniques: line coding, block coding, and scrambling. Line coding is always needed; block coding and scrambling may or may not be needed always.

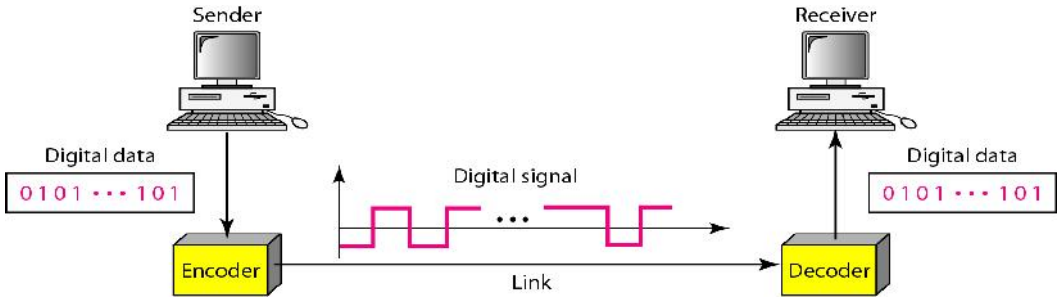


Fig. 2.7 Digital to Digital conversion

2.2 LINE ENCODING & BLOCK CODING

2.2.1 Line encoding

The waveform pattern of voltage or current used to represent the 1s and 0s of a digital signal on a transmission link is called line encoding. The common types of line encoding techniques as shown in fig 2.8 below are Unipolar, Polar, Bipolar and Multi level.

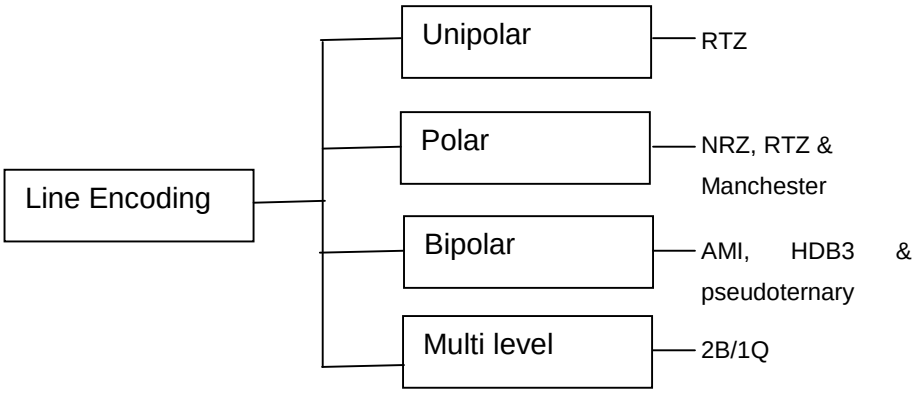


Fig. 2.8 Line encoding techniques

a. Unipolar Encoding

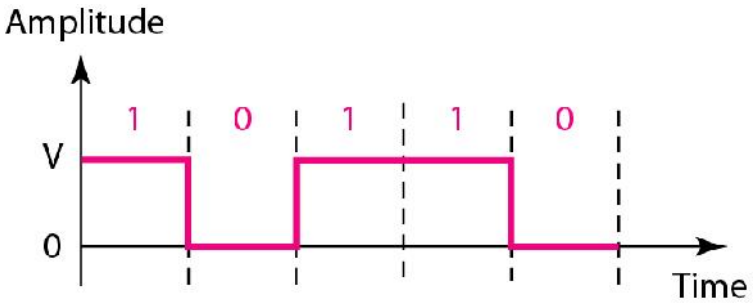


Fig. 2.9a unipolar encoding

Unipolar encoding has 2 voltage states, with one of the states being 0 volts. Since unipolar line encoding has one of its states at 0 Volts, it is also called Return to Zero (RTZ).

The average amplitude of unipolar encoded signal is non-zero. This creates a direct (DC) component (a component with zero frequency). When a signal contains a DC component, it cannot travel through media that cannot handle DC components.

Unipolar line encoding works well for inside machines—where the signal path is short—but is unsuitable for long distances, due to the presence of stray capacitance in the transmission medium. On long transmission paths, the constant level shift from 0 to 5 volts, which causes the stray capacitance to charge up (remember, the capacitor charging current is $i = i0 (1- e^{-t/RC})$. There will be a “stray” capacitor effect between any two conductors as shown in fig 2.9bthat are in close proximity to each other. For example, parallel running cables or wires are very suspect to stray capacitance.

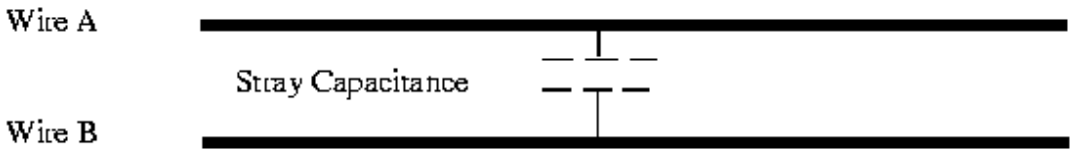


Fig. 2.9b stray capacitance effects

If there is sufficient capacitance on the line (and a sufficient stream of 1s) a DC voltage component will be added to the data stream. Instead of returning to 0 volts, it would only return to 2 or 3 volts, as shown in fig 2.9c. The receiving station may not recognize a digital low at voltage of 2 volts due to base lines wander.

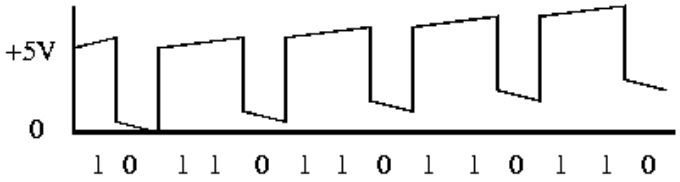


Fig. 2.9c base lines wander

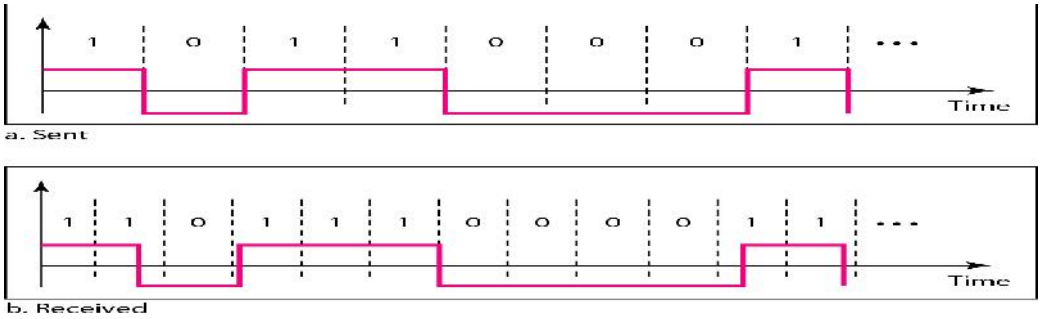


Fig. 2.9d Drifting of synchronization

Unipolar line encoding can have synchronization problems between the transmitter and receiver's clock oscillator. The receiver's clock oscillator locks on to the transmitted signal's level shifts (logic changes from 0 to 1) if there is a long series of logical 1s or 0s in a row. There is no level shift for the receiver's oscillator to lock to. The receiver oscillator's frequency may drift and become unsynchronized as shown in fig 2.9d it could lose track, of where the receiver is supposed to sample the transmitted data.

b. Polar Encoding

When the digital encoding is symmetrical—around 0 Volts—it is called a Polar Code. For example, the RS-232D interface uses Polar line encoding as shown in fig 2.10. The signal does not return to zero; it is either a +ve voltage or a -ve voltage. Polar line encoding is also called None Return to Zero (NRZ).

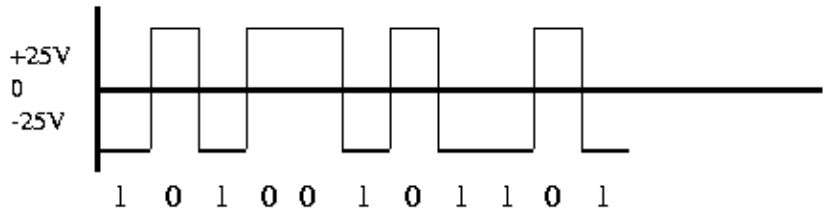


Fig. 2.10 RS 232D Polar encoding

Polar line encoding is the simplest pattern that eliminates most of the residual DC problem. Variation of Voltage levels for Polar encoding at Transmitter & Receiver end is shown in fig 2.11.

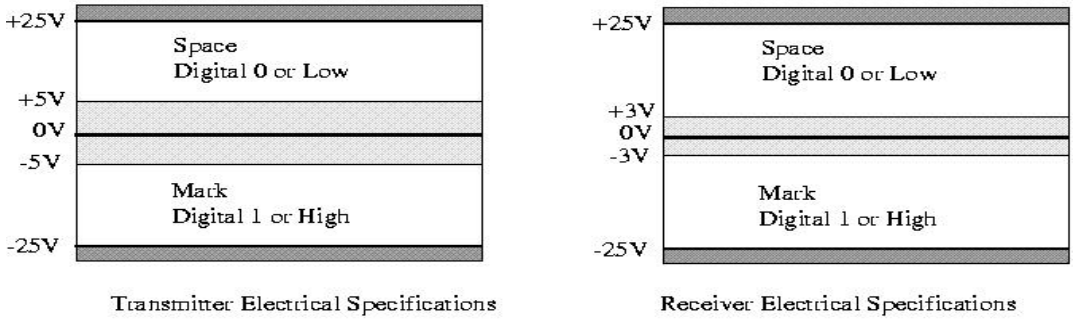


Fig. 2.11 Variation of Voltage levels

There is still a small residual DC problem, but Polar line encoding is a great improvement over Uni polar line encoding. Polar encoding has an added benefit in that it reduces the power required to transmit the signal by one-half.

i. NRZ Non return to Zero

1 = signal on

0 = signal off (no signal)

NRZ is used on low speed links, such as serial ports. Its problems are lack of clock recovery during long string of 0 or 1 bits and it has a DC component resulting in “baseline wander” during long strings of 0 or 1 bits as shown if fig 2.12

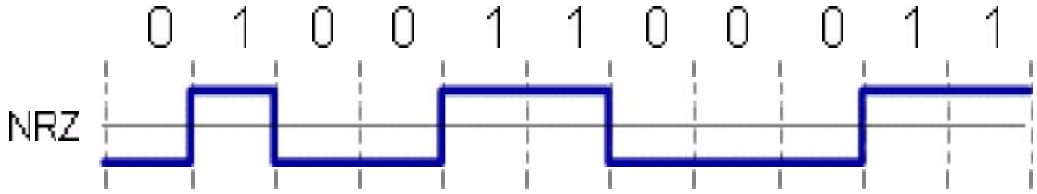


Fig. 2.12 NRZ Signal

ii. NRZI (Non return to Zero Inverted)

1 = change of signal level (on-off or off-on)

0 = no change of signal level

NRZI is a differential encoding used in 4B/5B on fast Ethernet. It fixes problems in clocking during long strings of 1 bit as shown in fig 2.13. The problems are the DC component and the lack of clock recovery during long string of 0 bits.

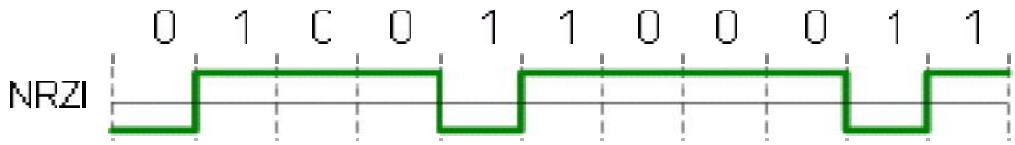


Fig. 2.13 NRZI Signal

iii. Manchester Line Encoding

In Manchester Line Encoding, there is a transition at the middle of each bit period. The mid-bit transition serves as a clocking mechanism (and also as data): a low to high transition represents a 1 and a high to low transition represents a 0as shown in the figure 2.14a.

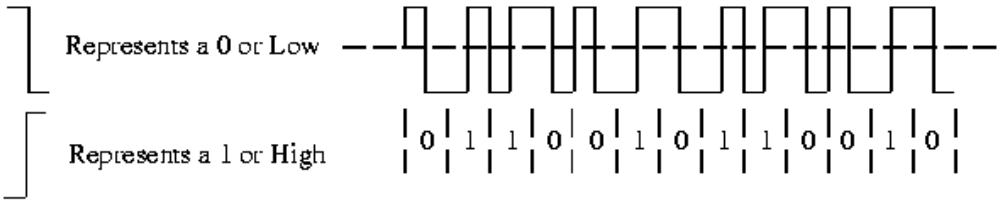


Fig. 2.14a Manchester line encoded Signal

Manchester line encoding has no DC component and there is always a transition available for synchronizing receives and transmits clocks. Manchester line encoding is also called self-clocking line encoding. It has the added benefit of requiring the least amount of bandwidth compared to the other line encoding.

Manchester line encoding requires 2 frequencies the base carrier and 2 x the carrier frequency. All others require a range from 0 hertz to the maximum transfer rate frequency as shown in fig 2.14b

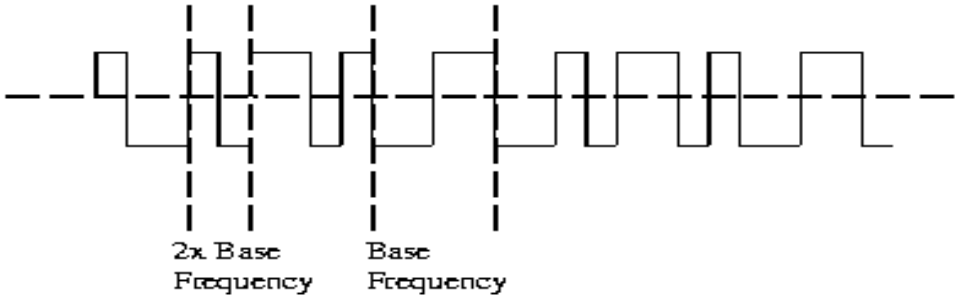


Fig. 2.14b Manchester line encoded Signal with base frequency

Manchester line encoding can detect errors during transmission: a transition is expected during every bit period. Therefore, the absence of a transition would indicate an error condition.

iv. Differential Manchester Encoding

Mid-bit transition is used only for clocking 0 = transition at beginning of bit period (low-to-high or high-to-low, depending on previous output level), 1 = no transition at beginning of bit period This coding is used in IEEE 802.5 (Token Ring) at 4Mbps and 16Mbps as shown in fig 2.15. It has the same properties as Manchester encoding, but a better signal detection and clocking in presence of noise. Still there is the inefficient use of bandwidth.

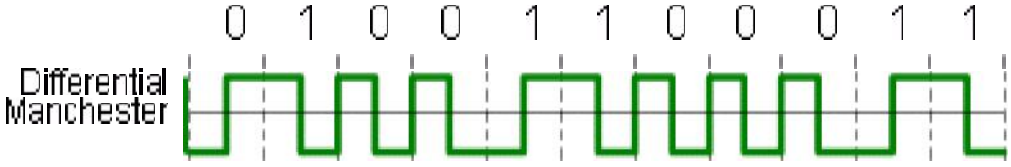


Fig. 2.15 Differential Manchester line encoded Signal

Polar and Unipolar line encoding both shares the same synchronization problem: if there is a long string of logical 1s or 0s, the receive oscillator may drift and become unsynchronized.

c. Bipolar Line Encoding

i. Alternate Mark Inversion (AMI)

Bipolar line encoding has 3 voltage levels. A low or 0 is represented by a 0 Volt level and a 1 is represented by alternating polarity pulses. By alternating the polarity of the pulses for 1s, the residual DC component cancels as shown in fig 2.16.

Bipolar line encoding is also called Alternate Mark Inversion (AMI).

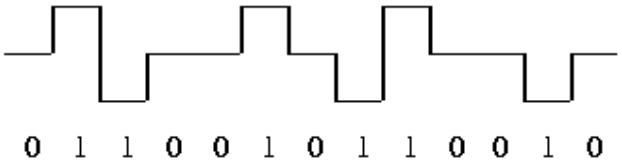


Fig. 2.16 Bipolar AMI Signal

ii. B8ZS Bipolar with 8 Zero Substitution

In this type of coding, a string of 8 zeros is substituted according to the following rules:

If the immediate preceding pulse is of (-) polarity, then code each group of 8 zeros as

0 0 0 - + 0 + -

If the immediate preceding pulse is of (z) polarity, then code each group of 8 zeros as 0 0 0 + - 0 - + as shown fig 2.17.

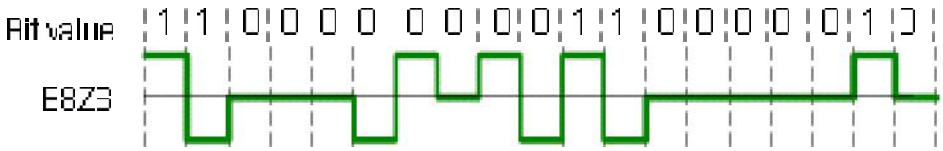


Fig. 2.17 B8Z8 Signal

iii. High Density Bipolar 3 (HDB3)

Another coding scheme is HDB3, high density bipolar 3, used primarily in Europe for 2.048MHz (E1) carriers as shown in fig 2.18. This code is similar to BNZS in that it substitutes bipolar code for 4 consecutive zeros according to the following rules:

If the polarity of the immediate preceding pulse is (-) and there have been an odd (even) number of logic 1 pulses since the last substitution, each group of 4 consecutive zeros is coded as 000-(+00+).

If the polarity of the immediate preceding pulse is (+) and there have been an odd (even) number of logic 1 pulses since the last substitution, each group of 4 consecutive zeros is coded as 000+(-00-).

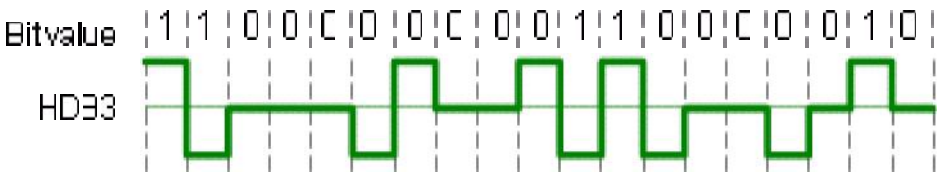


Fig. 2.18 HDB3 Signal

iv. Pseudoternary

Pseudoternary has the same behavior as Bipolar-AMI as shown in fig 2.19, except it reverses signaling:

1 = no signal (0 voltage)

0 = alternating +V and –V

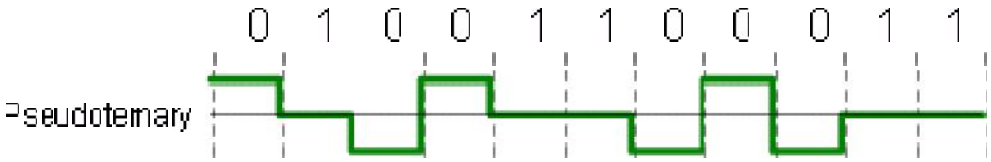


Fig. 2.19 Pseudoternary Signal

d. Multi Level Line Encoding

i. 2B1Q

The 2B1Q (two binary, one quaternary) line encoding scheme was intended to be used by the ISDN DSL and SDSL applications. This code is a four-level line code in which two binary bits (2B) represent one quaternary symbol (1Q)as shown in fig 2.20. The 2B1Q line coding was seen as a major enhancement over the original T1 line coding, because 2B1Q encoded two bits per signal change instead of just one per change.

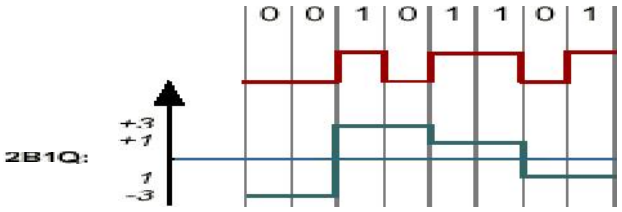


Fig. 2.20 2B1Q Signal

2.2.2 Block Coding

Block coding is normally referred to as ***m*B/*n*B** coding; it replaces each *m*-bit group with an *n*-bit group. Block coding concept is shown below (Fig 2.21)

.

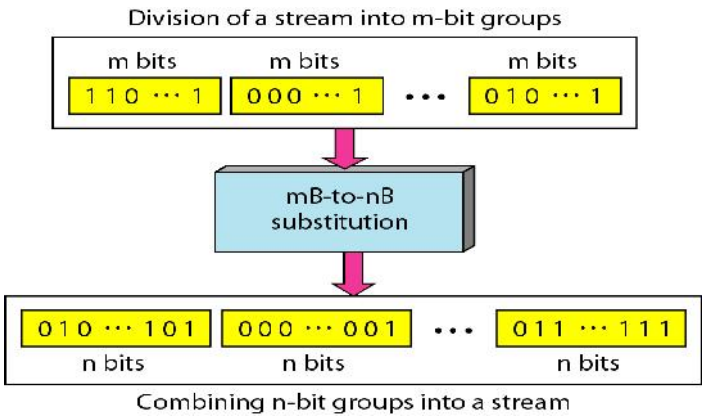


Fig. 2.21 Block coding concept

i. 4B5B (4 Bit / 5 Bit)

4B5B uses 5 bit signals for each 4 data bit. The 5 bit sequences are chosen so that there are never more than 3 consecutive zeros in the output stream. When used with NRZI, will have at least 2 signal transitions in every 5 bits. (Refer Fig. 2.22)

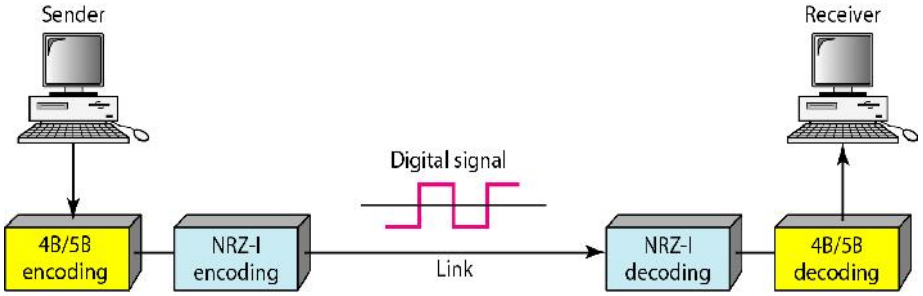


Fig. 2.22 4B/5B coding

ii. 8B10B (8 Bit / 10 Bit)

8B10B coding is used in interfaces as PCI Express, Fiber Channel and others. In these applications 8B10B transmission code provides the following functions:

- Improves transmission characteristics
- Enables bit- level clock recovery
- Improves error detection
- Separates data symbols from control symbols
- Derives bit and word synchronization

The data bytes are encoded into 10-bit data characters resulting into 1024 possible characters. 2x256=512 is reserved for the data byte transfers. One character representative has more 1's; the other has more 0's and is selected according to the current disparity (see below). 12 special characters are defined for special signaling. The rest of the 1024-512-12 are not allowed for transmission and indicate transmission errors or unsynchronized status once they are received at the destination. Ordered sets are flexible building blocks which may be used for in-band and or out-of-band protocol functions.

8B10B code recognizes the idea of a *Running Disparity* (the difference between the number of 1's and 0's transmitted). The sender keeps the running disparity around zero, the receiver checks the data stream according to this rules and is thus able to detect some transmission errors. Other neighboring coding schemes like 64B66B are available and are used in certain applications.

2.3 Transmission Media Categories

There are 2 basic categories of Transmission Media as shown in fig 2.23

a. Un-Guided Transmission Media
b. Guided Transmission Media

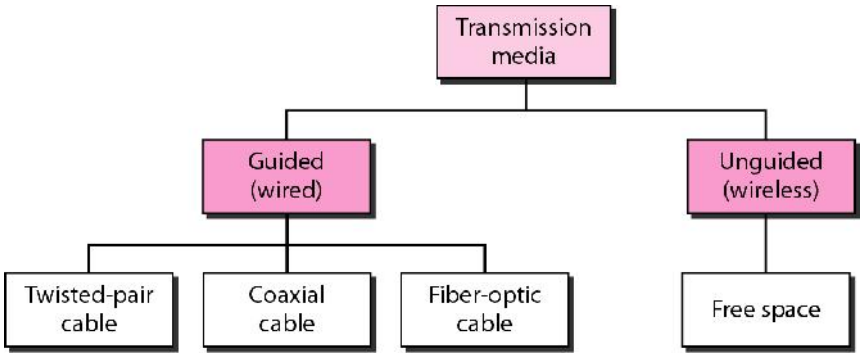


Fig. 2.23 Transmission Media Categories

2.3.1 Un-guided Transmission Media

Wireless communication is the base of un - guided media. It transports electromagnetic waves without using a physical conductor. The wireless media available for transmitting network packets are 3 types

a. Radio waves – used for wire-less LANs
b. Microwaves – used for satellite communication
c. Infrared waves – used for controlling devices like remote controls

2.3.2 Guided Transmission Media

There 4 basic types of Guided Media:

a. Open Wire
b. Coaxial Cable
c. Optical Fiber
d. Twisted Pair

Media versus Bandwidth

Comparison of usable bandwidth between the different guided transmission media is shown in table 2.1

Cable Type	Bandwidth
Open Wire	0 - 5 MHz
Coaxial Cable	0 - 600 MHz
Optical Fiber Cable	0 - 10 GHz
Twisted Pair Cable	0 - 100 MHz

Table. 2.1 Comparison of band width

i. Open wire

This open wire is not used in Data communications.

ii. Coaxial Cables

Two types of coaxial cable are used in data communications. **Thick net** (RG-8 and RG-11 coaxial cable) and **Thin net** (RG-58 coaxial cable). Thick net is a heavy-gauge coaxial cable that is fairly inflexible and requires special equipment (over and above a simple network card) to connect the computer to the network backbone. These co-axial cables are now not used much.

iii. Optical Fiber Cables

Fiber-optic cable is a high-speed alternative to copper wire and is often employed as the backbone of larger corporate networks. However, the drop in the price of fiber-optic cable has started to make it a possibility for other LAN uses. Fiber-optic cable uses glass or plastic filaments to move data and provides greater bandwidth as well as longer cable runs (up to 2 kilometers, depending on the network architecture).

iv. Twisted Pair cables

LAN cables are generically called twisted pair cables. There are two (2) types. One is UTP (Unshielded Twisted Pair) and the other is STP (Shielded Twisted Pair). UTP is predominantly used for indoor areas and whereas STP for outdoor & in special areas. These UTP cables are identified with a category rating.

UTP comes in two forms **SOLID** or **STRANDED**. SOLID refers to the fact that each internal conductor is made up of a single (solid) wire, STRANDED means that each conductor is made up of multiple smaller wires. The only obvious benefit of using **stranded** cable (which is typically more expensive) is that it has a smaller 'bend- radius' (we can squeeze the cable round tighter corners with lower loss) or where we plug and unplug the cable frequently. All other things being equal the performance of both types of cable is the same. In general solid cable is used for backbone wiring and stranded for PC to wall plug cables.

Maximum LAN cable runs are 100 meters (~300ft).

Crossed and Straight cables - when to use them

The following diagram (Fig. 2.24) shows the Normal **use of Crossed and Straight cables (see also the notes below).**

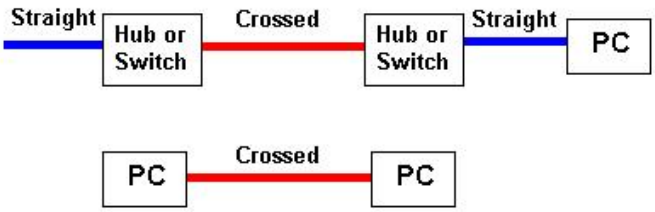


Fig. 2.24 Use of crossed and straight cables

Note:

We show Straight cables as **BLUE** and Crossed as **RED**. That is our convention the cable color can be anything you choose or more likely the vendor decides.

To avoid the need for Crossed cables many vendors provide **UPLINK** ports on Hubs or Switches - these are specially designed to allow the use of a STRAIGHT cable when connecting back-to-back Hubs or Switches. Read the manufacturers documentation carefully.

Category 5(e) (UTP) colour coding table

The following Fig. 2.25 shows the normal colour coding for category 5 cables (4 pair) based on the two standards supported by TIA/EIA

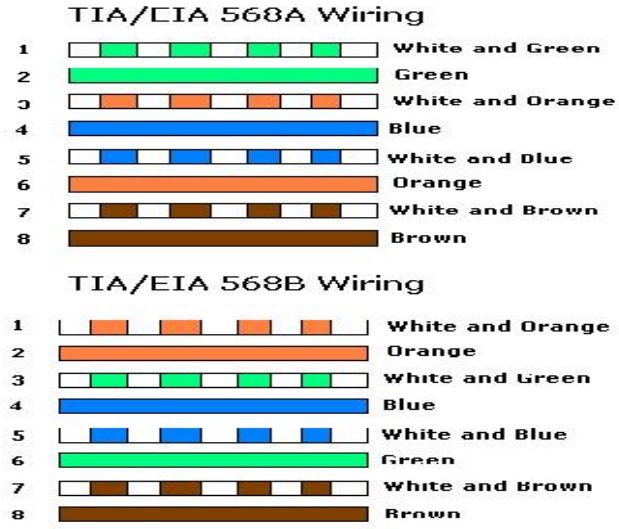


Fig. 2.25 TIA/EIA 568 wiring standard

The following description shows the wiring at both ends (male RJ45 connectors) of the crossed cable. **Note:** The diagrams (Fig. 2.26) below shows crossing of all 4 pairs and allows for the use of **cat 3/4** cables. Pairs 4, 5 and 7, 8 do not NEED to be crossed in 100base-TX wiring. See notes below.

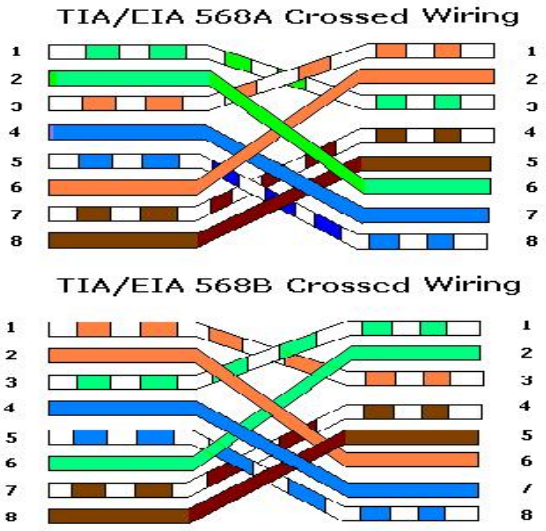


Fig. 2.26 TIA/EIA 568 Standard

NOTE:

All our crossed wiring is now done to the 100base-T4 spec which you can use with 10base-T networks - but NOT necessarily the other way around.

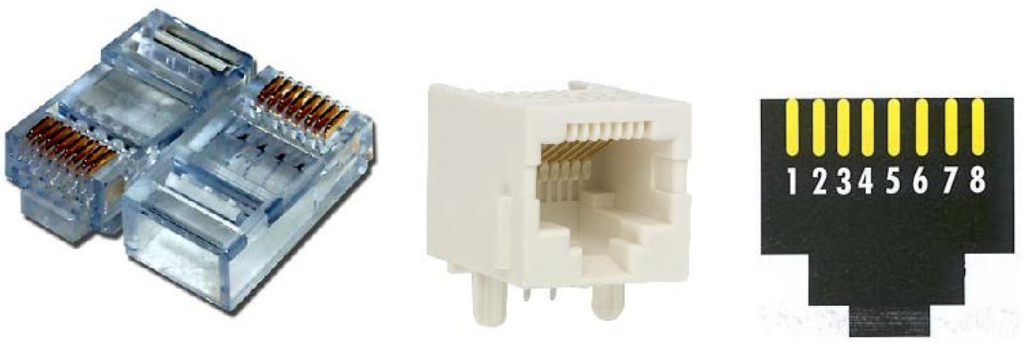
Most commercial cables these days seem not to cross pairs 4, 5 and 7, 8. If there is no cat3/4 wiring in the network is perfectly acceptable.

Gigabit Ethernet uses all 4 pairs so requires the full 4 pair (8 conductors) cross configuration (shown above).

If you are using Power-over-Ethernet (802.3af) then Mode A or Alternative A uses pairs 1, 2 and 3, 6 for both signals and power. Mode B or alternative B uses 4, 5 and 7, 8 to carry power. In all cases the spec calls for polarity insensitive implementation (using a diode bridge) and therefore crossing or not crossing pairs 4, 5 and 7, 8 will have no effect.

Crossed Gigabit Ethernet cables must cross all 4 pairs.

Different types of RJ45 connectors (Jacks, Sockets) and their pin numbering is shown in fig 2.27 below.



(a) (b) (c)

Fig. 2.27 RJ45 connector (a) Jack (b) Socket (c) Pin numbering

RJ45 Connections & Crimping

STEP 1: Cut the outer jacket of the wire about 1.5" to 2" from the end as shown in fig 2.28a. This will give you room to work with the wire pairs. Separate the pairs and align them in the order shown below. Begin flattening the wires into a "ribbon" as shown so that it will easily slip into the connector and into the individual channeled areas.

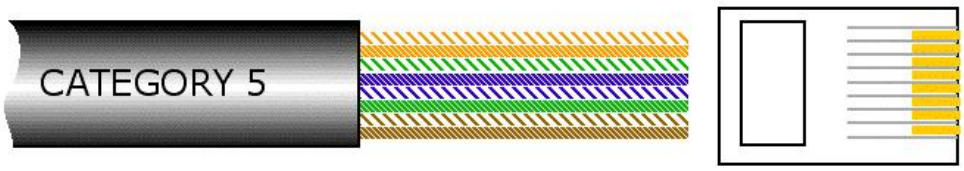


Fig. 2.28a RJ45 connector crimping (step1)

STEP 2: Once you have all the wires aligned and ready to insert, as shown in fig 2.28b you must trim them to approximately 1/2" in order to have as little "untwisted" wire in the connection as possible. Category 5 specifications require a certain number of twists per inch and even the connector counts!

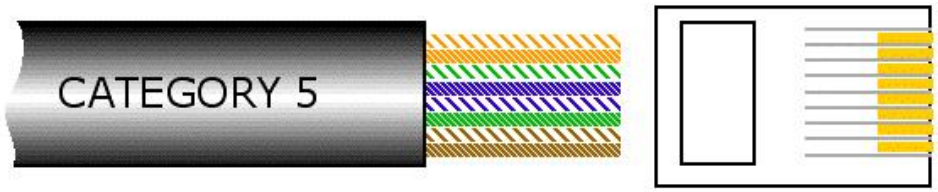


Fig. 2.28b RJ45 connector crimping (step2)

STEP 3: Insert the wires into the connector as shown in fig 2.28c making sure that each wire goes into its appropriate "channel" and extends all the way to the end of the the connector underneath the gold crimping connectors. Sometimes you can look at the end of the connector to see the copper wires if you're using solid copper cable. If the wires don't extend to the end of the connector, the crimp may not make contact.

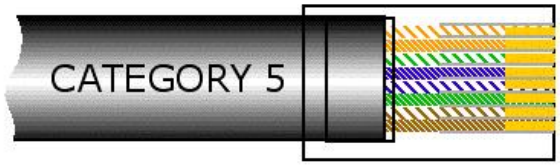


Fig. 2.28c RJ45 connector crimping (step3)

STEP 4: Press the cable and the jacket into the connector firmly so that the jacket will be crimped by the plastic wedge near the rear of the connector, and insert it into your crimping tool and crimp the cable. **RE-CRIMP** the cable to make sure all connections are made.

STEP 5: Repeat steps 1 thru 4 for the other end of the cable for a standard Ethernet cable.

2.4 CONNECTORS & INTERFACES

There are different types of connectors, interfaces & standards are used in connecting the datacom devices, like

EIA RS232-C Standard
X.21 Interface
V.35 Interface
G.703 Interface

2.4.1 EIA RS232-C STANDARD

This standard is used to connect serial devices like Modems to a Personal Computer. It specifies a 25 pin connector as the standard interface in data communication networks, with lettering pin designations for ground, data, and control and timing circuits. The table 2.2a shows the designations for each of the 25 pins of the standard and the direction of flow of signal.

INTERCHANGE	CIRCUIT No.	PIN No.	DESCRIPTION	Direction
AA	101	1	Protective Ground	--
BA	103	2	Transmit Data	DTE ⟶ DCE
BB	104	3	Receive Data	DTE ⟵ DCE
CA	105	4	Request To Send	DTE ⟶ DCE
CB	106	5	Clear To Send	DTE ⟵ DCE
CC	107	6	Data Set Ready	DTE ⟵ DCE
AB	102	7	Signal Ground	---
CF	109	8	Receive Line Carrier Detect	DTE ⟵ DCE
--	--	9	Reserved	+12V for test
--	--	10	Reserved	-12v for test
--	--	11	Unassigned	---
SCF	122	12	Secondary RLSD	DTE ⟵ DCE
SCB	121	13	Secondary CTS	DTE ⟵ DCE
SBA	118	14	Secondary TD	DTE ⟶ DCE
DB	114	15	Transmitter Signal Element Timing	DTE ⟵ DCE

SBB	119	16	Secondary RD	DTE ← DCE
DD	115	17	Receiver Signal Timing Element	DTE ← DCE
--	--	18	Unassigned	---
SCA	120	19	Secondary RTS	DTE → DCE
CD	108.2	20	Data Terminal Ready	DTE → DCE
CG	110	21	Signal Quality Detector	DTE ← DCE
CE	125	22	Ring Indicator	DTE ← DCE
CH/CI	111/112	23	Data Signal Rate Selector	DTE → DCE
DA	113	24	Transmit Signal Element Timing	DTE → DCE
--	--	25	Unassigned	---

Table 2.2a RS 232C standard 25 pin description

The following table 2.2b illustrates the 9 pin serial connector as found on most PC's today. This has all but replaced the previous 25 pin connector found on earlier PC's.

SIGNAL	PIN No.
Carrier Detect	1
Receive Data	2
Transmit Data	3
Data Terminal Ready	4
Signal Ground	5
Data Set Ready	6
Request To Send	7
Clear To Send	8
Ring Indicator	9

Table 2.2 RS 232C standard 9 pin description

EIA RS232-C Electrical Standard

All circuits carry bi-polar low-voltage signals, measured at the connector with respect to signal ground (AB), and may not exceed ±25 volts. Signals are valid in the range ±3 volts to ±25 volts. Signals within the range -3 volts to +3 volts are considered invalid.

For data lines, binary 1 (a high) is represented by -3 volts to -25 volts, whilst binary 0 is +3 volts to +25 volts.

For control lines, OFF is represented by -3 volts to -25 volts, whilst binary 0 is +3 volts to +25 volts.

EIA RS232-C Mechanical Standard & connectors

Female connector is connected to DCE and male connector to DTE. Short cables of less than 15 meters (50 feet) are recommended. The pin assignments detailed above must be used.

The following Fig. 2.29 shows the 25-pin connector used for the DTE interface. It is a MALE connector, which has 25 pins. Beneath it is the 25 pin FEMALE connector used on the DCE interface. Note that the connectors have a longer side at the top and a shorter side at the bottom. This is to prevent the plugs being inserted into the connectors the wrong way round.

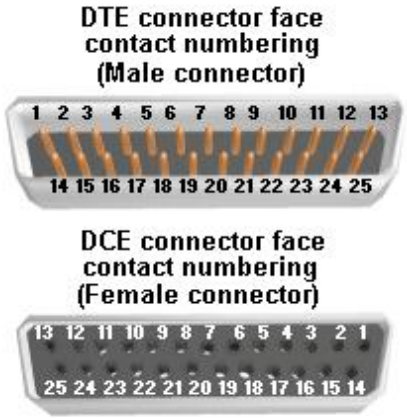


Fig. 2.29 RS-232 connectors

RS-232 Signals Functional Description

General: The first letter of the EIA signal name categorizes the signal into one of five groups, each representing a different "circuit":

A - Ground
B - Data
C - Control
D - Timing
S - Secondary channel

The Noise Margin Issue

Note that terminator (receiving end) voltages are not the same as driver required voltages. This voltage level definition compensates for voltage losses across the cable.

Signals traveling along the cable are attenuated and distorted as they pass. Attenuation increases as the length of the cable increases. This effect is largely due to the electrical capacitance of the cable.

The maximum load capacitance is specified as 2500pf (pico farad) by the standard. The capacitance of one meter of cable is typically around 130pf, thus the maximum cable

length is limited to around 17 meters. However, This is a nominal length defined by the standard, and it is possible to use longer cables up to 30 meters, with low-capacitance cables, or with slow data rates and a proper error correction mechanism.

Interface Mechanical Characteristics

The connection of the DCE and the DTE is done with a pluggable connector. The female connector should be associated with the DCE. The following table lists the pin assignments defined by the standard. The type of connector to be used is not mentioned in the standard, but the DB-25 (or on IBM-AT's, a minimal DB-9) connectors are almost always used.

2.4.2 X.21 interface

X.21 interface is a specification for differential communications introduced in the mid 1970's by the ITU-T. X.21 was first introduced as a means to provide a digital signaling interface for telecommunications between carriers and customer's equipment. This includes specifications for DTE/DCE physical interface elements, alignment of call control characters and error checking, elements of the call control phase for circuit switching services, and test loops.

When X.21 is used with V.11, it provides synchronous data transmission at rates from 100 kbit/s to 10 Mbit/s. There is also a variant of X.21 which is only used in select legacy applications, "circuit switched X.21". X.21 normally is found on a 15-pin D Sub connector and is capable of running full-duplex data transmissions.

The Signal Element Timing, or clock, is provided by the carrier (your telephone company), and is responsible for correct clocking of the data. X.21 is primarily used in Europe and Japan.

2.4.3 V.35 Interface

Basically, V.35 is a high-speed serial interface designed to support both higher data rates and connectivity between DTEs (data-terminal equipment) or DCEs (data-communication equipment) over digital lines.V.35 interface recognizable by its 34-pin connector, out of which only 18 pins are used. Its pin layout & connector is shown in **fig 2.30**

V.35 combines the bandwidth of several telephone circuits to provide the high-speed interface between a DTE or DCE and a CSU/DSU (Channel Service Unit/Data Service Unit). To achieve such high speeds and great distances, V.35 combines both balanced and unbalanced voltage signals on the same interface. Transmission is using a synchronous protocol. Although V.35 is commonly used to support speeds ranging anywhere from 48 to 64 Kbps, much higher rates are possible. V.35 cable distances theoretically can range up to 4000 feet (1200 m) at speeds up to 100 Kbps. Actual distances will depend on your equipment and the quality of the cable. Lan routers often come equipped with a V.35 electrical interface.

A - Common Chassis Ground
B - Common Signal Ground
C - DTE Request to Send
D - DCE Clear to Send
E - DCE Data Set Ready
F - DCE Data Carrier Detect
H - DTE Data Terminal Ready
J - DCE Ring Indicator
K - Local Test
L - Unassigned
M - Unassigned
N - Unassigned
P - DTE Send Data A Balanced
R - DCE Receive Data A Balanced
S - DTE Send Data B Balanced
T - DCE Receive Data B Balanced
U - DTE Terminal Timing A Balanced
V - DCE Receive Timing A Balanced
W - DTE Terminal Timing B Balanced
X - DCE Receive Timing B Balanced
Y - DCE Send Timing A Balanced
Z - Unassigned
AA - DCE Send Timing B Balanced
BB - Unassigned
CC - Unassigned
DD - Unassigned
EE - Unassigned
FF - Unassigned
HH - Unassigned
JJ - Unassigned
KK - Unassigned
LL - Unassigned
MM - Unassigned
NN - Unassigned

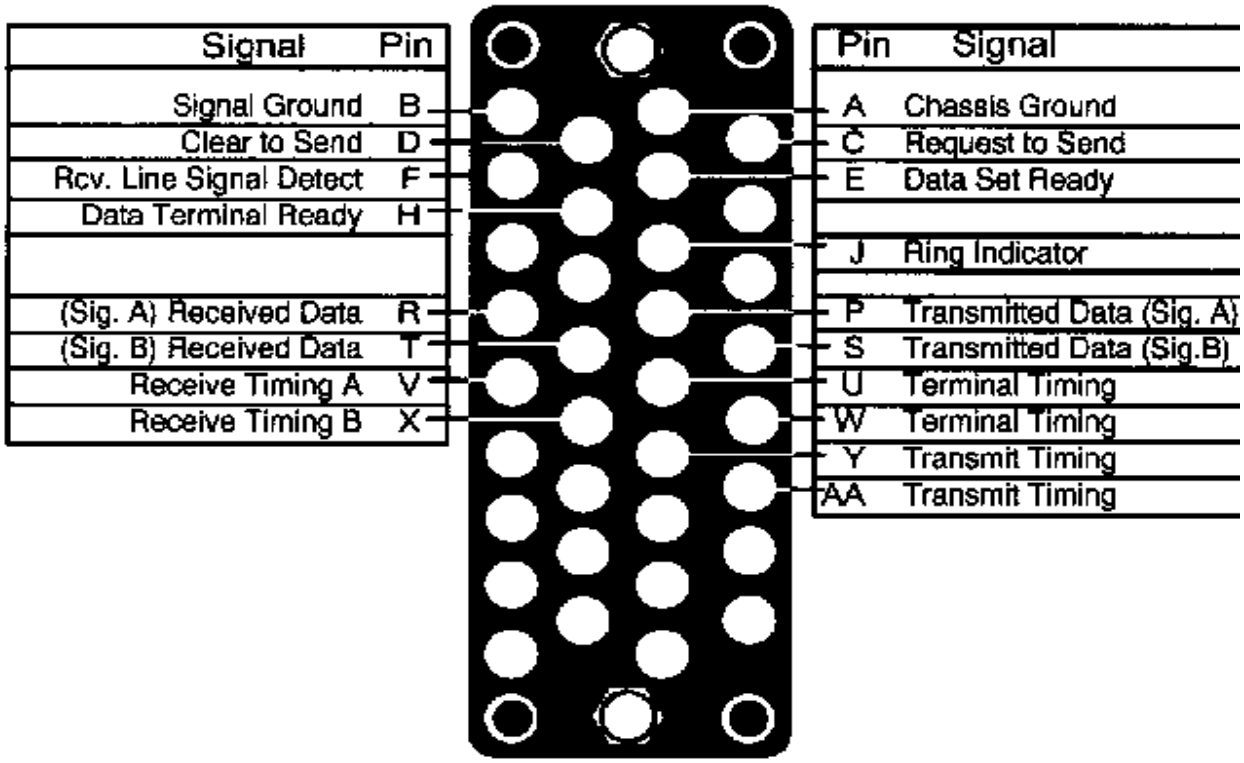


Fig 2.30 V.35 interface pin layout & connector

2.4.4 G.703 Interface

G.703 is an ITU-T standard for transmitting voice or data over digital carriers such as T1 and E1. G.703 provides specifications for pulse code modulation (PCM).

G.703 is typically transported over balanced 120 ohm twisted pair cables terminated in RJ45C jacks. However, some telephone companies' use unbalanced (dual 75 ohm coaxial cables) wires, also allowed by G.703.

i. Interface Standards

G.703 defines the electrical specification for 'E1' (or CEPT-E1) telecommunication lines used in Europe (and other territories operating networks using E1 lines) for services including primary rate ISDN.

ii. Interface Characteristics E1

E1 is a differential communications interface using either two pairs (TX and RX) connected through a single RJ-48C connector (also frequently written as RJ48, RJ-48 or RJ48c and also often incorrectly called RJ-45 or RJ45 - it is an RJ connector with 8 contacts assigned according to specification RJ-48C) or using two coaxial connections (TX and RX) via two BNC connectors. To enable reliable transmission and reception over thousands of meters of cable between customer premises and telephone exchanges, the data is encoded using HDB3 to produce a bipolar signal with the required characteristics. Note that timing information (i.e. the bit clock) is encoded within the signal to enable the receiver to recover a clock and correctly decode the received data.

iii. Interface Applications

Telecommunications companies (in the relevant territories) provide and support E1 or T1 services to end-users (usually business customers) in a variety of channel configurations with associated price structures. The organization of data carried using E1 or T1 services is defined within the G.704 standard.

E1 and T1 lines are used for a VERY wide variety of uses including Voice, Internet Access, X.25, Multiplexed data, ISDN. Both E1 and T1 lines are frequently connected to X.21 or V.35 connections by network interface converters before connection to the communications equipment.

2.4.5 DTE – DCE interface

DATA COMMUNICATIONS EQUIPMENT (DCE)

An example of a DCE is a modem. A DCE is fitted with a 25 pin female connector.

DATA TERMINAL EQUIPMENT (DTE)

An example of a DTE is a computer terminal. A DTE is fitted with a 25 pin male connector.

How to exchange information between a DCE and DTE

Now, let's look at the sequence that occurs when data is transferred between a DTE and a DCE. The data can only be transferred after the correct sequence of signals is followed, for instance, there is no point sending data if the modem is turned off. Let's go through each of the steps involved (i.e., signal line assertions required) to transmit and receive characters across the RS232 interface.

TRANSMITTING DATA (DTE to DCE)

1: Assert DTR and RTS
2: Wait for DSR
3: Wait for CTS
4: Transmit the data

Step 1 and 2 are essential to ensure that the modem is on-line and connected to another modem. Waiting for DSR checks that the modem is on-line.

RECEIVING DATA (DCE to DTE)

1: Assert DTR
2: Wait for DSR
3: Receive the data

CONNECTING TWO DTE DEVICES TOGETHER

Often, two DTE devices need to be connected together using a serial link. This is for file transfer or printer access. The problem is that DTE devices expect to talk directly to DCE devices, not another device of the same type.

DTE's cannot generate signals like DSR and CTS, so connecting two DTE's together will result in neither getting permission to send, and thinking that the modem is off-line (by not receiving DSR).

To allow the interconnection of two DTE devices without using DCE's as shown in fig 2.30 a special type of cable must be used. This is called a *Null Modem Cable*, which fools the DTE into thinking that it is connected to a DCE device. In this case, modems are not used, so the connection looks like.

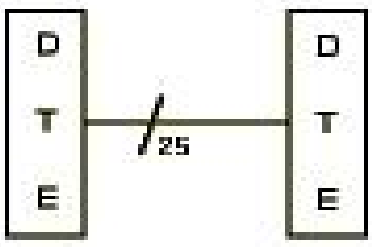


Fig. 2.30 Interconnection of two DTEs

DESIGNING A NULL-MODEM CABLE

In designing a NULL-MODEM cable, the DTE signals from one computer are swapped over as inputs to supply the DCE expected signals on the other DTE.

As we can see from the fig 2.31 when two DTE's are connected together, the signal lines from one DTE are transposed to the other DTE, fooling it into thinking that it is communicating with a DCE

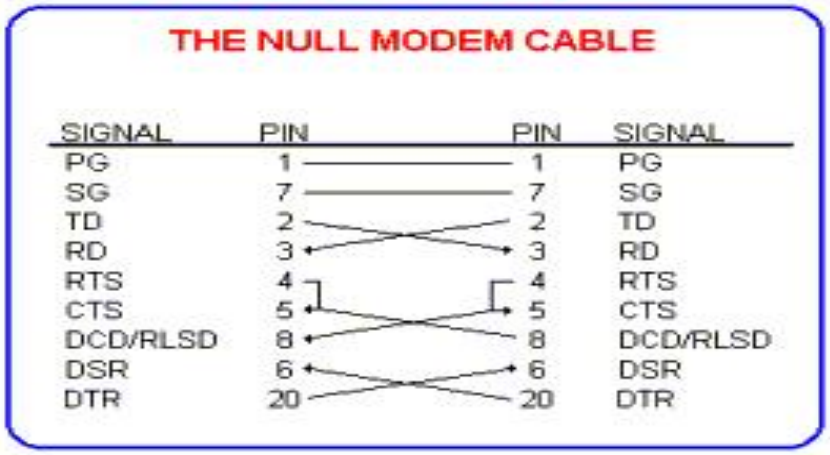


Fig. 2.31 Null Modem cable connection

SETTING UP OF CLOCK FOR DCE/DTE DEVICES

A general rule is that DCE devices provide the clock (internal clocking) and that the DTE device synchronizes on the provided clock (external clocking). So a straight cable between those devices is sufficient.

The three different options in clocking are internal, external, and received/recovered/loop clocking.

The actual difference is in the transmitted clock signal, because the received clock signal is always derived from the incoming data.

The outgoing clock (transmitted clock) will always be generated by an internal oscillator; the only difference between the three options is what is used as the phase reference.

When internal clocking is used the Tx clock is phase locked to the internal oscillator.

For the received/recovered/loop clocking (all those terms are used and all mean the same) the phase of the Tx clock is locked to the clock derived from the incoming data.

And when external clocking is used the phase of the Tx clock is phase locked to the one that is provided through the Rx clock.

Review Questions:

Subjective:

1. What is information, Data, Signal? Discuss the difference between them?
2. Why encoding of signal is required? Discuss the different methods?
3. What is meant by line coding & block coding? What is its relevance? Discuss its benefits?
4. Name two (2) major categories of transmission media? Discuss twisted pair category wise?
5. What is RS232 serial standard? Discuss?
6. Discuss the characteristics of DTE – DCE interfaces, mention the control leads required for DTE – DCE interface?
7. What are EIA / TIA 568A & 568B wiring standards? On which media it is used?

Objective:

1. _____ is a type of transmission impairment in which the signal loses strength due to the different propagation speeds of each frequency that makes up the signal.
a) Attenuation b) Distortion c) Noise d) Decibel

2. A _____ signal is a composite analog signal with an infinite bandwidth.
a) Digital b) Analog c) either (a) or (b) d) neither (a) nor (b)

3. Which encoding method uses alternating positive and negative values for 1s?
a) NRZ-I b) RZ c) Manchester d) AMI

4. In a _____ scheme, all the signal levels are on one side of the time axis, either above or below.
a) Polar b) Bipolar c) Unipolar d) All of the above

5. In _____ schemes, the voltages are on the both sides of the time axis. For example, the voltage level for 0 can be positive and the voltage level for 1 can be negative.
a) Polar b) Bipolar c) Unipolar d) All of the above

6. In _____ the level of the voltage determines the value of the bit.
a) NRZ-I b) NRZ-L c) Both (a) and (b) d) Neither (a) nor (b)

7. In Manchester and differential Manchester encoding, the transition at the middle of the bit is used for _____.
a) Bit transfer b) Baud transfer c) Synchronization d) None of the above

8. In _____encoding, we use three levels: positive, zero, and negative.
a) Unipolar b) Bipolar c) Polar d) None of the above

9. _____ substitutes eight consecutive zeros with 000VB0VB.
a) B4B8 b) HDB3 c) B8ZS d) None of the above

CHAPTER-3

DATA TRANSMISSION ON LAN

In this chapter, functions associated with "Data Transmission on LAN "are discussed.

Topics covered:

- *Data Link Control - Line discipline, Framing, Flow Control & Error Control*
- *Media Access Control & Ethernet Categories*
- *Connecting Devices*

3.1 DATA LINK CONTROL

3.1.1 FRAMING

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. A frame in a character-oriented protocol is shown in fig 3.1a & a frame in a bit-oriented protocol is shown in fig 3.1b

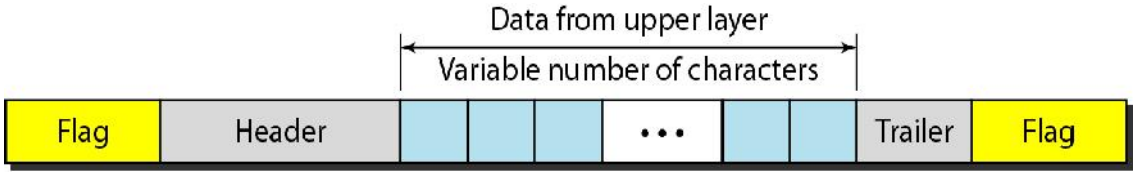


Fig. 3.1a Character-oriented protocol frame

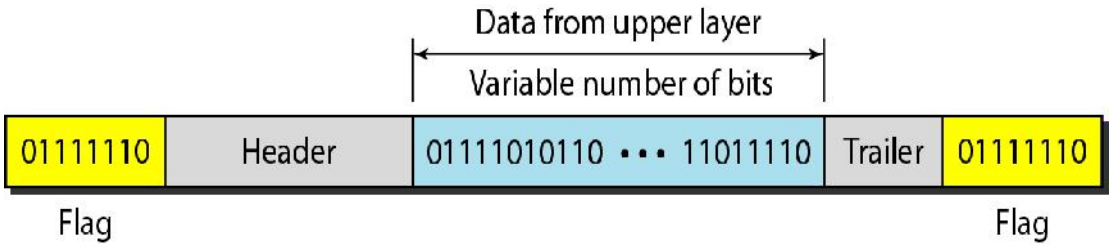


Fig. 3.1b Bit-oriented protocol frame

The most important function of a data link layer is LINE DISCIPLINE, FLOW CONTROL and ERROR CONTROL

3.1.2 LINE DISCIPLINE

Whatever the system, no device in it should be allowed to transmit until the device has the evidence that intended receiver is able to receive and is prepared to accept the transmission. What if the receiving device does not expect a transmission, is busy, or is out of commission? With no way to determine the status of the intended receiver, the transmitting device may waste its time sending data to a nonfunctioning receiver or may interfere with signals already on the link. The line discipline functions of the data link layer oversee the establishment of links and the right of a particular device to transmit at a given time.

Line discipline can be done in two ways: enquiry/acknowledgment (ENQ/ACK) and poll/select. The first method is used in peer-to-peer communication; the second method is used in primary-secondary communication.

i. Enquiry / Acknowledgement:

The initiator first transmits a frame called an enquiry (ENQ) asking if the receiver is available to receive data. The receiver must answer either with an acknowledge (ACK) frame if it is ready to receive, or with a negative acknowledge (NAK) frame if it is not. By requiring a response even if the answer is negative ENQ/ACK lets the initiator know that this enquiry was in fact received even if the receiver is currently unable to accept a transmission. If neither an ACK nor a NAK is received within a specified time limit, the initiator assumes that the ENQ frame was lost in transit, disconnects and sends a replacement. An initiating system ordinarily makes three such attempts to establish a link before giving up.

If the response to the ENQ is negative and three attempts have failed, the initiator disconnects and begins the process again at another time. If the response is positive, the initiator is free to send its data. Once all of its data have been transmitted, the sending system finished with an end of transmission (EOT) frame. This process is illustrated in figure 3.2

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.

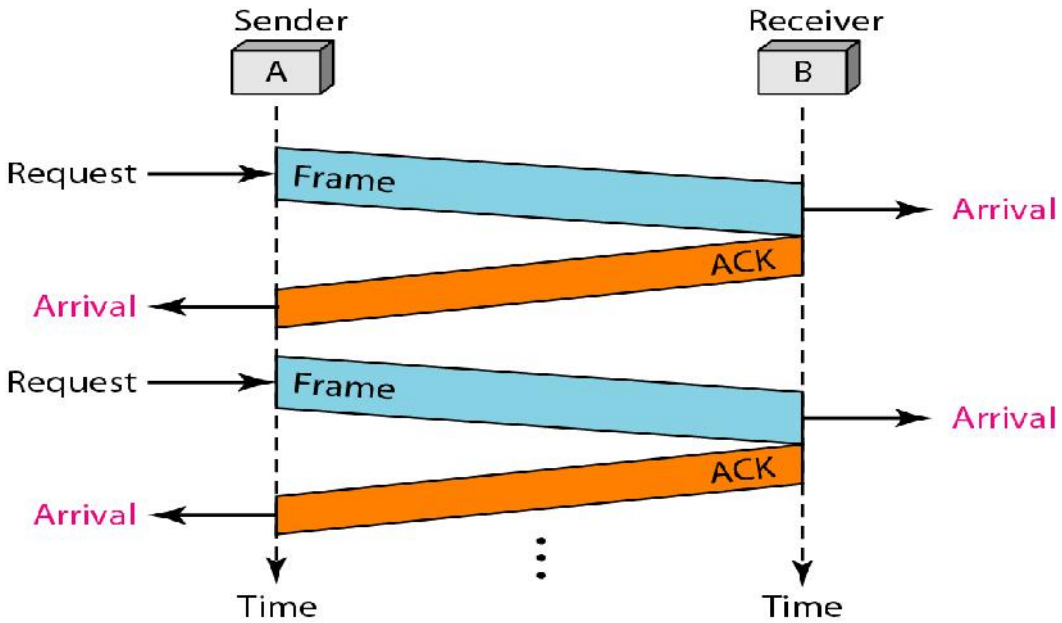


Fig. 3.2 Line discipline

ii. Poll/Select:

The poll/select method of line discipline works with topologies where one device to designate as primary and the other devices are secondary. Multipoint systems must coordinate several nodes, not just two. The question to be determined in these cases therefore is more than just, Are you ready? It is also, which of the several nodes has the right to use the channel?

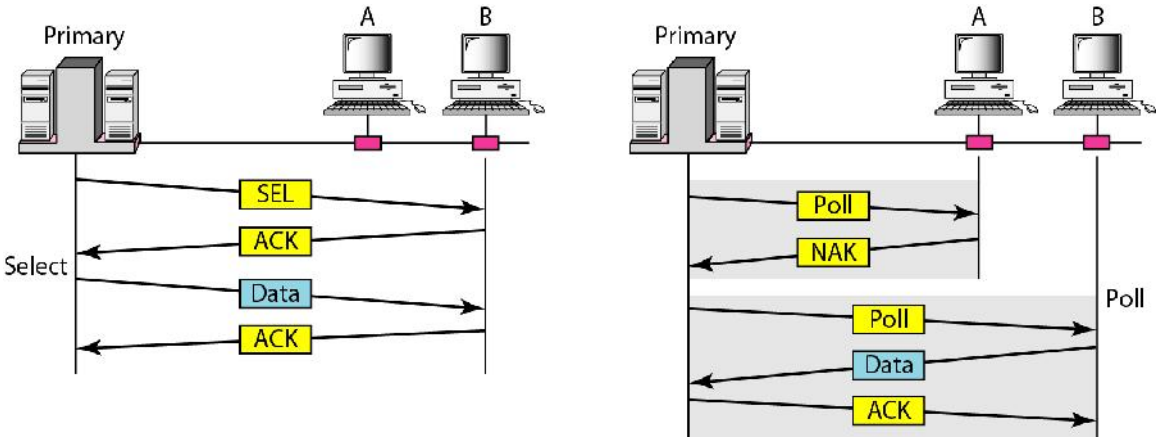


Fig. 3.3 Poll/Select protocol

How it Works: Whenever a multipoint link consists of a primary device and multiple secondary devices using a single transmission line, all exchanges must be made through the primary device even when the ultimate destination is a secondary device. (the concepts are the same for any multipoint configuration.) The primary device controls the link; the secondary allowed to use the channel at a given time). The primary, therefore, is always the initiator of a session. If the primary wants to receive data, it asks the secondaries if they have anything to send; this function is called polling. If the primary wants to send data, it tells the target secondary to get ready to receive; this function is called selecting.

Poll/select protocols identify each frame as being either to or from a specific device on the link (refer Fig. 3.3). Each secondary device has an address that differentiates it from the others. In any transmission, that address will appear in a specified portion of each frame called an address field or header depending on the protocol. If the transmission comes from the primary device, the address indicates the recipient of the data. If the transmission comes from a secondary device, the address indicates the originator of the data**.**

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

3.1.3 FLOW CONTROL

The second aspect of data link control, following line discipline, is flow control. In most protocols flow control is a set of procedures that tell the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. Two issues are at stake:

- The flow of data must not be allowed to overwhelm the receiver. Any 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. 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. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a buffer, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.
- As frames come in, they are acknowledged, either frame by frame or several frames at a time. If a frame arrives damaged, the receiver sends an error message (a NAK frame).

Flow control refers to a set of procedures used to restrict the amount of data the sender can send before waiting for acknowledgment.

Two methods have been developed to control the flow of data across communications links: **stop-and-wait** and **sliding window**.

i. Stop-and-Wait

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.

In a stop-and-wait method of flow control, the sender waits for an acknowledgment after every frame it sends (see figure 3.4).

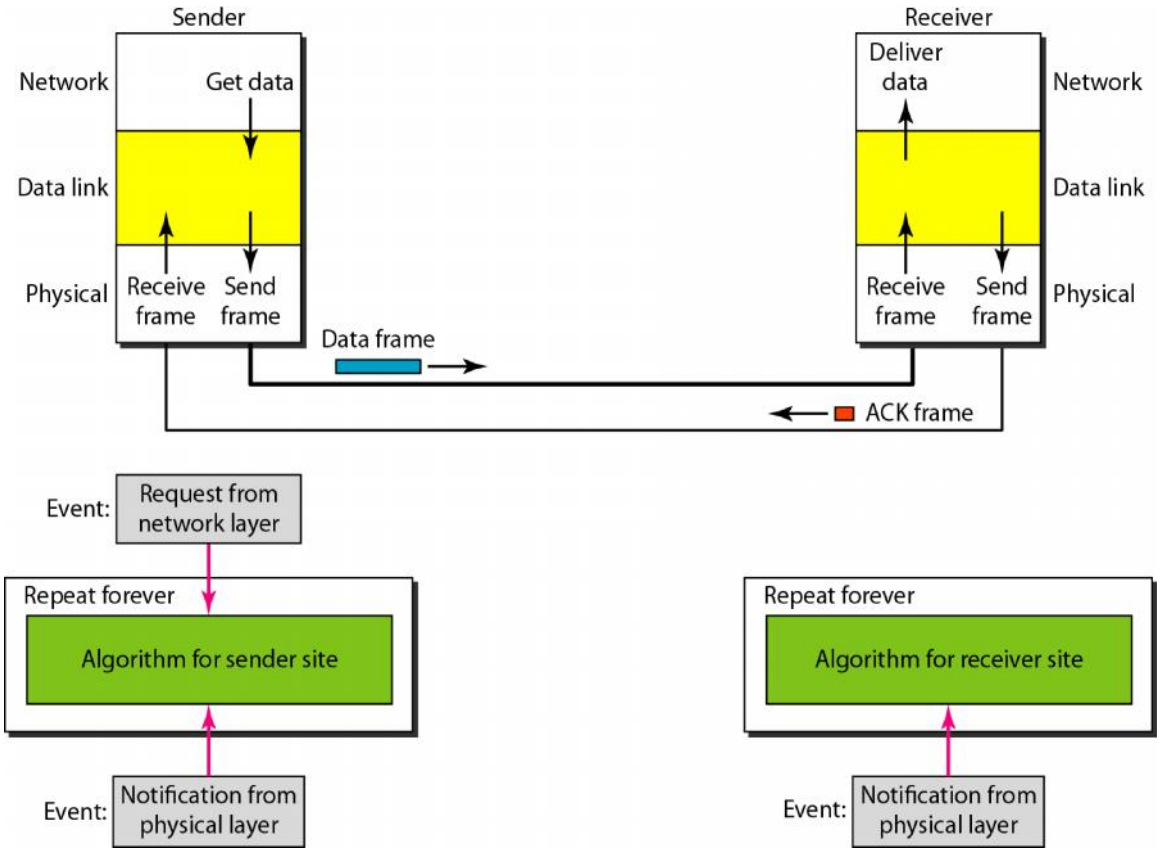


Fig 3.4 Stop-and-wait method of flow control

Only when an acknowledgment has been received is the next frame sent. This process of alternately sending and waiting repeats until the sender transmits and ends of transmission (EOT) frame. Stop-and–wait can be compared to a picky executive giving dictation: she says a work, her assistant say “OK” she says another word, her assistant says “OK”, and so on.

The advantage of stop-and-wait is simplicity: each frame is checked and acknowledged before the next frame is sent. The disadvantage is inefficiency; stop-and-wait is slow. Each frame must travel all the way to the receiver and an acknowledgment must travel all the way back before the next frame can be sent. In other words, each frame is alone on the line. Each frame sent and received uses the entire time needed to traverse the link. If the distance between devices is long, the time spent waiting for ACKs between each frame can add significantly to the total transmission time.

ii. Sliding Window

In the sliding window method of flow control, the sender can transmit several frames before needing an acknowledgment. Frames can be sent one right after another, meaning that the link can carry several frames at once and its capacity can be used efficiently. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.’

3.1.4 ERROR DETECTION & CORRECTION

Data can be corrupted during transmission. Some applications require that errors be detected and corrected.

Let us first discuss some issues related, directly or indirectly, to error detection and correction.

- In a single-bit error, only 1 bit in the data unit has changed as shown in fig 3.5a.

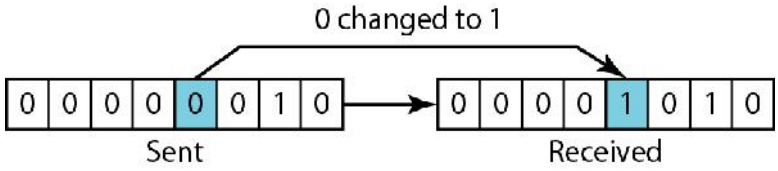


Fig 3.5a single bit error

- A burst error as shown in fig 3.5b means, that 2 or more bits in the data unit have changed.

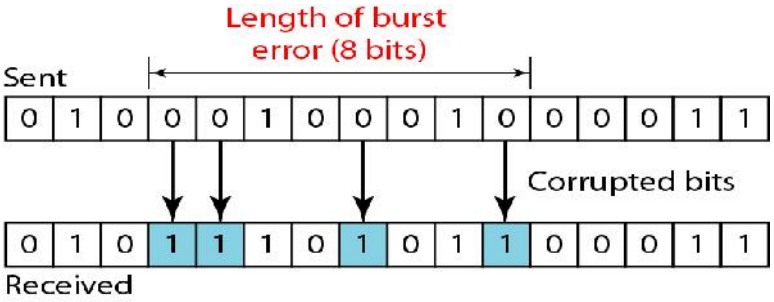


Fig 3.5b burst error

To detect or correct errors, we need to send extra (redundant) bits with data as shown in fig 3.6 below.

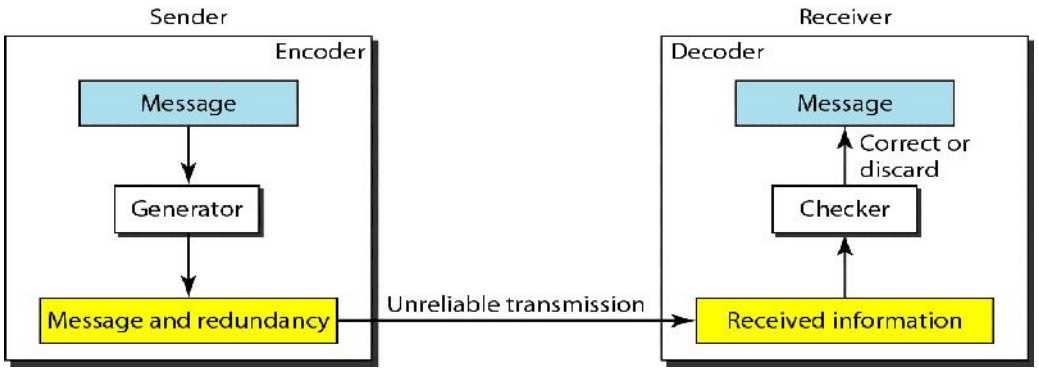


Fig. 3.6 sending redundant bits with data

In block coding, we divide our message into blocks, each of k bits, called data words. We add r redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called code words as shown in fig 3.7 below.

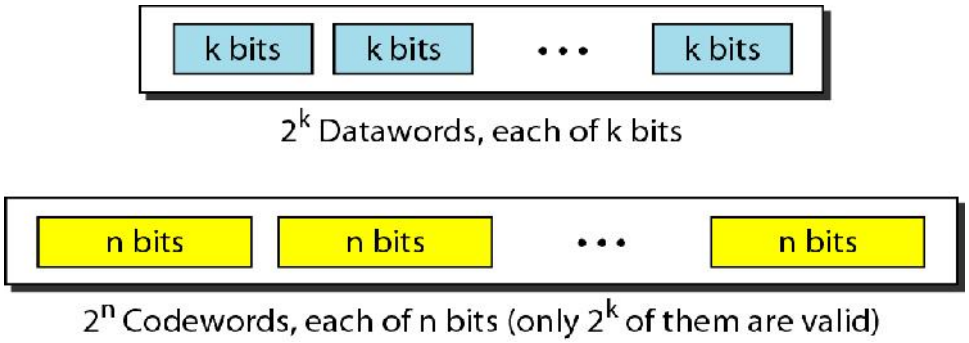


Fig 3.7 block coding (code words)

The 4b/5b block coding 4 is a good example of this type of coding. In this coding scheme, k = 4 and n = 5. As we have 2^k = 16 data words and 2^n = 32 codeword. We see that 16 out of 32 codeword are used for message transfer and the rest are either used for other purposes or unused.

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

Assume the sender encodes the data word 01 as 011 and sends it to the receiver. Consider the following cases as shown in Table 3.1.

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

Datawords	*Codewords*
00	000
01	011
10	101
11	110

Table 3.1 code for error detection

An error-detecting code can detect only the types of errors for which it is designed; other types of errors may remain undetected. A block diagram (fig. 3.8) is shown below.

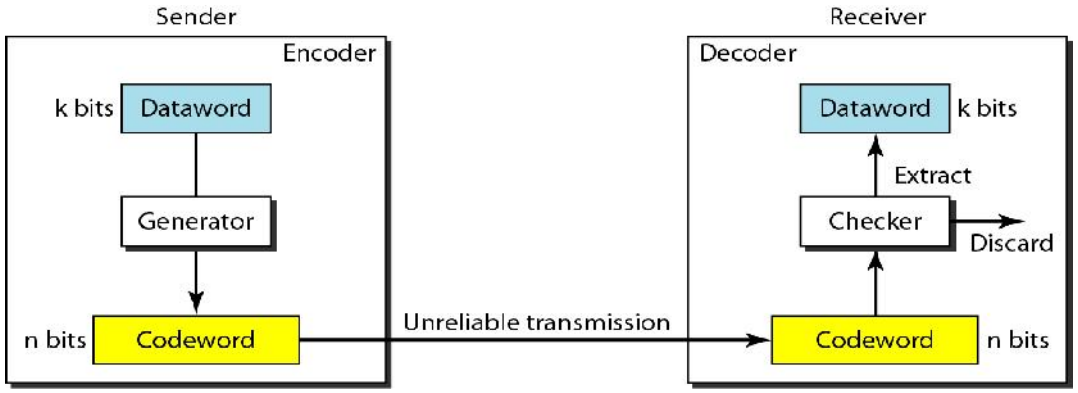


Fig.3.8 error-detecting coding

By adding more redundant bits to above Example, to see if the receiver can correct an error without knowing what was actually sent. We add 3 redundant bits to the 2-bit data word to make 5-bit code words. Table below shows the data words and code words. Assume the data word is 01. The sender creates the codeword 01011. The codeword is corrupted during transmission, and 01001 is received. First, the receiver finds that the received codeword is not in the table. This means an error has occurred. The receiver, assuming that there is only 1 bit corrupted, uses the following strategy to guess the correct data word as shown in Table 3.2 below.

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

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

3. The original codeword must be the second one in the table because this is the only one that differs from the received codeword by 1 bit. The receiver replaces 01001 with 01011 and consults the table to find the data word 01.

Dataword	*Codeword*
00	00000
01	01011
10	10101
11	11110

Table 3.2 code for error detection (adding more redundant bits)

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.

3.1.5 CYCLIC REDUNDANCY CHECK (CRC)

The divisor in a cyclic code is normally called the generator polynomial or simply the generator as shown in Table 3.3.

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

Table 3.3 Cyclic Redundancy Check (CRC) / Polynomial

The block diagram for encoder & decoder for cyclic redundant bits is shown in fig 3.9 below.

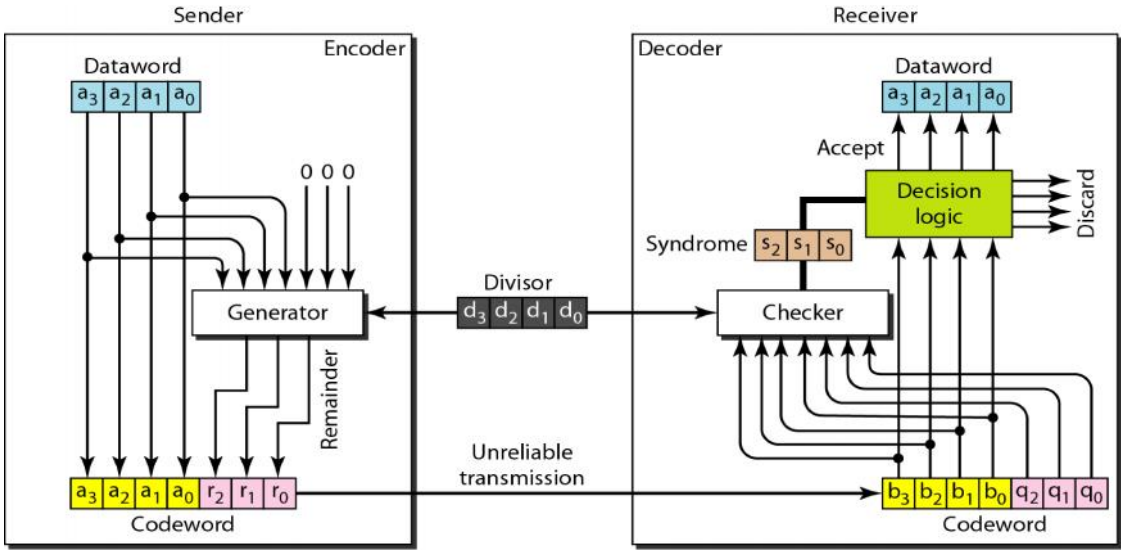


Fig. 3.9 Encoder & decoder for cyclic redundant bits.

An example for CRC is shown in fig 3.10, let a four bit data be 1001. If the divisor is a 1011 (four bit), then three 0's are augmented to data word. We get quotient and remainder. Remainder is added to data word to form the code word. This method is more popular.

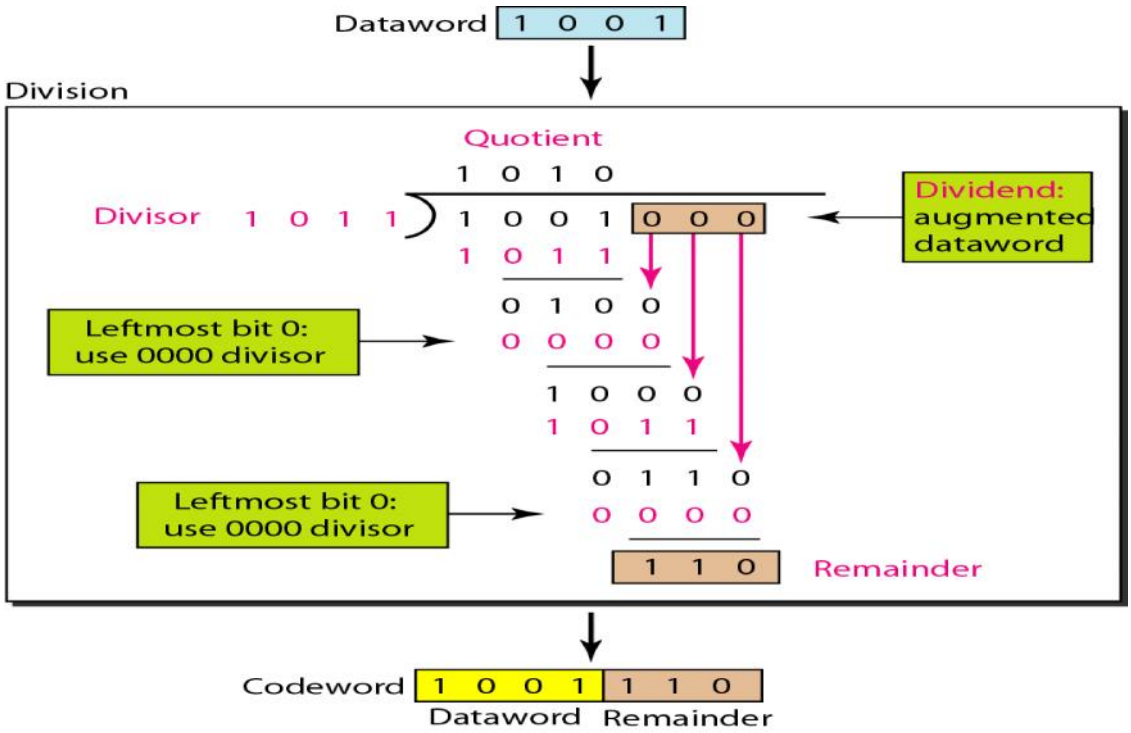


Fig. 3.10 Example for cyclic redundant check

3.1.6 CHECKSUM

The last error detection method we discuss here is called the checksum as shown in fig 3.11. The checksum is used in the Internet by several protocols although not at the data link layer. However, we briefly discuss it here to complete our discussion on error checking.

Suppose our data is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12, 0, 6, 36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise, there is an error somewhere and the data are not accepted.

We can make the job of the receiver easier if we send the negative (complement) of the sum, called the checksum. In this case, we send (7, 11, 12, 0, 6, −36). The receiver can add all the numbers received (including the checksum). If the result is 0, it assumes no error; otherwise, there is an error.

How can we represent the number 21 in one's complement arithmetic using only four bits?

The number 21 in binary is 10101 (it needs five bits). We can wrap the leftmost bit and add it to the four rightmost bits. We have (0101 + 1) = 0110 or 6.

How can we represent the number −6 in one's complement arithmetic using only four bits?

In one's complement arithmetic, the negative or complement of a number is found by inverting all bits. Positive 6 is 0110; negative 6 is 1001. If we consider only unsigned numbers, this is 9. In other words, the complement of 6 is 9. Another way to find the complement of a number in one's complement arithmetic is to subtract the number from $2^n - 1$ (16 − 1 in this case).

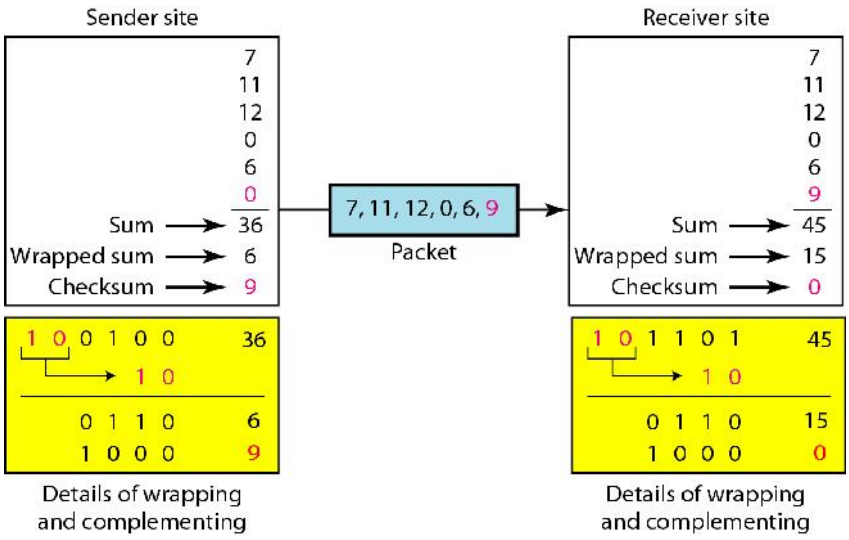


Fig. 3.11 Example for Checksum

Sender site:

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

Receiver site:

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

3.1.7 ERROR CONTROL

There are three protocols in this section that use error control. Only the first one is discussed here.

- Stop-and-Wait Automatic Repeat Request
- Go-Back-N Automatic Repeat Request
- Selective Repeat Automatic Repeat Request

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires. In Stop-and-Wait ARQ, we use sequence numbers to number the frames.

The sequence numbers are based on modulo-2 arithmetic. In Stop-and-Wait ARQ, the acknowledgment number always announces in modulo-2 arithmetic the sequence number of the next frame expected.

An example of Stop-and-Wait ARQ shown in fig 3.12. 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 0 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**.**

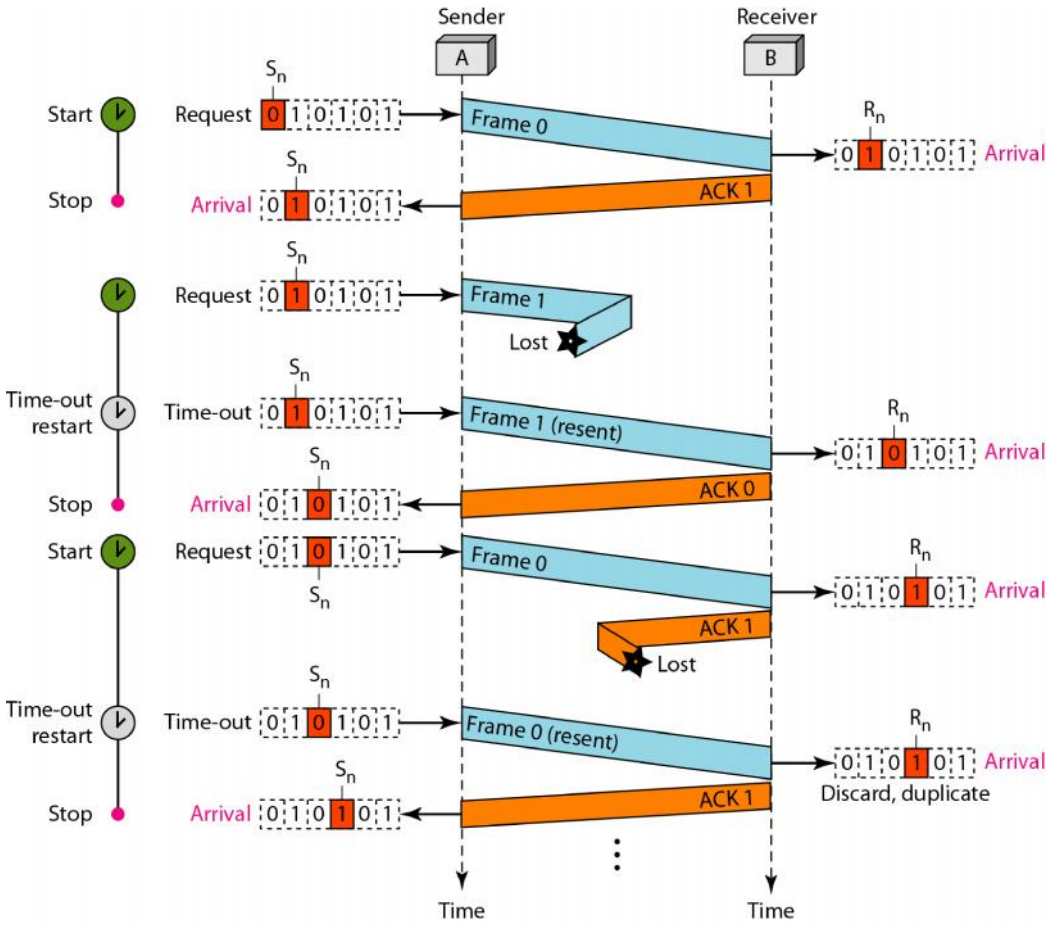


Fig. 3.12 Stop and Wait ARQ method

3.1.8 LAN PROTOCOLS:

For data transmission on LAN, protocols are used to form frames. Basically there two types of protocols are used. They are

1. Character Oriented protocols
2. Bit oriented protocols

i Character – oriented protocols

In character oriented protocols, data to be carried are 8 bit characters from a coding system such as ASCII. The header, which normally carries the source and destination address and other control information and trailer which carries error detection or error correction redundant bits are also multiples of 8 bits. To separate one frame from the next, an 8 bit flag is added at the beginning and end of the frame

Character orientated protocols are inefficient. This is because a character is used to convey meaning. As the number of meanings increase, the overhead involved also increases, as a character is used to signal the meaning.

ii Bit - oriented protocols

In bit-orientated protocols, each bit has significance. The position and value of each bit in the data stream determines its function. Thus, a single character can hold 256 different meanings in a bit orientated protocol. This reduces the information needed to convey additional information, thus increasing the efficiency of the protocol.

Examples of these types of protocols are,

- X.25 CCITT standard for packet data transmission
- HDLC high level data link control (adopted by ISO in 1970's)
- SDLC synchronous data link control (developed by IBM)
- Links between sender and receiver can be half duplex, full duplex or both. Information can be sent across the network in two different ways, traveling different routes to the receiver (*datagram*), or traveling the same route (*virtual circuit*).

Information is packaged into an envelope, called a FRAME. Each frame has a similar format

- *header* containing routing and control information
- *body* containing the actual data to be transmitted to destination and
- *tail* containing checksum data

Frames are responsible for transporting the data to the next point. Consider data that is to be sent from a source to a destination. This involves several intermediate points (called stations). The data is placed into a frame and sent to the next station, where the frame is checked for validity and if valid, the data extracted. The data is now repackaged into a new frame and sent by that station to the next station, and the process repeats till the data arrives at the destination.

When a station transmits a frame, it keeps a copy of the frame contents till the frame is acknowledged as correctly received by the next station. When a station receives a frame, it is temporarily stored in a buffer and checked for errors. If the frame has errors, the station will ask the previous station to resend the frame. Frames that are received without errors are also acknowledged, at which point the sending station can erase its copy of the frame.

A receiving station has a limited amount of buffer space to store incoming frames. When it runs out of buffer space, it signals other stations that it cannot receive any more frames.

Data is placed into frames for sending across a transmission link. The frame allows intelligent control of the transmission link, as well as supporting multiple stations, error recovery, intelligent (adaptive) routing and other important functions.

For the purposes of sending data on a link, there are two types of stations

- Primary station (issues commands)
- Secondary station (responds to commands)

a. Primary Station

The primary station is responsible for controlling the data link, initiating error recovery procedures, and handling the flow of transmitting data to and from the primary. In a conversation, there is one primary and one or more secondary stations involved.

b. Secondary Station

A secondary station responds to requests from a primary station, but may under certain modes of operation, initiate transmission of its own. An example of this is when it runs out of buffer space, at which point it sends RNR (receiver not ready) to the primary station. When the buffer space is cleared, it sends RR (receiver ready) to the primary station, informing the primary that it is now ready to receive frames again.

Because frames are numbered, it is possible for a primary station to transmit a number of frames without receiving an acknowledgement for each frame. The secondary can store the incoming frames and reply using a supervisory frame with the sequence number bits in the control field set so as to acknowledge a group of received frames.

If the secondary runs out of buffer space to store incoming Information frames, it can transmit a supervisory frame informing primary stations of its status. Primary stations will thus keep their Information frames and wait till the secondary is again able to process Information frames.

When a secondary cannot process Information frames, it must still be able to process incoming supervisory and unnumbered frames (because of status requests).

At any one time, a number of Information frames can be unacknowledged by a secondary station, and this is called the *sliding window value*, which defaults to 2, but can be negotiated when a call is first established.

3.1.9 HDLC

HDLC is the design of the ISO and has become the basis for all bit –oriented protocols in use today.

In 1975, IBM pioneered the development of bit-oriented protocols with synchronous data link control (SDLC) and lobbied the ISO to make SDLC the standard.

In 1979, the ISO answered with high-level data link control (HDLC), which was based on SDLC. Adoption of HDLC by the ISO committees led to its adoption and extension by other organizations.

The ITU-T was one of the first organizations to embrace HDLC. Since 1981, ITU-T has developed a series of protocols called link access protocols (LAPs: LAPB, LAPD, LAPM, LAPX, etc), all based on HDLC. Other protocols (such as frame relay, PPP, etc) developed by both ITU-T and ANSI also derive from HDLC, as do most LAN's access control protocols.

In short, all bit-oriented protocols in use today either derive from or are sources for HDLC. Through HDLC, therefore, we have a basis for understand the others.

All bit-oriented protocols are related to high-level data link control (HDLC) a bit-oriented protocol published by ISO.

i HDLC Modes of transmission

HDLC supports both half-duplex and full-duplex modes in point-to-point and multipoint configurations (Refer Fig. 3.13)

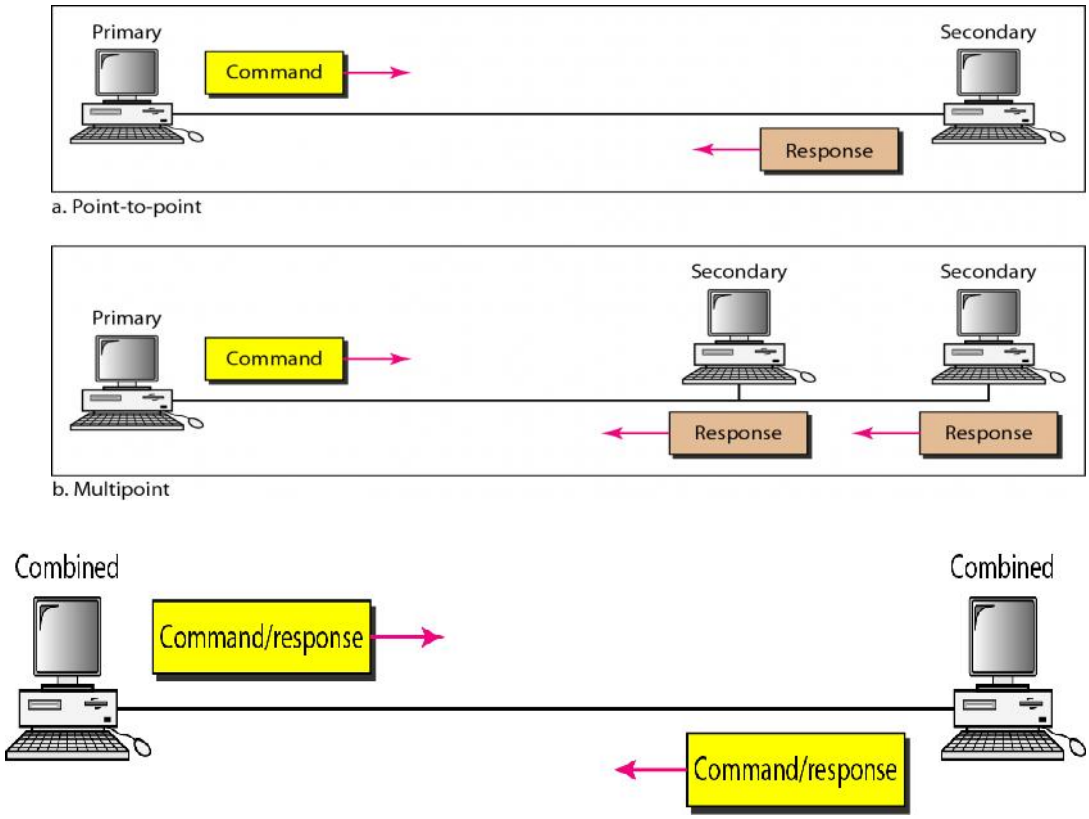


Fig 3.13 HDLC modes of transmission

ii HDLC FRAMES

There are three types of HDLC frames shown in fig 3.14

- Information frames, which contain data (the information field)
- Supervisory frames, which contain commands and responses
- Un-numbered frames, which contain commands and responses and sometimes data

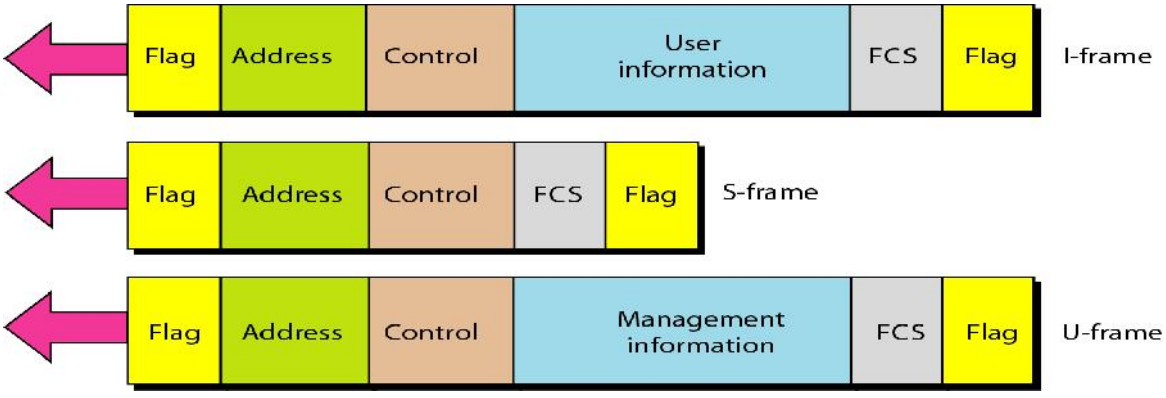


Fig. 3.14 Different HDLC frames

Information frames (I-frame)

- Are sequentially numbered
- Carry data, message acknowledgements, poll and final bits

Supervisory Frames (s-frame)

- Perform link supervisory control
- Message acknowledgements
- Retransmit requests
- Signal temporary hold on receipt on I frames (if secondary is busy)

Unnumbered Frames (U-frame)

- Provide flexible format for additional link control
- Do not have sequence numbers

iii Fields of HDLC frames

Data is packaged into frames to be sent across the HDLC link. Frames are a transport mechanism; their sole purpose is to transport the data across one link, not end to end. As the frame arrives at the other end of the link, it is checked to errors, and if it's okay, the data is stripped out of the frame, a new frame generated for it, the data inserted into the new frame, and then transmitted on the next link and so on until the data reaches its destination. The various fields of a frame are shown in table 3.4

Flag	Address	Control	Information	FCS	(Optional Flag)
8 bits	8 bits	8 or 16 bits	Variable length, 0 or more bits in multiples of 8	16 bits	8 bits

Table 3.4 fields of HDLC frame

Flag: Each frame begins and ends with a special 8 bit sequence, 7E hexadecimal (binary 01111110). The end flag can also be the start flag of the next frame.

Address Field: In command frames, this contains the address of the secondary (destination) station. In response frames (a reply to a primary station), the address specifies the secondary station sending the response.

Control Field: This field holds commands and responses. Examples are sequence numbers (frames are numbered to ensure delivery), and poll (must reply) and final (this is the last frame) bits.

Information Field: This field contains the data. It can contain any sequence of bits. It normal practice it is a multiple of 8 bits.

Frame Check Sequence Field: This field contains a 32 bit Cyclic Redundancy Check (CRC) which covers the A, C and I fields.

iv Control field format of HDLC frame.

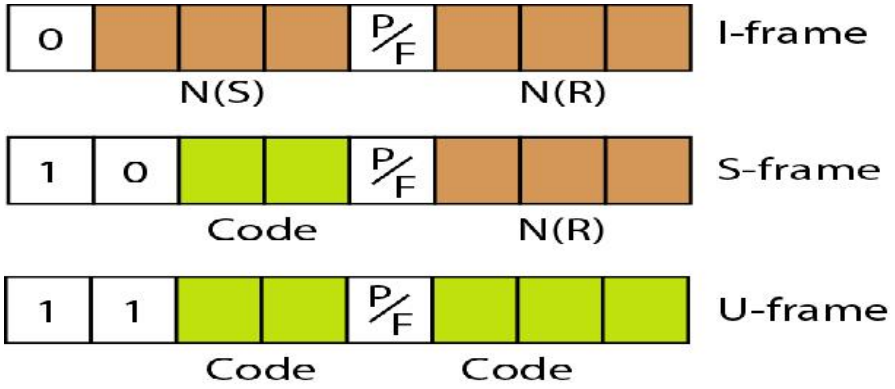


Fig. 3.15 Control field format for different HDLC frames

v. HDLC link Configurations

Link configurations can be categorized as being either:

- *Unbalanced*, which consists of one primary terminal, and one or more secondary terminals.
- *Balanced*, which consists of two peer terminals.

The three link configurations are:

Normal Response Mode (NRM) is an unbalanced configuration in which only the primary terminal may initiate data transfer. The secondary terminal transmits data only in response to commands from the primary terminal. The primary terminal polls the secondary terminal(s) to determine whether they have data to transmit, and then selects one to transmit.

Asynchronous Response Mode (ARM) is an unbalanced configuration in which secondary terminals may transmit without permission from the primary terminal. However, the primary terminal still retains responsibility for line initialization, error recovery, and logical disconnect.

Asynchronous Balanced Mode (ABM) is a balanced configuration in which either station may initiate the transmission.

3.1.10 X.25

It is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication. An X.25 WAN consists of packet-switching exchange (PSE) nodes as the networking hardware, and leased lines, Plain old telephone service connections or ISDN connections as physical links. X.25 is a family of protocols that was used especially during the 1980s by telecommunications companies and in financial transaction systems such as automated teller machines. X.25 was originally defined by the ITU-T

X.25 is today to a large extent replaced by less complex protocols, especially the Internet protocol (IP) although some telephone operators offer X.25-based communication via the signaling (*D*) channel of ISDN lines.

X.25 is one of the oldest packet-switched services available. It was developed before the Model. The protocol suite is designed as three conceptual layers, which correspond closely to the lower three layers of the seven-layer OSI model. It also supports functionality not found in the OSI Network Layer.

X.25 was developed in the era of dumb terminals connecting to host computers, although it also can be used for communications between computers. Instead of dialing directly “into” the host computer — which would require the host to have its own pool of modems and phone lines, and require non-local callers to make long-distance calls — the host could have an X.25 connection to a network service provider. Now dumb-terminal users could dial into the network’s local “PAD” (Packet Assembly/Disassembly facility), a gateway device connecting modems and serial lines to the X.25 link as defined by the X.29 and X.3 standards.

Having connected to the PAD, the dumb-terminal user tells the PAD which host to connect to, by giving a phone-number-like address in the X.121 address format (or by giving a host name, if the service provider allows for names that map to X.121 addresses). The PAD then places an X.25 call to the host, establishing a virtual call. Note that X.25 provides for virtual calls, so *appears* to be a circuit switched network, even though in fact the data itself is packet switched internally, similar to the way TCP provides connections even though the underlying data is packet switched. Two X.25 hosts could, of course, call one another directly; no PAD is involved in this case. In

theory, it doesn't matter whether the X.25 caller and X.25 destination are both connected to the same carrier, but in practice it was not always possible to make calls from one carrier to another.

For the purpose of flow-control, a sliding window protocol is used with the default window size of 2. The acknowledgements may have either local or end to end significance. A D bit (Data Delivery bit) in each data packet indicates if the sender requires end to end acknowledgement. When D=1, it means that the acknowledgement has end to end significance and must take place only after the remote DTE has acknowledged receipt of the data. When D=0, the network is permitted (but not required) to acknowledge before the remote DTE has acknowledged or even received the data.

3.2 MEDIA ACCESS

Data link layer divided into two functionality-oriented sub layers as shown in fig 3.16

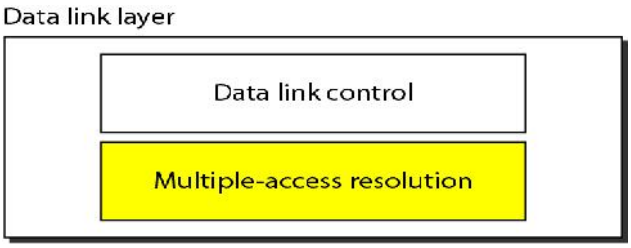


Fig. 3.16 sub layers of data link layer

Classification of multiple-access protocols is shown in fig 3.17

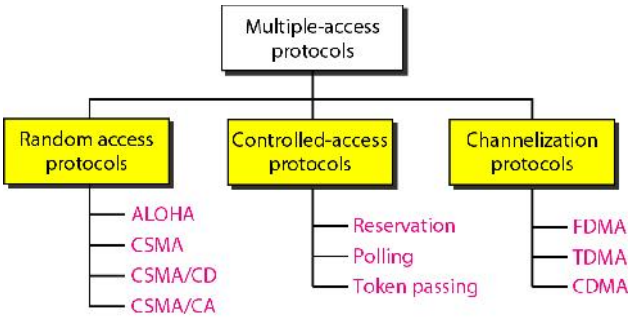


Fig. 3.17 classification of multiple-access protocol

In random access methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

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.

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.

3.2.1 MAC - Medium Access Control

The IEEE 802.3 Medium Access Control layer as shown in fig 3.18 is physically located in the firmware (ROM) of the Network Interface Card. It is the link between the Data Link Layer and the Physical Layer of the OSI model and logically resides in the lower portion of the Data Link Layer. There is only 1 MAC layer for all IEEE 802.3 versions: 802.3, 802.3a, 802.3b, 802.3i, etc.

OSI Model	IEEE				
Data Link Layer	802.2 LLC				
	802.3 MAC – CSMA/CD				
Physical Layer	802.3 10Base5 Thick Coax	802.3a 10Base2 Thin Coax	802.3b 10Broad 36 Braodband	802.3e 1Base5 StarLAN	802.3i 10BaseT Twisted Pair

Fig. 3.18 IEEE 802.3 MAC layer

The IEEE 802.3 Medium Access Control uses CSMA/CD (Carrier Sense Multiple Access/Collision Detect) to determine Bus Arbitration. The MAC layer is concerned with the order of the bits and converting the Datagram from the Network Layer into Packets/Frames as shown in fig 3.19.

Preamble	Start Frame Delimiter	Destination Address	Source Address	Length	Information Field	Frame Check Sequence

Fig 3.19 MAC layer frame format

Preamble:

The Preamble is used to synchronize the receiving station's clock. It consists of 7 bytes of 10101010.

Start Frame Delimiter (SFD)

The Start Frame Delimiter indicates the start of the frame. It consists of 1 byte of 10101011. It is an identical bit pattern to the preamble except for the last bit.

The Destination Address (DA)

Indicates the destination (receiving station) of the frame. It can be 2 or 6 octets long (16 or 48 bits), usually it is 6 octets (the 2 octet version is used for compatibility with the original Ethernet frame from XNS and is considered obsolete). The DA field as shown in fig 3.20 consists of

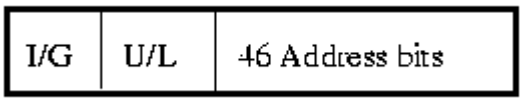


Fig 3.20 DA Field

I/G:

Stands for Individual/Group. It indicates whether the destination is for an individual or for a multicast broadcast.

It is one bit long:

0 = Individual 1 = Group

A multicast broadcast can be for everyone or for a group. For a multicast broadcast to all stations, the Destination Address = FFFFFFFFFFFFh (h - hexadecimal notation). To multicast to a specific group, the Network Administrator must assign unique addresses to each station.

U/L:

Stands for Universal/Local. It allows for unique addresses. It is used to indicate whether a local naming convention is used - administered by the Network Administrator (not recommended - incredible amount of work) or the burnt-in ROM address is used (recommended).

46 Bit Address:

46 bits address indicating the destination NIC cards address burnt into the firmware (ROM) of the card or the unique name assigned to the card during the card's initialization by the Network Administrator.

Source Address (SA)

The Source Address indicates the source or transmitting station of the frame. It is identical in format to the Destination Address but always has the I/G bit = 0 (Individual/Group Bit = Individual)

Length (L)

The Length field indicates the Length of the Information Field. It allows for variable length frames. The minimum Information Field size is 46 octets and the maximum size is 1500 octets. When the Information Field size is less than 46 octets, the Pad field is used. Due to the 802.3 MAC Frame having a Length field, there is no End Delimiter in the MAC Frame. The Length of the field is known and the receiving station counts the number of octets.

Information Field (Data)

The Information Field contains the Data from the next upper layer: Logical Link Control Layer. It is commonly referred to as the LLC Data. The minimum Information Field size is 46 octets and the maximum size is 1500 octets.

Pad

The Pad is used to add octets to bring the Information Field up to the minimum size of 46 octets if the Info Field is less than the minimum.

Frame Check Sequence (FCS)

The Frame Check Sequence is used for error-checking at the bit level. It is based on 32 bit CRC (Cyclic Redundancy Checking) and consists of 4 octets (4 x 8 = 32 bits). The FCS is calculated according to the contents of the DA, SA, L, Data and Pad fields.

Total Length of a MAC Frame is shown in table 3.5

	Min Size (octets)	**Max. Size (octets)**
Preamble	7	7
Start Frame Delimiter	1	1
Destination Address	6	6
Source Address	6	6
Length	2	2
Information Field	46	1500
Frame Check Sequence	4	4
TOTAL:	**72**	**1526 Octets**

Table 3.5 MAC frame length

MAC Frame structure is shown in fig 3.21

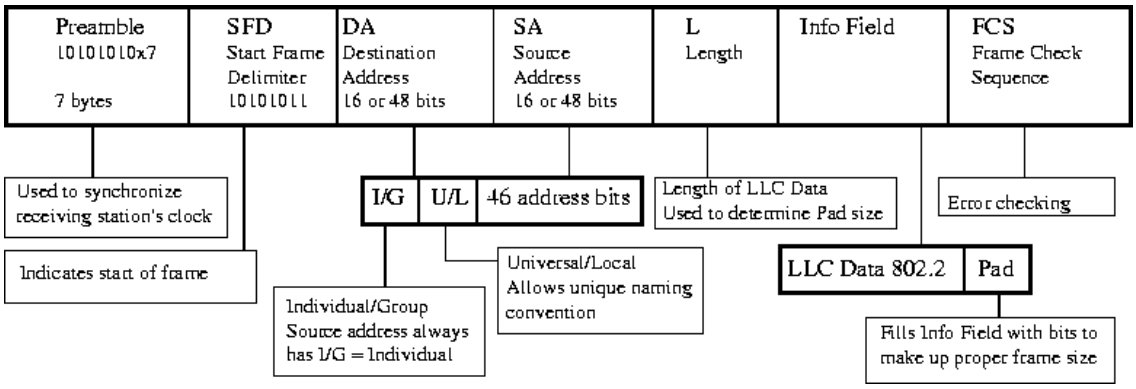


Fig 3.21 MAC frame structure

3.2.2 CSMA/CD (Carrier Sense Multiple Access/ Collision Detect)

Bus arbitration is performed on all versions of Ethernet using the CSMA/CD (Carrier Sense Multiple Access/ Collision Detect) protocol. Bus arbitration is another way of saying how to control who is allowed to talk on the (medium) and when. Put simply, it is used to determine whose turn it is to talk.

In CSMA/CD, all stations, on the same segment of cable, sense for the carrier signal. If the carrier is sensed, then it is treated that the segment of cable NOT free for communication.

In the absence of carrier, it is treated that the segment of cable is free for communication. This principle of working is called the Carrier Sense portion of CSMA/CD. Sender has to keep trying to access the media by way of sensing the presence/absence of carrier

All stations share the same segment of cable and can talk on it similar to a party line. This is the Multiple Access portion of CSMA/CD.

If 2 stations attempt to talk at the same time, a collision is detected and both stations back off for a random amount of time and then try again.

3.2.3 CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance)

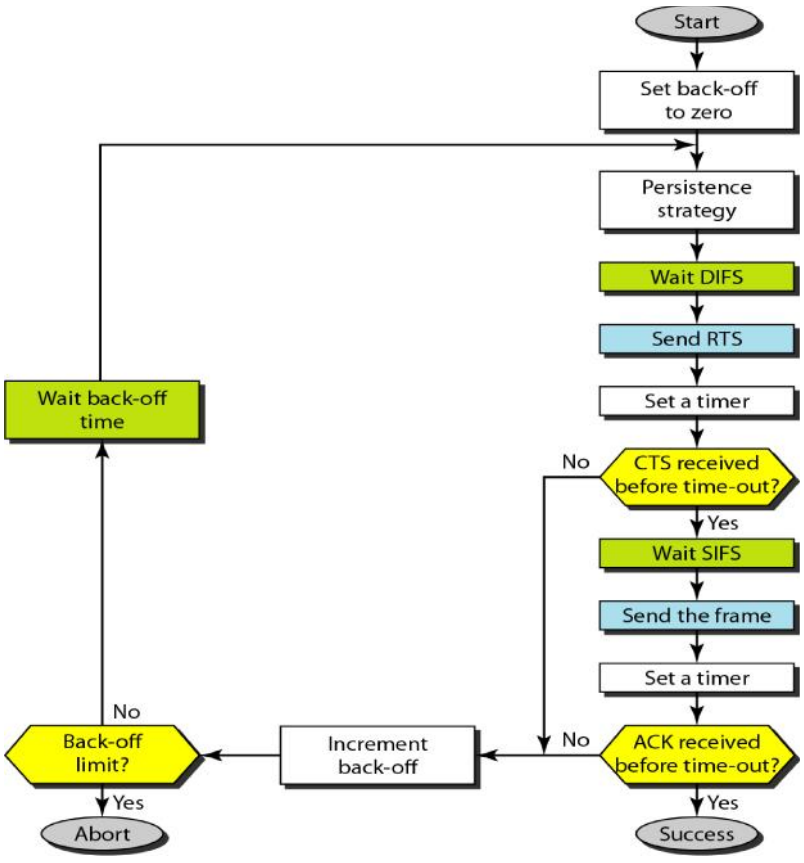


Fig 3.22 CSMA/CA flowchart

CSMA/CA stands for: **Carrier Sense Multiple Access** With **Collision Avoidance**. As per the CSMA/CA flow chart shown in fig 3.22, a station wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel. If the channel is sensed "idle" then the station is permitted to transmit. If the channel is sensed as "busy" the station has to defer its transmission. This is the essence of both CSMA/CA and CSMA/CD. In CSMA/CA (Local Talk), once the channel is clear, a station sends a signal telling all other stations not to transmit, and then sends its packet.

Collision avoidance is used to improve the performance of **CSMA** by attempting to be less "greedy" on the channel. If the channel is sensed busy before transmission then the transmission is deferred for a "random" interval. This reduces the probability of collisions on the channel.

CSMA/CA is used where CSMA/CD cannot be implemented due to the nature of the channel. CSMA/CA is used in 802.11 based wireless LANs and it is not possible to listen while sending, therefore collision detection is not possible.

3.3 ETHERNET

IEEE802.3 supports a LAN standard originally developed by Xerox and later extended by a joint venture between Digital Equipment Corporation, Intel Corporation and Xerox. This was called Ethernet. The evolution of Ethernet is in fig 3.23.

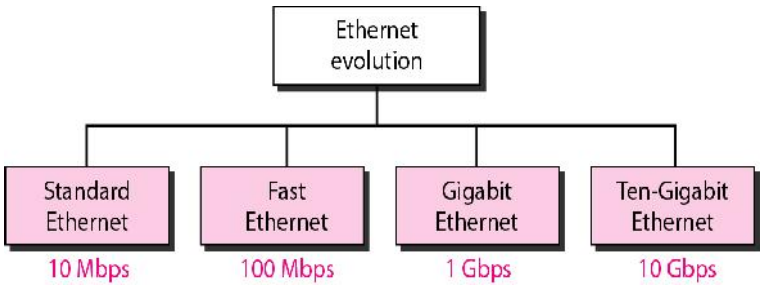


Fig 3.23 Ethernet evolution

IEEE divides the standard Ethernet implementation into four different standards as shown in fig 3.24: 10Base5, 10Base2, 10Base-T and 10Base-F. The first number (10) indicates data rate in MBPS. The last number or letter (5, 2, T and F) indicates maximum cable length or the type of cable. However, the maximum cable length restriction can be changed using networking devices such as repeaters or bridges.

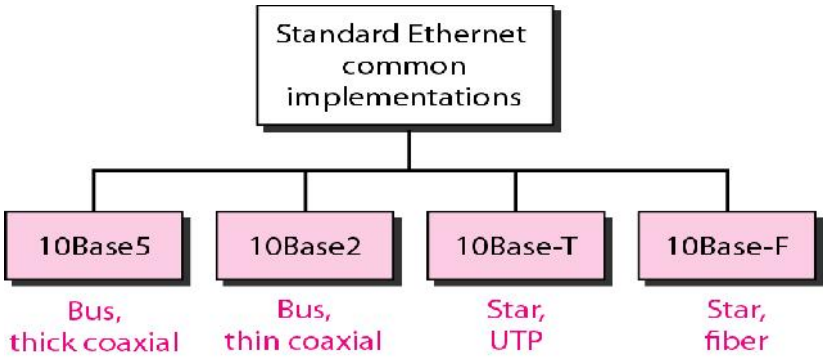
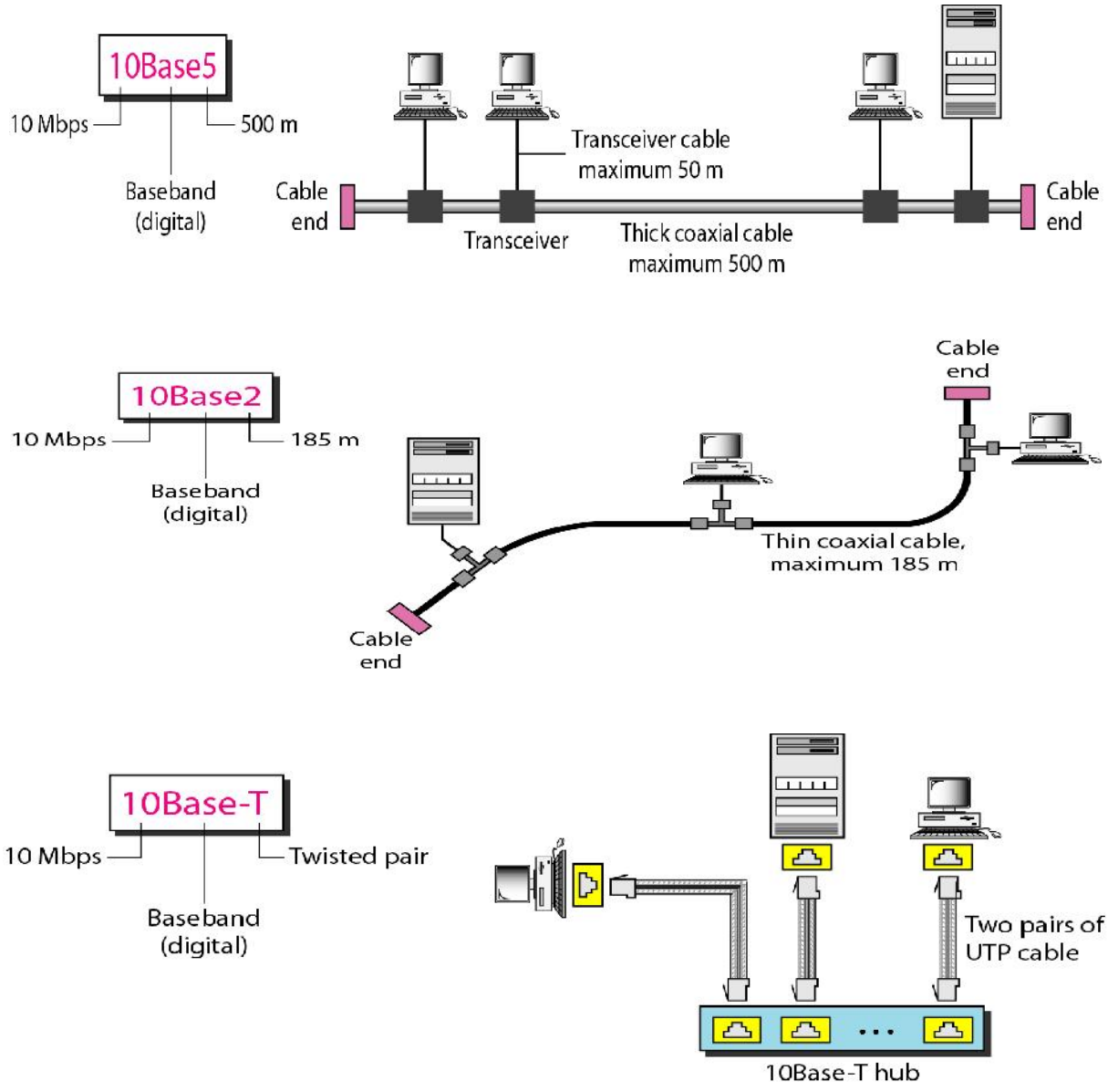


Fig 3.24 implementation of Ethernet

The backbone of wired Ethernet is coaxial, UTP, fiber in 10Base5, 10Base-T, 10 Base- F respectively. The diagram of each type of backbone is shown in fig 3.25 below.



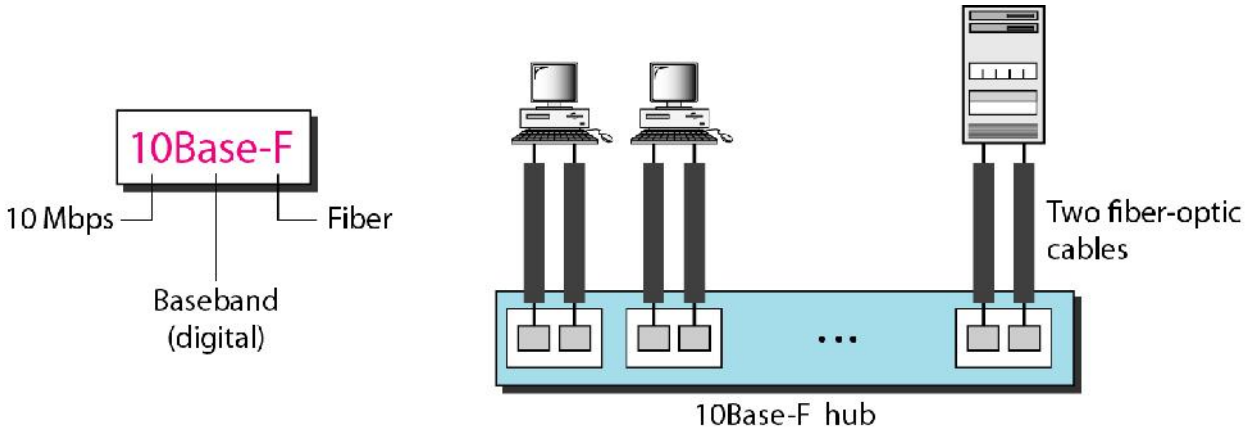


Fig. 3.25 Ethernet using different transmission media

Electrical Specification for Ethernet

Signaling

The baseband systems use Manchester digital encoding.

Data Rate

Ethernet LANs can support data rates between 1 and 100 Mbps.

Frame Format

IEEE 802.3 specifies one type of frame containing seven fields: preamble, SFD, DA, SA, length/type of PDU, 802.3 frame, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers. The format of the MAC frame in CSMA/CD.

Preamble: The first field of the 802.3 frame contains seven bytes (56bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its input timing. The pattern 1010101 provides only a alert and a timing pulse; it can be too easily aliased to be useful in indicating the beginning of the data stream. HDLC combined the alert, timing and start synchronization into a single field; the flag, IEEE 802.3 divides these three functions between the preamble and the second field, the start frame delimiter (SFD).

Start frame delimiter (SFD): The second field (one byte 10101011) of the 802.3 frame signals the beginning of the frame. The SFD tells the receiver that everything that follows is data, starting with the addresses.

Destination address (DA): The DA field is allotted six bytes and contains the physical address of the packet's next destination. A system's physical address is a bit pattern encoded on its network interface card (NIC). Each NIC has a unique address that distinguishes it from any other NIC. If the packet must cross from one LAN to another to reach its destination, the DA field contains the physical address of the router connecting the current LAN to the next one. When the packet reaches the target network, the DA field contains the physical address of the destination device.

Source address (SA): The SA field is also allotted six bytes and contains the physical address of the last device to forward the packet. That device can be the sending station or the most recent router to receive and forward the packet.

Length/type of PDU: These next two bytes indicate the number of bytes in the coming PDU. If the length of the PDU is fixed, this field can be used to indicate type, or as a base for other protocols. For exampl3e, Novell and the Internet use it to identify the network layer protocol that is using the PDU.

802.3 frame PDU: This field of the 802.3 frame contains the entire 802.3 frame as a modular, removable unit. The PDU can be anywhere from 46 to 1500 bytes long, depending on the type of frame and the length of the information field. The PDU is generated by the upper (LLC) sub layer, and then linked to the 802.3 frame.

CRC: The last field in the 802.3 frame contains the error detection information, in this case a CR C-32.

3.3.1 IEEE 802.3 defines 5 media types of IEEE 802.3 Ethernet Types:

IEEE Std	Name	Cabling	Transfer rate	Methodology	Distance limit
IEEE 802.3	10Base5	Thick Coax	10 Mbps	Baseband	500m
IEEE 802.3a	10Base2	Thin Coax	10 Mbps	Baseband	185m
IEEE803b	10Broad36	Broadband	10 Mbps	Broadband	3600m
IEEE802.3e	1Base5	Star LAN	1 Mbps	Baseband	500m
IEEE 802.3i	10BaseT	Cat 5 Twisted Pair	10 Mbps	Baseband	100m
IEEE 802.3u	100BaseT	Cat 5 Twisted Pair	100 Mbps Full Duplex	Baseband	100m
IEEE 802.3z	1GbaseT	Cat 5e Twisted Pair	1 Gbps Full Duplex	Baseband	100m

Table 3.6 Ethernet media types

Baseband - only a single stream of intelligence or data is transmitted. Ex. A television station broadcasts one television channel from its transmitter.

Broadband - multiple streams of intelligence or data is transmitted. Ex. A cable company broadcasts many television channels on its cable system.

IEEE 802.3 - 10Base5 (Thick Coax or thick net) was the original Ethernet configuration. Hasn't been used since the early 1990s. 10Base5 was replaced by Thin Coax .

IEEE 802.3a - 10Base2 (Thin Coax or thin net) was commonly used for new installations in the 1990s and was replaced by 10BaseT in the mid 1990s.

IEEE 802.3b - 10Broad36 is rarely used; it combined analog and digital signals together. Broadband means that a mixture of signals can be sent on the same medium. I have never seen or heard of a 10Broad36 installation.
IEEE 802.3e - Star LAN was a slow 1 Mbps standard that was used in the 1980s briefly.

IEEE 802.3i - 10BaseT (cheaper net) was commonly used to connect workstations to network hubs starting in the mid 1990s until the early 2000s. The network uses Cat5 cabling (Twisted Pair) to connect to other Hubs.

IEEE 802.3u - 100BaseT (fast Ethernet) is commonly used to connect workstations to network hubs and became common in the early 2000s. The network uses Cat5 cabling (Twisted Pair) to connect to other Hubs or switches.

IEEE 802.3z - 1000BaseT or 1GbaseT (Gigabit Ethernet) is commonly used to connect servers to high speed backbone networks through Cat5e cabling (Twisted Pair). The standard defines auto-negotiation of speed between 10, 100 and 1000 Mbit/s so the speed will fall to the maximum supported by both ends - ensuring inter-working with existing installations. Gigabit Ethernet uses all 4 pairs (8 conductors). The transmission scheme is radically different (PAM-5 amplitude modulation scheme is used) and each conductor is used for send and receive.

3.3.2 PoE (Power over Ethernet):

Power over Ethernet is a technology which allows a single cable to provide both data connection and electrical power to the devices.

It is not necessary to use two individual lines for Data & Power supply. One Ethernet line is sufficient. This technology is applicable for wide range of network products such as Access Points, Routers, IP cameras, modems, switches, embedded computers or other network products.

Power over Ethernet is defined by standard IEEE 802.3af / 15.4 W, (at the same time it is defined by new prepared standard IEEE 802.3at / 25.5 W). Power over Ethernet products using these standards contain of two individual active pieces **injector** and **splitter**. Each active piece includes an electrical circuit which ensures the function of this solution. There is guaranteed selected supply to 100 m / 328 ft at these standards.

Power over Ethernet, is a simple way of connecting the cables in order to transfer the data and power supply along the same Ethernet cable at the same time. Ethernet cable contains 8 wires. 4 wires (1, 2, 3, 6) are used for data transmission and the rest (4, 5, 7, 8) is used for supplying.

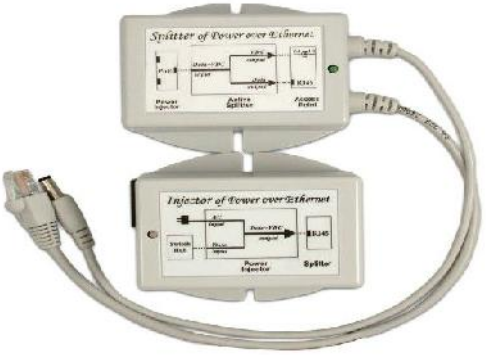


Fig 3.26 Power Over Ethernet (PoE)

3.4 CONNECTING DEVICES

The connecting devices are broadly classified into different categories based on the layer in which they operate in a network. They are REPEATERS, HUBS, BRIDGES, SWITCHES, ROUTERS & GATEWAYS. **(Routers & Gateways are discussed in chapter no. 4)**

3.4.1 REPEATERS

A repeater (or generator) is an electronic device that operates on only the physical layer of the OSI model (see figure). Signals that carry information within a network can travel a fixed distance before attenuation (weakening of the signal due to friction) or interference from noise endangers the integrity of the data. A repeater installed on a link receives the signal before it becomes too weak or corrupted, regenerates the original bit pattern and puts the refreshed copy back onto the link. In effect, the signal, with the corruption removed is transmitted a second time from a location closer to the destination.

A repeater allows us to extend only the physical length of a network. The repeater does not change the functionality of the network in any way (see figure 3.27a below).

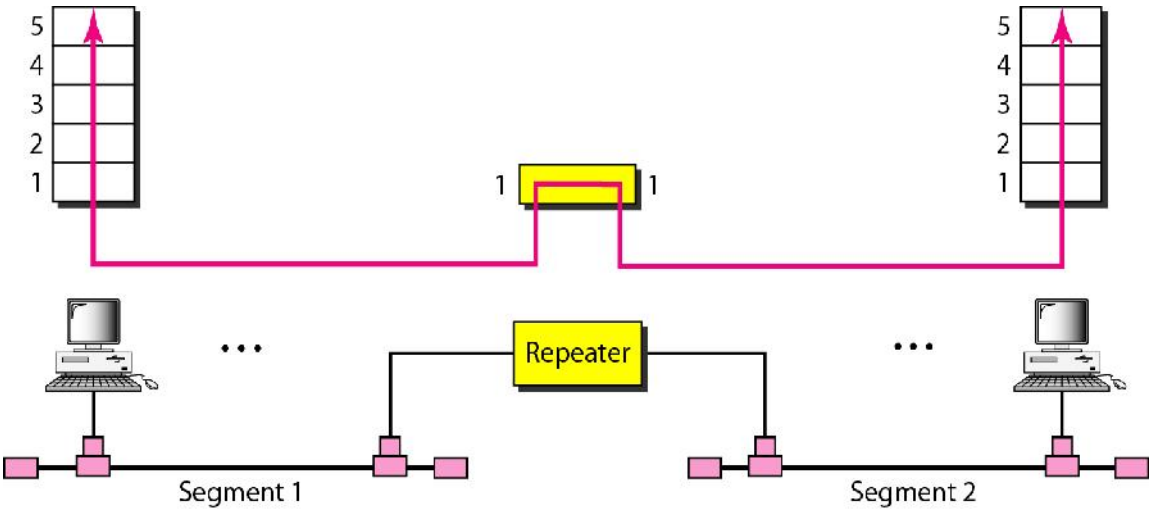


Fig 3.27a Repeater

It is tempting to compare a repeater to an amplifier, but the comparison is inaccurate. An amplifier cannot discriminate between the intended signal and noise; it amplifies equally everything fed into it. A repeater does not amplify the signal; it regenerates it as shown in fig 3.27b. When it receives a weakened or corrupted signal, it creates a copy bit for bit, at the original strength.

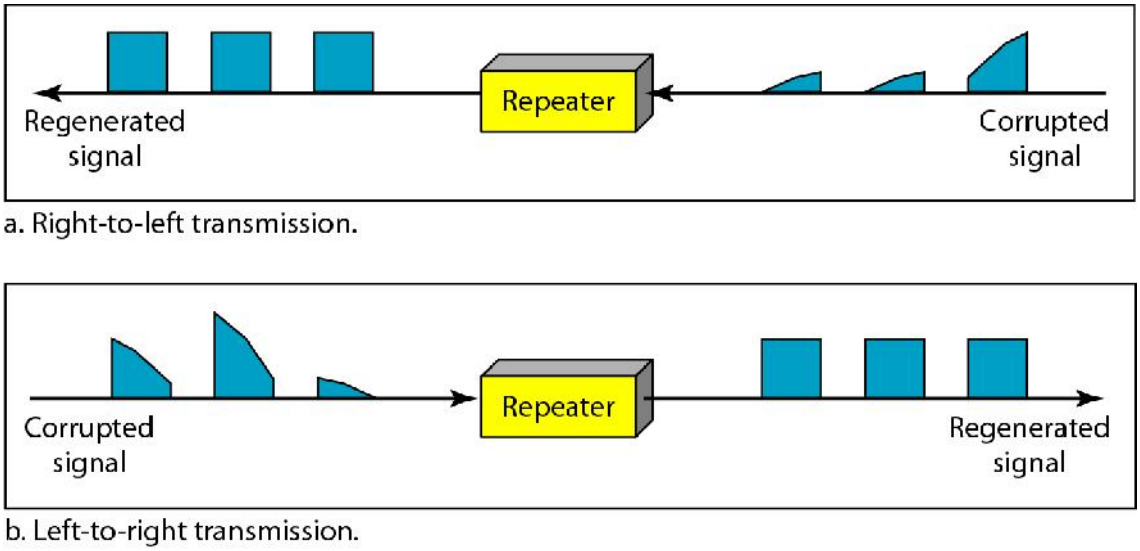


Fig 3.27b repeater as a generator

The location of a repeater on a link is vital. A repeater must be placed so that a signal reaches it before any noise changes the meaning of any of its bits. ***A repeater connects segments of a LAN.***

3.4.2 HUBS

Hubs are commonly used LAN connecting devices. They serve as the central connection points for LANs. Hubs are used on networks that use twisted-pair cabling. Ports available on the hub provide the connection points for the devices on the networks. Hub is basically un-intelligent device, it supports broadcast and hence always the bandwidth is shared among the ports. Hub works in one broadcast domain and one collision domain.

3.4.3 BRIDGES

Bridges operate in both the physical and the data link layers of the OSI model. Bridges divide a large network into smaller segments. They can also relay, frames between two originally separate segments of one type. Unlike repeaters, however bridges contain logic that allows them to keep the traffic for each segment separate. Bridges are repeaters that are smart enough to relay a frame only to the side of the segment containing the intended recipient. In this way, they filter traffic a fact that makes them useful for controlling congestion and isolating problem links. Bridges can also provide security through this partitioning of traffic.

Bridges do not modify the structure or contents of a packet in any way and therefore be used only between segments that use the same protocol.(Refer Fig.3.28a)

A bridge operates at the data link layer, giving it access to the physical addresses of all stations connected to it. When a frame enters a bridge, the bridge not only regenerates the signal but checks the address of the destination and forward the new copy only to the segment to which the address belongs. As a bridge encounters a packet, it reads the address contained in the frame and compares that address with a table of all the stations on both segments. When it finds a match, it discovers to which segment the station belongs and relays the packet only to that segment.

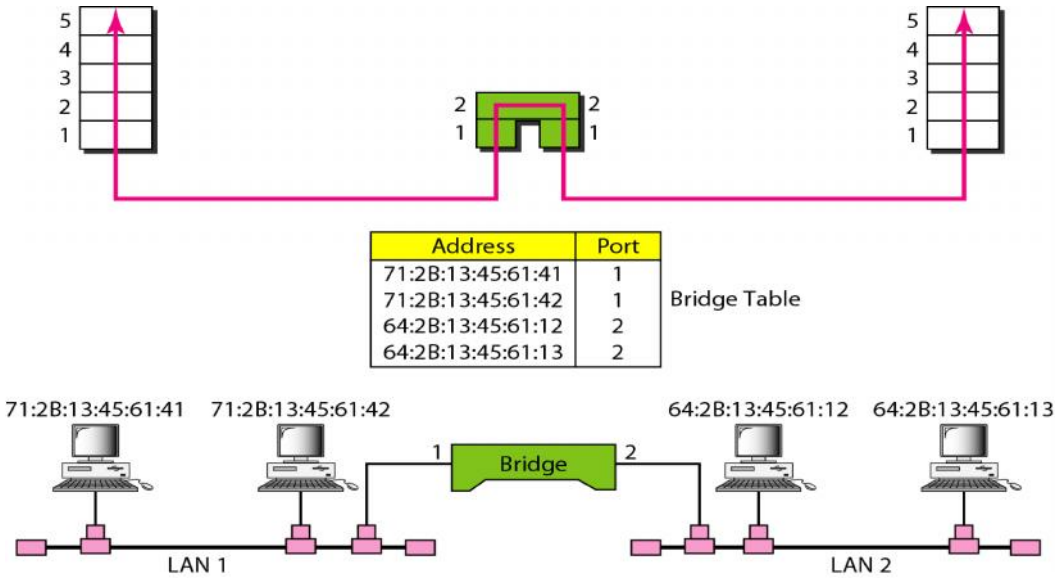


Fig 3.28a Bridge

To select between segments a bridge must have a look-up table that contains the physical addresses of every station connected to it. The table indicates to which segment each station belongs. How this table is generated and how many segments are connected by single bridge determine the type and cost of the bridge. There are three types of bridges: simple, learning and multiport. The details are not dealt here.

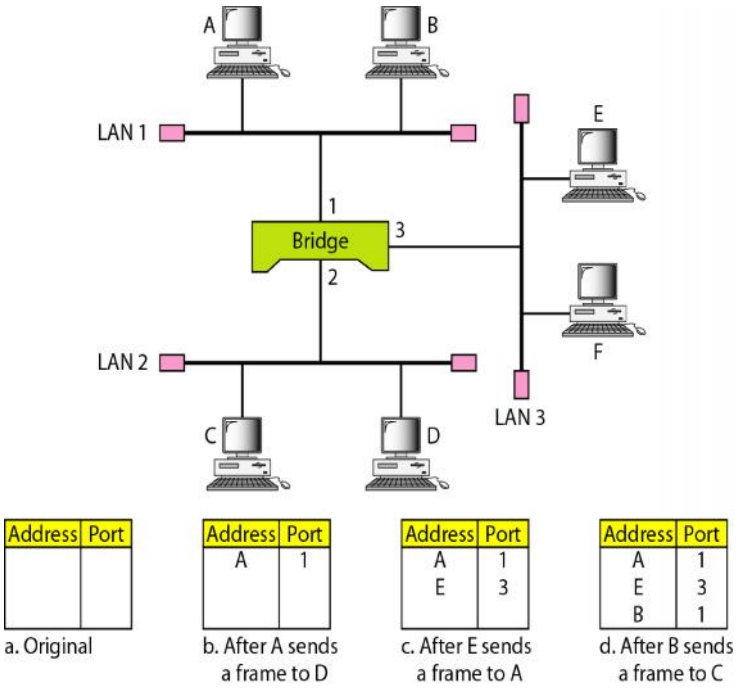


Fig 3.28b Segments joined by a bridge

The figure 3.28b shows, two segments joined by a bridge. A packet from station 'A' addressed to station 'B' arrives at the bridge. Station 'A' is on the same segment as station 'B'. Therefore the packet is blocked from crossing into the lower segment. Instead the packet is relayed to the entire upper segment and receives by station B.

3.4.4 SWITCHES

A network switch is a computer networking device that connects network segments. The network switch plays an integral part in most Ethernet LANs.

Switches may operate at one or more OSI layers, including physical, data link, network, or transport (i.e., end-to-end). A device that operates simultaneously at more than one of these layers is called a multilayer switch.

Switches provide many additional features not offered by older devices such as hubs and bridges. In particular switches provide the following benefits:

- Switch ports connected to a single device micro segment the LAN, providing dedicated bandwidth to that single device.

- Switches allow multiple simultaneous conversations between devices on different ports
- Switch ports connected to a single device support full duplex, in effect doubling the amount of bandwidth available to the device.
- Switches support rate adaptation, which means that devices that use different ethernet speeds can communicate through the switch (Hubs cannot).

Switches use Layer 2 logic, examining the Ethernet data-link header to choose how to process frames. In particular, switches make decisions to forward and filter frames, learn MAC addresses, and use STP (Spanning tree protocol) to avoid loops, as follows

Data forwarding Methods

Step 1:

Switches forward frames based on the destination address:

a) If the destination address is a broadcast, multicast or unknown destination unicast address, the switch floods the frame.

b) If the destination address is a known unicast address (a unicast address found in the MAC table):

i) If the outgoing interface listed in the MAC address table is different from the interface in which the frame was received, the switch forwards the frame to the outgoing interface.

ii) If the outgoing interface is the same as the interface in which the frame was received, the switch filters the frame, meaning that the switch simply ignores the frame and does not forward it.

Step 2:

Switches use the following logic to learn MAC address table entries:

a) For each received frame, examine the source MAC address and note the inter face from which the frame was received.

b) If they are not already in the table, add the address and interface, setting the in activity timer to 0.

c) If it is already in the table, reset the inactivity timer for the entry to 0.

Step 3:

Switches use STP to prevent loops by causing some interfaces to block, meaning that they do not send or receive frames.

General definitions for a collision domain and a broadcast domain are as follows:

- A collision domain is a set of network interface cards (NIC) for which a frame sent by one NIC could result in a collision with a frame sent by any other NIC in the same collision domain.

- A broadcast domain is a set of NICs for which a broadcast frame sent by one NIC is received by all other NICs in the same broadcast domain.

In the context of a standard 10/100 Ethernet switch, a switch operates at the data-link layer of the OSI model to create a different collision domain per switch port. If you have 4 computers A/B/C/D on 4 switch ports, then A and B can transfer data between them as well as C and D at the same time, and they will never interfere with each others' conversations. In the case of a "hub" then they would all have to share the bandwidth, run in Half duplex and there would be collisions and retransmissions. Using a switch is called micro-segmentation. It allows you to have dedicated bandwidth on point to point connections with every computer and to therefore run in Full duplex with no collisions.

In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fibre Channel, ATM and 802.11. This connectivity can be at any of the layers mentioned. While Layer 2 functionality is adequate for speed-shifting within one technology, interconnecting technologies such as Ethernet and token ring are easier at Layer 3.

Switch ports almost always default to Full duplex operation, unless there is a requirement for interoperability with devices that are strictly Half duplex. Switches" tended to use micro segmentation and Full duplex to prevent collisions among devices connected to Ethernets.

Once a switch learns the topology through a spanning tree protocol, it forwards data link layer frames using a layer 2 forwarding method. There are four forwarding methods a switch can use.

1. Store and forward: The switch buffers and, typically, performs a checksum on each frame before forwarding it on.
2. Cut through: The switch reads only up to the frame's hardware address before starting to forward it. There is no error checking with this method.
3. Fragment free: A method that attempts to retain the benefits of both "store and forward" and "cut through". Fragment free checks the first 64 bytes of the frame, where addressing information is stored. According to Ethernet specifications, collisions should be detected during the first 64 bytes of the frame, so frames that are in error because of a collision will not be forwarded. This way the frame will always reach its intended destination. Error checking of the actual data in the packet is left for the end device in Layer 3 or Layer 4 (OSI), typically a router.
4. Adaptive switching: A method of automatically switching between the other three modes.

i. Unmanaged switches

These switches have no configuration interface or options. They are plug_and_play. They are typically the least expensive switches.

ii. Managed switches

These switches have one or more methods to modify the operation of the switch. Common management methods include: a serial console or command line interface accessed via telnet or Secure Shell, an embedded Simple Network Management Protocol (SNMP) agent allowing management from a remote console or management station, or a web interface for management from a web browser. Examples of configuration changes that one can do from a managed switch include: enable features such as, set port speed, create or modify Virtual LANs (VLANs), etc. Two sub-classes of managed switches are marketed today:

- Smart (or intelligent) switches — these are managed switches with a limited set of management features. Likewise "web-managed" they provide a web interface (and usually no CLI access) and allow configuration of basic settings, such as VLANs, port-speed and duplex.
- Enterprise Managed (or fully managed) switches — These have a full set of management features, including Command Line Interface, SNMP agent, and web interface. They may have additional features to manipulate configurations, such as the ability to display, modify, backup and restore configurations. Compared with smart switches, enterprise switches have more features that can be customized or optimized, and are generally more expensive than "smart" switches. Enterprise switches are typically found in networks with larger number of switches and connections.

3.4.5 VLAN (Virtual LAN)

A **virtual LAN**, commonly known as a **VLAN**, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating

IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of **VLAN tagging** for Ethernet frames and the accompanying procedures to be used by switches in handling such frames.

Portions of the network which are *VLAN-aware* (i.e., IEEE 802.1Q conformant) can include VLAN tags. Traffic on a *VLAN-unaware* (i.e., IEEE 802.1D conformant) portion of the network will not contain VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the frame's port or the port / protocol combination, depending on whether port-based or port-and-protocol-based VLAN classification is being used. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the native (or default) VLAN.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain.

This is also useful if someone wants to create multiple Layer 3 networks on the same Layer 2 switch. For example, if a DHCP server (which will broadcast its presence) was plugged into a switch it will serve any host on that switch that was configured to use the server. By using VLANs you can easily split the network up so some hosts won't use that server and will obtain Link-local addresses.

Virtual LANs are essentially Layer 2 constructs, compared with IP subnets which are Layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN or have one subnet spread across multiple VLANs. Virtual LANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to one another and this correspondence is useful during the network design process.

By using VLANs, one can control traffic patterns and react quickly to relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.

By default all the ports of a switch are in VLAN1, hence VLAN1 is known as administrative VLAN (or) management VLAN. VLANs can be created from 2 to 1001. Fig 3.28 shows two VLANs (i.e.VLAN2 & VLAN3) in switch no.1 & no.2 are connected using the Trunk port.

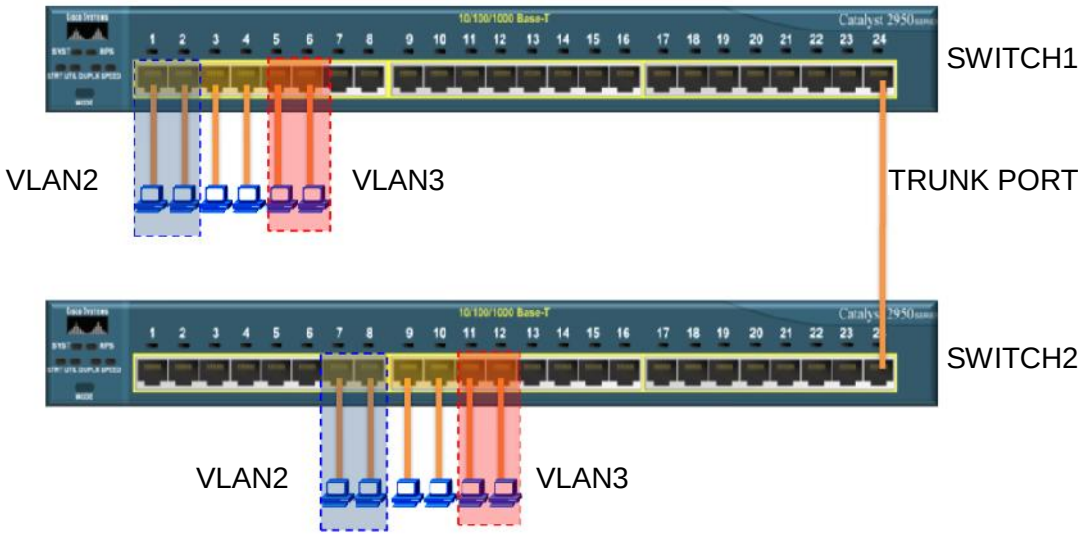


Fig 3.29 VLAN creation

Review Questions:

Subjective:

1. What are the different steps followed in Data link control? Describe flow control?
2. Discuss cyclic redundancy check (CRC) & Checksum? What for these are used?
3. What is automatic repeat request (ARR) method of error control? What are its protocols?
4. What is HDLC? Draw the frame structure and types? Mention which type of protocol it is?
5. What is Ethernet? Mention the standard that is equivalent to Ethernet? Draw the frame structure?
6. Mention how HDLC frame structure is different from Ethernet?
7. Why is Ethernet told to be scalable? How is it most suitable LAN technologies?
8. How multiple accesses are resolved over the media on data link layer? Explain CSMA / CD & CSMA / CA?

Objective:

1. HDLC is an acronym for _____.
   a) High-duplex line communication b) Half-duplex digital link combination
   c) High-level data link control d) Host double-level circuit

2. Flow control is needed to prevent _____.
   a) Overflow of the sender buffer b) Overflow of the receiver buffer
   c) Bit errors d) Collision between sender and receiver

3. When data and acknowledgment are sent on the same frame, this is called _____.
   a) Back packing b) Piggy packing c) Piggy backing d) A good idea

4. The shortest frame in HDLC protocol is usually the _____ frame.

   a) Information b) Management c) Supervisory d) None of the above

5. Which error detection method uses ones complement arithmetic?

   a) Simple parity check b) Checksum

   c) Two-dimensional parity check d) CRC

6. Which error detection method consists of just one redundant bit per data unit?

   a) Two-dimensional parity check b) CRC

   c) Simple parity check d) Checksum

7. Which error detection method involves polynomials?

   a) CRC b) Simple parity check

   c) Two-dimensional parity check d) Checksum

8. The Hamming code is a method of _____.

   a) Error detection b) Error correction

   c) Error encapsulation d) (A) and (B)

9. What is the efficiency of 4B/5B block encoding?

   a) 60 percent b) 80 percent c) 20 percent d) 40 percent

10. If an Ethernet destination address is 07-01-02-03-04-05, then this is a _____ address.

    a) Unicast b) Broadcast c) Multicast d) Any of the above

CHAPTER-4

DATA TRANSMISSION ON WAN

Introduction

*In the earlier chapters, essentials for the Data Transmission over a Physical media and over a LAN are discussed. When Data Communication Network extends from within a b****uilding to any where across the world, there comes the need for a WAN (Wide Area Network).***

WAN can be an Intranet or Internet otherwise called as Private Network or Public Network.

Functions performed by OSI Layer 3 (Network Layer) and Layer 4 (Transport Layer) are covered in brief in this chapter.

WAN is established with the help of Routers & Long distance communication links and suitable Network Layer Protocol (Ex. IP)

While data is carried over LAN in FRAMEs, WAN carries data in PACKETs

Majority of applications use, Internet Protocol (IP) and Transmission Control Protocol (TCP), together, are used for data transmission over a WAN. Therefore Routers & TCP / IP protocol suit are discussed.

WAN (Wide Area Network devices)
MPLS (Multi Protocol Label Switching)
VoIP (Voice over IP)

4.0 TCP/IP protocol

What is Internet Protocol (IP)?

Internet Protocol (IP) is a piece of software that operates at the NETWORK LAYER of the OSI MODEL.

IP provides the following:

- Unique Addresses
- Connectionless Communication
- Routing
- Data Transmission on IP

4.0.1 UNIQUE ADDRESSES

Everything connected to the Internet must have a unique numerical address. Just like, house has a unique address, so does each computer attached to the Internet. These addresses are not fixed, and can be changed when necessary. These addresses are represented in what is called 'dotted-decimal notation' which means is that there are numbers with dots in between them that look like this: 204.25.183.4.

Always remember that computers use these dotted-decimal 'IP Addresses' to communicate and never use letters or names.

4.0.2 CONNECTIONLESS COMMUNICATION

IP communication is CONNECTIONLESS, and does not bother to set up dedicated end-to-end connections for communication. Upper layer protocols such as TCP are used for setting up connections and tearing them down, managing the recovery of lost data and other errors. These protocols function at the TRANSPORT LAYER of the OSI MODEL or higher.

4.0.3 ROUTING

IP is aware when a computer's address is part of the local group of computers, or somewhere else. ROUTING is the part of IP that allows very intelligent and specialized routing devices (ROUTERS) to recognize that information is not part of the local group of machines, and needs to be forwarded to the destination. These devices are smart enough to 'figure out' how to get to destinations they aren't directly connected to. The process of forwarding the information is called *ROUTING*. ROUTING is covered in detail in ANOTHER SECTION.

4.0.4 DATA TRANSMISSION ON INTERNET PROTOCOL

1. Unicast
2. Broadcast
3. Multicast

Unicast: Unicast packets are sent from host to host. The communication is from a single host to another single host. There is one device transmitting a message destined for one receiver.

Broadcast: Broadcast is when a single device is transmitting a message to all other devices in a given address range. This broadcast could reach all hosts on the subnet, all subnets, or all hosts on all subnets. Broadcast packets have the host (and/or subnet) portion of the address set to all ones. By design, most modern *ROUTERS* will block IP broadcast traffic and restrict it to the local subnet.

Multicast: Multicast is a special protocol for use with IP. MULTICAST enables a single device to communicate with a specific set of hosts, not defined by any standard IP address and mask combination. This allows for communication that resembles a conference call. Anyone from anywhere can join the conference, and everyone at the conference hears what the speaker has to say. The speaker's message isn't broadcasted everywhere, but only to those in the conference call itself. A special set of addresses is used for MULTICAST communication.

4.1 IP ADDRESSES (INTERNET PROTOCOL ADDRESSES)

When using the INTERNET, humans use names such as *WWW.GOOGLE.COM* or *WWW.EBAY.COM*. We call those "web addresses" or "URLs" but those are names. They aren't actually addresses; they are just words that can be easily remembered by humans. The INTERNET uses its own set of addresses because computers run the Internet and computers use numbers.

COMPUTERS do their work over the INTERNET and across NETWORKS using numeric addresses. Either end systems are configured with IP addresses (the computer-server that is serving www.google.com for instance). To communicate, a connection is opened from one COMPUTER to the other computer using the IP addresses as the source and destination addresses for that communication.

A COMPUTER gets an address one of two ways, either the network administrator enters it into the COMPUTER manually, or it is learned by the COMPUTER dynamically using a protocol called DHCP. When the IP address is assigned by the NETWORK administrator manually, this is called a ´fixed´ or ´static´ IP address. If an IP address is learned by the COMPUTER automatically when the COMPUTER starts up (via DHCP), it's called a ´dynamic´ IP. DHCP of course, needs to be set up and running for our COMPUTER to learn an IP address.

IP addresses are two types

1. **IPv4 (IP version 4)**
2. **IPv6 (IP version 6)**

Till now there are only IPv4 addresses are used over the network, due to exhaustion of IPv4 address space, the world is moving towards IPv6. Introduction to IPv6 is given at the end of this chapter.

4.1.1 IPv4 Address

An IP address is a number used to identify the logical connection of a COMPUTER to a physical NETWORK, is a 32-bit BINARY address, composed of four, 8-bit numbers. IP ADDRESS is represented as four decimal numbers between 0 and 255 separated by dots; (e.g. 199.221.66.20). This is referred to as dotted-decimal notation. Anything attached to an IP NETWORK can be assigned an IP address. Addresses are always unique. Because IP addresses are software configured, it is easy to move hosts from one NETWORK to another simply by changing the IP ADDRESS or the network mask. This process is called *RENUMBERING*.

i. Network and Host Portion of an IP Address

When looking at an IP ADDRESS, the left-most portion of the address identifies which NETWORK the machine (host) belongs to. The right-most portion is used as the address of the host itself. A large number of addresses in use (but not all of them) look something like as shown in table 4.1

VALUE	NETWORK			HOST
IN DECIMAL	199	232	66	20
IN BINARY	11000111	11100100	001000010	00001010

Table 4.1 Network and Host Portion of an IP Address

In the example shown in table 4.1 above, the network address is 199.232.66 and the host portion of the address is 20, the complete IP address is 199.221.66.20. All the computers on the same local NETWORK would have the same network number in their address. Thus, two computers on the same NETWORK might be 199.221.66.20 and 199.221.66.41.

When two hosts with IP addresses communicate, they send IP data grams. IP DATA GRAMS contain the source and destination addresses of the hosts communicating. Only the addresses are recorded in the packet. There is no information stored in the packet to tell us which part of the address is network and which is host. If this is true, then how will we figure out which part of the address is the network portion, and which is the host portion?

First, we must remember that all hosts on the same NETWORK will have the same network address (the network portion will be the same for all hosts). Only the host portion will be different and unique for each host on the network.

Different networks also have different network addresses. Network A would have a different address from Network B. From the perspective of determining the correct network, the individual host address is irrelevant. We will need it later to find the host itself ON the network, but we don't need to look at it yet, since we need to find the correct NETWORK first.

To find a particular host, we first find the NETWORK that host is on and then ask that NETWORK to find the host. There are two solutions to handling this NETWORK vs. host address problem, and they are similar but separate addressing types: CLASSFUL, and CLASSLESS.

CLASSFUL was the first addressing scheme developed. It helped manage the IP space and make organization of networks and hosts possible, but it could not support the growing complexity of the INTERNET, and wasted a lot of address space, so an new scheme was developed called CLASSLESS.

i. Source Address

The IP ADDRESS of the HOST that sent the DATAGRAM (sender).

ii. Destination Address

The IP ADDRESS of the HOST the DATAGRAM is being sent to (receiver).

iii. MASK

The mask is a value that is stored in the configuration of a computer along with the IP address. The mask gives the computer a simple way to figure out whether the IP address of another computer is on the same local network, or on a different local network. Bear in mind that for this definition of a mask, a 'local network' is defined as a group of computers with IP addresses in a limited range.

iv. Subnet Mask

A piece of information stored on the local HOST that allows it to determine whether a remote HOST is part of the local NETWORK, or is part of a different outside NETWORK.

During the process of delivering (ROUTING) an IP DATAGRAM, only the destination IP ADDRESS is significant. In *CLASSFUL ADDRESSING* information about the HOST'S location and the NETWORK it is located on is assumed to be encoded into the IP ADDRESS within the DATAGRAM. There aren't any fields provided in an IP DATAGRAM to inform the receiver where the network portion of the IP ADDRESS leaves off and where the HOST portion of the IP ADDRESS begins. (See IPV4 ADDRESSING section for more information).

4.1.2 WHAT IS A CLASS?

Classful addressing divides the entire IP ADDRESS space (0.0.0.0 to 255.255.255.255) into 'classes', or special ranges of contiguous IP ADDRESSES (no addresses missing between the first and last address in the range). CLASSFUL ADDRESSING makes it possible to determine the NETWORK portion of the IP ADDRESS by looking at the first four bits of the first octet in the IP ADDRESS. The **FIRST FOUR BITS** are referred to as the 'most significant bits' of the first octet and are used to **DETERMINE WHAT CLASS OF IP ADDRESS IS BEING USED**. The value of the first four bits determines the range of actual numerical values of the first octet of the IP ADDRESSES in that class. From this information, a

receiving HOST can determine which part of the IP ADDRESS is being used to identify the specific network on which the HOST resides, and which portion of the IP ADDRESS is used to identify the HOST.

The different classes of IP ADDRESSES (Class A, Class B, Class C, Class D & Class E) were created to allow for carving up the entire set of all IP ADDRESSES into chunks of different sizes that would 'fit' the number of HOSTS on the NETWORK for which the IP ADDRESS SPACE was being supplied. The table 4.2 shown below gives a breakdown of how the Classful system breaks up the IP ADDRESS space.

FIRST OCTET		IP ADDRESS CHARACTERISTICS			
MOST SIGNIFICANT BITS	VALUE RANGES	ADDR. CLASS	NETWORK VS. HOST	# NETWORKS	# HOSTS
0000	0-126	A	N.h.h.h	256	16,777,214
--	127	-	-	*SPECIAL - LOCAL LOOPBACK*	
1000	128-191	B	N.N.h.h	65,536	65,534
1100	192-223	C	N.N.N.h	16,777,216	254
1110	224 - 239	D	Special	N/A	N/A
1111	240 +	E	Special	N/A	N/A

Table 4.2 Classful IP Addressing

It is possible to waste IP ADDRESSES by assigning blocks of IP ADDRESSES which fall along octet boundaries (the dots between the NUMBERS in the DECIMAL representation of the IP ADDRESS). Most often a class C address was supplied to anyone requesting space, as few NETWORKS had more than 256 hosts. But the networks grew to more than 256 HOSTS, and needed more space, so Class B addresses were given out. But if a NETWORK has only 500 HOSTS, and in the case of a class B IP ADDRESS block to that network, 65,034 addresses will go unused. This is a terribly inefficient use of space, and as NETWORKS grew larger the INTERNET grew; the need to use the IP ADDRESS space more and more efficiently became ever more critical.

One solution that was created for reduce utilization of IP ADDRESSES was NETWORK ADDRESS TRANSLATION. This involved the use of PRIVATE IP ADDRESSES and a device that translates PRIVATE IP ADDRESSES into PUBLIC IP ADDRESSES.

As the list of available IP ADDRESSES was depleted it became clear that a new solution was needed that provided more addresses and efforts turned towards developing what is called IP v6.

i. Classful Addressing

COMPUTERS communicating using INTERNET Protocol (IP) send DATA GRAMS. IP DATAGRAM contains a *SOURCE IP ADDRESS*, and a *DESTINATION IP ADDRESS*. However, an IP DATAGRAM does not contain any NETWORK subnet mask information, thus it is difficult to know which groups of COMPUTERS (HOSTS) formed a NETWORK.

ii. Classless Addressing

All IP addresses have a network and host portion. In classful addressing, the NETWORK portion ends on one of the separating dots in the address (on an octet boundary). Classless addressing uses a variable number of bits as shown in table 4.3 for the NETWORK and host portions of the address.

Decimal	192	160	20	48	
Binary	11000000	10100000	00010100	0011	0000
	<-------- 28 bits Network ------->				4 bits host

Table 4.3 Classless IP Addressing

Classful addressing divides an IP ADDRESS into the Network and Host portions along octet boundaries. Classless addressing treats the IP ADDRESS as a 32 bit stream of ones and zeroes, where the boundary between NETWORK and host portions can fall anywhere between bit 0 and bit 31. The network portion of an IP ADDRESS is determined by how many 1's are in the subnet mask.

Again, this can be a variable number of bits, and although it can fall on an octet boundary, it does not necessarily need to. A subnet mask is used locally on each host connected to a network, and masks are never carried in IPv4 data grams. All hosts on the same network are configured with the same mask, and share the same pattern of network bits. The host portion of each host's IP address will be unique.

4.1.3 SUBNETTING and SUPERNETTING

Originally the entire range of IP ADDRESSES WAS carved up into small, medium and large chunks of addresses. Networking equipment figured which addresses was all part of a NETWORK by looking at the first four bits of the address. There were five classes of addresses used. Sub netting is the process of borrowing bits from the host portion of an address to provide bits for identifying additional sub-networks. VLSM is most frequently referred to as sub netting.

i. Variable Length Subnet Masking (VLSM)

The INTERNET's explosive growth eventually required the more efficient use of the IP ADDRESS space available. Variable Length Subnet Masking is a technique used to allow more efficient assignment of IP ADDRESSES. Originally INTERNET addresses were carved up into small, medium and large size blocks of contiguous addresses based on the values of the first four bits in the first octet of the IP ADDRESS. These were often referred to as *CLASS FULL* addresses. By carving CLASS FULL address blocks into smaller CLASSLESS blocks, we waste fewer addresses. The process of carving out smaller blocks from the larger blocks was called *SUB NETTING.*

Many organization's networks started very small and were assigned class C addresses. A class C address range contains 256 addresses. Soon, these organizations grew and so did their networks. Networks that needed to expand beyond their original class C range used a technique called *SUPER NETTING* to allow them to turn two contiguous IP address blocks into one network.

ii. Super netting

Super netting is different. Super netting merges several smaller blocks of IP addresses (networks) that are continuous into one larger block of addresses. There can't be any 'holes' in the range. Super netting is done by borrowing network bits to combine several smaller networks into one larger network.

For instance, a class 'C' block has 256 possible addresses in it. This block could be split into four classless blocks of 64 addresses each by borrowing two bits from the host portion of the class 'C' address.

Note: *Even after borrowing 2 bits from the host portion towards network portion only two subnets can be created as* ***all bits zero & all bits one*** *condition is not allowed in the subnets.*

Standard Class 'C' network				
	Network	Network	Network	Host
CLASS 'C' ADDRESS	192	64	123	0
MASK (DECIMAL)	255	255	255	0
MASK (BINARY)	11111111	11111111	11111111	00000000

Table 4.4a

The mask and address shown in table 4.4a above combine to give a range of addresses from 192.64.123.1 through 192.64.123.254.

Subnet #1					
	Network	Network	Network	Subnet	Host
CLASS 'C' ADDRESS	192	64	123	64	
MASK (DECIMAL)	255	255	255	192	
MASK(BINARY)	11111111	11111111	11111111	11	000000

Table 4.4b

The mask and address shown in table 4.4b above combine to give a range of addresses from 192.64.123.65 through 192.64.123.126.

Subnet #2					
	Network	Network	Network	Subnet	Host
CLASS 'C' ADDRESS	192	64	123	128	
MASK (DECIMAL)	255	255	255	192	
MASK (BINARY)	11111111	11111111	11111111	11	000000

Table 4.4c

The mask and address shown in table 4.4c above combine to give a range of addresses from 192.64.123.129 through 192.64.123.190.

4.1.4 Special IP addresses

There are several IP addresses that are special in one way or another. These addresses are for special purposes or are to be put to special use.

- Addresses significant to every IP subnet
  - Network Address
  - Broadcast Address

- Addresses significant to individual hosts
  - Loopback Address
  - Private Addresses
  - Multicast Addresses
  - Reserved Addresses

NETWORK ADDRESS

A network address is an address where all host bits in the IP address are set to zero (0). In every subnet there is a NETWORK address. This is the first and lowest numbered address in the range. The network address is defined as the address that contains all zeroes in the host portion of the address and is used to communicate with devices that maintain the network equipment.

BROADCAST ADDRESS

A broadcast address is an address where all host bits in the IP address are set to one (1). This address is the last address in the range of addresses, and is the address whose host portion is set to all ones. All hosts are to accept and respond to the broadcast address. This makes special services possible.

LOOPBACK ADDRESS (127.0.0.1)

The 127.0.0.0 class 'A' subnet is used for only a single address: the loopback address 127.0.0.1. This address is used to test the local NETWORK interface device's functionality. All NETWORK interface devices should respond to this address. If we ping 127.0.0.1, we can be assured that the network hardware is functioning and that the network software is also functioning.

PRIVATE ADDRESSES

RFC 1918 defines a number of IP blocks which were set aside by the American Registry of Internet Numbers (ARIN) for use as PRIVATE ADDRESSES on private networks that are not directly connected to the INTERNET. The private addresses are shown in table 4.5.

Class	Start	End
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Table 4.5 Private IP Address

MULTICAST ADDRESSES

Multicast (class D) IP addresses shown in table 4.6 are used in special areas like in Routing algorithms (e.g. ospf uses multicast address for route advertisement) and video conferences etc. that cannot be used on the INTERNET.

Class	Start	End
D	224.0.0.0	239.255.255.255

Table 4.6 Multicast IP addresses

RESERVED ADDRESSES

There are a number of addresses that are reserved and set aside for future purpose like class E IP addresses. Some special address are shown in table 4.7

Address Block	CIDR Mask	Used for	Reference
0.0.0.0	/8	USED TO COMMUNICATE WITH "THIS" NETWORK	RFC1700, P. 4
10.0.0.0	/8	PRIVATE-USE NETWORKS	RFC 1918
14.0.0.0	/8	PUBLIC-DATA NETWORK	RFC1700, P.181
24.0.0.0	/8	CABLE TV NETWORKS	--
39.0.0.0	/8	PREVIOUSLY RESERVED AVAILABLE FOR REGIONAL ALLOCATION	RFC1797
127.0.0.0	/8	LOOPBACK ADDRESS	RFC1700, P. 5
128.0.0.0	/16	PREVIOUSLY RESERVED AVAILABLE FOR REGIONAL ALLOCATION	--
169.254.0.0	/16	LINK LOCAL (EG. MICROSOFT XP SYSTEMS USE AUTOMATIC PRIVATE IP ADDRESSING (APIPA) WHICH SELECTS ADDRESSES IN THIS RANGE.)	

Table 4.7 Special IP Addresses

4.2 IP ROUTING

Routing is the process of moving data from one NETWORK to another by forwarding PACKETS via GATEWAYS. With IP based NETWORKS, the routing decision is based on the destination address in the IP PACKET'S header. Routing can be classified as shown in fig 4.1

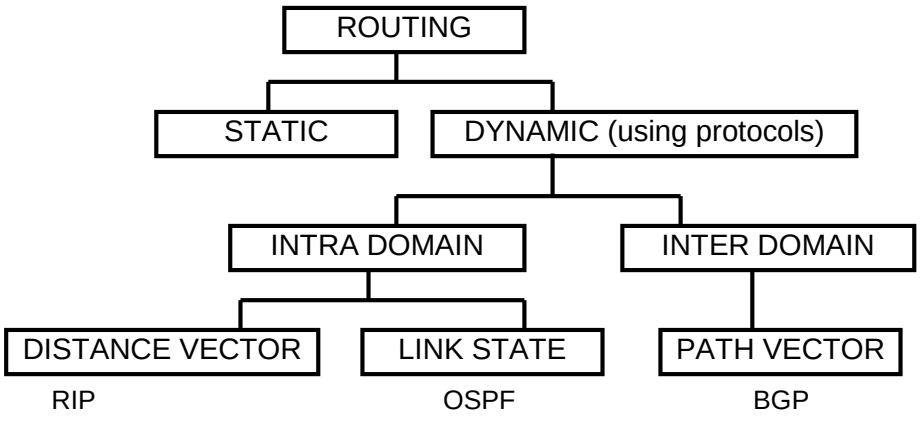


Fig 4.1 Routing

4.2.1 Static Routing

Static routing is the term used to refer to the manual method used to set up routing. An administrator enters routes into the router using configuration commands. This method has the advantage of being predictable, and simple to set up. It is easy to manage in small networks but does not scale well.

i. ADVANTAGES

- Simple to configure
- Easy to predict and understand in small networks

ii. DISADVANTAGES

- Requires extensive planning and has a high management overhead
- Does not dynamically adapt to network topology changes or equipment failures.
- Does not scale well in large networks.

iii. STATIC ROUTE CONFIGURATION (CISCO)

- Default Route
- Static Null Route
- Preferred Routes
- Backup Routes
- Static Load Balancing

a. Default Route

A default route is often called the 'route of last resort'. It is the last route tried when all other routes fail because it has the fewest number of network bits matching and is therefore less specific. A default route is configured on a *Cisco* router with the following command:

ip route 0.0.0.0 0.0.0.0 <next hop IP address > OR < exit interface type><No.>

b. Static Null Route

Null route, routes traffic to a non-existent interface, what is often called a 'bit bucket'. This traffic is effectively dropped as soon as it is received. A null route is useful for removing packets that cannot make it out of the network or to their destination, and decreases congestion caused by packets with no functional destination. During a denial of service attack, a Null route can temporarily be used near the destination to drop all traffic generated by the attack.

CISCO 'NULL ROUTE' COMMAND **:** **ip route <network> <mask> null0**

c. Preferred Routes

The route which has the greatest number of network bits matching the destination address is the preferred route to a destination. This is referred to as 'longest prefix match'.

ip route 202.148.224.0 255.255.255.252 e0

ip route 202.148.224.128 255.255.255.128 e1

d. Backup Routes

In cases where redundancy is required, a second route can be placed on another physical path so that if the first route fails, the second route over the less preferred path(s) will be used. By using a second pair of routes. This method can help compensate for NETWORK failures.

CISCO router commands:

SPECIFIC ROUTES (used unless down)

ip route 202.148.224.0 255.255.255.128 e0

ip route 202.148.224.128 255.255.255.128 e1

BACKUP ROUTES (used when one of the specified routes is down)

ip route 202.148.224.0 255.255.255.0 e0

ip route 202.148.224.0 255.255.255.0 e1

e. Static Load Balancing

We can create load balancing without using a dynamic routing protocol. Most routers will perform load balancing automatically if several equal cost paths to a destination exist on multiple interfaces. To configure this using static routing, we need only create multiple static routes for more than one interface. This creates more than one equal cost path which will balance the load.

CISCO router commands:

ip route 202.148.224.0 255.255.255.0 e0

ip route 202.148.224.0 255.255.255.0 e1

4.2.2 Dynamic Routing

- **Interior (Intra domain)**
  - **RIP** - Routing Information Protocol
  - **OSPF** - Open Shortest Path First
  - **IS-IS** - Intermediate System to Intermediate System
  - **IGRP** - Interior Gateway Routing Protocol
  - **EIGRP** - Enhanced Interior Gateway Routing Protocol
- **Exterior (Inter domain)**
  - **BGP** - Border Gateway Protocol

i. RIP (Routing Information Protocol)

The **Routing Information Protocol** (**RIP**) is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP). It uses the distance-vector routing algorithm. The routing algorithm used in RIP, the Bellman-Ford algorithm

RIP is a distance-vector routing protocol, which employs the hop count as a routing metric. The hold down time is 180 seconds. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

In most current networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF. It is easy to configure, because RIP does not require any parameters on a router unlike other protocols.

RIP Version2 is in vogue, it includes the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier versions.

ii. OSPF (Open Shortest Path First)

OSPF is an internal routing protocol. (Primarily used inside a single company, it can span multiple sites.) It's an open standard protocol. Like other dynamic routing protocols, OSPF enables routers to disclose their available routes to other routers.

OSPF is a link-state routing protocol that runs Dijkstra's algorithm to calculate the shortest path to other networks. Taking the bandwidth of the network links into account, it uses cost as it's metric. OSPF works by developing adjacencies with its neighbors, periodically sending hello packets to neighbors, flooding changes to neighbors when a link's status changes, and sending "paranoia updates" to neighbors of all recent link state changes every 30 minutes.

While OSPF is an excellent routing protocol for networks of all sizes, one of its weaknesses is that it can be quite complex to configure. On the other hand, it offers more features than simpler protocols such as RIP.

Here are some of OSPF's strengths:

- It converges quickly, compared to a distance vector protocol
- Routing update packets are small, as it does not send the entire Routing table
- It is not prone to routing loops.
- It scales very well for large networks
- It recognizes the bandwidth of a link and takes into account in link selection
- It supports VLSM or CIDR
- It supports a long list of optional features that many others don't

iii. BGP (Border Gateway Protocol)

The Border Gateway Protocol (BGP) is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule sets.

BGP was created to replace the Exterior Gateway Protocol (EGP) routing protocol to allow fully decentralized routing in order to allow the removal of the NSFNet Internet backbone network. This allowed the Internet to become a truly decentralized system. Now version four of the BGP is in use on the Internet. All previous versions are now obsolete.

The major enhancement in version 4 was support of Classless Inter-Domain Routing and use of route aggregation to decrease the size of routing tables.

Most Internet users do not use BGP directly. However, since most Internet service providers must use BGP to establish routing between one another (especially if they are multi homed). It is one of the most important protocols of the Internet.

Very large private IP networks use BGP internally, however. An example would be the joining of a number of large Open Shortest Path First (OSPF) networks where OSPF by itself would not scale to size. Another reason to use BGP is multi homing, a network for better redundancy either to multiple access points of a single ISP or to multiple ISPs.

BGP neighbors, or peers, are established by manual configuration between routers to create a TCP session on port 179. A BGP speaker will periodically send 19-byte keep-alive messages to maintain the connection (every 60 seconds by default). Among routing protocols, BGP is unique in using TCP as its transport protocol.

When BGP is running inside an autonomous system (AS), it is referred to as Internal BGP (iBGP or Interior Border Gateway Protocol). When it runs between autonomous systems, it is called External BGP (eBGP or Exterior Border Gateway Protocol). Routers on the boundary of one AS, exchanging information with another AS, are called border or edge routers.

4.3 IP COMMUNICATION

4.3.1 IP Datagram Structure

The term 'datagram' or 'packet' is used to describe a chunk of IP data. Each IP datagram contains a specific set of fields in a specific order so that the reader knows how to decode and read the stream of data received. The description of the IP datagram format in this tutorial is suitable for most purposes. An IP datagram is illustrated in fig 4.2 and its fields are described in table 4.8

<table>
<tr><th colspan="2">0 .. 7</th><th colspan="2">8 .. 15</th><th colspan="2">16 .. 23</th><th>24.. 31</th></tr>
<tr><td>Version</td><td>IHL</td><td colspan="2">TOS</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="3">Fragment Offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="7">Source IP Address</td></tr>
<tr><td colspan="7">Destination IP Address</td></tr>
<tr><td colspan="6">Options</td><td>Padding</td></tr>
<tr><td colspan="7">Payload (TCP/UDP/ICMP etc.)</td></tr>
</table>

Fig 4.2 IP datagram

VERSION (4 bits)	The version field is set to the value '4' in decimal or '0100' in binary. The value indicates the version of IP (4 or 6, there is no version 5).
IHL (4 bits)	The Internet Header Length (IHL) describes how big the header is in 32-bit words. For instance, the minimum value is 5, as that is the minimum size of an IP header that contains all the correct fields is 160 bits, or 20 bytes. This allows the receiver to know exactly where the payload data begins
TOS (8 bits)	Type of service allows the intermediate receiving stations (the routers) to have some notion of the quality of service desired. This allows the NETWORK to make adaptations for delay, throughput, or reliability.
TOTAL LENGTH (16 bits)	This informs the receiver of the datagram where the end of the data in this datagram is. This is the length of the entire datagram in octets, including the header. This is why an IP datagram can be up to 65,535 bytes long, as that is the maximum value of this 16-bit field.
IDENTIFICATION (16 bits)	Sometimes, a device in the middle of the NETWORK path cannot handle the datagram at the size it was originally transmitted, and must break it into fragments. If an intermediate system needs to break up the datagram, it uses this field to aid in identifying the fragments.
FLAGS (3 bits)	The flags field contains single-bit flags that indicate whether the datagram is a fragment, whether it is permitted to be fragmented, and whether the

	datagram is the last fragment, or there are more fragments. The first bit in this field is always zero.
FRAGMENT OFFSET (13 bits)	When a datagram is fragmented, it is necessary to reassemble the fragments in the correct order. The fragment offset numbers the fragments in such a way that they can be reassembled correctly.
TIME TO LIVE (8 bits)	This field determines how long a datagram will exist. At each hop along a NETWORK path, the datagram is opened and it's time to live field is decremented by one (or more than one in some cases). When the time to live field reaches zero, the datagram is said to have 'expired' and is discarded. This prevents congestion on the NETWORK that is created when a datagram cannot be forwarded to its destination. Most applications set the time to live field to 30 or 32 by default.
PROTOCOL (8 bits)	This indicates what type of protocol is encapsulated within the IP datagram. Some of the common values in decimal for ICMP is 1, IGMP is 2, TCP is 6 & UDP is 17
HEADER CHECKSUM (16 bits)	According to RFC 791, the header checksum formula is:"the 16-bit ones compliment of the ones compliment sum of all 16-bit words in the header." The checksum allows IP to detect data grams with corrupted headers and discard them. Since the time to live field changes at each hop, the checksum must be re-calculated at each hop. In some cases, this is replaced with a cyclic redundancy check algorithm.
SOURCE ADDRESS (32 bits)	This is the IP address of the sender of the IP datagram.
DESTINATION ADDRESS (32 bits)	This is the IP address of the intended receiver(s) of the datagram. If the host portion of this address is set to all 1's, the datagram is an 'all hosts' broadcast.
OPTIONS & PADDING (variable)	Various options can be included in the header by a particular vendor's implementation of IP. If options are included, the header must be padded with zeroes to fill in any unused octets so that the header is a multiple of 32 bits, and matches the count of bytes in the Internet Header Length (IHL) field

Table 4.8 Description of IP datagram

4.4 WAN DEVICES

4.4.1 ROUTER

A router is specialized computer connected to more than one NETWORK that runs software that allows it to move data from one NETWORK to another based on routing tables as shown in table 4.9 & routing functions are described in fig 4.3.

Mask (/ n)	Network Address	Next hop Address	Interface
/ 24	201.4.22.0	180.170.65.200	S1/0
/16	140.24.0.0	156.24.32.43	S2/0

Table 4.9 Typical Routing Table

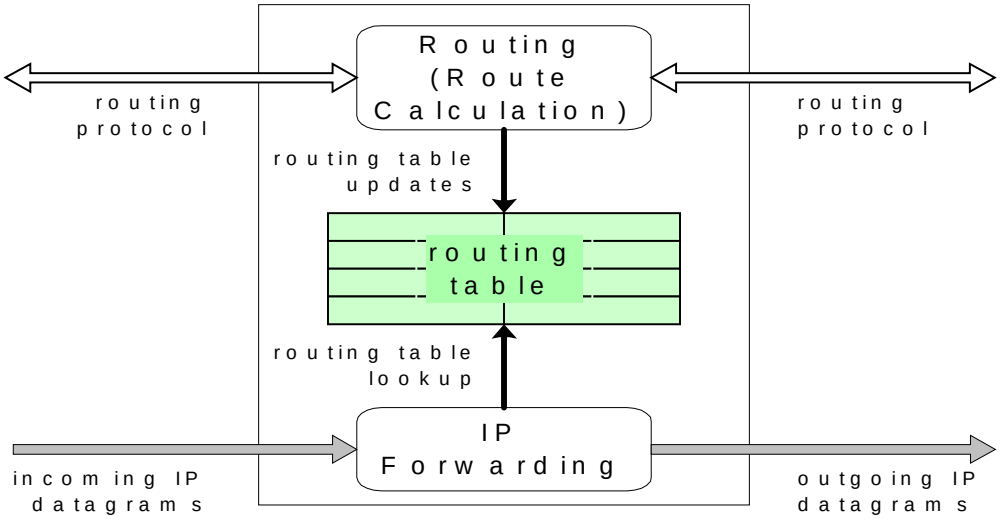


Fig 4.3 Routing functions

Routers operate at the NETWORK LAYER (OSI LAYER 3). The primary function of a router is to connect networks together and keep certain kinds of BROADCAST traffic under control. There are several companies that make routers: CISCO, JUNIPER, NORTEL, REDBACK, LUCENT, 3COM, and HP just to name a few. Routers operate in the physical, data link, and network layers of the OSI model.

The hardware setup of Router is shown in fig 4.4 and each device functionalities are described below.

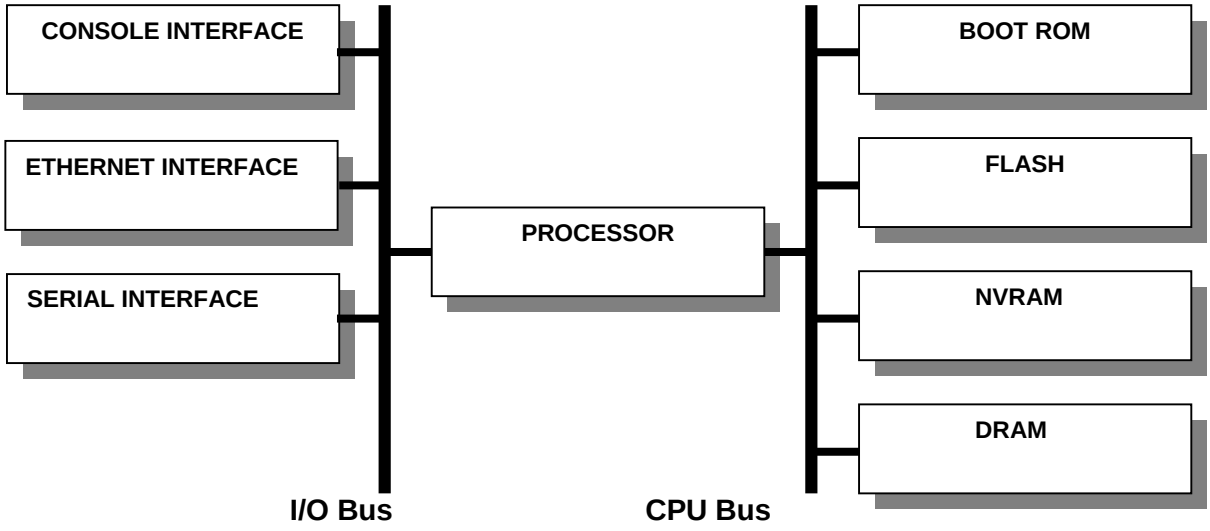


Fig 4.4 Router hardware setup

PROCESSOR executes instructions coded in operating system (IOS) to perform the basic operations necessary to accomplish the Router's functionality. (E.g. all the routing functions, network module high level control & system initialization). Generally the processors used are MPC 860 or higher.

BOOT ROM is not erasable and it is used for permanently storing startup diagnostic code (ROM Monitor). The main task for Boot ROM is to perform some hardware diagnostics during boot up on the router (Power on self test - POST) and to load the IOS software from the Flash to the Memory.

DRAM is logically divided into Main Processor memory and Shared Input/output (I/O) memory.

- **Main Processor Memory** It is used to store routing tables, fast switching cache, running configuration, and so on. It can take unused shared I/O memory, if needed.·
- **Shared I/O Memory** It is used for temporary storage of packets in system buffers at the time of process switching, and interface buffers during fast switching.

FLASH is the only way to permanently store and move a complete IOS software image, backup configurations, or any other files.

NVRAM is used for permanent storage of the startup configuration that is writeable. It is also used for permanent storage of hardware revision and identification information, and also Media Access Control (MAC) addresses for LAN interfaces. It is a battery backed Static RAM (SRAM).

CONSOLE INTERFACE is used for initial configuration of the Router using emulation software like **hyper terminal**

ETHERNET INTERFACE is used for connecting the local area network (LAN) of type Ethernet, Fast Ethernet & Gigabit Ethernet etc.

SERIAL INTERFACE is used for connecting wide area networks (WAN) of type synchronous serial, asynchronous serial and smart serial etc.

CPU Bus this is used by the CPU for accessing the various components of the router and transferring the instructions and data to or from specified memory addresses.

I/O Bus this is the bridge interface between the CPU bus and system bus (where the network modules and other interface boards are connected)

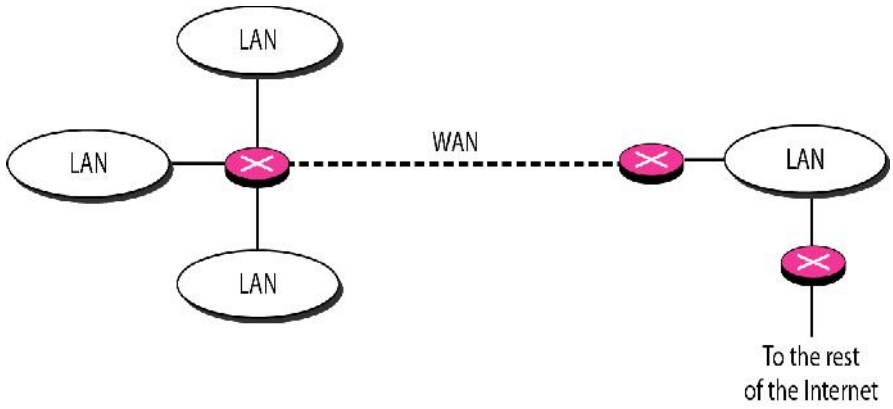


Fig 4.5 Routers connecting independent LANs and WANs

Routers relay packets among multiple interconnected networks like LANs & WANs as shown in fig 4.5 they route packets from one network to any of a number of potential destination networks on an internet. A packet sent from a station on one network to a station on a neighboring network goes first to the jointly held router, which switches it over to the destination network. If there is no one router connected to both the sending and receiving networks the sending router transfers the packet across one of the connected networks to the next router in the direction of the ultimate destination. That router forwards the packet to the next router on the path and so on until the destination is reached.

Routers act like stations on a network. But unlike most stations, which are members of only one network, routers have addresses on and link to two or more networks at the same time. In their simplest function they receive packets from one connected network and pass them to a second, connected, network. However, if a received packet is addressed to a node on a network of which the router is not a member, the router is capable of determining which of its connected networks is the best next relay point for the packet. Once a router has identified the best route for a packet to travel, it passes the packet along the appropriate network to another router. That route checks the destination address, finds what it considers the best route for the packet and passes it to the destination network (if that network is a neighbor), or across a neighboring network to the next router on the chosen path.

Routers perform the following functions as shown in fig 4.4a

- Restrict NETWORK broadcasts to the local LAN.
- Protocol bridging
- Act as the DEFAULT GATEWAY.
- Learn and advertise loop free paths between sub-networks.

i. Restrict Broadcasts to the Local LAN

NETWORKS use BROADCASTS (transmissions sent to all hosts on the NETWORK) to communicate certain kinds of information that the NETWORK uses to function properly (ARP, RARP, DHCP, IPX-SAP broadcasts etc.). As the number of hosts on the NETWORK increases, the amount of what is called "broadcast" traffic increases. If enough broadcast traffic is present on the network, then ordinary communication across the NETWORK becomes difficult.

To reduce BROADCASTS, a NETWORK administrator can break up a NETWORK with a large number of hosts into two smaller networks. BROADCASTS are then restricted to each NETWORK, and the router performs as the *DEFAULT GATEWAY* to reach the hosts on the other NETWORKS.

ii. Protocol Bridging

A router can take in an Ethernet frame, strip the Ethernet data and then drop the IP data into a frame of another type such as Token Ring, DS1/T1, SONET or FDDI. A router also performs 'protocol conversion', provided it has the appropriate hardware and software to support such a function. When converting between protocols, the closest equivalent function in the new protocol is set to mirror the old protocol from which the data was received. The idea is to forward the data from the interface it receives data on to another interface that retransmits the received data onto another interface serving another network using a different protocol.

iii. Act as the Default Gateway

Especially in today's networks, people are connecting to the INTERNET. When a PC wants to talk to a PC on another network, it does so by sending our data to the DEFAULT GATEWAY (our router). The router receives the datagram and, looks for the remote address of that far-off PC and then makes a routing decision. The router then forwards our data out a different interface that is closer to that remote PC. There could be several routers between the originating PC and the remote PC so several routers will take part in handing off the datagram, much like a fireman's bucket brigade.

This allows two networks managed by different organizations to exchange data. They create a NETWORK between them and exchange data between the routers on that network. Because a router can accept traffic from any kind of network it is attached to, and forward it to any other network, it can also allow networks that could not normally communicate with each other to exchange data. In technical terms, a TOKEN RING NETWORK and an ETHERNET NETWORK can communicate over a serial network. Routers make all this possible.

iv. Learn and advertise loop free paths between sub-networks.

Over time, networks grew in size. The connections between them outgrew administrator's ability to keep up with them. To make life simpler, routing protocols (RIP, OSPF, IS-IS, IGRP, EIGRP, BGP) were invented so that very large NETWORK systems with lots of sub-networks can automatically learn where each NETWORK is located and advertise that information automatically to other routers. This makes it possible for the networks to automatically learn how they are constructed, find the best ways to get from place to place and move all the data along those best routes as efficiently as possible. This is how data makes it across the INTERNET.

4.4.2 GATEWAY

If two networks operate according to different network protocols, a gateway is used to connect them. Gateways usually operate at OSI layer 4 or higher, and basically translate the protocols to allow terminals on two dissimilar networks to communicate. Some gateways also translate data codes. i.e. From ASCII to EBCDIC. This capability would be useful on a LAN when communication server routes traffic from a PC based network using ASCII to an IBM main frame that uses the EBCDIC code

Gateways can be either or combinations of hardware & software. They may be implemented on a specially designed circuit card by using specialized software in a standard PC. An Internet service provider, which connects users in a home to the internet, is a Gateway. The Computer routing traffic in an organization from individual work stns to an outside networks Web server is a Gateway.

Gateways can suffer from slow performance because of protocol translations, so their performance must be considered and tested when a Gateway installation is contemplated. A dedicated computer action as a gateway, if it is of reasonable speed, usually eliminated any performance problems.

Gateways perform an important role in allowing an organization to interconnect different types of LANs so that the network appears as a single entity to the user. The term Gateway is used in many contexts, but in general it refers to a software or hardware interface that enables two different types of networked systems or software to communicate. For example you might use a gateway to

- Convert commonly used protocols 9e.g. TCP/IP) to a specialized protocols
- Translates different addressing schemes.
- Direct electronic mail to the right network destination
- Connect network with different architectures.

4.5 Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is responsible for reliable end to end delivery of segments as shown in fig 4.6. Segments are the term that is used to describe the data that is transmitted and received at the Transport layer of the OSI model where TCP resides. TCP also redirects the data to the appropriate well known ports (upper level service) .

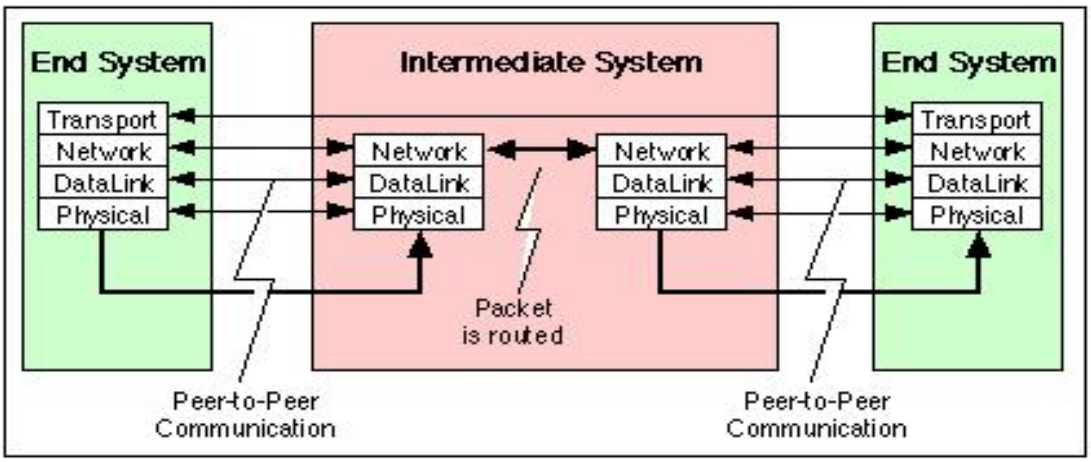


Fig 4.6 end to end delivery of segments

The reliable end to end delivery of data is accomplished by:

4.5.1 Connection-oriented service

Segments are acknowledged to the source when received by the destination. A sliding window is used to enable unacknowledged segments on the "wire" in order to speed up transmission rates

4.5.2 Sequencing of segments

Data is broken up into segments that are numbered (sequenced) when transmitted. The destination TCP layer keeps track of the received segments and places them in the proper order (re sequences).

4.5.3 Requesting retransmission of lost data

If a segment is lost in transmission (missing sequence number). The destination will timeout and request that all segments starting at the lost segment be retransmitted.

4.5.4 Error checking

Segments are checked for data integrity when received using a 32 bit CRC check.

The redirection of data to the upper level service is accomplished by using Source and Destination Port numbers. Multiple connections to the same service is allowed. For example, we may have many users (clients) connected to a single web server (http is normally port 80). Each client will have a unique Port number assigned (typically above 8000) but the web server will only use Port 80.

4.5.5 TCP Header

The Transmission Control Protocol (TCP) header is shown in fig 4.7 & its fields are described in Table 4.10

<table>
<tr><td>0 1 2 3 4 5 6 7</td><td>8 9 10 11 12 13 14 15</td><td>16 17 18 19 20 21 22 23</td><td>24 25 26 27 28 29 30 31</td></tr>
<tr><td colspan="2">Source Port (16 bits)</td><td colspan="2">Destination Port (16 bits)</td></tr>
<tr><td colspan="4">Sequence Number(32 bits)</td></tr>
<tr><td colspan="4">Acknowledgement Number(32 bits)</td></tr>
<tr><td>Offset (1st 4bits)</td><td>Not used (6 bits)</td><td>Flags (last6 bits)</td><td>Window</td></tr>
<tr><td colspan="2">Checksum</td><td colspan="2">Urgent Pointer</td></tr>
<tr><td colspan="4">Options + Padding</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

Fig 4.7 TCP Header

Source Port	The Source Port is a 16 bit number that Indicates the upper level service that the source is transmitting. For example:
Destination Port	The Destination Port is a 16 bit number that Indicates the upper level service that the source wishes to communicate with at the destination.
Sequence Number	The Sequence Number is a 32 bit number that indicates the first octet of information in the data field. This is used to number each TCP segment transmitted in order to keep track of segments for sequencing of segments and error checking of lost segments. The source numbers the sequence of transmitted segments.
Acknowledgement Number	The Acknowledgement Number is a 32 bit number that is used to acknowledge the receipt of segments by the destination. The acknowledgement is the next sequence number expected. If the sender does not receive an acknowledgement for a segment transmitted, the sender will time-out and retransmit
Offset (4 bits)	The Offset field consists of the first 4 bits (xxxx0000) of the first byte. The last 4 bits are reserved for future use and are set to 0. The Offset measures the number of **32 bit (4 byte)** words in the TCP header to where the Data field starts. This is necessary because the TCP header has a variable length. The minimum length of the TCP header is 20 bytes which gives an Offset value of 5.

Flags (last 6 bits)	The Flags Field consists of the last 6 bits (00xxxxxx) of the second byte with the first 2 bits reserved for future use and they are set to 0. The Flags field consists of the following flag bits: **URG (Urgent Flag)** When set indicates that the Urgent Pointer field is being used. **ACK (Acknowledge Flag)** When set indicates that the Acknowledgement Number is being used. **PSH (Push Flag)** An upper level protocol requires immediate data delivery and would use the Push (PSH) flag to immediately forward all of the queued data to the destination. **RST (Reset Flag)** When set the connection is reset. This is typically used when the source has timed out waiting for an acknowledgement and is requesting retransmission starting at a sequence number. **SYN (Synchronize Flag)** When set, it indicates that this segment is the first one in the sequence. The first sequence number assigned is called the Initial Sequence Number (ISN) **FIN (Finish Flag)** When set, it indicates that this is the last data from the sender.
Windows (16 bits)	This contains the number of unacknowledged segments that are allowed on the network at any one time. This is negotiated by the Source and Destination TCP layers.
Checksum	The Checksum field is 16 bits long and calculates a checksum based on the complete TCP Header and what is called the TCP Pseudo header. The TCP Pseudo header consists of the Source IP Address, Destination IP Address, Zero, IP Protocol field and TCP Length. The IP Protocol field value is 6 for TCP
Urgent Pointer	This field communicates the current value of the urgent pointer as a positive offset from the sequence number in this segment. The urgent pointer points to the sequence number of the octet following the urgent data. This field is only be interpreted in segments with the URG control bit set.
Options	Options may occupy space at the end of the TCP header and are a multiple of 8 bits in length. The allowed options are: • Kind 0 - End of option list. • Kind 1 - No Operation. Kind 2 - Length 4 Maximum Segment Size. This is used to indicate the maximum segment size allowed
Padding	The TCP header padding is used to ensure that the TCP header ends and data begins on a 32 bit boundary. The padding is composed of zeros.
Data	Consists of pure form of data (combination of bits) coming from upper layers

Table 4.10 Description of TCP header fields

4.6 User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless host to host service that operates at the Transport layer of the OSI model. UDP relies on the upper layer protocol for error correction and reliable service. The protocol is transaction oriented; its delivery and duplicate protection are not guaranteed. The major uses of this protocol are DNS and TFTP.

UDP has a small header and for all intensive purposes adds Port addressing to the IP header. The IP header routes data grams to the correct host on the network and UDP routes the datagram to the correct application.

UDP Header

The User datagram Protocol (UDP) header is shown in fig 4.8 & its fields are described in Table 4.11

0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
Source Port (16 bits)		Destination Port (16 bits)	
Length (16 bits)		Checksum (16 bits)	
Data			

Fig 4.8 UDP Header

Source Port	The Source Port is a 16 bit number that Indicates the upper level service that the source is transmitting. Appendix I is a complete listing of well known ports. UDP allows port numbers to be in the range from 0 to 65,535. The Source Port is optional and if not used, a field of 0s is inserted. Clients will have a unique port number assigned to them by the server. Typically the number will be above 8,000.
Destination Port	The Destination Port is a 16 bit number that Indicates the upper level service that the source wishes to communicate with at the destination.
Length	The Length field is 16 bits long and indicates the length of the UDP datagram and has a maximum value of 65, 535 bytes and a minimum value of 8 bytes.
Checksum	The Checksum field is 16 bits long and calculates a checksum based on the UDP header, Data field and what is called the UDP Pseudo header. The UDP Pseudo header consists of the Source IP Address, Destination IP Address, Zero, IP Protocol field and UDP Length. The IP Protocol field value is 17 for UDP.
Data	The data field contains the IP header and data. The Data field may be padded with zero octets at the end (if necessary) to make a multiple of two octets

Table 4.11 Description of UDP header fields

.

4.7 IPv6 Address

Internet Protocol Version 6 (IPv6) is the latest revision of the Internet Protocol (IP), the communications protocol that routes traffic across the Internet.

It is intended to replace IPv4, which still carries the vast majority of Internet traffic. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

Every device on the Internet must be assigned an IP address for identification and location addressing in order to communicate with other devices. With the ever-increasing number of new devices like mobile phones, smart phones, home & industrial appliances, integrated telephony, sensor networks, distributed computing, gaming and on line business etc. are being driven by the internet increasingly. The network security and QoS making transition from IPv4 to IPv6 inevitable.

IPv6 uses a 128-bit address, allowing for approximately 340 trillion addresses in contrast to the IPv4 (32-bit address) which is limited to approximately 4.3 billion addresses.

IPv6 will eliminate the need for Network Address Translation (NAT); the IP security protocol suite (IPSec) has been built into the IPv6 architecture thereby making way for an intrinsic security mechanism with IPv6 implementation.

An IPv6 address is represented by 8 groups of 16-bit values, each group represented as 4 hexadecimal digits and separated by colons **(:)** called as Hex-colon notation.

e.g. **2001:0db8:0000:0000:0000:ff00:0042:8329**

An IPv6 address may be abbreviated by using one or more of the following rules:

1. Remove one or more leading zeroes from one or more groups of hexadecimal digits; this is usually done to either all or none of the leading zeroes. (For example, convert the group **0042 to 42**)

2. Omit one or more consecutive sections of zeroes, using a double colon **(::)** to denote the omitted sections. **The double colon may only be used once in any given address,** as the address would be indeterminate if the double colon was used multiple times. (For example, **2001:db8::1:2** is valid, but **2001:db8::1::2** is not permitted.)

Below is an example of these rules:

Initial address: **2001:0db8:0000:0000:0000:ff00:0042:8329**
After removing all leading zeroes: **2001:db8:0:0:0:ff00:42:8329**
After doing both: **2001:db8::ff00:42:8329**

Another example is the loopback address, which can be abbreviated to**:: 1** by using both rules above

Initial address: **0000:0000:0000:0000:0000:0000:0000:0001**
After removing all leading zeroes: **0:0:0:0:0:0:0:1**
After doing both**::1**

3. Dotted-quad notation

During the transition of the Internet from IPv4 to the IPv6 it is typical to operate in a mixed addressing environment, and for this purpose a special notation has been introduced to express IPv4-compatible IPv6 addresses by writing the final 32 bits of an address in the familiar IPv4 dotted-quad notation. For example, the IPv4-mapped IPv6 address**:: ffff:c000:0280** is usually written as **`::ffff:192.0.2.128`**, thus expressing clearly the original IPv4 address that was mapped to IPv6.

IPv6 Address Types:

IPv6 addresses are classified as **unicast addressing**, **anycast addressing**, and **multicast addressing.**

A unicast address identifies a single network interface. The Internet Protocol delivers packets sent to a unicast address to that specific interface.

An anycast address is assigned to a group of interfaces, usually belonging to different nodes. A packet sent to an anycast address is delivered to just one of the member interfaces, typically the *nearest* host, according to the routing protocol's definition of distance. Anycast addresses cannot be identified easily, they have the same format as unicast addresses, and differ only by their presence in the network at multiple points. Almost any unicast address can be employed as an anycast address.

A multicast address is also used by multiple hosts, which acquire the multicast address destination by participating in the multicast distribution protocol among the network routers. A packet that is sent to a multicast address is delivered to all interfaces that have joined the corresponding multicast group.

IPv6 does not implement broadcast addressing. Broadcast's traditional role is subsumed by multicast addressing to the *all-nodes* link-local multicast group **`ff02::1`**. However, the use of the all-nodes group is not recommended, and most IPv6 protocols use a dedicated link-local multicast group to avoid disturbing every interface in the network.

Address formats

Unicast and anycast addresses are typically composed of two logical parts: a 64-bit network prefix used for routing, and a 64-bit interface identifier used to identify a host

General unicast address format (routing prefix size varies)

bits	48 (or more)	16 (or fewer)	64
field	*routing prefix*	*subnet id*	*interface identifier*

Network interface.

The network prefix (the routing prefix combined with the subnet id) is contained in the most significant 64 bits of the address. The size of the routing prefix may vary; a larger prefix size means a smaller subnet id size. The bits of the subnet identifier field are available to the network administrator to define subnets within the given network.

The 64-bit interface identifier is automatically generated from the interface's MAC address using the modified EUI-64 format, obtained from a DHCPv6 server, automatically established randomly, or assigned manually.

A link-local address is also based on the interface identifier, but uses a different format for the network prefix.

Link-local address format

bits	10	54	64
field	prefix	zeroes	interface identifier

The prefix field contains the binary value **`1111111010`**. The 54 zeroes that follow make the total network prefix the same for all link-local addresses, rendering them non-routable.

IPv6 Networks:

An IPv6 network uses an address block that is a contiguous group of IPv6 addresses of a size that is a power of two. The leading set of bits of the addresses is identical for all hosts in a given network, and is called the network's address or routing prefix.

Network address ranges are written in CIDR notation. A network is denoted by the first address in the block (ending in all zeroes), a slash (`/`), and a decimal value equal to the size in bits of the prefix. For example, the network written as `2001:db8:1234::/48` starts at address `2001:db8:1234:0000:0000:0000:0000:0000` and ends at `2001:db8:1234:ffff:ffff:ffff:ffff:ffff`.

The routing prefix of an interface address may be directly indicated with the address by CIDR notation. For example, the configuration of an interface with address `2001:db8:a::123` connected to subnet `2001:db8:a::/64` is written as `2001:db8:a::123/64`.

IPv6 address space:

The management of IPv6 address allocation process is delegated to the Internet Assigned Numbers Authority (IANA) by the Internet Architecture Board and the Internet Engineering Steering Group. Its main function is the assignment of large address blocks to the regional Internet registries (RIRs), which have the delegated task of allocation to network service providers and other local registries. The IANA has maintained the official list of allocations of the IPv6 address space since December 1995.

Only one eighth of the total address space is currently allocated for use on the Internet, `2000::/3`, in order to provide efficient route aggregation, thereby reducing the size of the Internet routing tables; the rest of the IPv6 address space is reserved for future use or for special purposes. The address space is assigned to the RIRs in large blocks of `/23` up to `/12`.

The RIRs assign smaller blocks to local Internet registries that distributes them to users. These are typically in sizes from `/19` to `/32`. The addresses are typically distributed in `/48` to `/56` sized blocks to the end users.

Each RIR can divide each of its multiple `/23` blocks into 512 `/32` blocks, typically one for each ISP; an ISP can divide its `/32` block into 65536 `/48` blocks, typically one for each customer; customers can create 65536 `/64` networks from their assigned `/48` block, each having 2^{64} addresses. In contrast, the entire IPv4 address space has only 2^{32} (about 4.3×10^{9}) addresses.

By design, only a very small fraction of the address space will actually be used. The large address space ensures that addresses are almost always available, which makes the use of network address translation (NAT) for the purposes of address conservation completely unnecessary.

Special allocation:

To allow for provider changes without renumbering, provider-independent address space – assigned directly to the end user by the RIRs – is taken from the special range `2001:678::/29`.

Internet Exchange Points (IXPs) are assigned special addresses from the range `2001:7f8::/29` for communication with their connected ISPs. Root name servers have been assigned addresses from the same range.

Reserved anycast addresses:

The lowest address within each subnet prefix (the interface identifier set to all zeroes) is reserved as the "subnet-router" anycast address. Applications may use this address when talking to any one of the available routers, as packets sent to this address are delivered to just one router.

The 128 highest addresses within each `/64` subnet prefix are reserved to be used as anycast addresses. These addresses usually have the 57 first bits of the interface identifier set to `1`, followed by the 7-bit anycast ID. Prefixes for the network, including subnets, are required to have a length of 64 bits, in which case the universal/local bit must be set to `0` to indicate the address is not globally unique. The address with value `0x7e` in the 7 least-significant bits is defined as a mobile IPv6 home agents anycast address. The address with value `0x7f` (all bits `1`) is reserved and may not be used. No more assignments from this range are made, so values `0x00` through `0x7d` are reserved as well.

Special addresses:

There are a number of addresses with special meaning in IPv6:

`Unicast Addresses:`

Unspecified address:

`::/128` — The address with all zero bits is called the unspecified address (corresponding to `0.0.0.0/32` in IPv4).

This address must never be assigned to an interface and is to be used only in software before the application has learned its host's source address appropriate for a pending connection. Routers must not forward packets with the unspecified address. Applications may be listening on one or more specific interfaces for incoming connections, which are shown in listings of active internet connections by a specific IP address (and a port number, separated by a colon). When the unspecified address is shown it means that an application is listening for incoming connections on all available interfaces.

Default route:

`::/0` — The default unicast route address (corresponding to `0.0.0.0/0` in IPv4).

Local addresses:

`::1/128` — The loopback address is a unicast local host address. If an application in a host sends packets to this address, the IPv6 stack will loop these packets back on the same virtual interface (corresponding to `127.0.0.0/8` in IPv4).

`fe80::/10` — Addresses in the link-local prefix are only valid and unique on a single link. Within this prefix only one subnet is allocated (54 zero bits), yielding an effective format of `fe80::/64`. The least significant 64 bits are usually chosen as the interface hardware address constructed in modified EUI-64 format. A link-local address is required on every IPv6-enabled interface—in other words, applications may rely on the existence of a link-local address even when there is no IPv6 routing. These addresses are comparable to the auto-configuration addresses `169.254.0.0/16` of IPv4.

Unique local addresses:

`fc00::/7` — Unique local addresses (ULAs) are intended for local communication. They are routable only within a set of cooperating sites (analogous to the private address ranges `10.0.0.0/8`, `172.16.0.0/12`, and `192.168.0.0/16` of IPv4). The addresses include a 40-bit pseudorandom number in the routing prefix intended to minimize the risk of conflicts if sites merge or packets are misrouted into the Internet.

IPv6 Migration:

IPv4 and IPv6 will continue to coexist, for some years, the true potential of the digital economy and next-generation services can only be realized once operators plan their IPv6 migration. And it is extremely important that all software and hardware aspects are clearly evaluated before launching a migration, as any gaps can have direct impact on the availability of many critical services

A variety of technologies are available to facilitate the migration to IPv6. These technologies are

1. **Dual stack** – support of both IPv4 and IPv6 on network devices
2. **Tunneling** – encapsulation of an IPv6 packet within an IPv4 packet for transmission over an IPv4 network
3. **Translation** – address (or) port translation of addresses such as via a gateway device (or) translation code in the TCP/IP code of the host (or) router

Dual-Stack Approach:

The dual-stack approach consists of implementing both IPv4 and IPv6 protocol stacks on devices requiring access to both network-layer technologies, including routers, other infrastructure devices and end-user devices. Such devices would be configured with both IPv4 and IPv6 addresses

Dual-stack deployment:

Deployment of dual-stacked devices sharing a common network interface implies the operation of both IPv4 and IPv6 over the same physical link.

Dual-stacked routers support IPv4 and IPv6 and route IPv4 packets among native IPv4 hosts and IPv6 packets among IPv6-capable hosts.

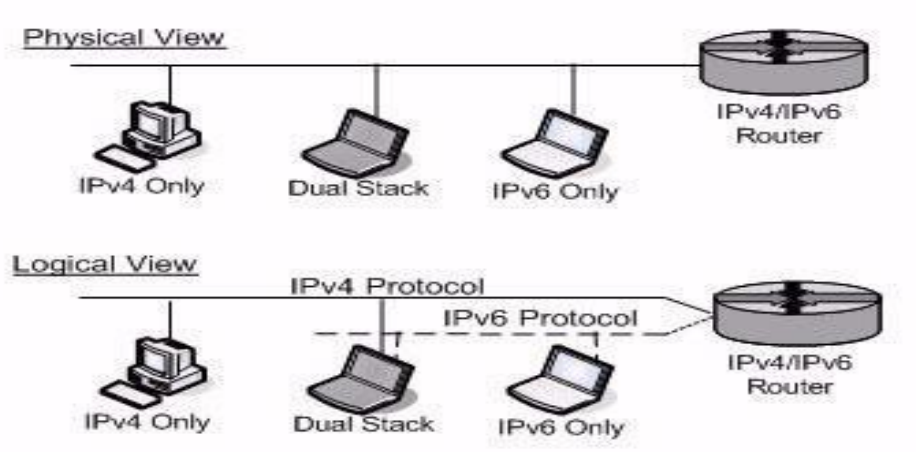


Fig. 4.9: Dual-stacked Network Perspectives

Tunneling Approaches:

A variety of tunneling technologies has been developed to support IPv4 over IPv6 as well as IPv6 over IPv4 tunneling. These technologies are generally categorized as configured (or) automatic. Configured tunnels are predefined, whereas automatic tunnels are created and torn down “on the fly.”

Tunnel types:

While the process of tunneling is the same for all types of tunnels, there is a variety of scenarios based on defined tunnel endpoints. Probably the most common configuration is a router-to-router tunnel, which is the typical approach for configured tunnels. Created and torn down “on the fly.”

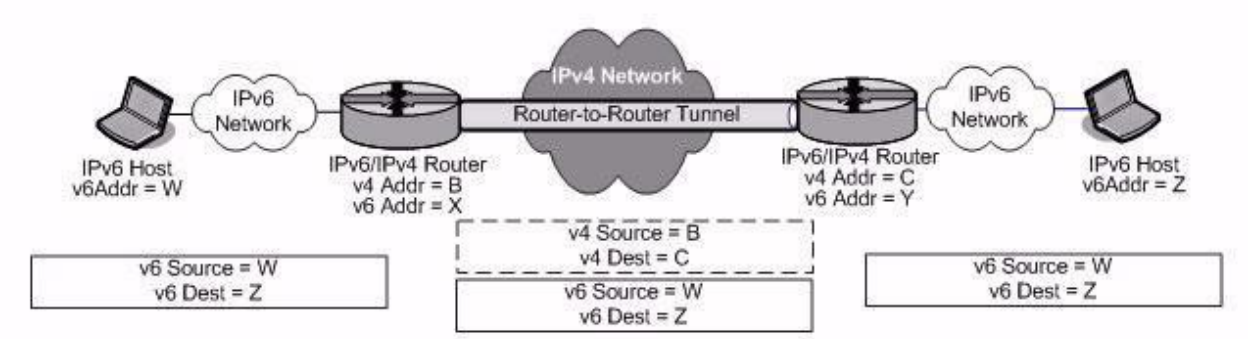


Figure 4.10: Router-to-Router Tunnel

In the above figure, the originating IPv6 host on the left has an IPv6 address of W. A packet destined for the host on the far end of the diagram with an IPv6 address of Z is sent to a router serving the subnet. This router (with an IPv4 address of B and an IPv6 address of X) receives the IPv6 packet. Configured to tunnel packets destined for the network on which host Z resides, the router encapsulates the IPv6 packet with an IPv4 header. The router uses its IPv4 address (B) as the source IPv4 address and the tunnel endpoint router (with an IPv4 address of C) as the destination address, which is depicted beneath the IPv4 network in the center of the figure. The endpoint router decapsulates the packet, stripping off the IPv4 header and routes the original IPv6 packet to its intended destination (Z).

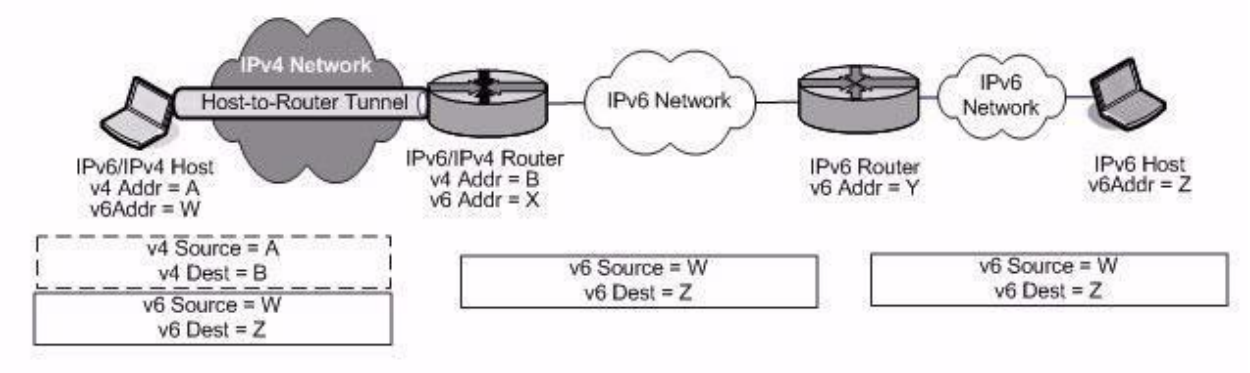


Figure 4.11: Host-to-Router Tunneling Configuration

Another tunneling scenario features an IPv6/IPv4 host capable of supporting both IPv4 and IPv6 protocols, tunneling a packet to a router, which in turn decapsulates the packet and routes it natively via IPv6. The tunneling mechanism is the same as in the router-to-router case, but the tunnel endpoints are different.

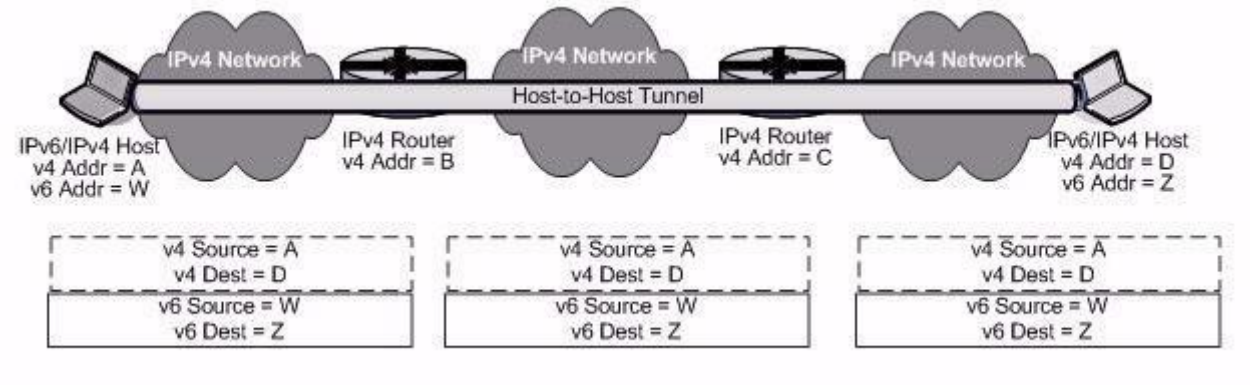


Figure 4.12: Host-to-Host Tunnel Configuration

The final tunneling configuration is one that spans end-to-end, from host-to-host. If the routing infrastructure has not yet been upgraded to support IPv6, this tunneling configuration enables two IPv6/IPv4 hosts to communicate via a tunnel over an IPv4 network

***Automatic tunnelling of IPv6 packets over IPv4 networks*:**

Tunnels are either configured or automatic. Configured tunnels are pre- defined by administrators in advance of communications, much as static routes would be pre- configured.

An automatic tunnel does not require pre-configuration. Tunnels are created based on information contained in the IPv6 packet, such as the source or destination IP address. The following automatic tunnelling techniques are described in this section:

1. 6 to 4 – automatic router-to-router tunneling based on a particular global address prefix and embedded IPv4 address
2. ISATAP – automatic host-to-router, router-to-host or host-to-host tunneling based on a particular IPv6 address format with inclusion of an embedded IPv4 address
3. 6 over 4 – automatic host-to-host tunneling using IPv4 multicasting
4. Tunnel Brokers – automatic tunnel setup by a server acting as a tunnel broker in assigning tunnel gateway resources on behalf of hosts requiring tunneling
5. Teredo – automatic tunnelling through NAT firewalls over IPv4 networks
6. Dual-Stack Transition Mechanism – enables automatic tunneling of IPv4 packets over IPv6 networks

Translation Approaches:

Translation techniques perform IPv4-to-IPv6 translation (and vice versa) at a particular layer of the protocol stack, typically the network, transport or application layer. Unlike tunneling, which does not alter the tunneled data packet, translation mechanisms do modify or translate IP packets commutatively between IPv4 and IPv6. Translation approaches are generally recommended in an environment with IPv6-only nodes communicating with IPv4-only nodes.

Stateless IP/ICMP Translation (SIIT) algorithm:

SIIT provides translation of IP packet headers between IPv4 and IPv6. SIIT resides on an IPv6 host and converts outgoing IPv6 packet headers into IPv4 headers, and incoming IPv4 headers into IPv6. To perform this task, the IPv6 host must be assigned an IPv4 address either configured on the host or obtained via a network service. When the IPv6 host desires to communicate with an IPv4 host, based on DNS resolution to an IPv4 address, the SIIT algorithm would convert the IPv6 packet header into IPv4 format. The SIIT algorithm recognizes such a case when the IPv6 address is an IPv4-mapped address, The mechanism to convert the resolved IPv4 address into an IPv4-mapped address is provided by bump-in-the-stack (BIS) or bump-in-the-API (BIA) techniques

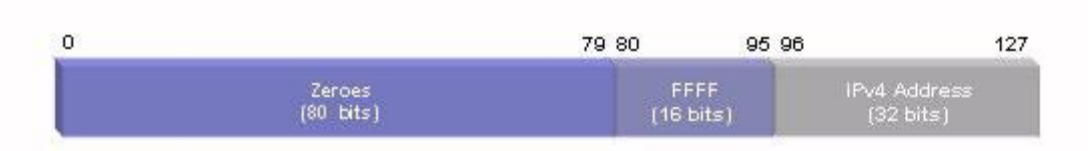


Figure 4.13: IPv4 Mapped Address Format

Based on the presence of the IPv4-mapped address format as the destination IP address, the SIIT algorithm performs header translation to yield an IPv4 packet for transmission via the data link and physical layers. The source IP address uses a different format, that of the IPv4-translated format,. The IPv4-mapped address format is invalid as a source address for tunneling .Therefore, its use as the source address would disqualify communications through any intervening tunnels. The use of the IPv4-translated format bypasses this potential restriction.

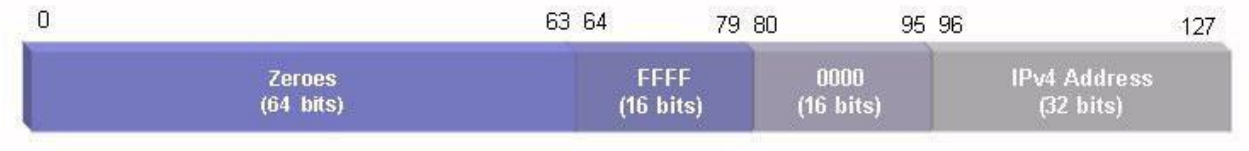


Figure 4.14: IPv4-Translated Address Format used within SIIT

4.8 MPLS ARCHITECTURE

MPLS is a mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next with the help of labels.

MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols. MPLS is a highly scalable, protocol agnostic, data-carrying mechanism.

In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol.

The primary benefit is to eliminate dependence on a particular Data Link Layer technology, such as ATM, frame relay, SONET or Ethernet, and eliminate the need for multiple Layer 2 networks to satisfy different types of traffic. MPLS belongs to the family of packet-switched networks.

4.8.1 How MPLS works

MPLS works by pre pending packets with an MPLS header, containing one or more ‘labels’. This is called a label stack as shown in fig 4.9.

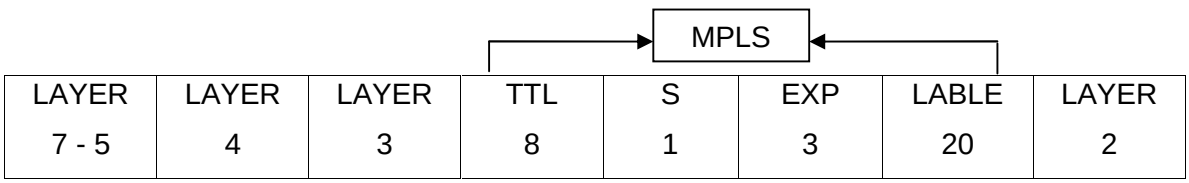


Fig 4.15: MPLS label stack

Each label stack entry contains four fields:

- A 20-bit label value.
- A 3-bit field for QoS priority (experimental).
- A 1-bit *bottom of stack* flag. If this is set, it signifies the current label is the last in the stack.
- An 8-bit TTL (time to live) field.

These MPLS labeled packets are switched after a Label Lookup/Switch instead of a lookup into the IP table. Label Lookup and Label Switching may be faster than usual RIB lookup because it can take place directly into the switching fabric and not the CPU.

Routers that are performing routing based only on Label Switching are called Label Switch Routers (LSR) and the Routers that are at the exit points of an MPLS network are called Label Edge Routers (LER). Remember that a LER is not usually the one that is popping the label. For more information see Penultimate Hop Popping.

Devices that function as ingress and/or egress routers are often called PE (Provider Edge) routers. Devices that function only as transit routers are similarly called P (Provider) routers. The job of a P router is significantly easier than that of a PE router, so they can be less complex and may be more dependable because of this.

When an unlabeled packet enters the ingress router and needs to be passed on to an MPLS tunnel, the router first determines the forwarding equivalence class the packet should be in, and then inserts one or more labels in the packet's newly created MPLS header. The packet is then passed on to the next hop router for this tunnel.

When a labeled packet is received by an MPLS router, the topmost label is examined. Based on the contents of the label a *swap*, *push* (*impose*) or *pop* (*dispose*) operation can be performed on the packet's label stack. Routers can have prebuilt lookup tables that tell them which kind of operation to do based on the topmost label of the incoming packet so they can process the packet very quickly. In a *swap* operation the label is swapped with a new label, and the packet is forwarded along the path associated with the new label.

In a *push* operation a new label is pushed on top of the existing label, effectively "encapsulating" the packet in another layer of MPLS. This allows the hierarchical routing of MPLS packets. Notably, this is used by MPLS VPNs.

In a *pop* operation the label is removed from the packet, which may reveal an inner label below. This process is called "de capsulation". If the popped label was the last on the label stack, the packet "leaves" the MPLS tunnel. This is usually done by the egress router.

During these operations, the contents of the packet below the MPLS Label stack are not examined. Indeed transit routers typically need only to examine the topmost label on the

stack. The forwarding of the packet is done based on the contents of the labels, which allows “protocol independent packet forwarding” that does not need to look at a protocol-dependent routing table and avoids the expensive IP longest prefix match at each hop.

At the egress router, when the last label has been popped, only the payload remains. This can be an IP packet, or any of a number of other kinds of payload packet. The egress router must therefore have routing information for the packet’s payload, since it must forward it without the help of label lookup tables. An MPLS transit router has no such requirement.

In some special cases, the last label can also be popped off at the penultimate hop (the hop before the egress router). This is called Penultimate Hop Popping (PHP). This may be interesting in cases where the egress router has lots of packets leaving MPLS tunnels, and thus spends inordinate amounts of CPU time on this. By using PHP, transit routers connected directly to this egress router effectively offload it, by popping the last label themselves.

MPLS can make use of existing ATM network infrastructure, as its labelled flows can be mapped to ATM virtual circuit a identifiers, and vice-versa.

4.8.2 Installing and removing MPLS paths

There are two standardized protocols for managing MPLS paths: CR-LDP (Constraint-based Routing Label Distribution Protocol) and RSVP-TE, an extension of the RSVP protocol for traffic engineering.

An MPLS header does not identify the type of data carried inside the MPLS path. If one wants to carry two different types of traffic between the same two routers, with different treatment from the core routers for each type, one has to establish a separate MPLS path for each type of traffic.

4.8.3 Comparison of MPLS versus IP

MPLS cannot be compared to IP as a separate entity because it works in conjunction with IP and IP’s IGP routing protocols. MPLS gives IP networks simple traffic engineering, the ability to transport Layer3 (IP) VPNs with overlapping address spaces, and support for Layer2 pseudo wires Routers with programmable CPUs and without TCAM/CAM or another method for fast lookups may also see a limited increase in performance.

MPLS relies on IGP routing protocols to construct its label forwarding table, and the scope of any IGP is usually restricted to a single carrier for stability and policy reasons. As there is still no standard for carrier-carrier MPLS it is not possible to have the same MPLS service (Layer2 or Layer3 VPN) covering more than one operator

4.8.4 MPLS local protection

In the event of a network element failure when recovery mechanisms are employed at the IP layer, restoration may take several seconds which is unacceptable for real-time applications (such as VoIP). In contrast, MPLS local protection meets the requirements of real-time applications with recovery times comparable to those of SONET rings (up to 50ms).

4.8.5 Comparison of MPLS versus ATM

While the underlying protocols and technologies are different, both MPLS and ATM provide a connection-oriented service for transporting data across computer networks. In both technologies connections are signaled between endpoints, connection state is maintained at each node in the path and encapsulation techniques are used to carry data across the connection. Excluding differences in the signaling protocols (RSVP/LDP for MPLS and PNNI for ATM) there still remain significant differences in the behavior of the technologies.

The most significant difference is in the transport and encapsulation methods. MPLS is able to work with variable length packets while ATM transports fixed-length (53 byte) cells. Packets must be segmented, transported and re-assembled over an ATM network using an adaption layer, which adds significant complexity and overhead to the data stream. MPLS, on the other hand, simply adds a label to the head of each packet and transmits it on the network.

Differences exist, as well, in the nature of the connections. An MPLS connection (LSP) is uni-directional - allowing data to flow in only one direction between two endpoints. Establishing two-way communications between endpoints requires a pair of LSPs to be established. Because 2 LSPs are required for connectivity, data flowing in the forward direction may use a different path from data flowing in the reverse direction. ATM point-to-point connections (Virtual Circuits), on the other hand, are bi-directional, allowing data to flow in both directions over the same path (bi-directional are only svc ATM connections; PVC ATM connections are uni-directional).

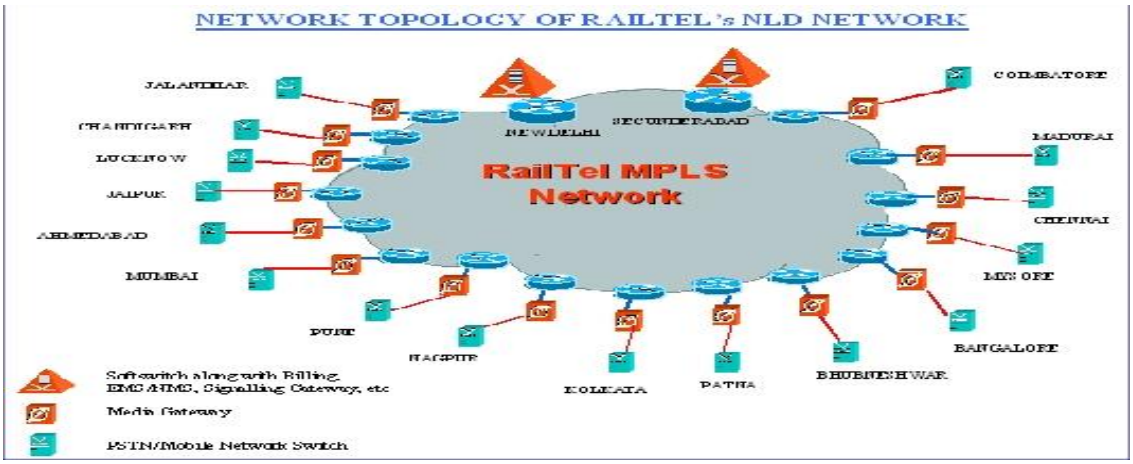
Both ATM and MPLS support tunneling of connections inside connections. MPLS uses label stacking to accomplish this while ATM uses *Virtual Paths*. MPLS can stack multiple labels to form tunnels within tunnels. The ATM Virtual Path Indicator (VPI) and Virtual Circuit Indicator (VCI) are both carried together in the cell header, limiting ATM to a single level of tunneling.

The biggest single advantage that MPLS has over ATM is that it was designed from the start to be complementary to IP. Modern routers are able to support both MPLS and IP natively across a common interface allowing network operators great flexibility in network design and operation. ATM's incompatibilities with IP require complex adaptation making it largely unsuitable in today's predominantly IP networks.

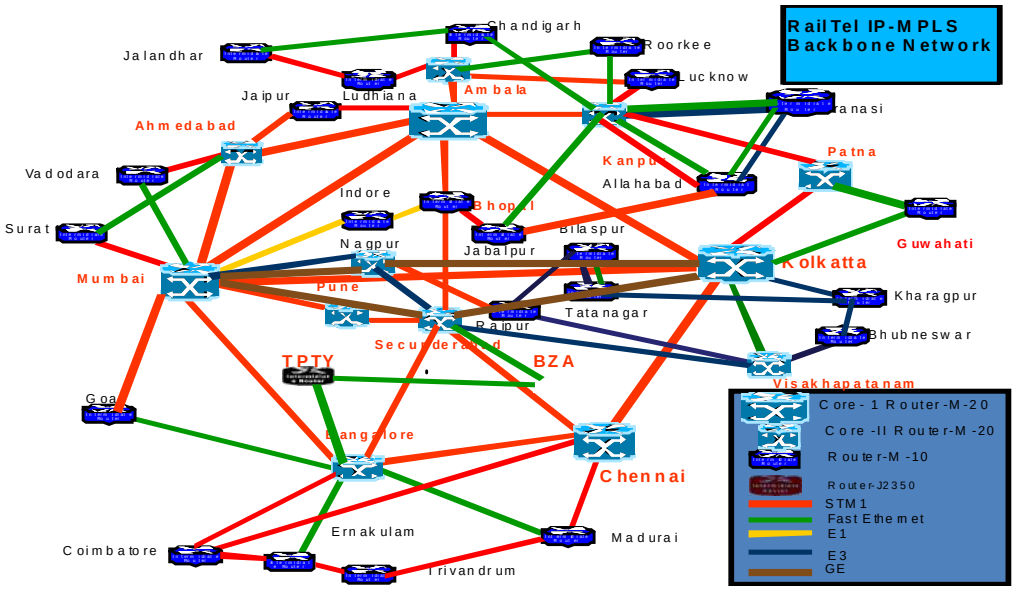
4.8.6 MPLS deployment

MPLS is currently in use in large “IP Only” networks, and is standardized by IETF in RFC 3031. In practice, MPLS is mainly used to forward IP data grams and Ethernet traffic. Major applications of MPLS are Telecommunications traffic engineering and MPLS VPN.

RailTel MPLS Network Connectivity



RailTel MPLS Backbone Connectivity



4.9.1 VPN (Virtual Private Network):

A virtual private network (VPN) extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

The VPN connection across the Internet is technically a wide area network (WAN) link between the sites but *appears to the user* as a private network link—hence the name "virtual private network".

Security mechanisms:

VPNs provide security through tunneling protocols and security procedures such as encryption. Their security model provides:

- Confidentiality such that even if traffic is sniffed, an attacker would only see encrypted data which they cannot understand
- Allowing sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any instances of transmitted messages having been tampered with

Secure VPN protocols include the following:

VPN (Virtual Private Network) is a network of secure links over a public IP infrastructure. Technologies that fit in this category include PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 tunneling protocol) and IPSec.

- IPSec (Internet Protocol Security) was developed by the Internet Engineering Task Force (IETF), and was initially developed for IPv6, which requires it. This standards-based security protocol is also widely used with IPv4. Layer 2 Tunneling Protocol frequently runs over IPSec. Its design meets most security goals: authentication, integrity, and confidentiality. IPSec functions through encrypting and encapsulating an IP packet inside an IPSec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic, as it does in the Open VPN project, or secure an individual connection. A number of vendors provide remote access VPN capabilities through SSL. (Secured Socket Layer) An SSL VPN can connect from locations where IPSec runs into trouble with Network Address Translation and firewall rules.
- Datagram Transport Layer Security (DTLS) is used in Cisco Any Connect VPN, to solve the issues SSL/TLS has with tunneling over UDP.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft's Secure Socket Tunneling Protocol (SSTP), introduced in Windows Server 2008 and in Windows Vista Service Pack 1. SSTP tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel.
- Secure Shell (SSH) VPN – Open SSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or inter-network links. Open SSH server provides a limited number of concurrent tunnels and the VPN feature itself does not support personal authentication.

Authentication:

Tunnel endpoints must authenticate before secure VPN tunnels can be established. User-created remote access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.

Network-to-network tunnels often use passwords or digital certificates, as they permanently store the key to allow the tunnel to establish automatically and without intervention from the user

Types of VPN:

VPNs can be either remote-access (connecting an individual computer to a network) or site-to-site (connecting two networks together). In a corporate setting, remote-access VPNs allow employees to access their company's intranet from home or while traveling outside the office, and site-to-site VPNs allow employees in geographically separated offices to share one cohesive virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, two IPv6 networks over an IPv4 network.

I

n the VPN topologies you can set up with PacketiX VPN, It can be divided into three types:

1. PC-to-PC VPN,
2. Remote Access VPN,
3. LAN-to-LAN VPN.

PC-to-PC VPN:

This is the simplest network topology to construct using PacketiX VPN. A PC-to-PC VPN is most useful under the following conditions:

- Only one to a few dozen computers will connect to the VPN.
- VPN Client can be installed on each of the client computers.
- The VPN network does not need to be able to connect to a physical LAN. (When you want the entire network to be the VPN only.)

In order to connect to the VPN using this method you must install VPN Client on each client computer. VPN Client will then directly connect to the layer 2 network created by the Virtual HUB on a VPN Server connected to the Internet.

Using this method you can set up a VPN which will allow only those computers connected to the Virtual HUB via a physical network such as the Internet to communicate with each other. Therefore, as long as functions such as local bridging or

routing on a client computer are not used the physical network will not affect the VPN and vice-versa.

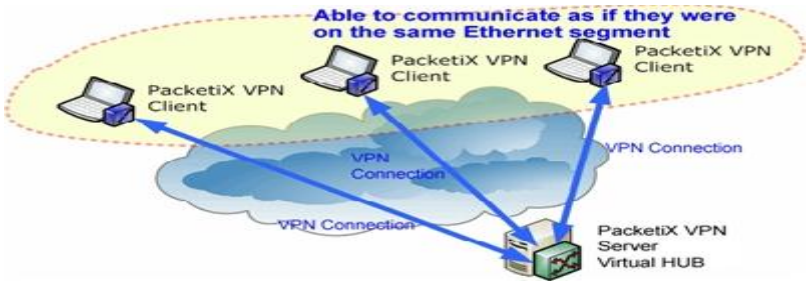


Fig. 4.16: PC-to-PC VPN

Furthermore, once you have VPN Client installed you can stay connected to a specified VPN server's Virtual HUB whenever the computer is on. By installing VPN Client on a server computer and having it stay connected to a specified VPN at all times, you can set up a server which can only be accessed by computers connected to that VPN.

Remote Access VPN:

A remote access VPN is used to allow remote access from an external location to a physical layer 2 network.

Using this type of VPN it is possible to connect to a company LAN from outside the office (for example, from an employee's house or from a hotel on a business trip) just as if they were connected by an extremely long Ethernet cable.

To use a remote access VPN you will make a connection between the network adapter connected to the LAN and the VPN Server's Virtual HUB. This is achieved via a local bridge, As a result, a VPN Client connected to the proper Virtual HUB will automatically be connected to the LAN connected by the local bridge, and will be able to operate through the VPN as if it was right there inside the office.

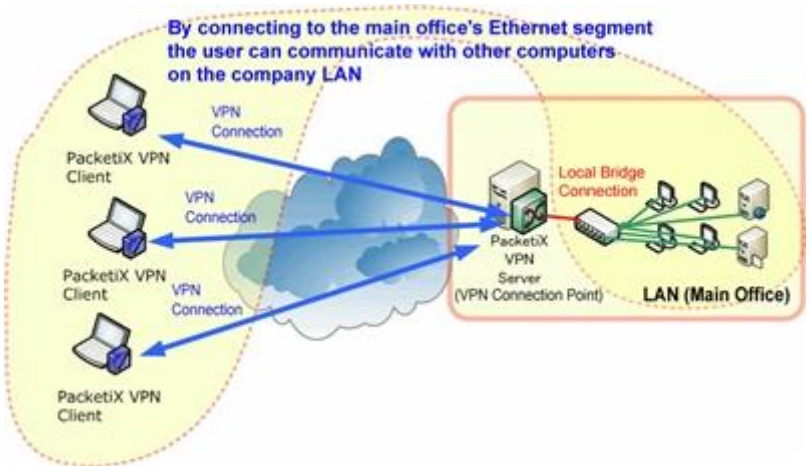


Fig. 4.17: Remote Access VPN

LAN-to-LAN VPN:

A LAN-to-LAN VPN links existing physical layer 2 networks at different sites together into a single network.

By using PacketiX VPN you can create a faster, more flexible, and more stable LAN-to-LAN network compared to current layer 3 based LAN-to-LAN connections such as private network services, frame relay services, or older VPN protocols such as L2TP/IPSec and layer 2 based connections such as wide area Ethernet.

To connect more than 2 LANs together you must install VPN Server on one LAN (such as at your company's main office) and VPN Bridge on all the others. Now you have two options. On each LAN, connect the Virtual HUB to the physical network adapter via a local bridge connection or create a cascade connection to the VPN Server from VPN Bridge. This will allow layer 2 segments at different sites to function as a single segment.

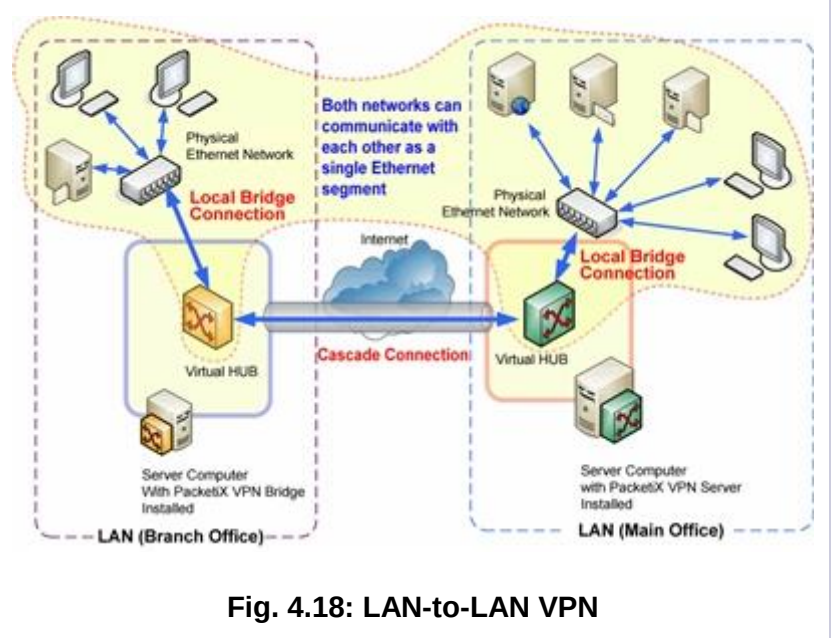


Fig. 4.18: LAN-to-LAN VPN

4.9.2 IPSecurity:

The Internet Architecture Board (IAB) issued a report entitled "Security in the Internet Architecture". The report stated the general consensus that the Internet needs more and better security, and it identified key areas for security mechanisms. Among these were the need to secure the network infrastructure from unauthorized monitoring and control of network traffic and the need to secure end-user-to-end-user traffic using authentication and encryption mechanisms.

The most serious types of attacks included IP spoofing, in which intruders create packets with false IP addresses and exploit applications that use authentication based on IP address; and various forms of eavesdropping and packet sniffing, in which attackers read transmitted information, including logon information and database contents.

In response to these issues, the IAB included authentication and encryption as necessary security features in the next-generation IP, which has been issued as IPv6. Fortunately, these security capabilities were designed to be usable both with the current IP (IPv4) and IPv6, meaning that vendors can begin offering these features now, and many vendors do now have some *IP Security Protocol* (IPSec) capability in their products.

Applications of IPSec

The Internet community has developed application-specific security mechanisms in numerous application areas, including electronic mail (*Privacy Enhanced Mail, Pretty Good Privacy* [PGP]), network management (*Simple Network Management Protocol Version 3* [SNMPv3]), Web access (Secure HTTP, *Secure Sockets Layer* [SSL]), and others.

IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.

The principal feature of IPSec that enables it to support these varied applications is that it can encrypt (or) authenticate all traffic at the IP level. Thus, all distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured.

An organization maintains LANs at dispersed locations. Traffic on each LAN does not need any special protection, but the devices on the LAN can be protected from the un-trusted network with firewalls.

The user workstation can establish an IPSec tunnel with the network devices to protect all the subsequent sessions. After this tunnel is established, the workstation can have many different sessions with the devices behind these IPSec gateways. The packets going across the Internet will be protected by IPSec but will be delivered onto each LAN as a normal IP packet.

Benefits of IPSec:

- When IPSec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- IPSec is below the transport layer (TCP, UDP), so is transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper layer software, including applications, is not affected.
- IPSec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- IPSec can provide security for individual users if needed. This feature is useful for offsite workers and also for setting up a secure virtual subnetwork within an organization for sensitive applications.

The Scope of IPSec

IPSec provides three main facilities: an authentication-only function, referred to as *Authentication Header* (AH), a combined authentication / encryption function called *Encapsulating Security Payload* (ESP), and a key exchange function.

For virtual private networks, both authentication and encryption are generally desired, because it is important both to (1) assure that unauthorized users do not penetrate the virtual private network and (2) assure that eavesdroppers on the Internet cannot read messages sent over the virtual private network. Because both features are generally desirable, most implementations are likely to use ESP rather than AH. The key exchange function allows for manual exchange of keys as well as an automated scheme.

Security Associations

A key concept that appears in both the authentication and confidentiality mechanisms for IP is the *Security Association* (SA). An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. If a peer relationship is needed, for two-way secure exchange, then two security associations are required. Security services are afforded to an SA for the use of AH or ESP, but not both. A security association is uniquely identified by three parameters:

Hence, in any IP packet, the security association is uniquely identified by the destination address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP).

An IPSec implementation includes a security association database that defines the parameters associated with each SA.

The key management mechanism that is used to distribute keys is coupled to the authentication and privacy mechanisms only by way of the security parameters index. Hence, authentication and privacy have been specified independent of any specific key management mechanism.

SA Selectors

IPSec provides the user with considerable flexibility in the way in which IPSec services are applied to IP traffic. IPSec provides a high degree of granularity in discriminating between traffic that is afforded IPSec protection and traffic that is allowed to bypass IPSec, in the former case relating IP traffic to specific SAs.

The means by which IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPSec) is the nominal *Security Policy Database* (SPD). In its simplest form, an SPD contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic. In more complex environments, there may be multiple entries that potentially relate to a single SA or multiple SAs associated with a single SPD entry.

Encryption and Authentication Algorithms

The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service. If the algorithm used to encrypt the payload requires cryptographic synchronization data, such as an *Initialization Vector* (IV), then this data may be carried explicitly at the beginning of the Payload Data field. If included, an IV is usually not encrypted, although it is often referred to as being part of the ciphertext. The current specification dictates that a compliant implementation must support the *Data Encryption Standard* (DES). A number of other algorithms have been assigned identifiers and could, therefore, be used for encryption; these include:

- Three-key triple DES
- RC5
- International Data Encryption Algorithm (IDEA)
- Three-key triple IDEA
- CAST
- Blowfish

It is now well known that DES is inadequate for secure encryption, so it is likely that many future implementations will use triple DES and eventually the *Advanced Encryption Standard* (AES). As with AH, ESP supports the use of a MAC, using HMAC.

Common Uses of IPSec in Real Networks

Figure 5 shows two ways in which the IPSec ESP service can be used. In the upper part of the figure, encryption (and optionally authentication) is provided directly between two hosts. Figure 5b shows how tunnel mode operation can be used to set up a *Virtual Private Network* (VPN). In this example, an organization has four private networks interconnected across the Internet. Hosts on the internal networks use the Internet for transport of data but do not interact with other Internet based hosts. By terminating the tunnels at the security gateway to each internal network, the configuration allows the hosts to avoid implementing the security capability. The former technique is supported by a transport mode SA, while the latter technique uses a tunnel mode SA.

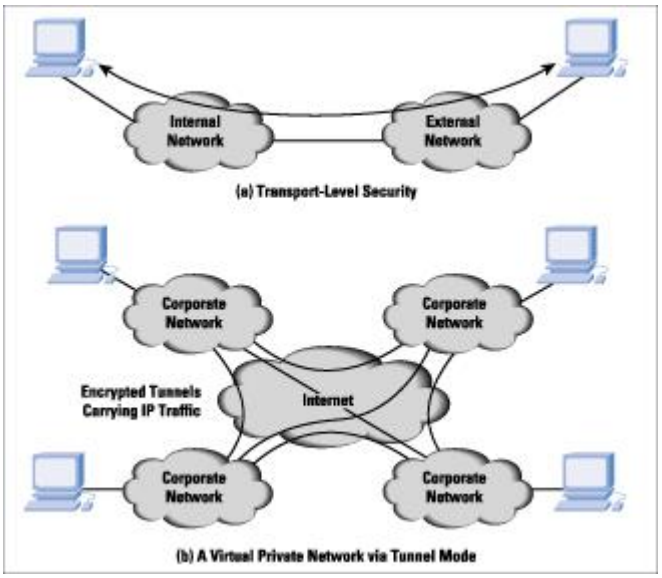


Figure 4.19: Transport-Mode versus Tunnel-Mode Encryption

Key Management

The key management portion of IPSec involves the determination and distribution of secret keys. The IPSec Architecture document mandates support for two types of key management:

- *Manual*: A system administrator manually configures each system with its own keys and with the keys of other communicating sys-tems. This is practical for small, relatively static environments.
- *Automated*: An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration. An automated system is the most flexible but requires more effort to configure and requires more software, so smaller installations are likely to opt for manual key management.

The default automated key management protocol for IPSec is referred to as *Internet Key Exchange* (IKE). IKE provides a standardized method for dynamically authenticating IPSec peers, negotiating security services, and generating shared keys. IKE has evolved from many different protocols and can be thought of as having two distinct capabilities. One of these capabilities is based on the *Internet Security Association and Key Management Protocol* (ISAKMP). ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes. ISAKMP by itself does not dictate a specific key exchange algorithm; rather, ISAKMP consists of a set of message types that enable the use of a variety of key exchange algorithms. The actual key exchange mechanism in IKE is derived from Oakley and several other key exchange protocols that had been proposed for IPSec. Key exchange is based on the use of the Diffie Hellman algorithm, but provides added security. In particular, Diffie-Hellman alone does not authenticate the two users that are exchanging keys, making the protocol vulnerable to impersonation. IKE includes mechanisms to authenticate the users.

Public Key Certificates

An important element of IPSec key management is the use of public key certificates. In essence, a public key certificate is provided by a trusted *Certificate Authority* (CA) to authenticate a user's public key. The essential elements include:

- Client software creates a pair of keys, one public and one private. The client prepares an unsigned certificate that includes a user ID and the user's public key. The client then sends the unsigned certificate to a CA in a secure manner.
- A CA creates a signature by calculating the hash code of the unsigned certificate and encrypting the hash code with the CA's private key; the encrypted hash code is the signature. The CA attaches the signature to the unsigned certificate and returns the now signed certificate to the client.

- The client may send its signed certificate to any other user. That user may verify that the certificate is valid by calculating the hash code of the certificate (not including the signature), decrypting the signature using the CA's public key, and comparing the hash code to the decrypted signature.

If all users subscribe to the same CA, then there is a common trust of that CA. All user certificates can be placed in the directory for access by all users. In addition, a user can transmit his or her certificate directly to other users. In either case, once B is in possession of A's certificate, B has confidence that messages it encrypts with A's public key will be secure from eavesdropping and that messages signed with A's private key are unforgeable.

If there is a large community of users, it may not be practical for all users to subscribe to the same CA. Because it is the CA that signs certificates, each participating user must have a copy of the CA's own public key to verify signatures. This public key must be provided to each user in an absolutely secure (with respect to integrity and authenticity) way so that the user has confidence in the associated certificates. Thus, with many users, it may be more practical for there to be many CAs, each of which securely provides its public key to some fraction of the users. In practice, there is not a single CA but rather a hierarchy of CAs. This complicates the problems of key distribution and of trust, but the basic principles are the same.

4.9.3 QoS (Quality of Service):

In telephony field, quality of service is a service that covers all aspects of necessity in the use of telecommunication service. The necessities include service response time, loss, signal-to-noise ratio, echo, interrupts, frequency response, loudness level, and so on. In the computer networking field, QoS is defined as the ability of the network to provide a service at an assured service level.

In Internet, QoS is a technology that acts as additional support to the best-effort service in handling data transfer during load congestions and superiorly response to more problems, such as latency, corrupted files, lost connection, jitter, out-of-order delivery, data loss or insufficient bandwidth.

QoS provides priority to different applications, users or data flow based on the load service requirements, and network conditions to ensure that the most important data reach the destination first.

A defined quality of service may be desired or required for certain types of network traffic, for example:

- Streaming media specifically
- IP telephony also known as Voice over IP (VoIP)
- Videoconferencing
- Circuit Emulation Service
- Safety-critical applications such as remote surgery where availability issues can be hazardous
- Network operations support systems either for the network itself, or for customers' business critical needs
- Online games where real-time lag can be a factor
- Industrial control systems protocols such as Ethernet/IP which are used for real-time control of machinery

These types of service are called **inelastic,** meaning that they require a certain minimum level of bandwidth and a certain maximum latency to function. By contrast, **elastic** applications can take advantage of however much or little bandwidth is available. Bulk file transfer applications that rely on TCP are generally elastic

Circuit switched networks, especially those intended for voice transmission, such as Asynchronous Transfer Mode (ATM) or GSM, have QoS in the core protocol and do not need additional procedures to achieve it. Shorter data units and built-in QoS were some of the unique selling points of ATM for applications such as video on demand.

End-to-end quality of service

End-to-end quality of service can require a method of coordinating resource allocation between one autonomous system and another.

The Internet Engineering Task Force (IETF) defined the Resource Reservation Protocol (RSVP) for bandwidth reservation. RSVP is an end-to-end bandwidth reservation protocol. The traffic engineering version, RSVP-TE, is used in many networks to establish traffic-engineered Multiprotocol Label Switching (MPLS) label-switched paths. The IETF also defined Next Steps in Signaling (NSIS) with QoS signaling as a target. NSIS is a development and simplification of RSVP.

4.9.4 Network Address Translation (NAT)

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

The most common form of network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255). The private addressing scheme works well for computers that only have to access resources inside the network, like workstations needing access to file servers and printers. Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.

A workstation inside a network makes a request to a computer on the Internet. Routers within the network recognize that the request is not for a resource inside the network, so they send the request to the firewall. The firewall sees the request from the computer with the internal IP. It then makes the same request to the Internet using its own public address, and returns the response from the Internet resource to the computer inside the private network. From the perspective of the resource on the Internet, it is sending information to the address of the firewall. From the perspective of the workstation, it appears that communication is directly with the site on the Internet. When NAT is used in this way, all users inside the private network access the Internet have the same public IP address when they use the Internet. That means only one public addresses is needed for hundreds or even thousands of users.

There are other uses for Network Address Translation (NAT) beyond simply allowing workstations with internal IP addresses to access the Internet. In large networks, some servers may act as Web servers and require access from the Internet. These servers are assigned public IP addresses on the firewall, allowing the public to access the servers only through that IP address. However, as an additional layer of security, the firewall acts as the intermediary between the outside world and the protected internal network. Additional rules can be added, including which ports can be accessed at that IP address. Using NAT in this way allows network engineers to more efficiently route internal network traffic to the same resources, and allow access to more ports, while restricting access at the firewall. It also allows detailed logging of communications between the network and the outside world.

Additionally, NAT can be used to allow selective access to the outside of the network, too. Workstations or other computers requiring special access outside the network can be assigned specific external IPs using NAT, allowing them to communicate with computers and applications that require a unique public IP address. Again, the firewall acts as the intermediary, and can control the session in both directions, restricting port access and protocols.

NAT is a very important aspect of firewall security. It conserves the number of public addresses used within an organization, and it allows for stricter control of access to resources on both sides of the firewall.

4.9.5 Access Control list (ACL):

ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface.

When activating an ACL on an interface, you must specify in which direction the traffic should be filtered:

- Inbound (as the traffic comes into an interface)
- Outbound (before the traffic exits an interface)

Inbound ACLs:

Incoming packets are processed before they are routed to an outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet will be discarded after it is denied by the filtering tests. If the packet is permitted by the tests, it is processed for routing.

Outbound ACLs:

Incoming packets are routed to the outbound interface and then processed through the outbound ACL.

Universal fact about Access control list

1. ACLs come in two varieties: Numbered and named
2. Each of these references to ACLs supports two types of filtering: standard and extended.
3. Standard IP ACLs can filter only on the source IP address inside a packet.
4. Whereas an extended IP ACLs can filter on the source and destination IP addresses in the packet.
5. There are two actions an ACL can take: permit or deny.
6. Statements are processed top-down.
7. Once a match is found, no further statements are processed—therefore, order is important.
8. If no match is found, the imaginary implicit deny statement at the end of the ACL drops the packet.
9. An ACL should have at least one permit statement; otherwise, all traffic will be dropped because of the hidden implicit deny statement at the end of every ACL.

No matter what type of ACL you use, though, you can have only one ACL per protocol, per interface, per direction. For example, you can have one IP ACL inbound on an interface and another IP ACL outbound on an interface, but you cannot have two inbound IP ACLs on the same interface.

Access List Ranges

Type	Range
IP Standard	1–99
IP Extended	100–199
IP Standard Expanded Range	1300–1999
IP Extended Expanded Range	2000–2699

Standard ACLs

A standard IP ACL is simple; it filters based on source address only. You can filter a source network or a source host, but you cannot filter based on the destination of a packet, the particular protocol being used such as the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP), or on the port number. You can permit or deny only source traffic.

Extended ACLs:

An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.

Named ACLs

One of the disadvantages of using IP standard and IP extended ACLs is that you reference them by number, which is not too descriptive of its use. With a named ACL, this is not the case because you can name your ACL with a descriptive name. The ACL named DenyMike is a lot more meaningful than an ACL simply numbered 1. There are both IP standard and IP extended named ACLs. Another advantage to named ACLs is that they allow you to remove individual lines out of an ACL. With numbered ACLs, you cannot delete individual statements. Instead, you will need to delete your existing access list and re-create the entire list.

Configuration Guidelines

- Order of statements is important: put the most restrictive statements at the top of the list and the least restrictive at the bottom.
- ACL statements are processed top-down until a match is found, and then no more statements in the list are processed.
- If no match is found in the ACL, the packet is dropped (implicit deny).
- Each ACL needs either a unique number or a unique name.
- The router cannot filter traffic that it, itself, originates.
- You can have only one IP ACL applied to an interface in each direction (inbound and outbound)—you can't have two or more inbound or outbound ACLs applied to the same interface. (Actually, you can have one ACL for each protocol, like IP and IPX, applied to an interface in each direction.)
- Applying an empty ACL to an interface permits all traffic by default: in order for an ACL to have an implicit deny statement, you need at least one actual permit or deny statement.
- Remember the numbers you can use for IP ACLs.Standard ACLs can use numbers ranging 1–99 and 1300–1999, and extended ACLs can use 100–199 and 2000–2699.
- Wildcard mask is not a subnet mask. Like an IP address or a subnet mask, a wildcard mask is composed of 32 bits when doing the conversion; subtract each byte in the subnet mask from 255.

There are two special types of wildcard masks:

0.0.0.0 and 255.255.255.255

0.0.0.0 Wildcard mask is called a host mask

255.255.255.255. If you enter this, the router will cover the address and mask to the keyword any.

Placement of ACLs:

Standard ACLs should be placed as close to the destination devices as possible. Extended ACLs should be placed as close to the source devices as possible.

Because a standard access list filters only traffic based on source traffic, all you need is the IP address of the host or subnet you want to permit or deny. ACLs are created in global configuration mode and then applied on an interface. The syntax for creating a standard ACL is

4.9.6 Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks.

The basic steps involved in VoIP are conversion of the analog voice signal to digital format and compression/translation of the signal into Internet protocol (IP) packets for transmission over the Internet; the process is reversed at the receiving end.

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. Codec use is varied between different implementations of VoIP (and often a range of codecs are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs.

VoIP has been implemented in various ways using both proprietary and open protocols and standards. Examples of technologies used to implement Voice over Internet Protocol include:

- H.323
- IMS
- SIP
- RTP

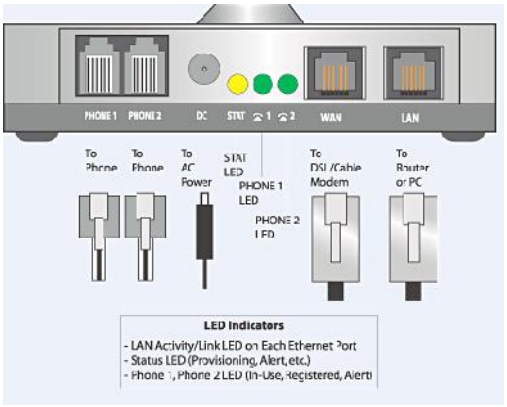


Fig 4.20 VoIP connection

There are three common methods of connecting to VoIP service providers as shown in fig 4.10 above.

- An Analog Telephone Adapter (ATA) may be connected between an IP network (such as a broadband connection) and an existing telephone jack in order to provide service nearly indistinguishable from PSTN providers on all the other telephone jacks in the residence. This type of service, which is fixed to one location, is generally offered by

broadband Internet providers such as cable companies and telephone companies as a cheaper flat-rate traditional phone service.

- Dedicated VoIP phones are phones that allow VoIP calls without the use of a computer. Instead they connect directly to the IP network (using technologies such as Wi-Fi or Ethernet). In order to connect to the PSTN they usually require service from a VoIP service provider; most people therefore will use them in conjunction with a paid service plan.
- A soft phone (also known as an Internet phone or Digital phone) is a piece of software that can be installed on a computer that allows VoIP calling without dedicated hardware.

PSTN and mobile network providers

It is becoming increasingly common for telecommunications providers to use VoIP telephony over dedicated and public IP networks to connect switching stations and to interconnect with other telephony network providers; this is often referred to as "IP backhaul".

Many telecommunications companies are looking at the IP Multimedia Subsystem (IMS) which will merge Internet technologies with the mobile world, using a pure VoIP infrastructure. It will enable them to upgrade their existing systems while embracing Internet technologies such as the Web, email, instant messaging, presence, and video conferencing. It will also allow existing VoIP systems to interface with the conventional PSTN and mobile phone networks.

"Dual mode" telephone sets, which allow for the seamless handover between a cellular network and a Wi-Fi network, are expected to help VoIP become more popular.

4.9.7 Advantages & Benefits

Because of the bandwidth efficiency and low costs that VoIP technology can provide, businesses are gradually beginning to migrate from traditional copper-wire telephone systems to VoIP systems to reduce their monthly phone costs.

VoIP solutions aimed at businesses have evolved into "unified communications" services that treat all communications—phone calls, faxes, voice mail, e-mail, Web conferences and more—as discrete units that can all be delivered via any means and to any handset, including cell phones. Two kinds of competitors are competing in this space: one set is focused on VoIP for medium to large enterprises, while another is targeting the small-to-medium business (SMB) market. VoIP runs both voice and data communications over a single network, which can significantly reduce infrastructure costs.

The prices of extensions on VoIP are lower than for PBXs and key systems. VoIP switches run on commodity hardware, such as PCs or Linux systems, so they are easy to configure and troubleshoot. Rather than closed architectures, these devices rely on standard interfaces.

VoIP devices have simple, intuitive user interfaces, so users can often make simple system configuration changes. Dual-mode cell phones enable users to continue their conversations as they move between an outside cellular service and an internal Wi-Fi network, so that it is no longer necessary to carry both a desktop phone and a cell phone. Maintenance becomes simpler as there are fewer devices to oversee.

4.9.8 Operational cost

VoIP can be a benefit for reducing communication and infrastructure costs. Examples include:

- Routing phone calls over existing data networks to avoid the need for separate voice and data networks.
- Conference calling, IVR, call forwarding, automatic redial, and caller ID features that traditional telecommunication companies (Telco's) normally charge extra for are available free of charge from open source VoIP implementations such as Asterisk or Free SWITCH.
- Costs are lower, mainly because of the way Internet access is billed compared to regular telephone calls. While regular telephone calls are billed by the minute or second, VoIP calls are billed per megabyte (MB). In other words, VoIP calls are billed per amount of information (data) sent over the Internet and not according to the time connected to the telephone network. In practice the amount charged for the data transferred in a given period is far less than that charged for the amount of time connected on a regular telephone line.

4.9.9 Flexibility

VoIP can facilitate tasks and provide services as shown in **fig 4.11** that may be more difficult to implement using the PSTN. Examples include:

- The ability to transmit more than one telephone call over a single broadband connection without the need to add extra lines.
- Secure calls using standardized protocols (such as Secure Real-time Transport Protocol.) Most of the difficulties of creating a secure telephone connection over

traditional phone lines, such as digitizing and digital transmission, are already in place with VoIP. It is only necessary to encrypt and authenticate the existing data stream.

- Location independence. Only a sufficiently fast and stable Internet connection is needed to get a connection from anywhere to a VoIP provider.
- Integration with other services available over the Internet, including video conversation, message or data file exchange during the conversation, audio conferencing, managing address books, and passing information about whether other people are available to interested parties.

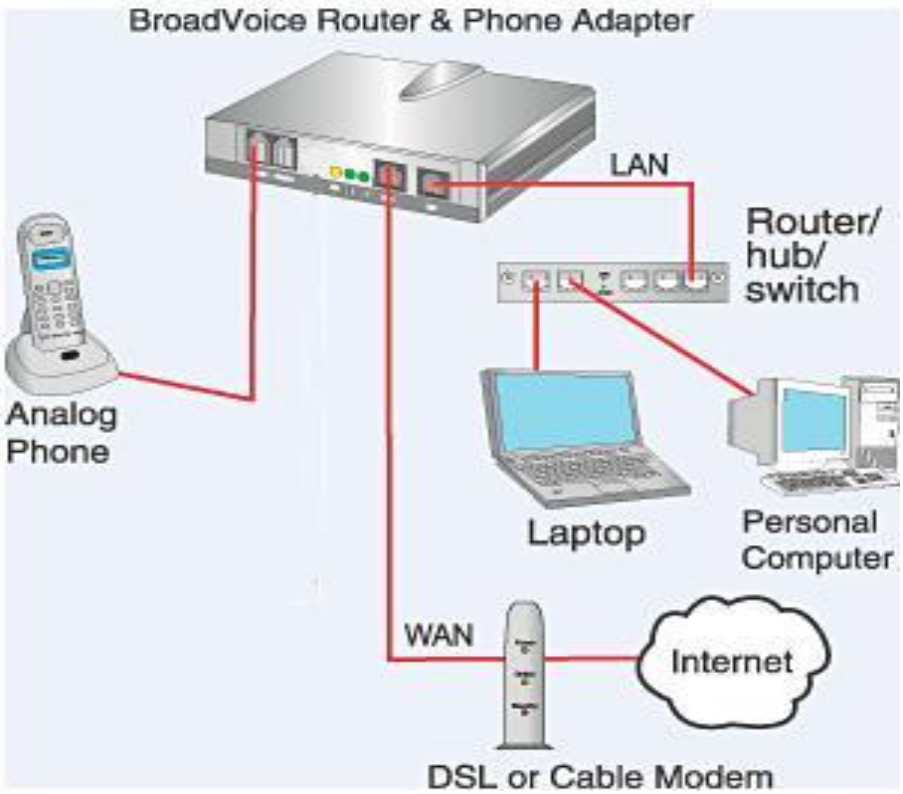


Fig 4.21 VoIP services

Review Questions:

Subjective:

1. What is Internet Protocol (IP)? How it is related to functioning of network?
2. Discuss IP addressing scheme in detail?
3. Why sub netting is required in Networks? Mention the methods for the same?
4. What is routing? How routing is accomplished in Networks? Mention different methods of routing?
5. Draw & explain IP datagram structure?
6. Explain how Router is a WAN device? What functions it performs in Networks?
7. How Routers are intelligent? Mention the elements that make the Router to decide the routes for movement of packets?
8. What is MPLS? Explain briefly?

Objective:

1. Identify the class of IP address 191.1.2.3.

   a) Class A b) Class B c) Class C d) Class D

2. A subnet mask in class B has nineteen 1s. How many subnets does it define?

   a) 128 b) 8 c) 32 d) 64

3. Given the IP address 18.250.31.14 and the subnet mask 255.255.0.0, what is the subnet address?

   a) 18.9.0.14 b) 18.0.0.14 c) 18.31.0.14 d) 18.250.0.0

4. _____ is a client-server program that provides an IP address, subnet mask, IP address of a router, and IP address of a name server to a computer.

   a) NAT b) DHCP c) CIDR d) ISP

5. In _____, each packet of a message need not follow the same path from sender to receiver.

   a) The virtual approach to packet switching
   b) The datagram approach to packet switching
   c) Message switching
   d) None of the above

6. In _____ routing, the mask and destination addresses are both 0.0.0.0 in the routing table.

   a) Default b) Next-hop c)Network-specific d)Host-specific

7. In which type of switching do all the packets of a message follow the same channels of a path?

   a) Virtual circuit packet switching b) Message switching
   c) Datagram packet switching d)None of the above

8. A routing table contains _____.

a) The destination network ID
b) The hop count to reach the network
c) The router ID of the next hop
d) All the above

9. An area border router can be connected to _____

a) Only another router b) Only another network
c) Only another area border router d) Another router or another network

10. Which type of network using the OSPF protocol can have five routers attached to it?

a) Transient b) Stub c) Point-to-point d) All the above

11. Which layer produces the OSPF message?

a) Data link b) Transport c) Application d) Network

11. OSPF is based on _____.

a) Distance vector routing
b) Path vector routing
c) Link state routing
d) (A) and (B)

12. _____ is a multicasting application.

a) Teleconferencing
b) Distance learning
c) Information dissemination
d) All the above

13. Dijkstra's algorithm is used to _____.

a) Create LSAs
b) Flood an internet with information
c) Create a link state database
d) Calculate the routing tables

14. RIP is based on _____.

a) Link state routing
b) Dijkstra's algorithm
c) Path vector routing
d) Distance vector routing

CHAPTER-5

LONG DISTANCE DATA TRANSMISSION

In this chapter, following topics which are applicable to Railway owned networks (PRS, FOIS, UTS etc.,), Internet / Railnet connectivity over a Digital Subscriber Loop and extending ISDN are covered.

5.0 Modem

A modem is like a telephone set for a computer. Modems let digital devices like computers talk to each other over the ordinary analog telephone system.

5.0.1 Modem working

The conventional Plain Old Telephone System (POTS) is more than 100-years old now. Another common term for POTS is the PSTN (Public Switched Telephone Network). The PSTN was not designed for transmission of digital electronic computer signals, as electronic computers did not exist with the original design of the PSTN. The PSTN was originally designed only to send analog Voice frequency signals; therefore it can only pass low frequency analog signals in the range of 300-to-4000 cycles per second.

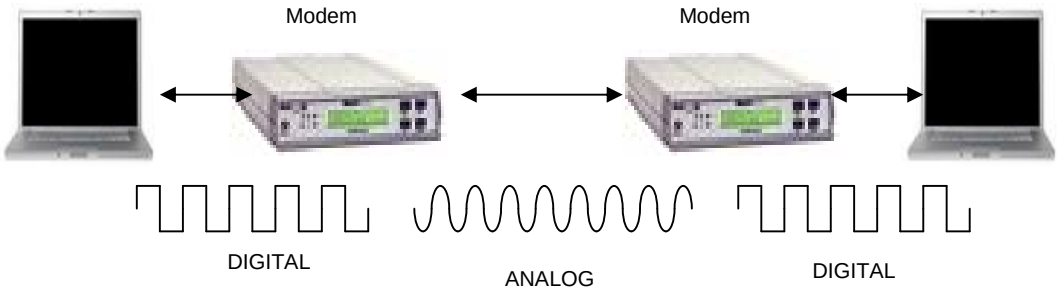


Fig. 5.1 Application of modem for Data communication over Analog media

Therefore, modems were invented to use the PSTN to send digital data as shown in fig 5.1 A modem changes, or modulates, digital data into electronic analog signals that the telephone network can carry.

At the other end of the connection, another modem demodulates, or interprets the telephone signals and converts them back to digital computer data signals. The word **"modem"** is an acronym that comes from combining the words "**Mo**dulate" and "**Dem**odulate."

i. Data sent over ordinary telephone lines

Fundamentally, modems send analog data bits sequentially over telephone lines similar to how the telegraph systems sent signals in the form of dots and dashes (Morse Code) to represent information. Morse code is a binary coding system that represents all the letters of the alphabet, punctuation and numerals. Like Morse code used in telegraph systems, modems also use a binary coding system called "ASCII" (American Standard

Computer Information Interchange) code. ASCII code is used to represent the alphabet, punctuation and numerals with a unique series of seven ones or zeros in all combinations, which gives the possibility of sending 128 different characters. High-speed modems can send data over the PSTN at rates ranging from 300-to-56,000 bits per second (bps).

ii. Modem speed

Signaling standards determine the modem's speed. Modem speed is measured in bits-per-second (bps). Bps refers to how many bits of data per second a modem can send and receive over the telephone line. 56K for example is 56,000 bits per second. 56K is defined under the ITU V.90 standard. The ITU V.34 standard defines an upper limit data speed of 33,600 bps or 33.6K bps. There are also several other lower speed standards defined by the ITU.

5.0.2 CLASSIFICATION OF MODEMS

i. Classifying Modems according to Range

a. Short Haul

Short haul modems are cheap solutions to systems of short ranges (up to 15 km), which use private lines and are not part of a public system. Short haul modems can also be used, even if the end-to-end length of the direct connection is longer than 15 km, when both ends of the line are served by the same central office in the telephone system. These lines are called "local loops". Short haul modems are distance-sensitive, because signal attenuation occurs as the signal travels through the line. The transmission rate must be lowered to ensure consistent and error-free transmission on longer distances.

Short haul modems tend to be cheaper than other modems for two reasons:

1. No circuitry is included in them to correct for differences between the carrier frequency of the demodulator and the frequency of the modulator.
2. Generally no circuitry is included to reduce/correct for noise rejection, which is less of a problem over short distances than over long distances.

There are two main types of short haul modems:

Analog modems

Using a simple modulation method, without sophisticated devices for error control or equalizers. These modems usually operate at a maximum rate of 9600 bps, but there are some which supports higher rates (up to 64,000 bps).

Line drivers

Increase the digital signal, which transmit to the communication channel and do not transmit the carrier signal, as conventional modems. Line drivers are very cheap and tiny and connect to the RS232 connector of the terminal (since they lack a power supply, they use the signal voltage of the DTE-DCE interface for DC power supply).

b. Voice Grade (VG)

Voice-grade modems are used for unlimited destination, using a moderate to high data rate. These modems are expensive and their maintenance and tuning are sophisticated. Communication channels are leased lines and dial-up.

Voice-band telephone network is used for data transmission. A user-to-user connection may be either dedicated or dialed. The links in the connection are the same in the two cases, and the only difference for the user is that for some impairment (particularly attenuation and delay distortion), a dedicated (*private* or leased) line is guaranteed to meet certain specifications, whereas a dialed connection can only be described statistically.

c. Wideband

Wideband modems are used in large-volume telephone-line multiplexing, dedicated computer-to-computer links. These modems exceed high data rates.

ii. Classifying Modems according to: Line Type

a. Dial up

Dial-up modems can establish point-to-point connections on the PSTN by any combination of manual or automatic dialing or answering. The quality of the circuit is not guaranteed, but all phone companies establish objectives. The links established are almost always 2-wire because 4-wire dialing is tedious and expensive.

b. Leased

Leased lines (usually 4-wire) are for the exclusive use of "leased-line" modems - either pair (in a simple point-to-point connection) or several (on a multidrop network for polling or a contention system). If the medium is the telephone network, their transmission characteristics are usually guaranteed to meet certain specifications, but if the link includes any radio transmission, the quality of it may be as variable as that of a switched (i.e. non dedicated) line.

iii. Classifying Modems according to: Operation Mode

a. Half Duplex

Half duplex means that signals can be passed in either direction, but not in both simultaneously

b. Full Duplex

Full duplex means that signals can be passed in either direction, simultaneously. Full duplex operation on a two-wire line requires the ability to separate a receive signal from

the reflection of the transmitted signal. This is accomplished by either FDM (frequency division multiplexing) in which the signals in the two directions occupy different frequency bands and are separated by filtering, or by Echo Canceling (EC).

The implication of the term *full-duplex* is usually that the modem can transmit and receive simultaneously at *full* speed.

c. Simplex

Simplex means that signals can be passed in one direction only. A remote modem for a telemeter system might be simplex and a 2-wire line with a common unidirectional amplifier is Simplex.

iv. Classifying Modems according to: Synchronization

a. Asynchronous Modems

Most of the modems that operate in slow and moderate rates, up to 1800 bps, are asynchronous (using asynchronous data). Asynchronous modems operate in FSK modulation and use two frequencies for transmission and another two for receiving.

In a 2-wire line, full duplex operation can be achieved by splitting the channel into two-sub channels as shown in fig. 5.2.

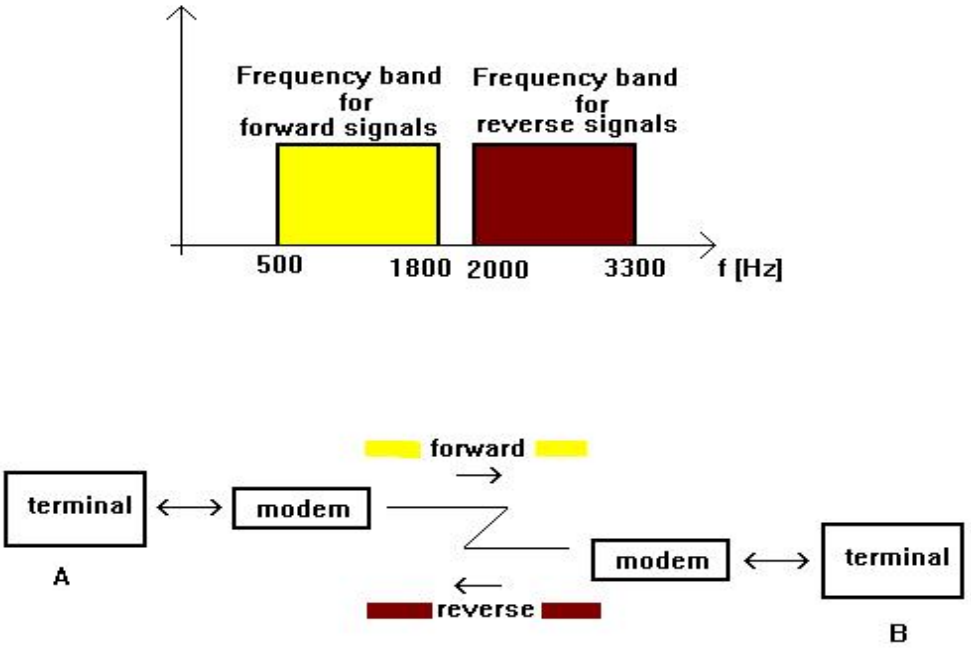


Fig. 5.2 Operating Asynchronous modem in a 2 Wire line

Asynchronous data is not accompanied by any clock, and the transmitting and receiving modems know only the nominal data rate. To prevent slipping of the data relative to the modems' clocks, this data is always grouped in very short blocks (characters) with framing bits (start and stop bits). The most common code used for this is the seven-bit ASCII code with even parity.

b. Synchronous Modems

Synchronous modems operate in the audio domain, at rates up to 28800 bps in audio lines, used in telephones systems (using synchronous data). The usual modulation methods are the phase modulation and integrated phase and amplitude (at higher rates than 4800 bps).

In synchronous modems, equalizers are used, in order to offset the misfit of the telephone lines. These equalizers are inserted in addition to the equalizers that sometimes already exist in the telephone lines.

These equalizers can be classified into three main groups:

Fixed/statistical equalizer - these equalizers offset the signal according to the average of the known attenuation in each frequency. Tuning the equalizer is sometimes done in the factory and stays fixed; usually they are used to operate at low rates in a dial up line.

Manually adjusted equalizer - these equalizers can be tuned to optimal performance to a given line. These equalizers should be re-tuned when the line is replaced and periodically. Specially, it should be tuned frequently when the line is of a low quality and it's parameters are changed frequently. Tuning is done using a button inside the modem (or on the external board).

Automatic equalizer - these equalizers are tuned automatically when the connection is established. Depending on the line quality in a specific moment, in a process of about 15ms to 25ms, after the first tuning, the equalizer samples the line continually and adjusts itself to the changed conditions, so the modem operates at each moment under optimal conditions. The fitness process operates, in some modems, at rates of 2400 times in a second.

Synchronous modems operate in the same manner asynchronous modems. However, synchronous modems operate at higher rates and since the requirements to transmit at these rates are increasing, most of the innovations are implemented for synchronous modems.
In synchronous modems the channel can be split for several consumers at various speeds. Modems who have this ability are called SSM - Split System Modem. These modems can use a simple split or a split using multipoint connection.

Synchronous data is accompanied by a clock signal. Synchronous data is almost always grouped in blocks, and it is the responsibility of the data source to assemble those blocks with framing codes and any extra bits needed for error detecting and/or correcting according to one of many different protocols (BISYNC, SDLC, HDLC, etc.). The data source and destination expect the modem to be transparent to this type of data; conversely, the modem can ignore the blocking of the data.

v. Classifying Modems according to: MODULATION

Communication channels like telephone lines are usually analog media. Analog media is a bandwidth-limited channel. In the case of telephone lines the usable bandwidth frequencies is in the range of 300 Hz to 3300 Hz.

Data communication means moving digital information from one place to another through communication channels. These digital information signals have the shape of square waves and the meaning of "0" and "1"

If such digital signals were transmitted on analog media the square waves of the digital signals would be distorted by the analog media. The receiver, which receives these distorted signals, will be unable to interpret accurately the incoming signals. These digital signals must be converted into analog signals so that the communication channels can carry the information from one place to another. The technique, which enables this conversion, is called *modulation like QAM, QPSK etc.*

i. Data Rate

The number of signal changes transmitted per unit of time is called the *data rate* of the modem. That rate is usually expressed in terms of a unit known as a baud. The baud is the number of times per second the line condition can switch from "1" to "0". Data rate and transmission speed, which is expressed in terms of bits per second, usually are not the same, as several bits may be transmitted through the channel by the modem in each signal change (a few bits can be transmitted as one symbol).

Claude Shannon showed, in 1948 that the maximum capacity (bit rate) of a bandwidth limited transmission line with limited signal to noise ratio is:

*C = W * log (1 + S/N) / log (2)*

Where C is the maximum capacity, W is the limited bandwidth and S/N is the power of the signal to noise ratio.

C = 3000 log2 (1+1000) = 3000 log2 (1024) = 3000 x 10 = 30kbps approx.

A telephone line, for example, has a bandwidth of 3000 Hz and maximum S/N of about 1000 (30db). Thus the theoretically maximum data rate that can be achieved is about 30 K bps (bits per second). Earliest modems that worked through telephone lines had 1.2 K bps. Today's modems reach data rates of 28.8 K bps.

Vi Modem Diagnostics:

Base band modems are provided with inbuilt loop diagnostics (V.54 protocol ITU-T standard) to check the integrity of the leased line connectivity.

V.54 is an ITU standard for various loop back tests that can be incorporated into modems for testing the telephone circuit and isolating transmission problems.

Operating modes includes local & remote loop backs with Digital as well as Analog tests.

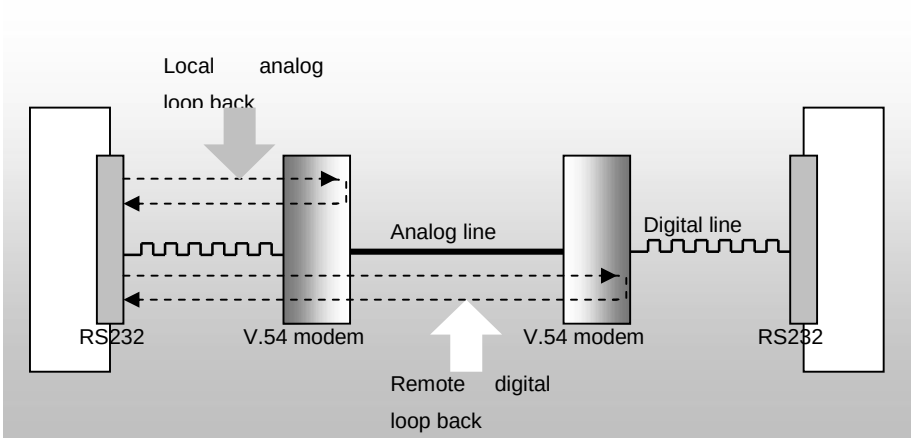
1. Local ANALOG loop: (**defined in the V.54 protocol as Loop 3**) tests the integrity of the Serial connector chord, the cable connecting the chord to the modem, and the local modem.

2. Remote DIGITAL loop: (**defined in the V.54 protocol as Loop 2**) tests the integrity of the Serial connector chord, the cable connecting the chord to the modem, the local modem, the carrier connection, and the remote modem.

Built in BERT, if activated (the modem starts generating and checking standard 511- bit pseudo random pattern) in **remote digital loop** test mode for quick fault isolation on communication link.

3. Local DIGITAL loop: To extend digital loop from local modem for fault isolation on communication link on remote side.

Bit-error-rate testing and loopbacks are used by carriers and ISPs to help resolve problems as well as test the quality of T1/E1 links. By early detection of poor quality links and quick problem isolation to improve network's quality of service



5.1 Terminal server

A terminal server is a device to connect multiple, possibly remote, input/output devices to a central processing unit.

5.1.1 History

Historically, a terminal server was a device that attaches to serial RS-232 devices, such as green screen 'VT' terminals or serial printers, and transports this traffic via TCP/IP TELNET, SSH or other vendor-specific protocol (i.e. LAT)

Originally, the first terminal servers were devices providing a connection between a so-called "green screen" dumb terminal and a host computer via an Ethernet connection. These terminals were also referred to as 80x24 since they included 24 lines of text displayed up to 80 columns across. Digital Equipment Corporation's DEC server 100 (1985), 200 (1986) and 300 (1991) are early examples of this technology. (An earlier version of this product, known as the DECSA Terminal Server was actually a test-bed or proof-of-concept for using the proprietary Local Area Transport (LAT) protocol in commercial production networks.) With the introduction of inexpensive flash memory components, Digital's later DEC server 700 (1991) and 900 (1995) no longer shared with their earlier units the need to download their software from a 'load host' (usually a Digital VAX or Alpha) using Digital's proprietary MOP protocol. In fact, these later terminal server products now also included much larger flash memory and full support for the TELNET part of the TCP/IP protocol suite.

Starting in the mid-1990s, several manufacturers such as US Robotics produced "modem terminal servers". Instead of having RS-232 ports, these would directly incorporate an analog modem. These devices were commonly used by Internet service providers to allow consumer dial-up. Modern versions interface to an ISDN PRI instead of having analog modem ports.

As of 2006 serial terminal servers are often used for connection to the console ports of UNIX servers. This then allows system administrators to connect to the servers over the network. This is important for rebooting the system and for hardware debugging, where the operating system will not boot correctly.

5.1.2 Modern usage

Lately the term 'terminal server' can mean either a network access server or a server operating system that provides a graphical user interface (GUI) of a Windows or a Linux desktop to user terminals that don't have this capability themselves. Alternatively, the desktop is provided to a remote computer in order to enable tele working.

The terminal server client is referred to as a thin client. Protocols that the client and server use to communicate with each other are Remote Desktop Protocol, Citrix ICA and NX technology.
Connection to Terminal Server remains fast, because in a Terminal Server environment, only what is actually displayed on the screen needs to be sent across the Internet/WAN, and mouse and keyboard commands are the only things that need to be sent back to the server.

Since all of the processing and storage occurs at the server, the requirements for client devices are minimal. Client devices can be anything from a thin client (network computer) to a fully configured personal computer (thick client). The speed and power of the client computer matters very little since it is doing very little in the process.

5.1.3 Modern terminal servers

Modern terminal servers are used in many different ways. They are usually implemented with one terminal server which can emulate up to 40 or 50 machines simultaneously. The end-user uses a workstation (typically a rather inexpensive computer) to connect to the terminal server. The workstation typically acts as if it were running a full version of Linux or Windows (by using Terminal Services). This is advantageous for several reasons:

One only needs to purchase a single very expensive terminal server rather than hundreds of expensive machines.

Any single instance on the terminal server has access to whatever resources are not being used at the moment. This setup is ideal in a situation where the end-user needs to Perform resource intensive tasks, but only intermittently. Since the terminal server may have very impressive specifications, this can help everyone have access to a powerful computer should they at some point need to perform such a task.

The user's computer state is saved on the terminal server. Many systems are set up so that the end-user can login to their workstation from any location that has internet access (for example, by using Remote Desktop Connection).

Lastly, it provides a centralized location where administrators can backup a single terminal server, rather than hundreds of individual machines.

5.2 Digital subscriber line & XDSL Modems

Telephone Company developed another technology called as DSL, to provide high speed access to Internet. DSL technology supports High-speed digital communication

Over the existing local loops. DSL technology is a set of technologies, each differing in first letter (ADSL, VDSL, HDSL and SDSL). The set is often referred to as XDSL, where X can be replaced by A, V, H, or S.

5.2.1 ADSL

The first technology in the set is asymmetric DSL (ADSL). ADSL, like a 56K modem, provides higher speed (bit rate) in the downstream direction (from the Internet to the resident) than in the upstream direction (from the resident to the Internet). That is the reason it is called asymmetric. Unlike the asymmetry in 56K modems, the designers of ADSL specifically divided the available bandwidth of the local loop unevenly for the residential customer. The service is not suitable for business customers who need a large bandwidth in both directions.

i. Using Existing Local Loops

One interesting point is that ADSL uses the existing local loops. But how does ADSL reach a data rate that was never achieved with traditional modems? The answer is that the twisted-pair local loop is actually capable of handling bandwidths up to 1.1MHz, but the filter installed at the end office of the telephone company where each local loop terminates limits the bandwidth to 4 KHz (sufficient for voice communication). If the filter is removed, however, the entire 1.1MHz is available for data and voice communications.

ii. Adaptive Technology

Unfortunately, 1.1 MHz is just the theoretical bandwidth of the local loop. Factors such as the distance between the residence and the switching office, the size of the cable, the signaling used, and so on affect the bandwidth. The designers of ADSL technology were aware of this problem and used an adaptive technology that tests the condition and bandwidth availability of the line before settling on a data rate. The data rate of ADSL is not fixed; it changes based on the condition and type of the local loop cable.

iii. Discrete Multi tone Technique

The modulation technique that has become standard for ADSL is called the discrete multi tone technique (DMT), which combines QAM and FDM. There is no set way that the bandwidth of a system is divided. Each system can decide on its bandwidth division. Typically, an available bandwidth of 1.104 MHz is divided into 256 channels. Each channel uses a bandwidth of 4.312 KHz, figure 5.3 shows how the bandwidth can be divided into the following:

- Voice. Channel 0 is reserved for voice communication
- Idle. Channels 1 to 5 are not used and provide a gap between voice and data communication.

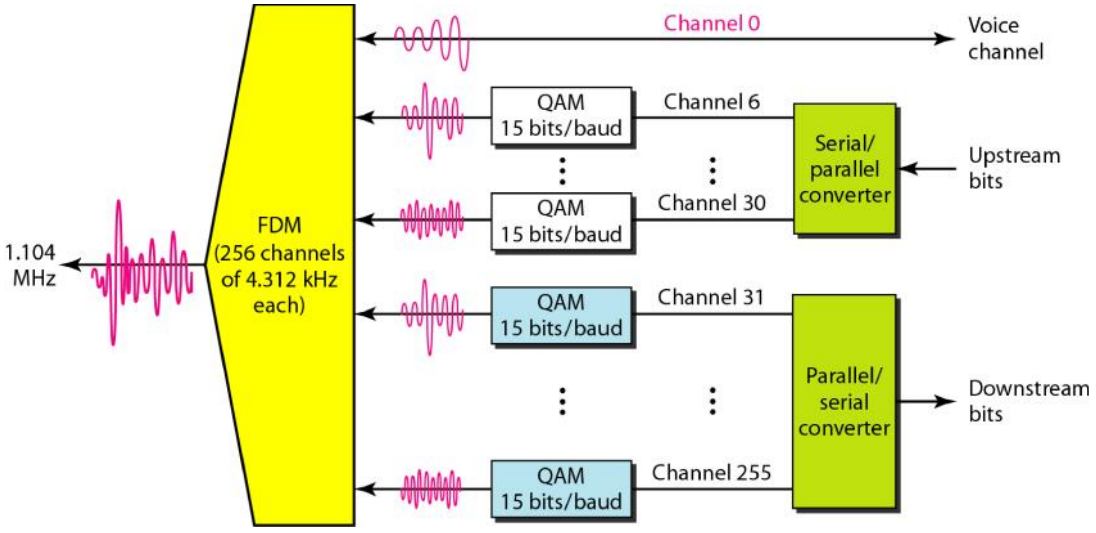


Fig. 5.3 Discrete Multi tone Technique

iv. Bandwidth division in ADSL

Refer Fig. 5.4

- Upstream data and control. Channels 6 to 30 (25 channels) are used for upstream data transfer and control. One channel is for control and 24 channels are for data transfer. If there are 24 channels, each using 4 KHz (out of 4.312 KHz available) with QAM modulation, we have 24 x 4000 x 15, or a 1.44 Mbps bandwidth, in the upstream direction. However, the data rate is normally below 500 kbps because some of the carriers are deleted at frequencies where the noise level is large. In other words, some of channels may be unused.

- Downstream data and control. Channels 31 to 255 (255 channels) are used for downstream data transfer and control. One channel is for control and 224 channels are for data. If there are 224 channels, we can achieve up to 224 x 4000 x 15, for 13.4 Mbps. However, the data rate is normally below 8 Mbps because some of the carriers are deleted at frequencies where the noise level is large. In other words, some of channels may be unused.

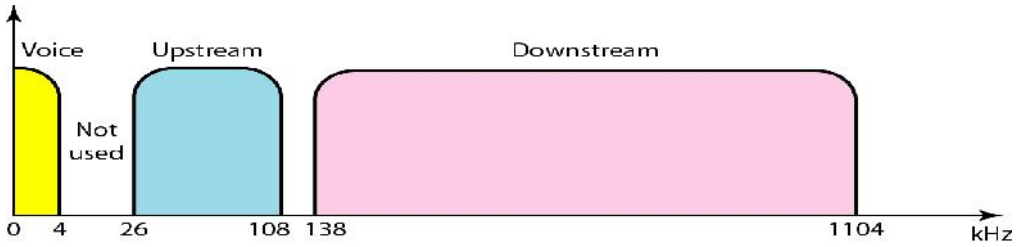


Fig. 5.4 Bandwidth division in ADSL

v. Customer Site: ADSL Modem

Figure 5.5 shows an ADSL modem installed at a customer's site. The local loop connects to a splitter, which separates voice and data communications. The ADSL modem modulates and demodulates the data, using DMT (Discrete Multitone Technique**)**, and creates downstream and upstream channels.

Note that the splitter needs to be installed at the customer's premises, normally by a technician from the telephone company. The voice line can use the existing telephone wiring in the house, but the data line needs to the installed by a professional. All this makes the ADSL line expensive. We have an alternative technology - Universal ADSL or (ADSL Lite).

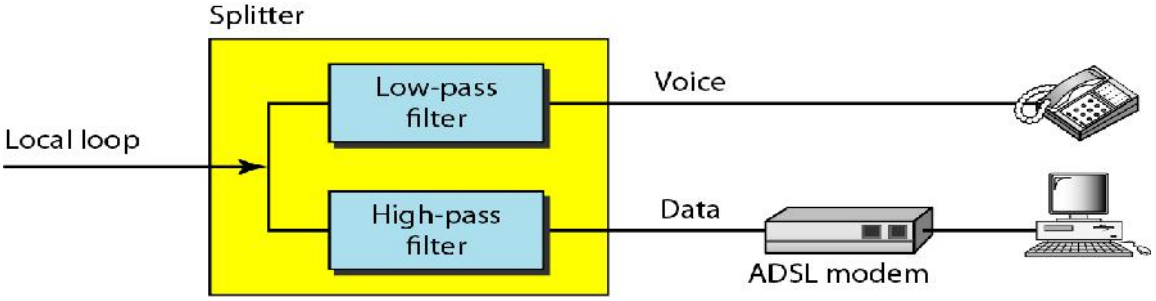


Fig. 5.5 Customer Site: ADSL modem

vi. Telephone Company Site: DSLAM

At the telephone company site, the situation is different. Instead of an ADSL modem, a device called a digital subscriber line access multiplexer (DSLAM) is installed that functions similarly. In addition, it packetizes the data to be sent to the Internet (ISP server). Figure 5.6 shows the configuration.

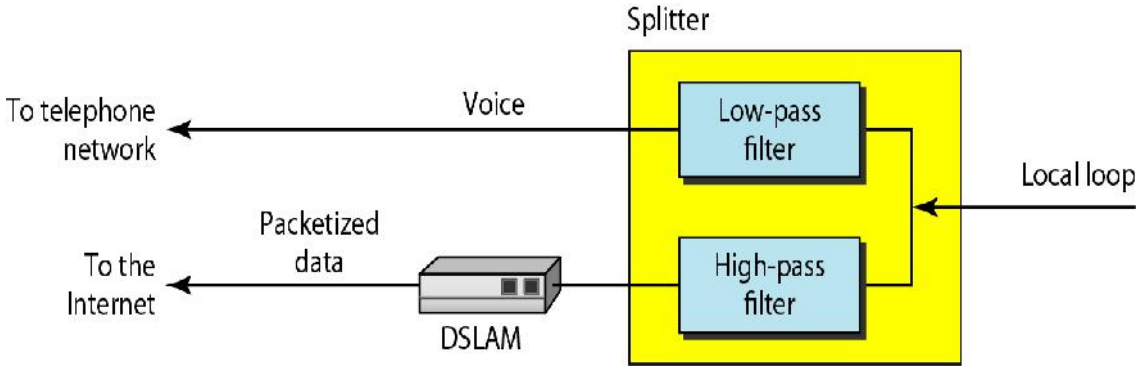


Fig. 5.6 Telephone Company Site: DSLAM

5.2.2 HDSL

The high-bit-rate digital subscriber line (HDSL) was designed as an alternative to the T-1 line (1.544 Mbps). The T-1 line uses alternate mark inversion (AMI) encoding which is very susceptible to attenuation at high frequencies. This limits the length of a T-1 line to 3200 ft (1 km). For longer distances, a repeater is necessary, which means increased costs.

HDSL uses 2B1Q encoding (see chapter4), which is less susceptible to attenuation. A data rate of 1.544 Mbps (sometimes up to 2 Mbps) can be achieved without repeaters upto a distance of 12,000 ft (3.86km). HDSL uses two twisted pairs (one pair for each direction) to achieve full-duplex transmission.

5.2.3 SDSL

The symmetric digital subscriber line (SDSL) is a one twisted- pair version of HDSL. It provides full-duplex symmetric communication supporting up to 768 kbps in each direction. SDSL which provides symmetric communication can be considered an alternative to ADSL. ADSL provides asymmetric communication, with a downstream bit rate that is much higher than the upstream bit rate. Although this feature meets the needs of most residential subscribers, ti is not suitable for business that sends and receives data in large volumes in both directions.

5.2.4 VDSL

The very high – bit-rate digital subscriber line (VDSL), and alternative approach that is similar to ADSL, uses coaxial, fiber-optic, or twisted-pair cable for short distance. The modulating technique is DMT. It provides a range of bit rates (25 to 55 Mbps) for upstream communication at distances of 3000 to 10,000 ft. The downstream rate is normally 3.2 Mbps.

5.2.5 Configurations

XDSL provides for both symmetric and asymmetric configurations as shown in table 5.1

Asymmetric	Symmetric
Bandwidth is higher in one direction	Bandwidth same in both directions
Suitable for Web Browsing	Suitable for video-conferencing

Table 5.1

5.2.6 Variations

In XDSL there are currently six (6) variations available p as shown in table 5.2

XDSL Technology	Meaning	Rate
DSL	Digital Subscriber Line	2 x 64Kbps circuit switched 1 x 16Kbps packet switched (similar to ISDN-BRI)
HDSL	High-bit-rate DSL	2.048Mbps over two pairs at a distance up to 4.2Km
S-HDSL/SDSL	Single-pair or Symmetric High-bit-rate DSL	768Kbps over a single pair
ADSL	Asymmetric DSL	up to 6Mbps in one direction
RADSL	Rate Adaptive DSL	An extension of ADSL which supports a variety of data rates depending upon the quality of the local loop
VDSL	Very High-bit-rate asymmetric DSL	Up to 52Mbps in one direction and 2Mbps in the other direction.

Table 5.2

5.3 ISDN (Integrated Services Digital Network)

Integrated Services Digital Network (ISDN) is comprised of digital telephony and data-transport services offered by regional telephone carriers. ISDN involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires. The emergence of ISDN represents an effort to standardize subscriber services, user/network interfaces, and network and internet work capabilities. ISDN applications include high-speed image applications (such as Group IV facsimile), additional telephone lines in homes to serve the telecommuting industry, high-speed file transfer, and videoconferencing. Voice service is also an application for ISDN. This chapter summarizes the underlying technologies and services associated with ISDN.

The ISDN services, protocols, frame formats are explained elaborately in TCS4 (ISDN Exchange) notes.

5.4 LAN extender:

A **LAN extender (**also **network extender** or **Ethernet extender**) is a device used to extend an Ethernet or network segment beyond its inherent distance limitation which is approximately 100 meters (330 ft) for most common forms of twisted pair Ethernet.

The extender forwards traffic between LANs transparent to higher network-layer protocols over distances that far exceed the limitations of standard Ethernet.

Extenders that use copper wire include 2 and 4 wire variants using unconditioned copper wiring (without load coils), to extend a LANs. Network extenders use various methods (line encodings), such as TC-PAM, 2B1Q or DMT, to transmit information.

The LAN extender (Ethernet-Extender) is used in pairs.
Different Types of LAN extenders:

- **2BASE-TL** — Full-duplex long reach Point-to-Point link over voice-grade copper wiring. 2BASE-TL PHY can deliver a minimum of 2 Mbit/s and a maximum of 5.69 Mbit/s over distances of up to 2700 m (9,000 ft), using ITU-T G.991.2 (G.SHDSL.bis) technology over a single copper pair.

- **10PASS-TS** — Full-duplex short reach Point-to-Point link over voice-grade copper wiring. 10PASS-TS PHY can deliver a minimum of 10 Mbit/s over distances of up to 750 m (2460 ft), using ITU-T G.993.1 (VDSL) technology over a single copper pair

Fig. 5.7 LAN Extender Unit

5.5 Media Converters:

Media Converters (also Ethernet-Fiber Converters) enable connections of UTP copper-based Ethernet equipment over a fiber optic link to take advantage of the benefits of fiber which include;

- ✓ Extending links over greater distances using fiber optic cable
- ✓ Protecting data from noise and interference
- ✓ Future proofing your network with additional bandwidth capacity

Copper-based Ethernet connections are limited to a data transmission distance of only 100 meters when using unshielded twisted pair (UTP) cable. By using an Ethernet to fiber conversion solution, fiber optic cabling can now be used to extend this link over a greater distance.

An Ethernet to Fiber Media Converter can also be used where there is high level of electromagnetic interference or EMI which is a common phenomenon found in industrial plants. This interference can cause corruption of data over copper-based Ethernet links. Data transmitted over fiber optic cable however is completely immune to this type of noise. An Ethernet to Fiber Optic Converter therefore enables you to inter-connect your copper-Ethernet devices over fiber ensuring optimal data transmission across the plant floor.

The copper transceiver used in an Ethernet-Fiber Converter transforms the signal from a UTP / RJ45 Ethernet link to one that can be used by a fiber optic transceiver. Media converters can connect to various optical fiber cable such as multimode, single mode or single strand fiber cable. Options exist for many distances to suit the needs of a particular Ethernet to fiber application. And, fiber interface connectors can be dual ST, dual SC, dual LC or single SC type.

Fig. 5.8 Media Converter

Review Questions:

Subjective:

1. What is Modem? Why it is require d in long distance data transmission?
2. What is Digital Subscriber Line (DSL)? Explain the working of DSL modems with a suitable diagram?

Objective:

1. Dial-up modems are
   a. Synchronous b) Simplex c) Asynchronous d) None of the above
2. Modem pair required for WAN connectivity over leased lines are
   a. Asynchronous V.35 + G.703 b) Synchronous V.35 + G.703
   c) Synchronous V.35 + V.35 d) None of the above
3. ADSL modem uses modulation method
   a. QAM + FDM b) TDM+FSK c) FDM+FSK d) All above
4. HDSL modem uses line coding technique
   a. HDB3 b) 2B1Q c) Manchester d) AMI
5. Modulation technique adopted for DSL modems are
   a. Frequency shift keying b) Discrete multi tone c) QPSK d) None of the above
6. DSLAM stands for ----------
7. ADSL is a widely accepted ---------- technology

CHAPTER-6

WIRELESS LAN

In this chapter topics which are most essential for "wireless LAN" are covered.

Topics are

- *WLAN*
- *Wi-Fi*
- *Access point*
- *WAP*
- *WLAN architecture*
- *IEEE 802.11 Protocol layer*
- *IEEE WLAN Standards*
- *Wi-Max*
- *Bluetooth*

6.0 WLANs

Provide wireless network communication over short distances using radio or infrared signals instead of traditional network cabling.

6.1 Wi-Fi (**wireless fidelity**)

Wi-Fi belongs to wireless local area network (WLAN) devices. Wi-Fi is often used as a synonym for IEEE 802.11 technology & it is also called as IP Radio. A Wi-Fi enabled device such as a personal computer, video game console, mobile phone, MP3 player or personal digital assistant can connect to the Internet when within range of a wireless network connected to the Internet.

Wi-Fi uses both single-carrier direct-sequence spread spectrum radio technology (part of the larger family of spread spectrum systems) and multi-carrier orthogonal frequency-division multiplexing (OFDM) radio technology. The deregulation of certain radio-frequencies for unlicensed spread spectrum deployment enabled the development of Wi-Fi products

6.2 Access points (AP)

Access points are specially configured nodes on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of WLAN radio signals. Access points used in home or small business networks are generally small, dedicated hardware devices featuring a built-in network adapter, antenna, and radio transmitter. Access points support **Wi-Fi** wireless communication standards.

6.3 Wireless Application Protocol (WAP)

WAP defines network architecture for content delivery over wireless networks. WAP implements several new networking protocols that perform functions similar to the well-known Web protocols HTTP, TCP and SSL. WAP protocol suite is ment to enable global wireless communication across different wireless technologies
e.g. GSM, GPRS, UMTS & 3G.

6.4 WLAN architecture

It consists of WLAN Stations (STA) & Access Point (AP) as building blocks.

- WLAN Stations (STA)
  - Locate & connect to access points to reach network resources.
  - Identified by an IEEE 48-bit data link control address
- Access Point (AP)
  - Connect WLAN stations to the wired or “Distribution” network
  - Bridges frames to / from WLAN and Distribution network
  - Identifies by 48-bit data link control address
  - Range at which stations can communicate with AP is the Basic Service Area

Service Set means all the devices associated with a specific local or enterprise 802.11 wireless LAN(s). There are a few interrelated terms associated with service sets.

6.4.1 Independent Basic Services Set (IBSS) / Ad hoc network

A single BSS can be used to form an ad hoc network, with 802.11 it is possible to create an ad-hoc network of client devices without a controlling Access Point as shown in fig 6.1 below called an Independent Basic Service Set (IBSS), in such case the SSID is chosen by the client device that starts the network, and broadcasting of the SSID is performed in a pseudo-random order by all devices that are members of the network. An ad-hoc network typically temporary in nature. They can be formed spontaneously anywhere and be dis-band after a limited period of time.

6.4.2 Basic Service Set (BSS):

It is the basic building block of the IEEE 802.11 architecture. A BSS is defined as a group of stations that co-ordinate their access to the medium under a given instance of the medium access control as shown in fig 6.1 below.

The geographical area covered by the BSS is known as the basic service area (BSA). A BSA may extend over an area with the diameter of tens of meters. Conceptually all the stations in a BSS can communicate directly with all other stations in a BSS.

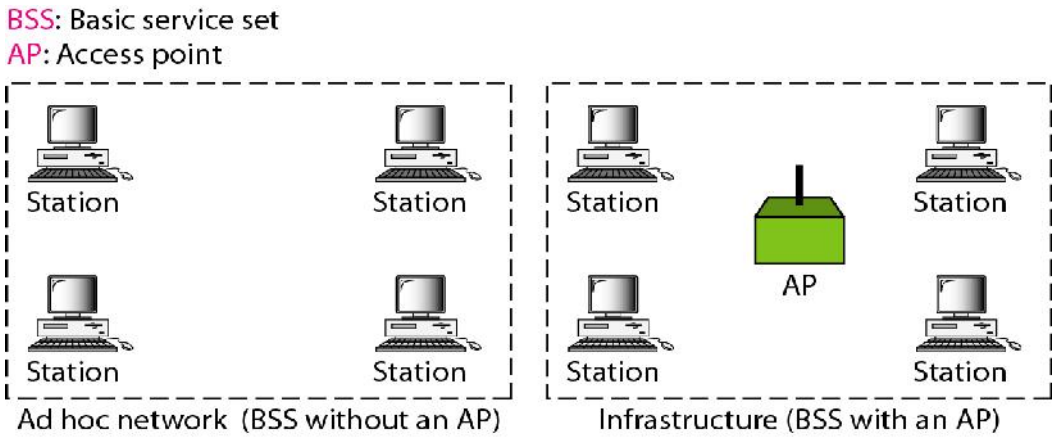


Fig. 6.1 Typical IBSS & BSS setup

It consists of BSS Master & BSS Client

i. BSS Master

- Access point connected to a wired LAN
- 802.11 functionality provided by the access point
- Acts as a gateway between the wireless clients and the wired network
- Clients on the WLAN communicate with one another through the access point
- BSS is identified by the Service Set Identity (SSID)
    - Alphanumeric, 2-32 characters, case sensitive
    - SSID appears in beacons, probe requests and probe responses.

ii. BSS Clients

- Wireless stations
- Use the same SSID to connect to the BSS

6.4.3 Extended service set:

An Extended Service Set is a set of one or more interconnected BSSs and integrated local area networks (LANs) as shown in fig 6.2 below that appear as a single BSS to the logical link control layer at any station associated with one of those BSSs.The set of interconnected BSSs must have a common service set identifier (SSID). They can work on the same channel, or work on different channels to boost aggregate throughput. This is also termed as Bridging mode.

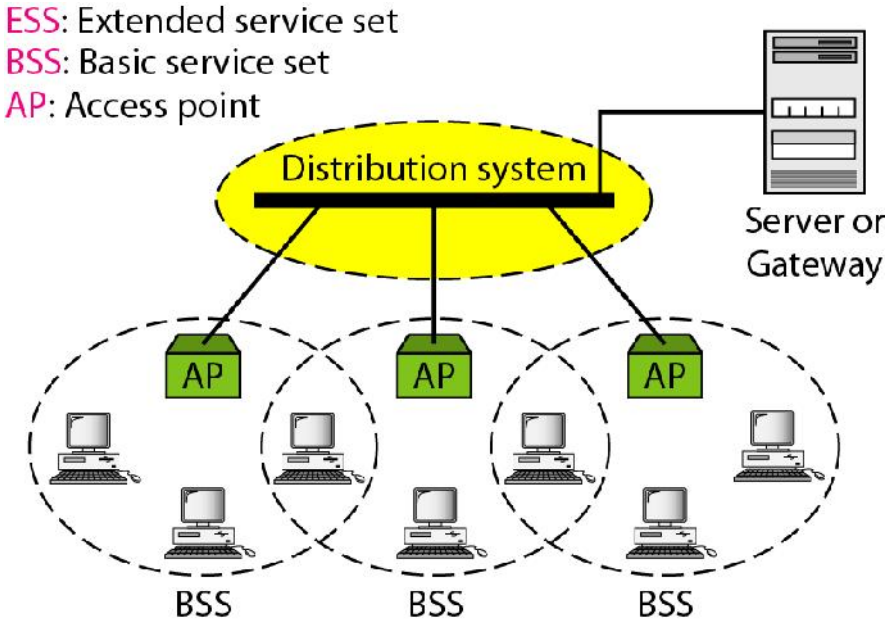


Fig. 6.2 Typical ESS setup

6.5 IEEE 802.11 Protocol Layer

The 802.11 standard defines layered protocol architecture to implement the services as given below.

- Association: Establishes an initial association between a station and an access point.
- Re-association: Enables an established association to be transferred from one access point to another, allowing a mobile station to move
- Dis-association: A notification from either a station or an access point that an existing association is terminated
- Authentication: Used to establish the identity of station to each other
- Privacy: used to prevent the content of message from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.

Network remains an important issue for WLANs. Authentication is done by the following identifiers.

6.5.1 Service set identifier (SSID):

It is a name that identifies a particular 802.11 wireless LAN. A client device receives broadcast messages from all access points within range advertising their SSIDs. The client device can then either manually or automatically—based on configuration—select the network with which to associate. The SSID can be up to 32 characters long. As the SSID displays to users, it normally consists of human-readable characters. However, the standard does not require this. The SSID is defined as a sequence of 1–32 octets each of which may take any value.

It is legitimate for multiple access points to share the same SSID if they provide access to the same network as part of an extended service set

6.5.2 Basic service set identifier (BSSID)

A related field is the BSSID or Basic Service Set Identifier, which uniquely identifies each BSS (the SSID however, can be used in multiple, possibly overlapping, BSSs). In an infrastructure BSS, the BSSID is the MAC address of the wireless access point (WAP). In an IBSS, the BSSID is a locally administered MAC address generated from a 48-bit random number. The individual/group bit of the address is set to 0. The universal/local bit of the address is set to 1.

A BSSID with a value of all 1s is used to indicate the broadcast BSSID. A broadcast BSSID may only be used during probe requests.

6.6 IEEE WLAN standards

The IEEE Wireless LAN standards and their frequencies, bandwidths & performance are shown in table 6.1 .

Standards	Radio frequency	Bandwidth	Performance
802.11	2.4 GHz	2 Mbps	Too slow, now obsolete
802.11b	2.4GHz	11 Mbps	In use, low cost
802.11a	5.0GHz	54 Mbps	High cost, short range & easily obstructed
802.11g	2.4 GHz	54 Mbps	Widely used, combination of all above standards but costly
802.11n	2.4 GHz	108 Mbps	Standards not yet finalized
802.11 h & j (Blue tooth)	2.4 GHz	1 – 3 Mbps	Very short distance (approx. 10 mtrs), suitable for handheld applications
802.16d	2.4 GHz	10 Mbps	Long distance (approx. in Kilo Mtrs) ,known as fixed Wimax
802.16e	2.4 GHz	10 Mbps	Long distance (approx. in Kilo Mtrs), known as mobile Wimax

Table 6.1 IEEE wireless LAN standards

6.7 Wireless LAN (WLANs) Security:

In wireless LANs security is a big concern, wireless networks are less stable, due to interference from other wire-less devices & networks. Whereas in wired LANs only authorized systems are connected by extending a dedicated physical cable to gain the access to that network.

In Wireless networks, Access Points (APs) create the hot spot areas (wireless coverage area). The systems with appropriate wireless adopters of that hot spot area can gain access to those network services, since there is no need of physical connection. This is a very serious security problem in wireless network.

The administrator as well as the users of wireless networks to be very strict vigilant to take appropriate precautions to prevent this serious problem of gaining unauthorized access to wireless networks. Otherwise their data security is under serious threat.

Hence, the administrator as well users have to take the advance security precautions while configuring their wireless networks.

There's no way to selectively hide the presence of your network from strangers, but you can prevent unauthorized people from connecting to it, and you can protect the data traveling across the network from prying eyes. By turning on a wireless network's encryption feature, you can scramble the data and control access to the network.

Wireless network hardware supports several standard encryption schemes, but the most common are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2).

WEP:

It is a security algorithm for IEEE 802.11 wireless networks; its intention is to provide data confidentiality comparable to that of a traditional wired network. Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws & it is the oldest and least secure method and should be avoided. WPA and WPA2 are good choices, but provide better protection when you use longer and more complex passwords (all devices on a wireless network must use the same kind of encryption and be configured with the same password).

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

WPA:

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled.

WPA uses a message integrity check algorithm called *Michael* to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the key stream from short packets to use for re-injection and spoofing.

WPA2:

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.

Unless you intend to provide public access to your wireless network — and put your business data or your own personal data at risk — you should consider encryption mandatory.

Securing Access Points (APs): (Administrator prospective**)**

A wireless (Wi-Fi) administrator has to configure, the following on access points (APs).

- SSID (Service Set Identifier): APs broadcast their SSIDs to advertise themselves to the wireless clients and the client can see a list of all available APs and decide which one to join. Disabling SSID broadcasting makes APs harder to identify (invisible mode). This measure is the first and the easiest step toward securing a wireless network.

- Default IP, Username and Password of AP: APs come with default IP numbers like 192.168.0.1 or 192.168.1.1, default username like admin or user and default password like admin or user & sometimes without any password. Change the default IP and password with longest possible password with combination of lower case, upper case, numerical and special character and change it every month or so.

- DHCP service: In APs by default DHCP service will be enabled, with this any unauthorized user coming in the vicinity of AP will get a valid IP address and can access the services. To prevent unauthorized access it is advised to disable DHCP service.

- MAC Filtering: MAC is the unique hardware address of 48 bit usually embedded on the NIC. This address is used by the systems to communicate each other with in that

network. Collect the list of MAC addresses of all authorized wireless systems and configuring the MAC filtering (white table) thereby prevent unauthorized access.

- Encryption Protocols (WEP, WPA): For more advance security encryption protocols like wired equivalent protocol (WEP) & Wi-Fi protected access (WPA) protocols are configured. These protocols exchange the data in the encrypted form and there by prevent unauthorized access.

- Firewall: Enabling firewall feature built in APs prevents hackers on the Internet from getting access to local services

Securing Systems: (User prospective)

A wireless (Wi-Fi) user while using the services, the following security measures are to be taken for data security.

- Public hotspots generally don't use any encryption protocols or any other security measures; hence users are not advised to make important data transactions.

- Make sure it's a legitimate hotspot otherwise, user may be trapped by the fake public hotspots like (SSID) "airport", can capture users' log-on information and other valuable data.

- Verify PC's software firewall is turned on, and that Windows' file-sharing feature is off.

- While using wireless networks it is better not to do important bank transactions, credit card transactions, confidential e-mail access or any other sensitive data transactions unless you're sure you're on a secured network.

- Always turn off Wi-Fi service on your system when not in use, otherwise Hackers can use it to create peer-to-peer Wi-Fi connections.

6.8 Wi-MAX (*Worldwide Interoperability for Microwave Access*)

It is a telecommunications technology that provides wireless transmission of data, designed for long-range networking (spanning miles or kilometers) as opposed to local area wireless networks, using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access as shown in fig 6.3. The technology provides up to 10 Mbps broadband speed without the need for cables. The technology is based on the IEEE 802.16 standard (also called Broadband Wireless Access).

The name "WiMAX" was created by the WiMAX Forum, which was formed in June 2001 to promote conformity and interoperability of the standard. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL".

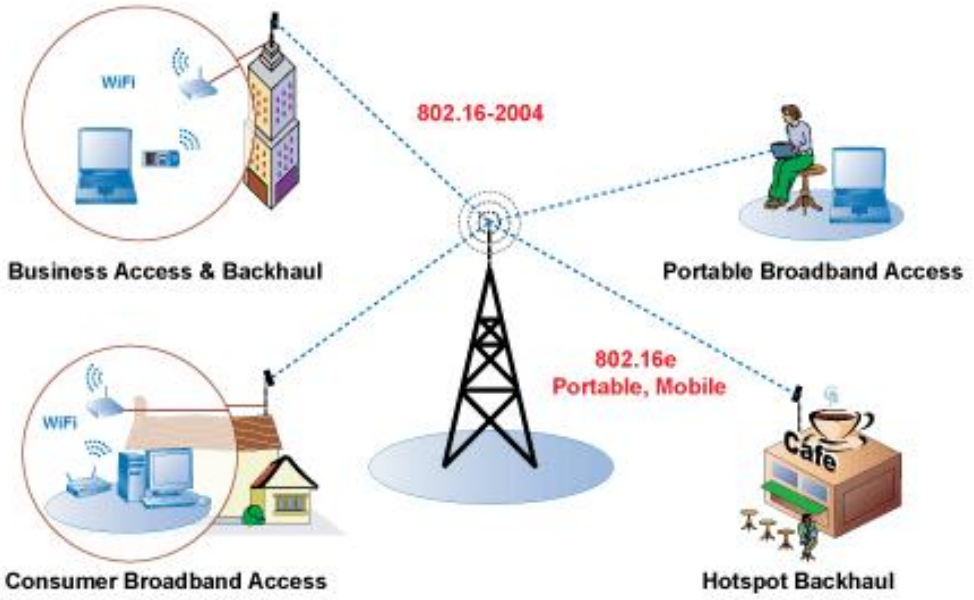


Fig. 6.3 Typical Wi-Max setup

6.7.1 Wi-Max Standards & applications

- **802.16-2004** is also known as 802.16d, which refers to the working party that has developed that standard. It is sometimes referred to as "fixed WiMAX," since it has no support for mobility.
- **802.16e-2005**, often abbreviated to 802.16e, is an amendment to 802.16-2004. It introduced support for mobility, among other things and is therefore also known as "mobile WiMAX".

The bandwidth and range of WiMAX make it suitable for the following potential applications:

- Connecting Wi-Fi hotspots to the Internet.
- Providing a wireless alternative to cable and DSL for "last mile" broadband access.
- Providing data, telecommunications and IPTV services.
- Providing a source of Internet connectivity as part of a business continuity plan. That is, if a business has both a fixed and a wireless Internet connection, especially from unrelated providers, they are unlikely to be affected by the same service outage.
- Providing portable connectivity.
- WiMAX is a long range system, covering many kilometers that uses licensed or unlicensed spectrum to deliver a point-to-point connection to the Internet.

- Different 802.16 standards provide different types of access, from portable (similar to a cordless phone) to fixed (an alternative to wired access, where the end user's wireless termination point is fixed in location.)
- Wi-Fi uses unlicensed spectrum to provide access to a network.
- Wi-Fi is more popular in end user devices.
- WiMAX and Wi-Fi have quite different quality of service (QoS) mechanisms:
    - WiMAX uses a QoS mechanism based on connections between the base station and the user device. Each connection is based on specific scheduling algorithms.
    - Wi-Fi has a QoS mechanism similar to fixed Ethernet, where packets can receive different priorities based on their tags. For example VoIP traffic may be given priority over web browsing.
- Wi-Fi runs on the Media Access Control's CSMA/CA protocol, which is connectionless and contention based, whereas WiMAX runs a connection-oriented MAC.
- Both 802.11 and 802.16 define Peer-to-Peer (P2P) and ad hoc networks, where an end user communicates to users or servers on another Local Area Network (LAN) using its access point or base station.

6.8 Bluetooth

Bluetooth is an open wireless protocol for exchanging data over short distances (using short length radio waves) from fixed and mobile devices, creating personal area networks (PANs). It was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.

It is an alternative wireless network technology that followed a different development path than the 802.11 family. Bluetooth supports a very short range (approximately 10 meters) and relatively low bandwidth (1-3 Mbps in practice) designed for low-power network devices like handhelds as shown in fig 6.4, but it is rarely used for general-purpose WLAN networking due to the range and speed considerations.

Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 bands of 1 MHz width in the range 2402-2480 MHz. This is in the globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band

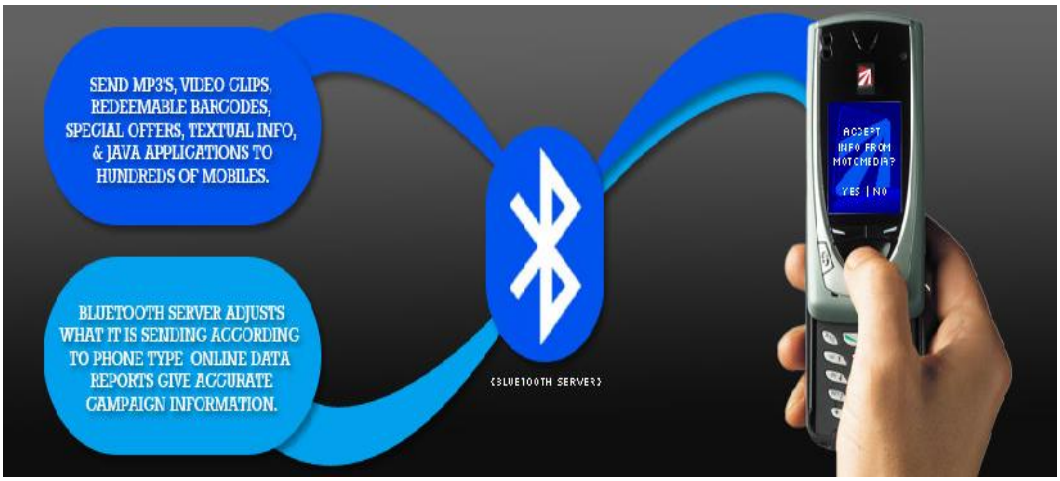


Fig. 6.4 Typical Bluetooth setup

In its basic rate (BR) mode, the modulation is Gaussian frequency-shift keying (GFSK). It can achieve a gross data rate of 1 Mbit/s. In extended data rate (EDR) π/4-DQPSK and 8DPSK are used, giving 2, and 3 Mbit/s respectively. Bluetooth provides a secure way to connect and exchange information between devices such as mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles.

6.9 Radio Over IP (RoIP)

Radio over Internet Protocol (RoIP) is a method of transmitting and receiving radio communications via Internet Protocol (IP), a data communications standard used to power the Internet as well as home and business computer networks.

RoIP, is similar to VoIP, it uses standard VoIP techniques to transfer the analog audio, used by Land Mobile Radio systems, digitally over the Internet (or LAN), with an added command layer to control basic radio functions such as push-to-talk (PTT), frequency change, etc. It removes high cost of leased phone lines to remote controlled base stations by using standard Internet connections already located at sites.

It can be implemented like any other radio network. With RoIP, at least one node of a network is a radio (or a radio with an IP interface device) connected via IP to other nodes in the radio network, the other nodes can be two-way radios.

RoIP can be deployed over private networks as well as the public Internet. It is useful in land mobile radio systems used by public safety departments and fleets of utilities spread over a broad geographic area. Like other centralized radio systems such as trunked radio systems, issues of delay or latency and reliance on centralized infrastructure can be impediments to adoption by public safety agencies.

Use of RoIP

In its most basic form, RoIP technology provides a method of linking two or more radios or repeaters using a LAN/WAN or Internet connection. This is known as **Site Linking or Point-to-Point linking.**

Another common application is **IP Dispatch or remote base station**. This allows users the ability to operate transceivers remotely, but distance is not limited by cable length. Dispatchers use a software-based **IP Console** which typically runs on the Windows operating system, or in some cases Linux.

Radio-over-IP has become a major enabler of interoperability, allowing otherwise incompatible radio systems to communicate seamlessly, sharing a common data connection.

Push-to-talk for mobile phones and PDAs, known as **P2T** may be used in conjunction with RoIP networks. This allows **Smart Phone** users to communicate directly with radio users and dispatchers.

Fig. 6.5 Typical RoIP setup

Review Questions:

Subjective:

1. Describe the architecture & standards of WLAN?
2. Explain briefly about Wi-Fi & WI Max technologies?
3. Write short notes on Blue tooth?

Objective:

1. IEEE standard for WLAN is
    a) 802.11
    b) 802.2
    c) 802.3
    d) 802.10
2. Access Protocol for WLAN is
    a) CSMA
    b) CSMA / CD
    c) CSMA / CA
    d) None of the above
3. BSSID of access point is
    e) 48 bit IP address
    f) 32 bit MAC address
    g) 48 bit MAC address
    h) None of the above
4. RF band used for WLAN is
    i) 0.4 GHz
    j) 2.4 GHz
    k) 1.2 GHz
    l) None of the above
5. The bandwidth available in 802.11a WLAN is
    m) 2 Mbps
    n) 54 Mbps
    o) 11 Mbps
    p) 108 Mbps