KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2018 onwards)

DEPARTMENT OF COMPUTER SCIENCE,CA & IT

SUBJECT : **COMPUTER NETWORKS**	**SEMESTER**: III	**L T P C**
SUBJECT CODE: **18CSU303**	**CLASS** : II B.Sc.CS -A	**4 0 0 4**

Course Objectives

- To master the fundamentals of data communications networks by gaining a working knowledge of data transmission concepts,
- To understand the operation of all seven layers of OSI Model and the protocols used in each layer.

Course Outcomes(COs)

1. Various transmission media, their comparative study, fiber optics and wireless media
2. Categories and topologies of networks (LAN and WAN) Layered architecture (OSI and TCP/IP) and protocol suites.
3. Channel error detection and correction, MAC protocols, Ethernet and WLAN.
4. Details of IP operations in the INTERNET and associated routing principles

Unit I - INTRODUCTION TO COMPUTER NETWORKS

Network definition; network topologies; network classifications; network protocol; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite. **Data** Communication Fundamentals and Techniques: Analog and digital signal; data-rate limits; digital to digital line encoding schemes; pulse code modulation; parallel and serial transmission;
digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media.

Unit II - NETWORKS SWITCHING TECHNIQUES AND ACCESS MECHANISMS

Circuit switching; packet switching - connectionless datagram switching, connection-oriented virtual circuit switching; dial-up modems; digital subscriber line; cable TV for data transfer.

Unit III - DATA LINK LAYER FUNCTIONS AND PROTOCOL

Error detection and error correction techniques; data-link control- framing and flow control; error recovery protocols- stop and wait ARQ, go-back-n ARQ; Point to Point Protocol on Internet.

Unit IV - MULTIPLE ACCESS PROTOCOL AND NETWORKS

CSMA/CD protocols; Ethernet LANS; connecting LAN and back-bone networks- repeaters, hubs, switches, bridges, router and gateways; Networks Layer Functions and Protocols: Routing; routing algorithms; network layer protocol of Internet- IP protocol, Internet control protocols.

Unit V - TRANSPORT LAYER FUNCTIONS AND PROTOCOLS

Transport services- error and flow control, Connection establishment and release- three way handshake; Overview of Application layer protocol: Overview of DNS protocol; overview of WWW &HTTP protocol.

SUGGESTED READINGS

1. Forouzan, B. A. (2012). Data Communications and Networking. 4th edition. New Delhi: THM.
2. Tanenbaum, A. S. (2002). Computer Networks. 4th edition. New Delhi: PHI.

WEB SITES

1. en.wikipedia.org/wiki/Internet_protocol_suite
2. http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies
3. www.yale.edu/pclt/COMM/**TCPIP**.HTM
4. www.w3schools.com/**tcpip**/default.asp

STAFF **HOD**

Enable | Enlighten | Enrich
KARPAGAM
ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established Under Section 3 of UGC Act, 1956)

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2018 onwards)

DEPARTMENT OF COMPUTER SCIENCE,CA & IT

SUBJECT : **COMPUTER NETWORKS** **SEMESTER**: III **L T P C**
SUBJECT CODE: **18CSU303** **CLASS** : II B.Sc.CS -A **4 0 0 4**

Unit I - INTRODUCTION TO COMPUTER NETWORKS

Network definition; network topologies; network classifications; network protocol; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite.

Data Communication Fundamentals and Techniques: Analog and digital signal; data-rate limits; digital to digital line encoding schemes; pulse code modulation; parallel and serial transmission; digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media.

Unit II - NETWORKS SWITCHING TECHNIQUES AND ACCESS MECHANISMS

Circuit switching; packet switching - connectionless datagram switching, connection-oriented virtual circuit switching; dial-up modems; digital subscriber line; cable TV for data transfer.

Unit III - DATA LINK LAYER FUNCTIONS AND PROTOCOL

Error detection and error correction techniques; data-link control- framing and flow control; error recovery protocols- stop and wait ARQ, go-back-n ARQ; Point to Point Protocol on Internet.

Unit IV - MULTIPLE ACCESS PROTOCOL AND NETWORKS

CSMA/CD protocols; Ethernet LANS; connecting LAN and back-bone networks- repeaters, hubs, switches, bridges, router and gateways; Networks Layer Functions and Protocols: Routing; routing algorithms; network layer protocol of Internet- IP protocol, Internet control protocols.

Unit V - TRANSPORT LAYER FUNCTIONS AND PROTOCOLS

Transport services- error and flow control, Connection establishment and release- three way handshake; Overview of Application layer protocol: Overview of DNS protocol; overview of WWW &HTTP protocol.

SUGGESTED READINGS

1. Forouzan, B. A. (2012). Data Communications and Networking. 4th edition. New Delhi: THM.
2. Tanenbaum, A. S. (2002). Computer Networks. 4th edition. New Delhi: PHI.

WEB SITES

1. en.wikipedia.org/wiki/Internet_protocol_suite
2. http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies
3. www.yale.edu/pclt/COMM/**TCPIP**.HTM
4. www.w3schools.com/**tcpip**/default.asp

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2018 onwards)

DEPARTMENT OF COMPUTER SCIENCE, CA & IT

SUBJECT : COMPUTER NETWORKS

SEMESTER : III **L T P C**

SUBJECT CODE: 18CSU303 CLASS : II B.Sc.CS A& B **4 0 0 4**

LECTURE PLAN

Unit I

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	**Introduction toComputerNetworks** : Network definition, network topologies	**W1**
2	1	network classifications, network protocol	**T1: 13-15, T1: 19**
3	1	layered network architecture	**T1: 27-28**
4	1	overview of OSI reference model	**T1: 29-33,R1:41**
5	1	overview of TCP/IP protocolsuite.	**T1: 42-45,R1:45**
6	1	**Data Communication FundamentalsandTechniques**:Analog and digital signal, data-ratelimits	**T1: 57-58, T1: 85-88**
7	1	digital to digital line encoding schemes	**T1: 101-106**
8	1	pulse code modulation, parallel and serial transmission	**T1: 121-128,** **T1: 131-132**
9	1	Recapitulation and Discussion of Important Questions	
		Total hours planned for UNIT- 1: 9 hrs	

Text Book:

T1→Forouzan, B. A.(2007). Data Communications and Networking(4thed.). New Delhi: THM.

Reference Book:

R1→Tanenbaum, A.S. (2002). Computer Networks(5th ed.). New Delhi: PHI.

Websites:

W1→https://www.studytonight.com/computer-networks/overview-of-computer-networks

Prepared By K.Kathirvel,K.Yuvaraj, Department Of Computer Science,CA& IT

Unit – II

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	digital to analog modulation	**T1: 141-148**
2	1	multiplexing techniques- FDM, TDM Transmission media.	**T1: 161-179** **T1: 191-207,R1:95-99**
3	1	Networks Switching Techniques and access mechanisms: Circuit switching	**T1: 213-218**
4	1	Packetswitching	**W2,R1:356-361**
5	1	connectionless datagram switching,	**W3,R1:356-361**
6	1	connection-oriented virtual circuit switching	**W3,R1:356-361**
7	1	dial-up modems	**T1: 248-250**
8	1	digital subscriber line cable TV for data transfer.	**T1: 251-255,** **T1: 257-260**
9	1	Recapitulation and Discussion of Important Questions	
		Total hours planned for UNIT- 2: 9 hrs	

Text Book:

T1→Forouzan, B. A.(2007). Data Communications and Networking(4th ed.). New Delhi: THM.

Reference Book:

R1→Tanenbaum, A.S. (2002). Computer Networks(5th ed.). New Delhi: PHI.

Websites:

W2→https://www.tutorialspoint.com/data_communication_computer_network/ecomputernotes.com › Computer Networking › Switching

W3→https://thehelios.wordpress.com/tag/connectionless-packet-switching/

Unit – III

S.No	**Lecture Duration (Hours)**	**Topics to be Covered**	**Support Materials**
1	1	**Data Link Layer FunctionsandProtocol**: Error detection techniques	**T1: 267-269, 272** **R1:209**
2	1	error correction techniques	**T1: 273-274,R1:204**
3	1	data-link control- framing	**T1: 307-308**
4	1	Flow control	**T1: 311,R1:194-201**
5	1	error recovery protocols-	**T1: 312**
6	1	stop and wait ARQ,	**T1: 318-323, W4**
7	1	go-back-n ARQ	**T1: 324-331,W4**
8	1	Point to Point Protocol on Internet.	**T1: 346-355**
9	1	Recapitulation and Discussion of Important Questions	
		Total hours planned for UNIT- 3: 9 hrs	

Text Book:

T1→Forouzan, B. A.(2007). Data Communications and Networking(4th ed.). New Delhi: THM.

Reference Book:

R1→Tanenbaum, A.S. (2002). Computer Networks(5th ed.). New Delhi: PHI.

Websites:

W4→https://www.geeksforgeeks.org/stop-and-wait-arq/

Unit – IV

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	**Multiple Access ProtocolandNetworks**: CSMA/CD protocols	**T1: 363-377**
2	1	Ethernet LANS	**T1: 395-402**
3	1	connecting LAN and back-bone networks- repeaters, hubs, switches, bridges, router andgateways	**T1: 445-457** **R1:340**
4	1	**Networks Layer FunctionsandProtocols**: Routing	**T1: 647-655**
5	1	routing algorithms	**T1: 658-684,** **R1:362-389**
6	1	network layer protocol of Internet-	**T1: 579-582**
7	1	IP protocol,	**T1: 582-602**
8	1	Internet control protocols	**T1: 621-627, W5**
9	1	Recapitulation and Discussion of Important Questions	
		Total hours planned for UNIT- 4: 9 hrs	

Text Book:

T1→Forouzan, B. A.(2007). Data Communications and Networking(4th ed.). New Delhi: THM.

Reference Book:

R1→Tanenbaum, A.S. (2002). Computer Networks(5th ed.). New Delhi: PHI.

Websites:

W5→https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/

Unit V

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	**Transport Layer FunctionsandProtocols**: Transport services	**T1: 715, W6**
2	1	error control	**T1: 731-734**
3	1	flow control	**T1: 728-730**
4	1	Connection establishment and release	**T1: 703-707**
5	1	Three way handshake	**R1:516-517**
6	1	**Overview of Applicationlayerprotocol**: Overview of DNS protocol	**T1: 799-801, 803-805** **W7**
7	1	overview of WWW &	**T1: 851-860**
8	1	Overview of HTTP protocol.	**T1: 861-868**
9	1	Recapitulation and Discussion of Important Questions	
10	1	Discussion of Previous year ESE Question Paper	
11	1	Discussion of Previous year ESE Question Paper	
12	1	Discussion of Previous year ESE Question Paper	
		Total hours planned for UNIT- 5: 12 hrs	
		Total No Of Hours Planned For Overall: 48	

Text Book:

T1→Forouzan, B. A.(2007). Data Communications and Networking(4th ed.). New Delhi: THM.

Reference Book:

R1→Tanenbaum, A.S. (2002). Computer Networks(5th ed.). New Delhi: PHI.

Websites:

W6→https://www.studytonight.com/computer-networks/osi-model-transport-layer

W7→https://www.geeksforgeeks.org/protocols-application-layer/

Unit I

SYLLABUS

Introduction to Computer Networks : Network definition; network topologies; network classifications; network protocol; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite. **Data Communication Fundamentals and Techniques**: Analog and digital signal; data-rate limits; digital to digital line encoding schemes; pulse code modulation; parallel and serial transmission; digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media.

INTRODUCTION TO COMPUTER NETWORKS:

Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork.

Definition: A set of devices often mentioned as nodes connected by media link is called a Network.

A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called **Communication channels**.

Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network. The best example of computer network is **Internet.**

NETWORK DEFINITION

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

Data communication:

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

Components:

A data communications system has five components;

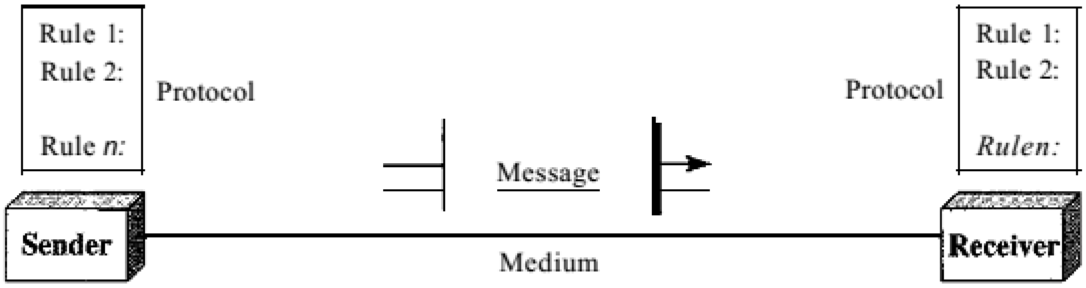
1. Message. The message is the information (data) to be communicated. Popularforms of information include text, numbers, pictures, audio, and video.

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

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

4. Transmission medium. The transmission medium is the physical path by whicha message travels from sender to receiver. Some examples of transmission mediainclude twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

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



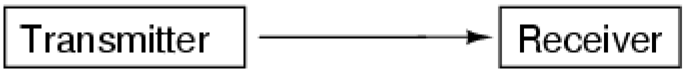
Data Representation

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

Data Flow

Buses and networks are designed to allow communication to occur between individual devices that are interconnected. The flow of information, or data, between nodes, can take a variety of forms: simplex, half-duplex, or full-duplex.

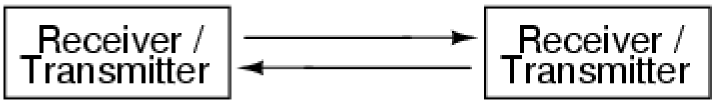
Simplex communication



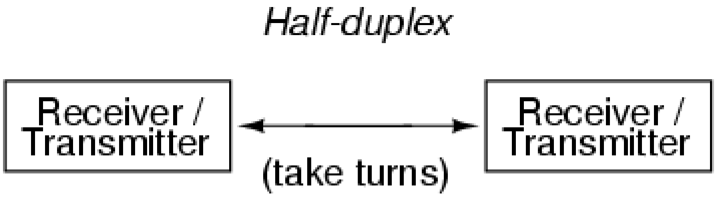
With **simplex communication**, all data flow is unidirectional: from the designated transmitter to the designated receiver.

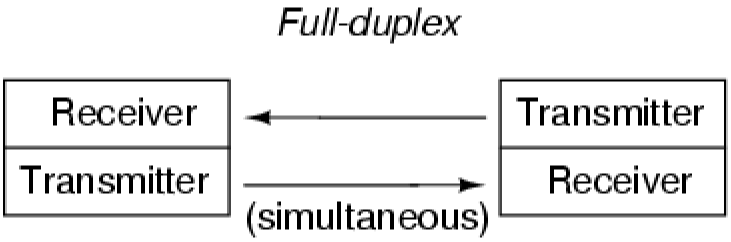
Keyboard and Monitor is an example of simplex communication.

Duplex communication



With **duplex communication**, the flow of information is bi-directional for each device. Duplex can be further divided into two sub-categories:





In **half-duplex mode**, each station can both transmit and receive, but not at the same time: When one device is sending, the other can only receive, and vice versa.
Example: Walkie-talkies and CB (citizens band) radios,intercom are both half-duplex systems.

In **full-duplex mode** (also called duplex), both stations can transmit and receive simultaneously.
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.

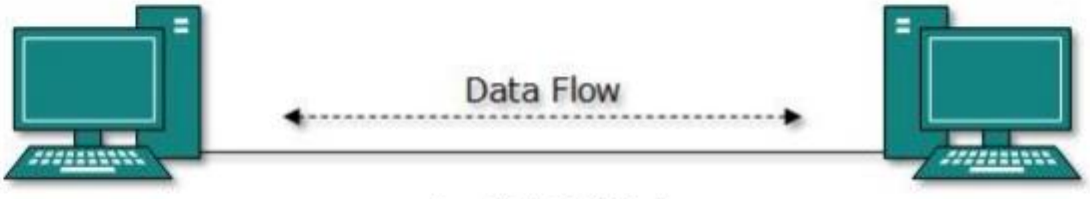
We can use this for multipurpose data communication at the same time like internet, cable TV and phone etc with the same cable.

NETWORK TOPOLOGIES:

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

POINT-TO-POINT

Point-to-point networks contains exactly two hosts (computer or switches or routers or servers) connected back toback using a single piece of cable. Often, the receiving end of one host is connected to sending end of the otherend and vice-versa.

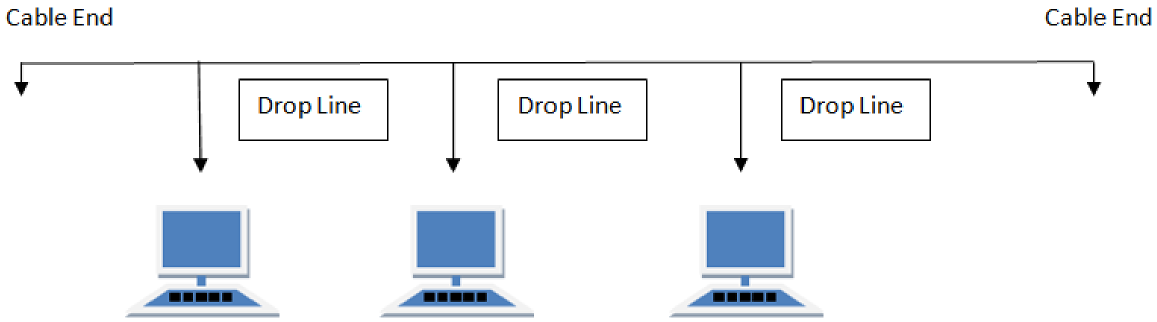


[Image: Point-to-point Topology]

If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hostsare unaware of underlying network and see each other as if they are connected directly.

BUS TOPOLOGY

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

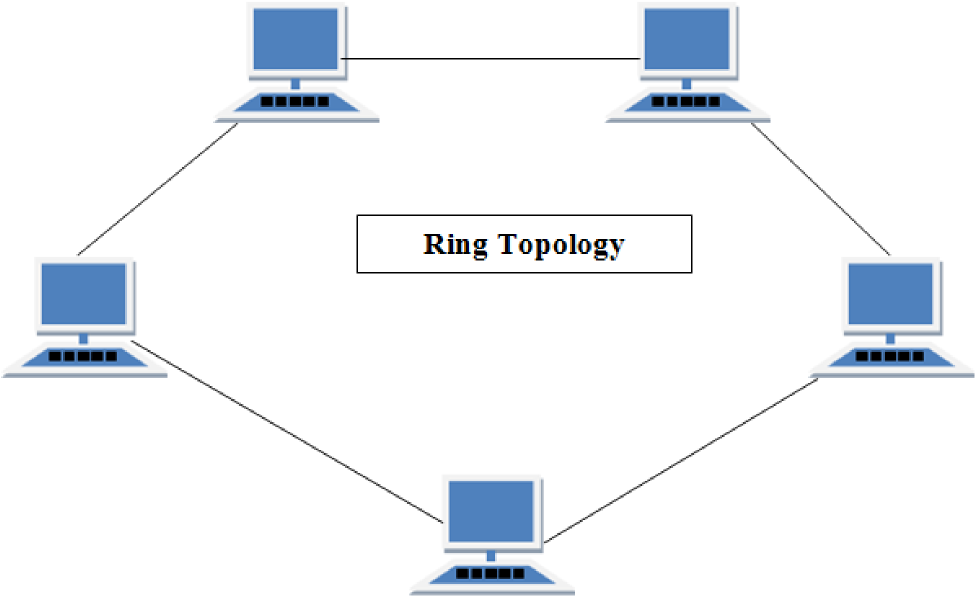
RING TOPOLOGY

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

]

Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.



Advantages of Ring Topology

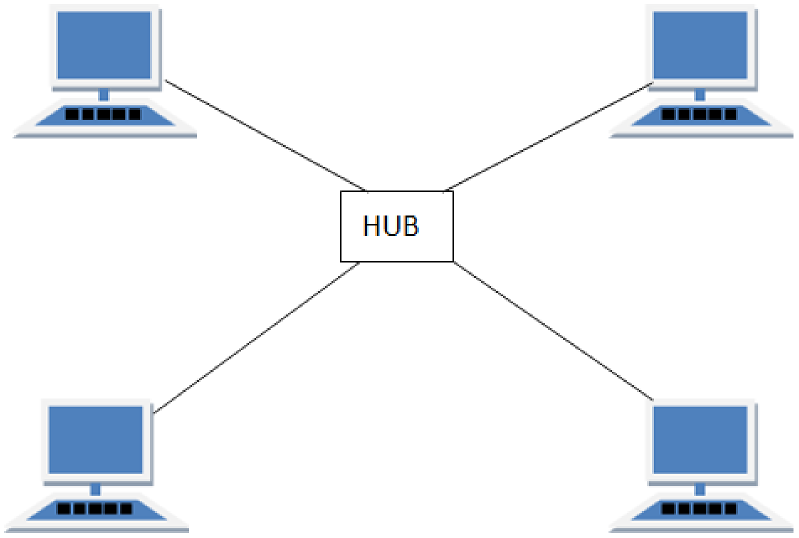
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR TOPOLOGY

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH TOPOLOGY

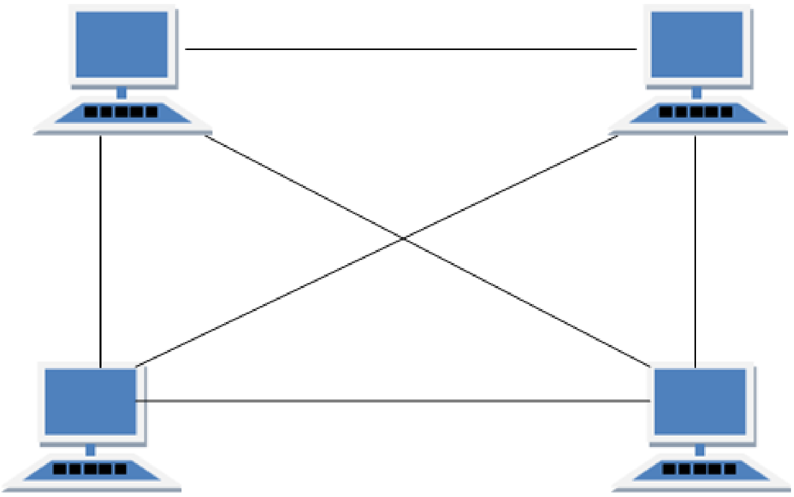
It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.



MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

Types of Mesh Topology

1. **Partial Mesh Topology :**In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :**Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

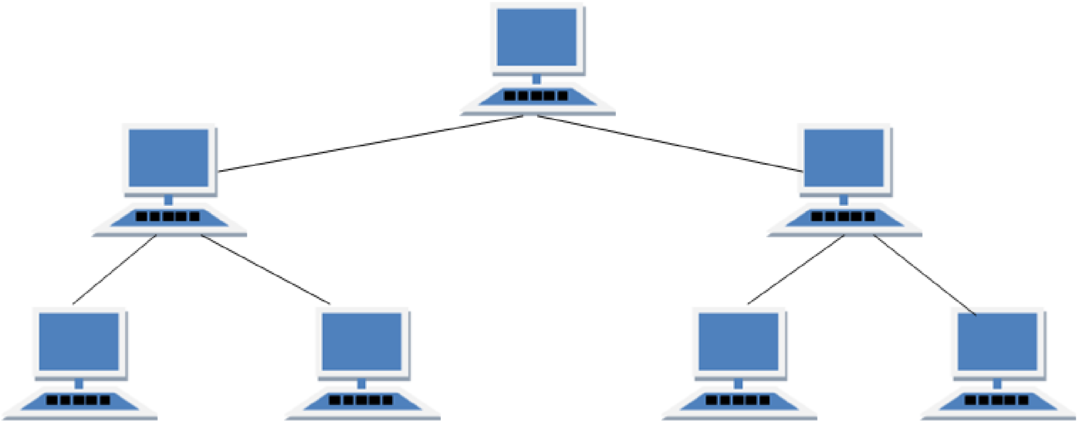
Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology



1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

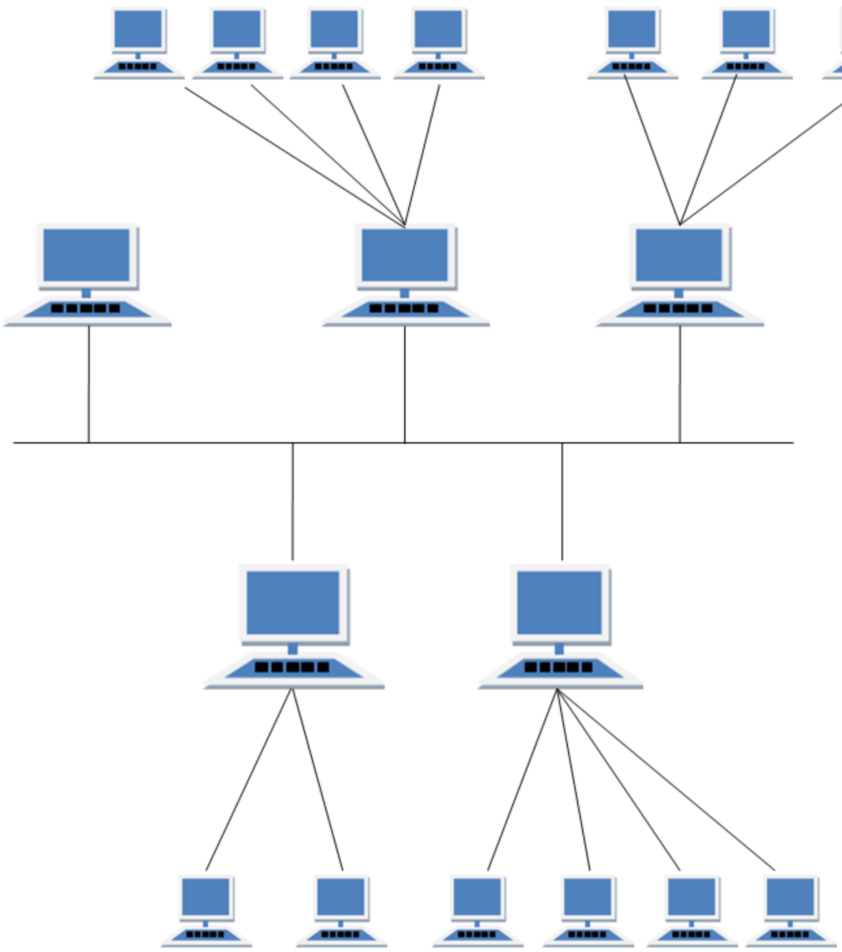
1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included



Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

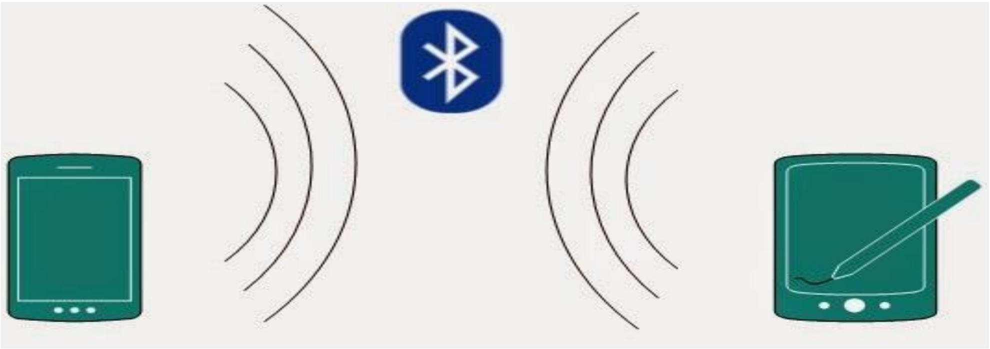
1. Complex in design.
2. Costly.
3.

NETWORK CLASSIFICATIONS

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the Internet itself, covering the whole geographical world, i.e. the Earth.

Personal Area Network

A Personal Area Network or simply PAN, is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes for example.

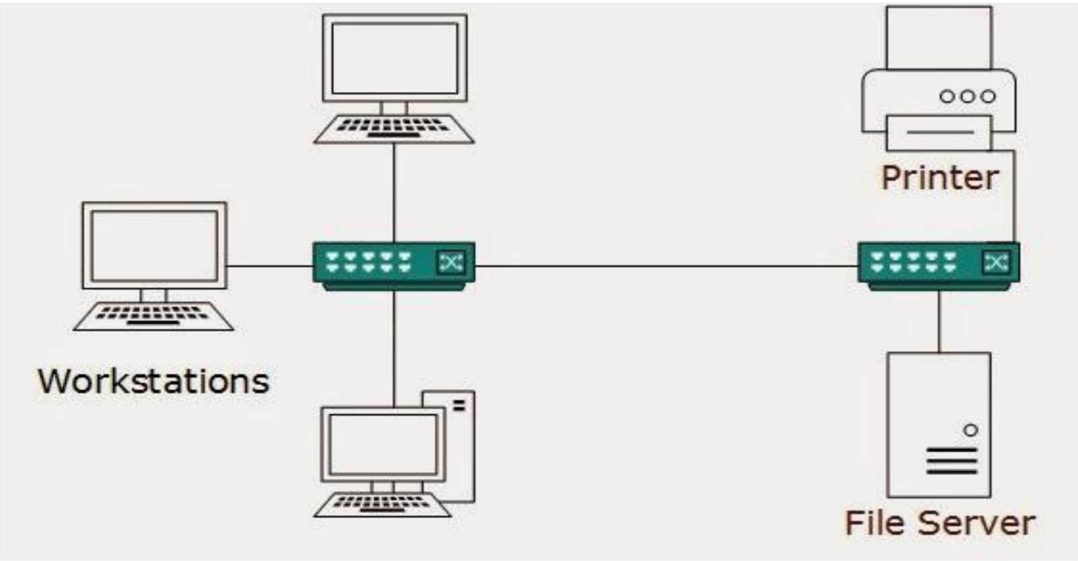


Piconet is an example Bluetooth enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network. Usually, Local Area Network covers an organization's offices, schools, college/universities etc. Number of systems may vary from as least as two to as much as 16 million

LAN provides a useful way of sharing resources between end users. Resources like Printers, File Servers, Scanners and internet is easy sharable among computers.



Local Area Networks are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and generally do not involve heavy routing. LAN works under its own local domain and controlled centrally.

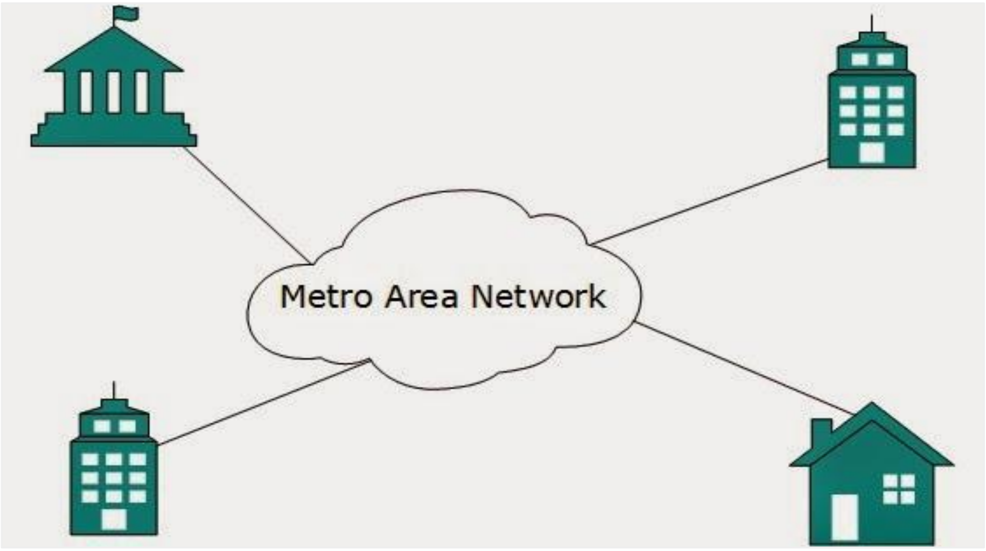
LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology while Token-ring is rarely seen.

LAN can be wired or wireless or in both forms at once.

Metropolitan Area Network

MAN, generally expands throughout a city such as cable TV network. It can be in form of Ethernet, Token-ring, ATM or FDDI.

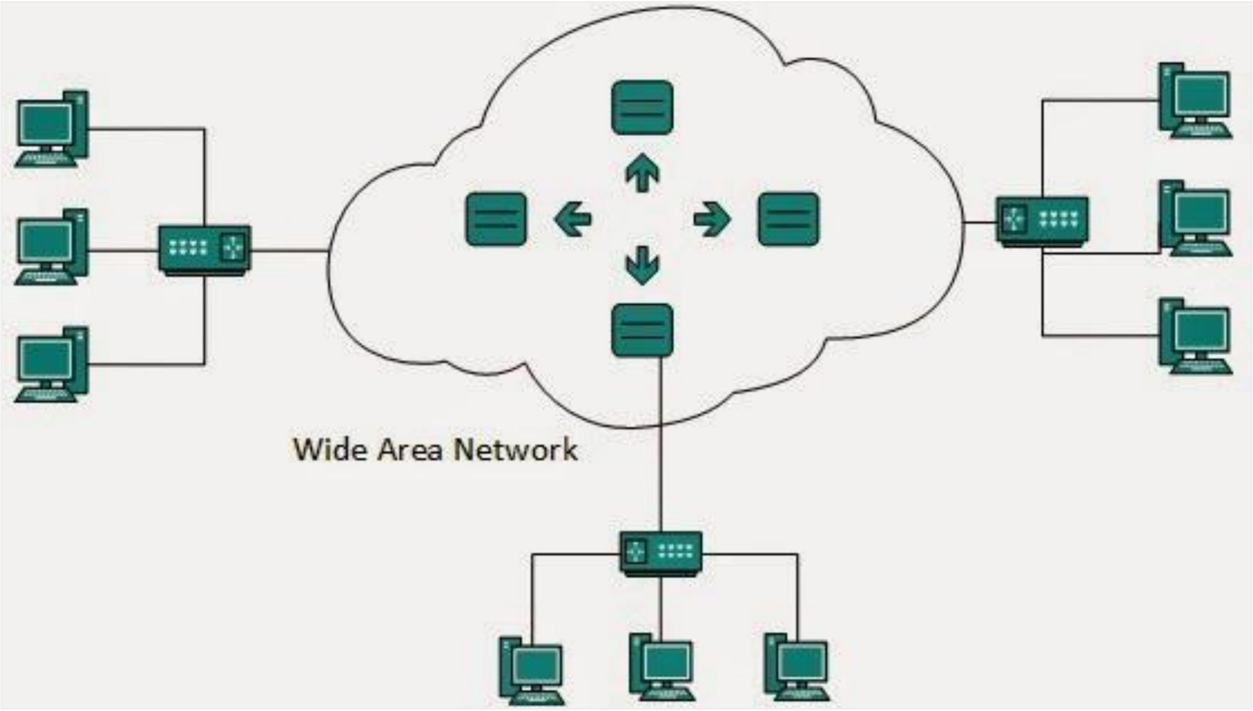
Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a City.



Backbone of MAN is high-capacity and high-speed fiber optics. MAN is works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or Internet.

Wide Area Network

As name suggests, this network covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provides connectivity to MANs and LANs. Equipped with very high speed backbone, WAN uses very expensive network equipment.



WAN may use advanced technologies like Asynchronous Transfer Mode (ATM), Frame Relay and SONET. WAN may be managed under by more than one administration.

Internetwork

A network of networks is called internetwork, or simply Internet. It is the largest network in existence on this planet. Internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses www, ftp, email services, audio and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by some client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very lownetwork protocol; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite.

NETWORK PROTOCOLS

Network protocols are formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network. Network protocols govern the end-to-end processes of timely, secure and managed data or network communication.

Network protocols incorporate all the processes, requirements and constraints of initiating and accomplishing communication between computers, servers, routers and other network enabled devices. Network protocols must be confirmed and installed by the sender and receiver to ensure network/data communication and apply to software and hardware nodes that communicate on a network. There are several broad types of networking protocols, including:

Network communication protocols example:

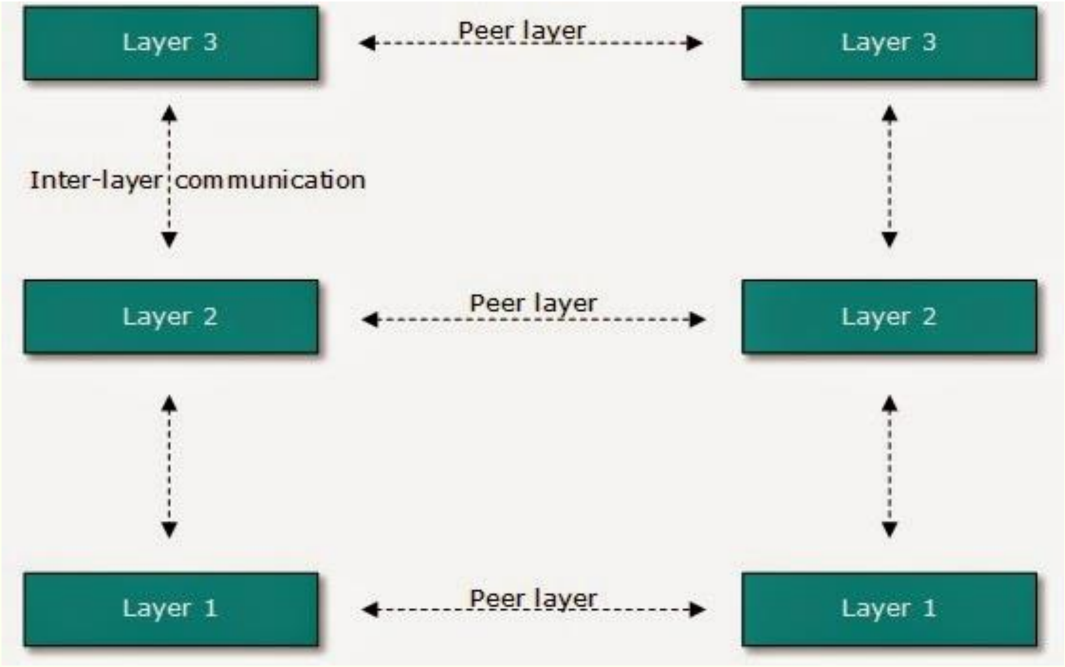
Basic data communication protocols, such as TCP/IP and HTTPNetwork securityprotocols: Implement security over network communications and include HTTPS, SSL and SFTP.

Network management protocols: Provide network governance and maintenance and include SNMP and ICMP.

LAYERED NETWORK ARCHITECTURE

In layered architecture of Network Models, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.

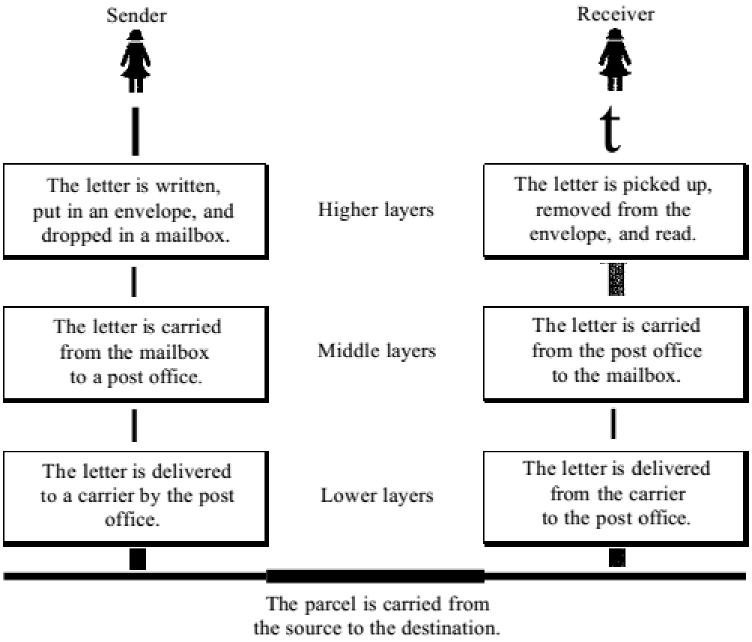
In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by top most layer it is then passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and pass on to lower layer. If the task is initiated by lowest most layer the reverse path is taken.



Every layer clubs together all procedures, protocols, methods which it requires to execute its piece of task. All layers identify their counterparts by means of encapsulation header and tail.

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal maiLThe process of sending a letter to a friend would be complex if there were no services available from the post office. Figure 2.1 shows the steps in this task.

Figure 2.1 *Tasks involved in sending a letter*


Sender
Receiver
The letter is written, put in an envelope, and dropped in a mailbox.
Higher layers
The letter is picked up, removed from the envelope, and read.
The letter is carried from the mailbox to a post office.
Middle layers
The letter is carried from the post office to the mailbox.
The letter is delivered to a carrier by the post office.
Lower layers
The letter is delivered from the carrier to the post office.
The parcel is carried from the source to the destination.

Sender, Receiver, and Carrier In Figure 2.1 we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site
Let us first describe, in order, the activities that take place at the sender site.o Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

o Middle layer. The letter is picked up by a letter carrier and delivered to the post office.
o Lower layer. The letter is sorted at the post office; a carrier transports the letter.

On the Way The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

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

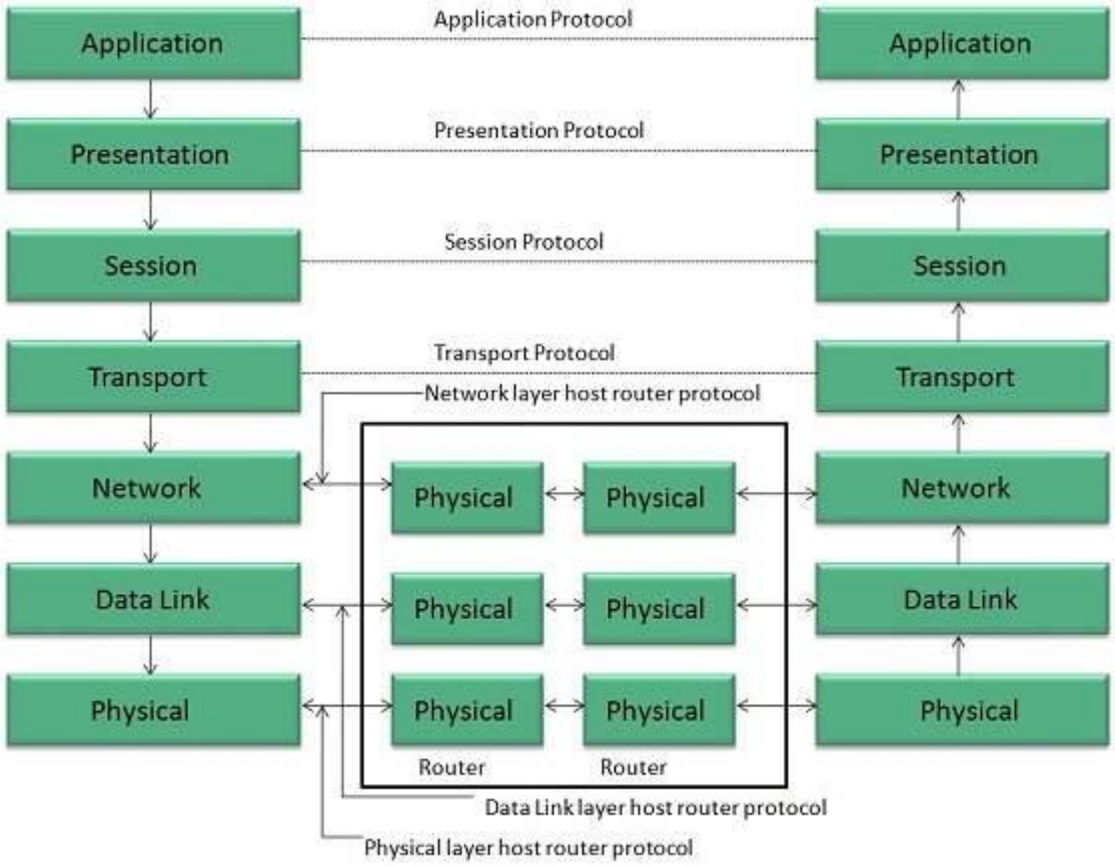
o Middle layer. The letter is sorted and delivered to the recipient's mailbox.

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

OVERVIEW OF OSI REFERENCE MODEL

OSI is acronym of **Open System Interface**. This model is developed by the **International organization of Standardization (ISO)** and therefore also referred as **ISO-OSI** Model.

The OSI model consists of seven layers as shown in the following diagram. Each layer has a specific function, however each layer provide services to the layer above.



Physical Layer

The Physical layer is responsible for the following activities:

- Activating, maintaining and deactivating the physical connection.
- Defining voltages and data rates needed for transmission.
- Converting digital bits into electrical signal.
- Deciding whether the connection is simplex, half duplex or full duplex.

Data Link Layer

The data link layer performs the following functions:

- Performs synchronization and error control for the information which is to be transmitted over the physical link.
- Enables error detection, and adds error detection bits to the data which are to be transmitted.

Network Layer

Following are the functions of Network Layer:

- To route the signals through various channels to the other end.
- To act as the network controller by deciding which route data should take.
- To divide the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

Transport Layer

The Transport layer performs the following functions:

- It decides if the data transmission should take place on parallel paths or single path.
- It performs multiplexing, splitting on the data.
- It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.

The Transport Layer guarantees transmission of data from one end to other end.

Session Layer

The Session layer performs the following functions:

- Manages the messages and synchronizes conversations between two different applications.
- It controls logging on and off, user identification, billing and session management.

Presentation Layer

The Presentation layer performs the following functions:

- This layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.

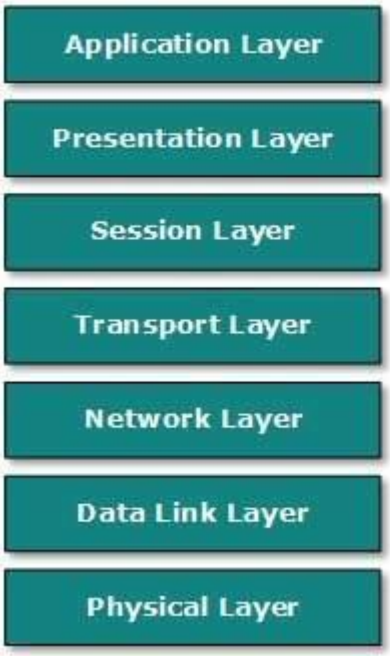
Application Layer

The Application layer performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.
- The functions such as LOGIN or password checking are also performed by the application layer.

OSI Model

Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). This model has seven layers:



- **Application Layer**: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.
- **Presentation Layer**: This layer defines how data in the native format of remote host should be presented in the native format of host.
- **Session Layer**: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.
- **Transport Layer**: This layer is responsible for end-to-end delivery between hosts.
- **Network Layer**: This layer is responsible for address assignment and uniquely addressing hosts in a network.
- **Data Link Layer**: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
- **Physical Layer**: This layer defines the hardware, cabling wiring, power output, pulse rate etc.

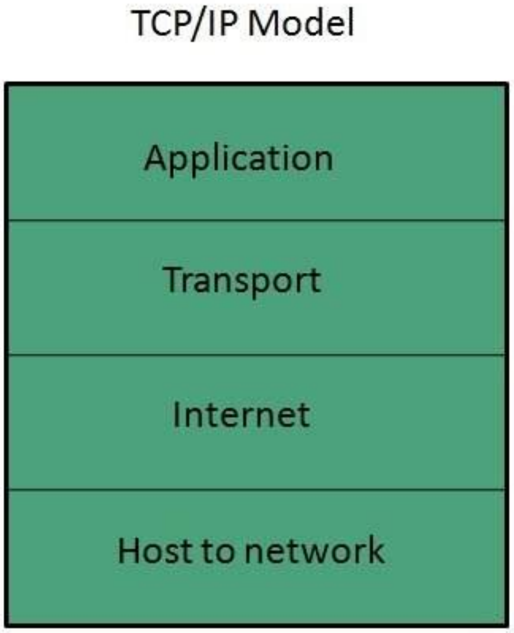
OVERVIEW OF TCP/IP PROTOCOL SUITE

Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but Internet Model is what Internet uses for all its communication. Internet is independent of its underlying network architecture so is its Model.

TCP/IP Model

TCP/IP model is practical model and is used in the Internet. TCP/IP is acronym of Transmission Control Protocol and Internet Protocol.

The **TCP/IP** model combines the two layers (Physical and Data link layer) into one layer i.e. **Host-to-Network** layer. The following diagram shows the various layers of TCP/IP model:



Application Layer

This layer is same as that of the OSI model and performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.
- The functions such as LOGIN or password checking are also performed by the application layer.

Protocols used: TELNET, FTP, SMTP, DN, HTTP, NNTP are the protocols employed in this layer.

Transport Layer

It does the same functions as that of transport layer in OSI model. Here are the key points regarding transport layer:

- It uses **TCP** and **UDP** protocol for end to end transmission.
- TCP is reliable and **connection oriented protocol.**
- TCP also handles flow control.
- The UDP is not reliable and a **connection less protocol** also does not perform flow control.

Protocols used: TCP/IP and **UDP** protocols are employed in this layer.

Internet Layer

The function of this layer is to allow the host to insert packets into network and then make them travel independently to the destination. However, the order of receiving the packet can be different from the sequence they were sent.

Protocols used: Internet Protocol (IP) is employed in Internet layer.

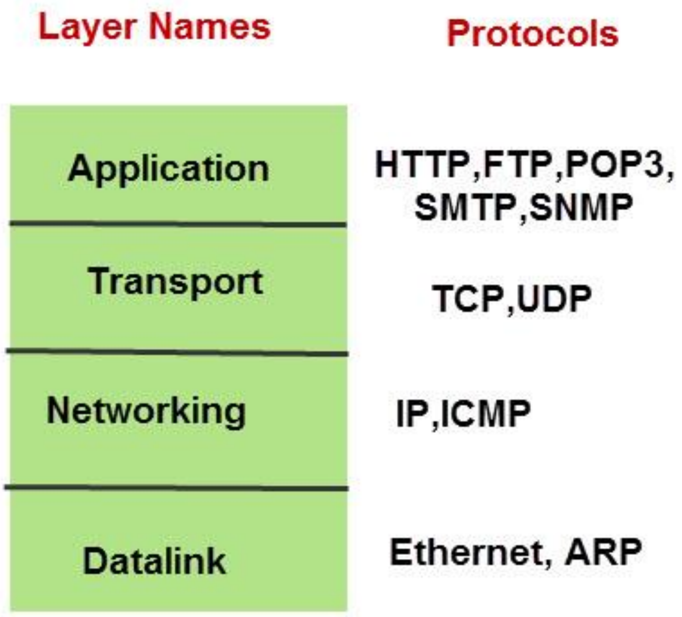
Host-to-Network Layer

This is the lowest layer in TCP/IP model. The host has to connect to network using some protocol, so that it can send IP packets over it. This protocol varies from host to host and network to network.

The TCP/IP Protocol Suite

The TCP/IP protocol suite consists of many protocols that operate at one of 4 layers.

The protocol suite is named after two of the most common protocols – **TCP** (transmission Control Protocol) and **IP** (internet Protocol).



TCP/IP Networking Model

TCP/IP was designed to be independent of networking Hardware and should run across any connection media.

The earliest use, and the most common use is over **Ethernet networks.**

Ethernet is a **2 layer protocol/standard** covering the **physical and data link layer**, shown in the diagram above.

HTTP (hypertext transfer protocol) -This is the workhorse of the Web.

SMTP,POP3,IMap4 – These are email protocols

TCP (Transmission control protocol) is a connection orientated protocol and is used to provides a reliable end to end connection.

UDP (used datagram protocol) is connection less protocol and doesn't guarantee delivery.

Applications will choose which transmission protocol to use based on their function. HTTP, POP3, IMAP4, SMTP and many more use TCP.

UDP is used more in utility applications like DNS, RIP (routing information protocol), DHCP.

IP (Internet Protocol) – This is the main networking protocol. There are two version of IP (IPv4 and IPV6).

ARP (address resolution Protocol) -Translates an IP address to a MAC or physical address.(IP4 networks)

DATA COMMUNICATION FUNDAMENTALS AND TECHNIQUES:

One of the major functions of the physical layer is to move data in the form of electromagnetic signals across a transmission medium.
To be transmitted, data must be transformed to electromagnetic signals.
Analog and digital signal
Both data and the signals that represent them can be either **analog or digital** in form.

ANALOG AND DIGITAL DATA

Data can be analog or digital.
The term **analog data** refers to information that is continuous;
When someone speaks, an analog wave is created in the air. This can be captured by amicrophone and converted to an analog signal or sampled and converted to a digitalsignal.

Digital data refers to information that has discrete states. Analog data, such as the sounds made by a human voice, take on continuous values.

Digital data take on discrete values. For example, data are stored in computermemory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

ANALOG AND DIGITAL SIGNALS

When data is sent over physical medium it needs to be first converted into electromagnetic signals. Data itself canbe analog such as human voice, or digital such as file on the disk. Data (both analog and digital) can berepresented in digital or analog signals.

 Digital Signals

Digital signals are discrete in nature and represents sequence of voltage pulses. Digital signals are used withinthe circuitry of a computer system.

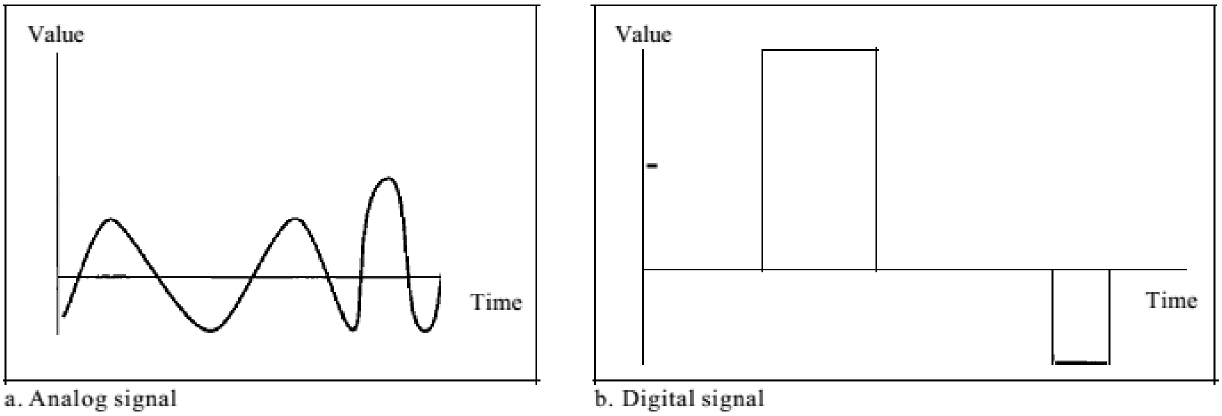
An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value *A* to value *B,* it passes through and includes an infinite number of values along its path.

 Analog Signals
Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.

A digital signal, on the other hand, can have only a limited number of defined values.
Although each value can be any number, it is often as simple as 1 and 0.

Analog and Digital Signals:

Like the data they represent, signals can be either analog or digital. An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value *A* to value *B,* it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and O. The simplest way to show signals is by plotting them on a pair of perpendicular axes. The vertical axis represents the value or strength of a signal. The horizontal axis represents time. Figure below illustrates an analog signal and a digital signal. The curve representing the analog signal passes through an infinite number of points. The vertical lines of the digital signal, however, demonstrate the sudden jump that the signal makes from value to value.



a. Analog signal b. Digital signal

Comparison of analog and digital signals

Periodic and Nonperiodic Signals:

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.

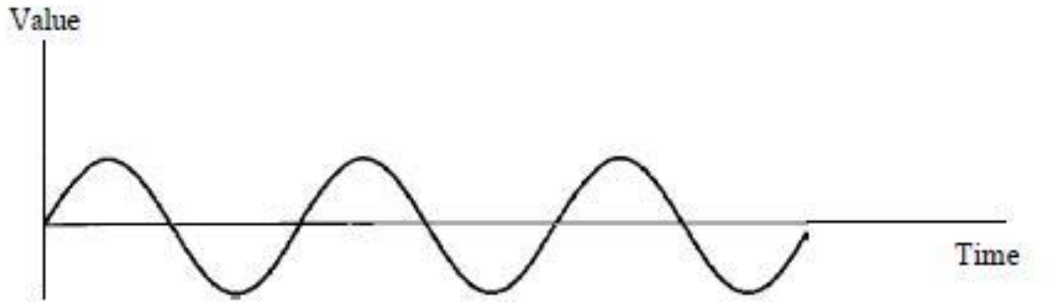
PERIODIC ANALOG SIGNALS:

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.

Sine Wave

The sine wave is the most fundamental form of a periodic analog signal. When we visualize it as a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow. Figure below shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it.

A sine wave

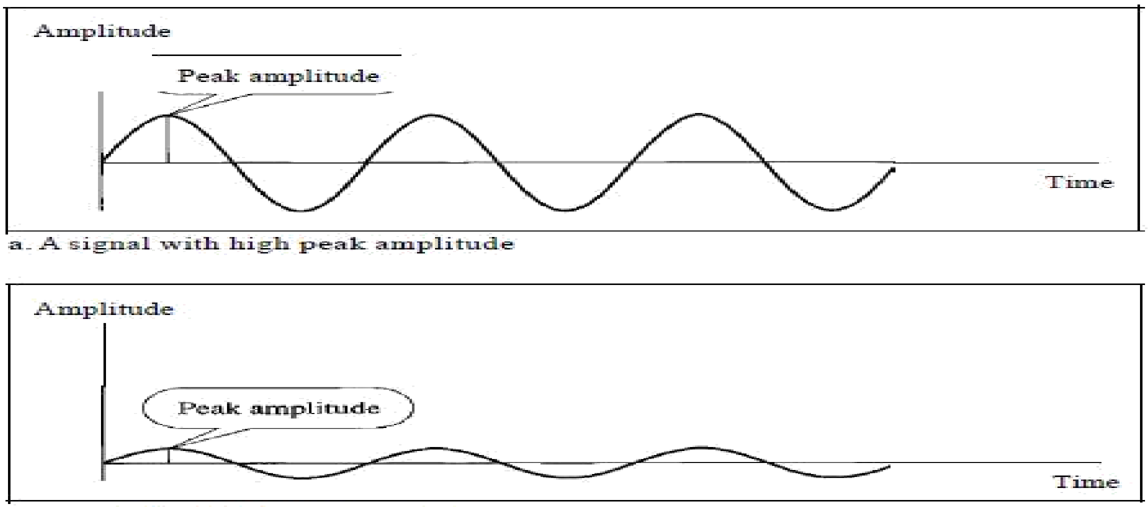


Characteristics of Signals:

1. ***Peak Amplitude***

The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries. For electric signals, peak amplitude is normally measured in *volts.* Figure below shows two signals and their peak amplitudes.

Two signals with the same phase and frequency, but different amplitudes



a. A signal with high peak amplitude

b. A signal with low peak amplitude

2. ***Period and Frequency***

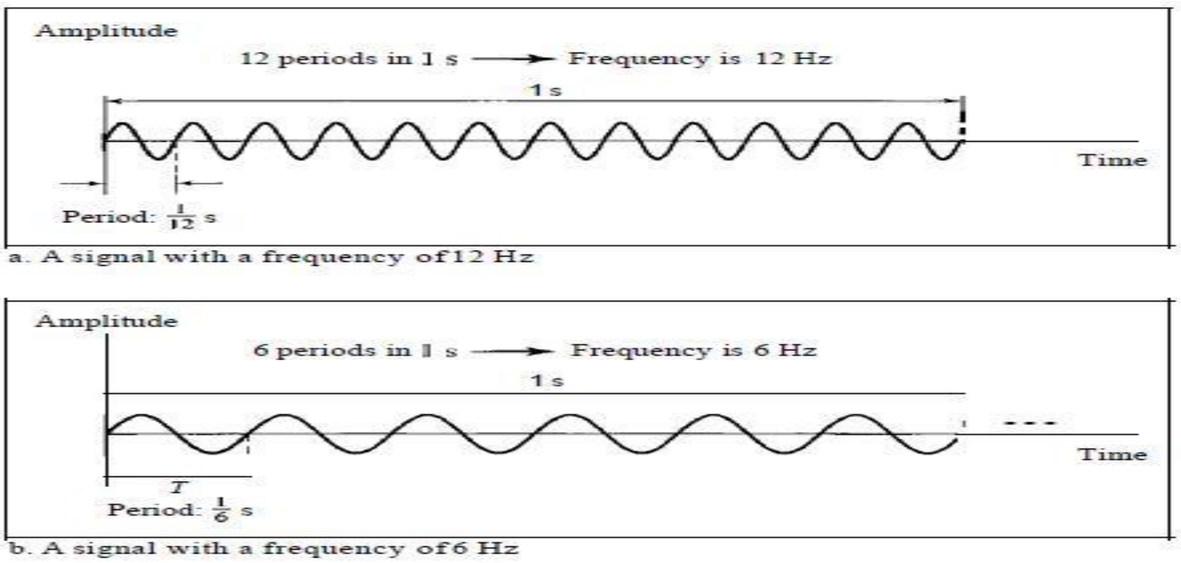
Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle.

Frequency refers to the number of periods in I s. Note that period and frequency are just one characteristic defined in two ways. Period is the inverse of frequency, and frequency is the inverse of period, as the following formulas show.

f=1/T and T=1/f

Period is formally expressed in seconds. Frequency is formally expressed in Hertz (Hz), which is cycle per second.

Two signals with the same amplitude and phase, but different frequencies



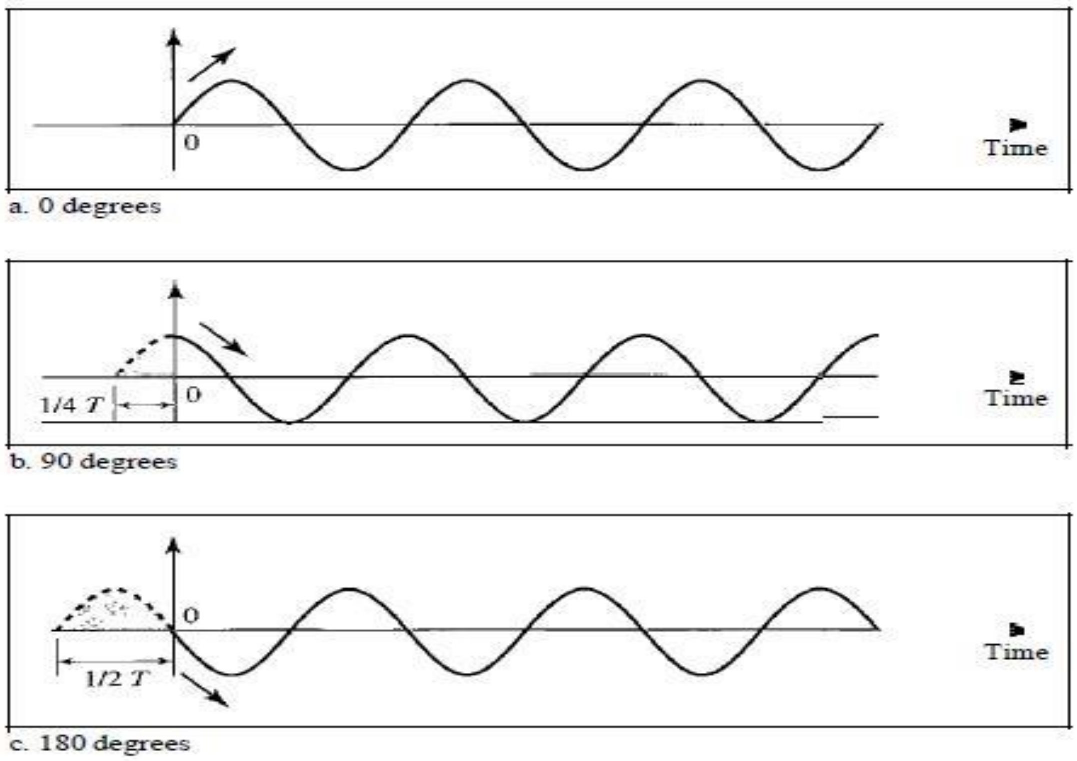
a. A signal with a frequency of12 Hz

b. A signal with a frequency of6 Hz

3. ***Phase***

The term phase describes the position of the waveform relative to time O. If we think of the wave as something that can be shifted backward or forward along the time axis, phase describes the amount of that shift. It indicates the status of the first cycle. Phase is measured in degrees or radians [360° is *2n* rad; 1° is *2n/360* rad, and 1 rad is *360/(2n)]*. A phase shift of 360° corresponds to a shift of a complete period; a phase shift of 180° corresponds to a shift of one-half of a period; and a phase shift of 90° corresponds to a shift of one-quarter of a period.

Three sine waves with the same amplitude andfrequency, but differentphases



a. 0 degrees

b. 90 degrees

c. 180 degrees

I. A sine wave with a phase of 0° starts at time 0 with a zero amplitude. The amplitude is increasing.
II. A sine wave with a phase of 90° starts at time 0 with a peak amplitude. The amplitude is decreasing.
III. A sine wave with a phase of 180° starts at time 0 with a zero amplitude. The amplitude is decreasing.

4. ***Wavelength***

Wavelength is another characteristic of a signal traveling through a transmission medium. Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium. While the frequency of a signal is independent of the medium, the wavelength depends on both the frequency and the medium. Wavelength is a property of any type of signal. In data communications, we often use wavelength to describe the transmission of light in an optical fiber. The wavelength is the distance a simple signal can travel in one period. Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal. However, since period and frequency are related to each other, if we represent wavelength by λ, propagation speed by c (speed of light), and frequency by *f*, we get Wavelength=Propagation speed * Period = propagation speed/frequency

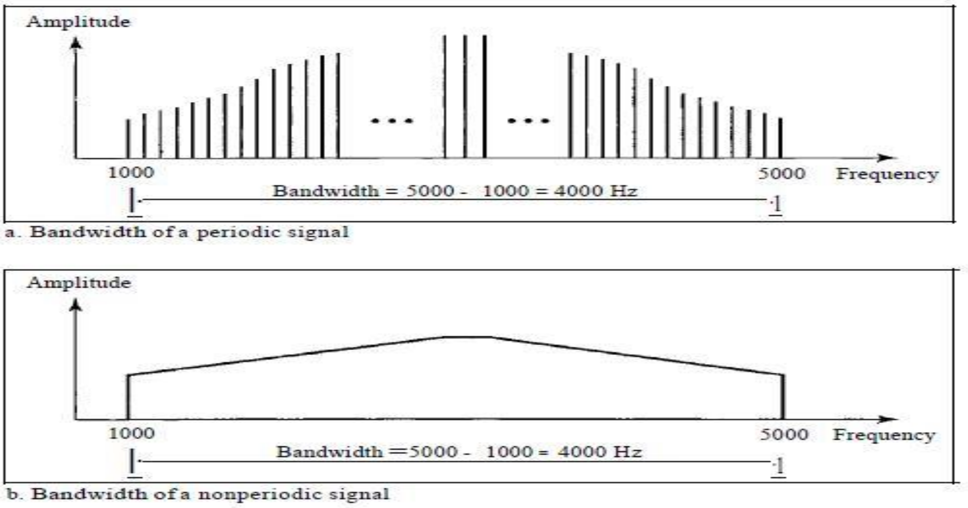
$$\lambda = c/f$$

The wavelength is normally measured in micrometers (microns) instead of meters.

Bandwidth

The range of frequencies contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 - 1000, or 4000. Figure 3.12 shows the concept of bandwidth. The figure depicts two composite signals, one periodic and the other nonperiodic. The bandwidth of the periodic signal contains all integer frequencies between 1000 and 5000 (1000, 100 I, 1002, ...). The bandwidth of the nonperiodic signals has the same range, but the frequencies are continuous.

Figure 3.12 *The bandwidth ofperiodic and nonperiodic composite signals*



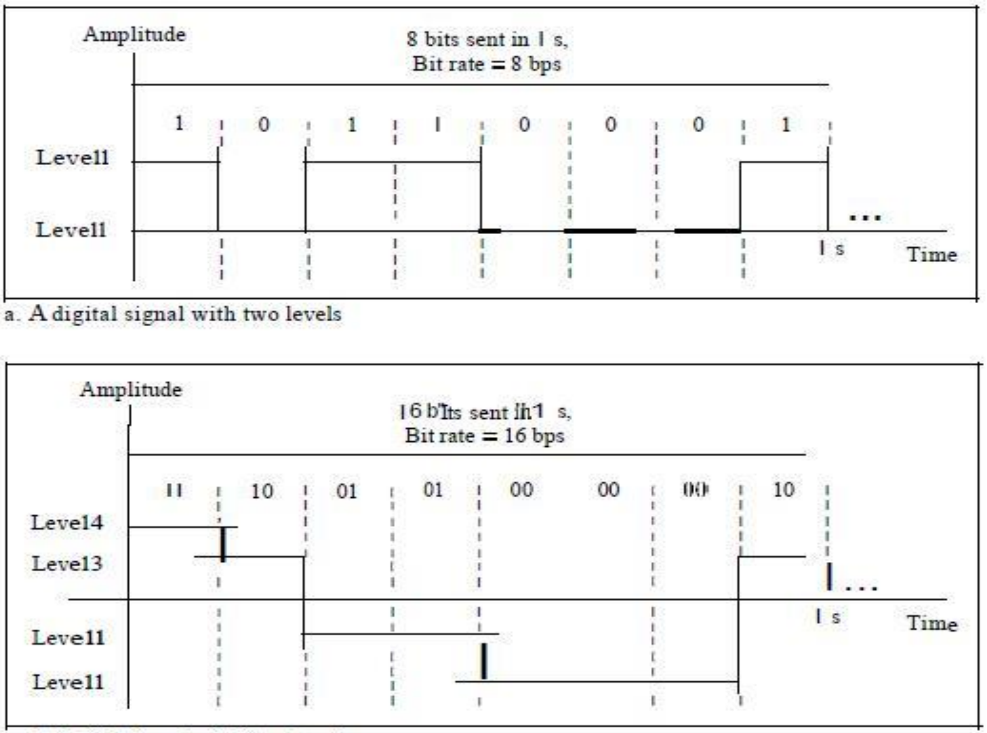
a. Bandwidth of a periodic signal

b. Bandwidth of a nonperiodic signal

DIGITAL SIGNALS

In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level. Figure 3.16 shows two signals, one with two levels and the other with four.

Figure 3.16 *Two digital signals: one with two signal levels and the other with four signal levels*



a. A digital signal with two levels

b. A digital signal with four levels

We send 1 bit per level in part a of the figure and 2 bits per level in part b of the figure. In general, if a signal has *L* levels, each level needs *log2L* bits.

Bit Rate

Most digital signals are nonperiodic, and thus period and frequency are not appropriate characteristics. Another *term-bit rate is* used to describe digital signals. The bit rate is the number of bits sent in 1s, expressed in bits per second (bps). Figure 3.16 shows the bit rate for two signals.

Bit Length

We discussed the concept of the wavelength for an analog signal: the distance one cycle occupies on the transmission medium. We can define something similar for a digital signal: the bit length. The bit length is the distance one bit occupies on the transmission medium.

Bit length =propagation speed x bit duration

DATA RATE LIMITS

A very important consideration in data communications is how fast we can send data, in bits per second. over a channel. Data rate depends on three factors:

1. The bandwidth available

2. The level of the signals we use

3. The quality of the channel (the level of noise)

Two theoretical formulas were developed to calculate the data rate: one by **Nyquist** for a noiseless channel. another by **Shannon** for a noisy channel.

Noiseless Channel: Nyquist Bit Rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

$$\textbf{BitRate = 2 x bandwidth x 10g2 } L$$

In this formula, bandwidth is the bandwidth of the channel, *L* is the number of signal levels used to represent data, and BitRate is the bit rate in bits per second. According to the formula, we might think that, given a specific bandwidth, we can have any bit rate we want by increasing the number of signa11eve1s. Although the idea is theoretically correct, practically there is a limit. When we increase the number of signal1eve1s, we impose a burden on the receiver. If the number of levels in a signal is just 2, the receiver can easily distinguish between a 0 and a 1. If the level of a signal is 64, the receiver must be very sophisticated to distinguish between 64 different levels. In other words, increasing the levels of a signal reduces the reliability of the system.

Noisy Channel: Shannon Capacity

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

$$\textbf{Capacity =bandwidth X log2 (1 +SNR)}$$

In this formula, bandwidth is the bandwidth of the channel, SNR is the signal-to-noise ratio, and capacity is the capacity of the channel in bits per second. Note that in the Shannon formula there is no indication of the signal level, which means that no matter how many levels we have, we cannot achieve a data rate higher than the capacity of the channel. In other words, the formula defines a characteristic of the channel, not the method of transmission.

Bandwidth in Bits per Seconds

The term *bandwidth* can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

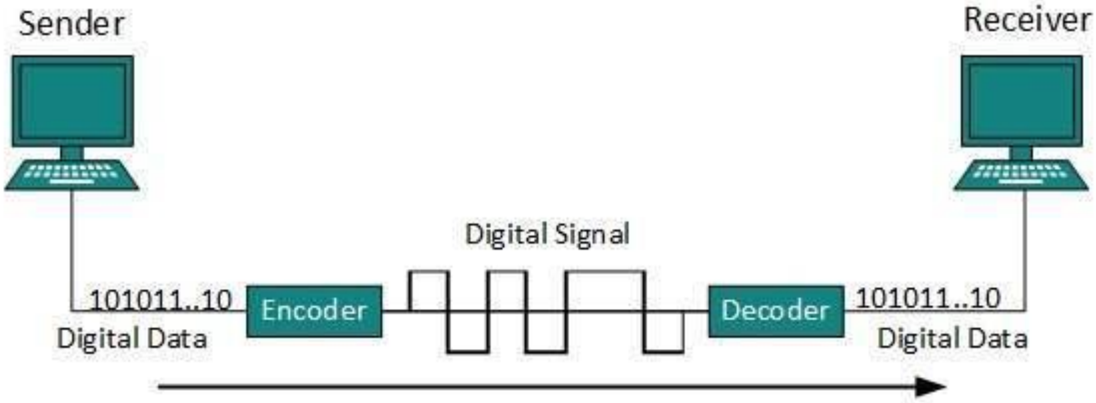
DIGITAL TO DIGITAL LINE ENCODING SCHEMES

Data or information can be stored in two ways, analog and digital. For a computer to use that data is must

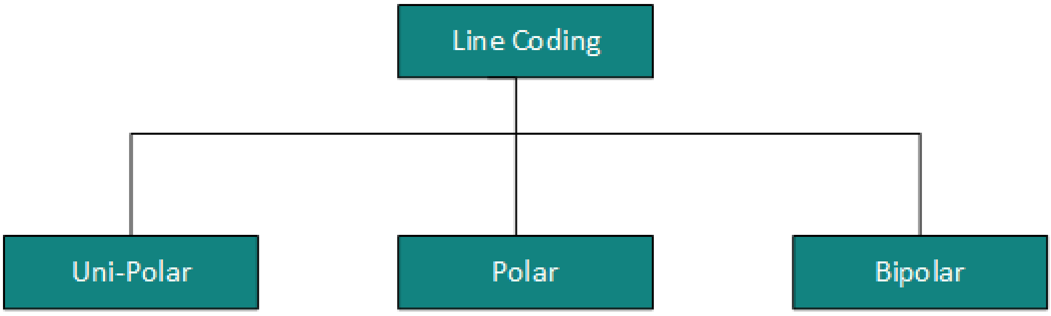
be in discrete digital form. Like data, signals can also be in analog and digital form. To transmit data digitally it needs to be first converted to digital form.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format.It is represented (stored) internally as series of 1s and 0s.

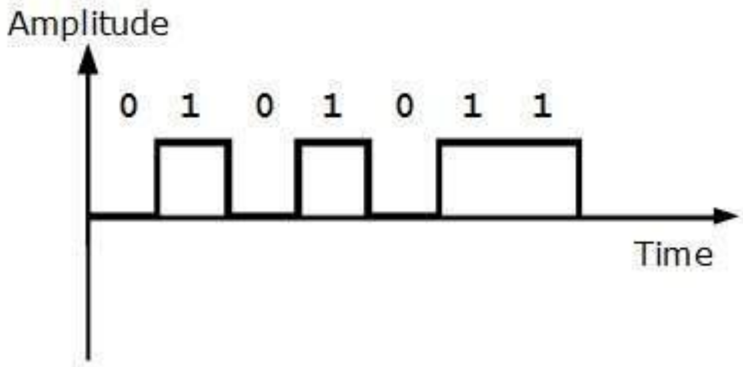


Digital signal is denoted by discreet signal, which represents digital data.Thereare three types of line coding schemes available:



Uni-polar Encoding

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.

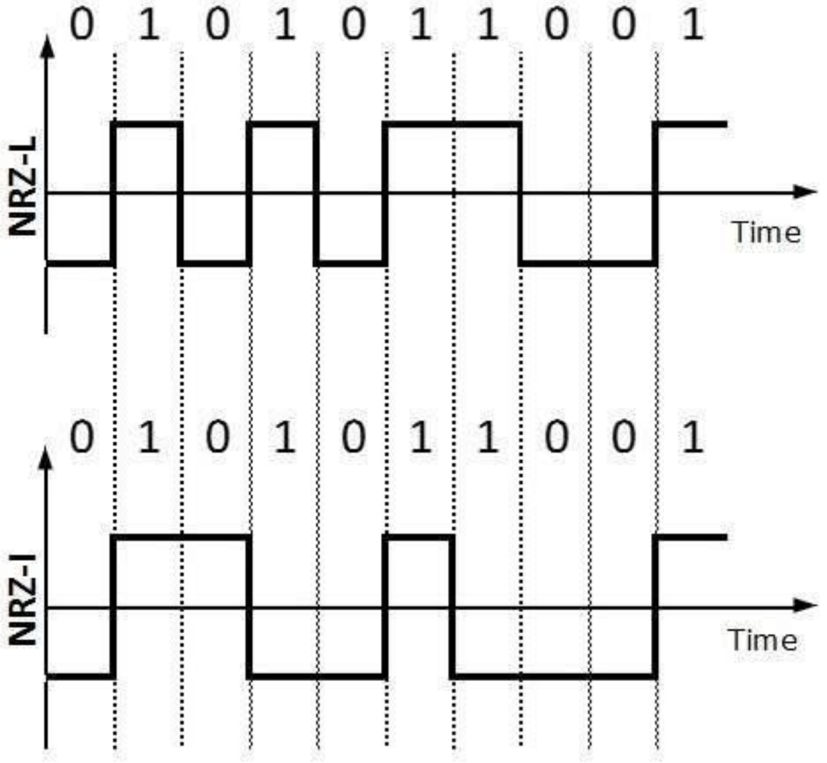


Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

- **Polar Non-Return to Zero (Polar NRZ)**

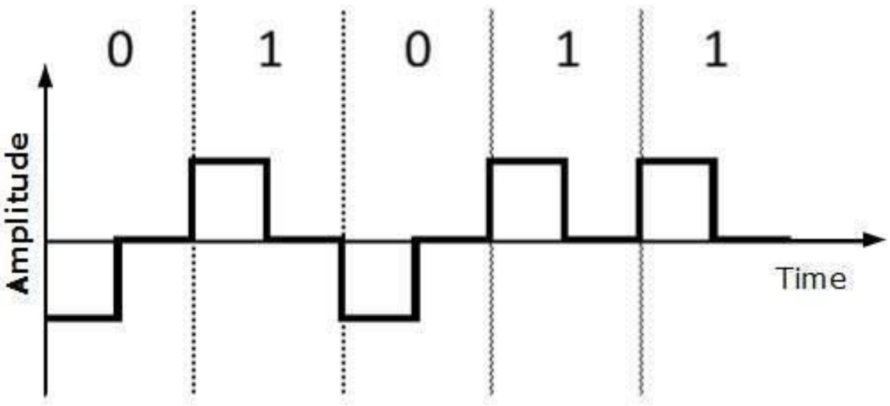
It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition. NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

- **Return to Zero (RZ)**

Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver’s clock are not synchronized.



RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

- **Manchester**

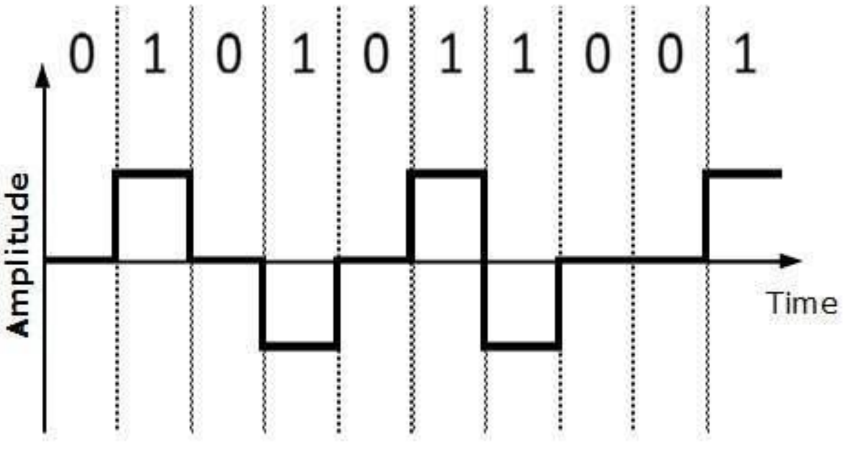
This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

- **Differential Manchester**

This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Block Coding

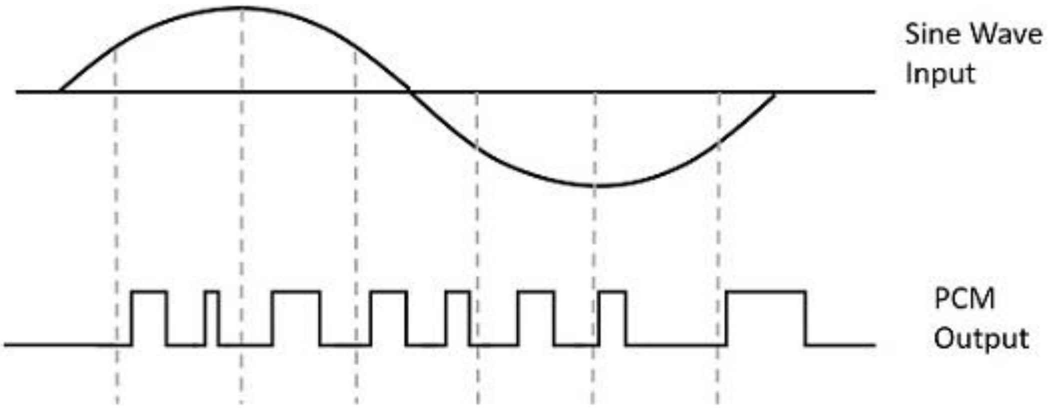
To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.

PULSE CODE MODULATION

Modulation is the process of varying one or more parameters of a carrier signal in accordance with the instantaneous values of the message signal.

The message signal is the signal which is being transmitted for communication and the carrier signal is a high frequency signal which has no data, but is used for long distance transmission.
There are many modulation techniques, which are classified according to the type of modulation employed. Of them all, the digital modulation technique used is **Pulse Code Modulation (PCM)**.

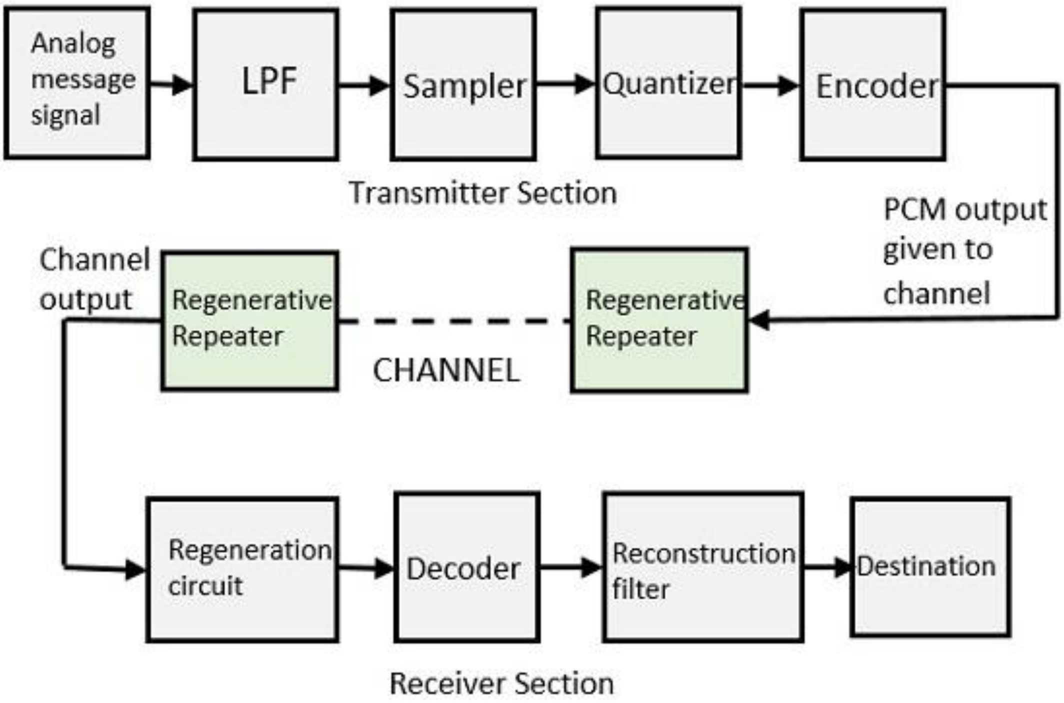
A signal is pulse code modulated to convert its analog information into a binary sequence, i.e., **1s** and **0s**. The output of a PCM will resemble a binary sequence. The following figure shows an example of PCM output with respect to instantaneous values of a given sine wave.



Instead of a pulse train, PCM produces a series of numbers or digits, and hence this process is called as **digital**. Each one of these digits, though in binary code, represent the approximate amplitude of the signal sample at that instant.

In Pulse Code Modulation, the message signal is represented by a sequence of coded pulses. This message signal is achieved by representing the signal in discrete form in both time and amplitude.

Basic Elements of PCM
The transmitter section of a Pulse Code Modulator circuit consists of **Sampling, Quantizing** and **Encoding**, which are performed in the analog-to-digital converter section. The low pass filter prior to sampling prevents aliasing of the message signal.
The basic operations in the receiver section are **regeneration of impaired signals, decoding,** and **reconstruction** of the quantized pulse train. Following is the block diagram of PCM which represents the basic elements of both the transmitter and the receiver sections.



Low Pass Filter

This filter eliminates the high frequency components present in the input analog signal which is greater than the highest frequency of the message signal, to avoid aliasing of the message signal.

Sampler

This is the technique which helps to collect the sample data at instantaneous values of message signal, so as to reconstruct the original signal. The sampling rate must be greater than twice the highest frequency component **W**of the message signal, in accordance with the sampling theorem.

Quantizer

Quantizing is a process of reducing the excessive bits and confining the data. The sampled output when given to Quantizer, reduces the redundant bits and compresses the value.

Encoder

The digitization of analog signal is done by the encoder. It designates each quantized level by a binary code. The sampling done here is the sample-and-hold process. These three sections (LPF, Sampler, and Quantizer) will act as an analog to digital converter. Encoding minimizes the bandwidth used.

Regenerative Repeater

This section increases the signal strength. The output of the channel also has one regenerative repeater circuit, to compensate the signal loss and reconstruct the signal, and also to increase its strength.

Decoder

The decoder circuit decodes the pulse coded waveform to reproduce the original signal. This circuit acts as the demodulator.

Reconstruction Filter

After the digital-to-analog conversion is done by the regenerative circuit and the decoder, a low-pass filter is employed, called as the reconstruction filter to get back the original signal.

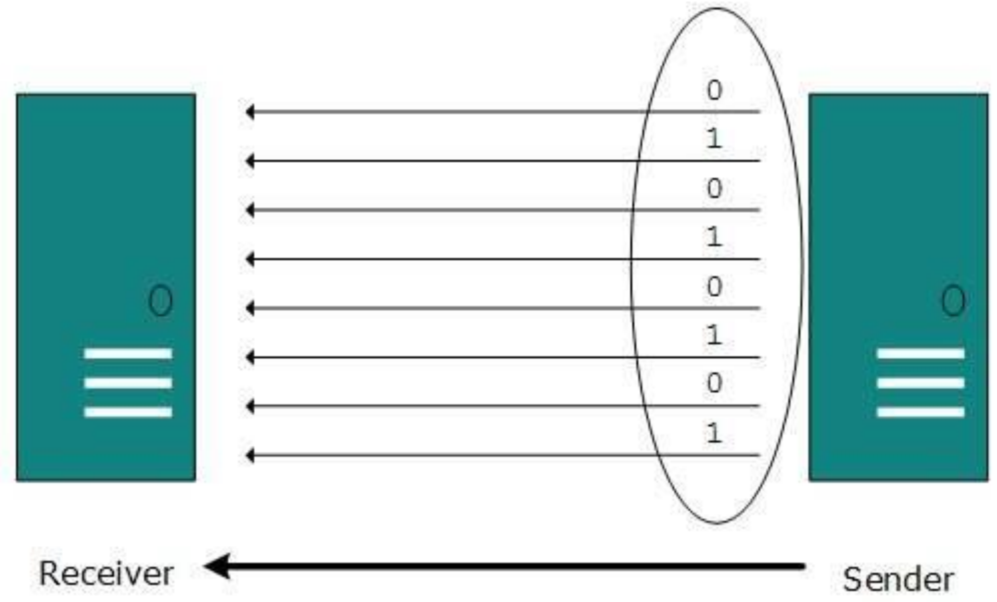
Hence, the Pulse Code Modulator circuit digitizes the given analog signal, codes it and samples it, and then transmits it in an analog form. This whole process is repeated in a reverse pattern to obtain the original signal.

PARALLEL AND SERIAL TRANSMISSION

Transmission Modes

The transmission mode decides how data is transmitted between two computers.The binary data in the form of 1s and 0s can be sent in two different modes: Parallel and Serial.

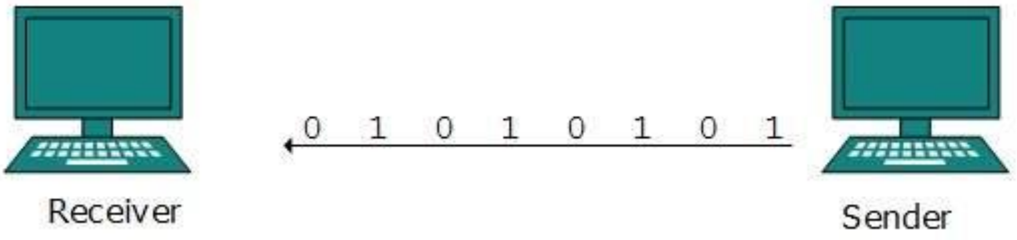
Parallel Transmission



The binary bits are organized in-to groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines.Because the data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go. Advantage of Parallel transmission is high speed and disadvantage is the cost of wires, as it is equal to the number of bits sent in parallel.

Serial Transmission

In serial transmission, bits are sent one after another in a queue manner. Serial transmission requires only one communication channel.



Serial transmission can be either asynchronous or synchronous.

Asynchronous Serial Transmission
It is named so because there'is no importance of timing. Data-bits have specific pattern and they help receiver recognize the start and end data bits.For example, a 0 is prefixed on every data byte and one or more 1s are added at the end.

Two continuous data-frames (bytes) may have a gap between them.

Synchronous Serial Transmission
Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits.There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes (8-bits). Single burst of data bits may contain a number of bytes. Therefore, timing becomes very important.

It is up to the receiver to recognize and separate bits into bytes.The advantage of synchronous transmission is high speed, and it has no overhead of extra header and footer bits as in asynchronous transmission.

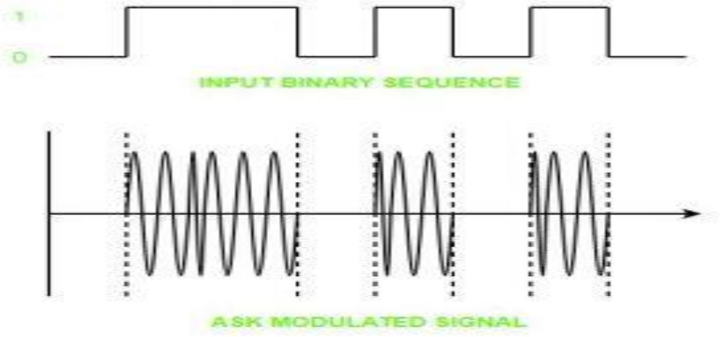
DIGITAL-TO-ANALOG CONVERSION

Digital Signal – A digital signal is a signal that represents data as a sequence of discrete values; at any given time it can only take on one of a finite number of values.

Analog Signal – An analog signal is any continuous signal for which the time varying feature of the signal is a representation of some other time varying quantity i.e., analogous to another time varying signal.
The following techniques can be used for Digital to Analog Conversion:

1. Amplitude Shift keying – Amplitude Shift Keying is a technique in which carrier signal is analog and data to be modulated is digital. The amplitude of analog carrier signal is modified to reflect binary data.

The binary signal when modulated gives a zero value when the binary data represents 0 while gives the carrier output when data is 1. The frequency and phase of the carrier signal remain constant.



Advantages of amplitude shift Keying –

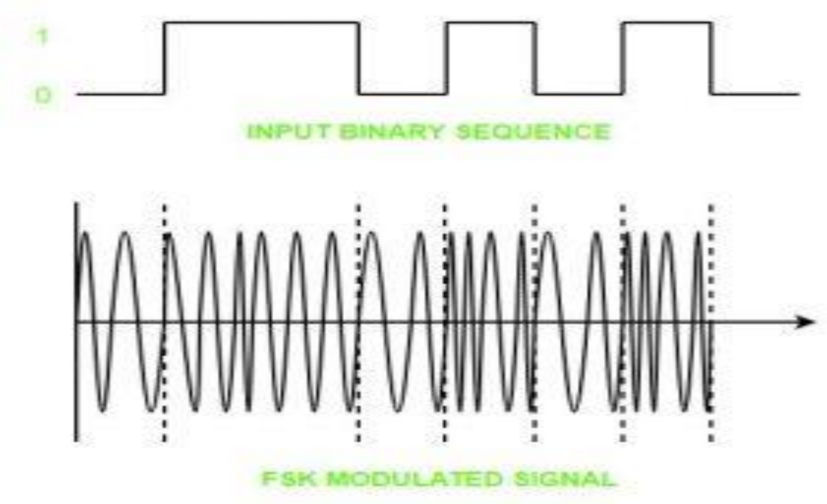
- It can be used to transmit digital data over optical fiber.
- The receiver and transmitter have a simple design which also makes it comparatively inexpensive.
- It uses lesser bandwidth as compared to FSK thus it offers high bandwidth efficiency.

Disadvantages of amplitude shift Keying –

- It is susceptible to noise interference and entire transmissions could be lost due to this.
- It has lower power efficiency.

2. Frequency Shift keying – In this modulation the frequency of analog carrier signal is modified to reflect binary data.

The output of a frequency shift keying modulated wave is high in frequency for a binary high input and is low in frequency for a binary low input. The amplitude and phase of the carrier signal remain constant.



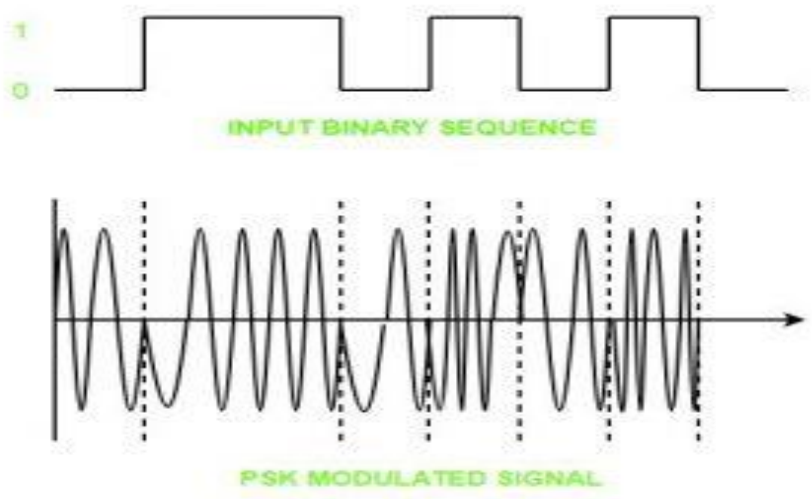
Advantages of frequency shift Keying –

- Frequency shift keying modulated signal can help avoid the noise problems beset by ASK.
- It has lower chances of an error.
- It provides high signal to noise ratio.
- The transmitter and receiver implementations are simple for low data rate application.

Disadvantages of frequency shift Keying –

- It uses larger bandwidth as compared to ASK thus it offers less bandwidth efficiency.
- It has lower power efficiency.

3. Phase Shift keying – In this modulation the phase of the analog carrier signal is modified to reflect binary data.The amplitude and frequency of the carrier signal remains constant.



It is further categorized as follows:

1. **Binary Phase Shift Keying (BPSK):**
   BPSK also known as phase reversal keying or 2PSK is the simplest form of phase shift keying. The Phase of the carrier wave is changed according to the two binary inputs. In Binary Phase shift keying, difference of 180 phase shift is used between binary 1 and binary 0.
   This is regarded as the most robust digital modulation technique and is used for long distance wireless communication.
2. **Quadrature phase shift keying:**
   This technique is used to increase the bit rate i.e we can code two bits onto one single element. It uses four phases to encode two bits per symbol. QPSK uses phase shifts of multiples of 90 degrees.
   It has double data rate carrying capacity compare to BPSK as two bits are mapped on each constellation points.

Advantages of phase shift Keying –

- It is a more power efficient modulation technique as compared to ASK and FSK.
- It has lower chances of an error.
- It allows data to be carried along a communication signal much more efficiently as compared to FSK.

Disadvantages of phase shift Keying –

- It offers low bandwidth efficiency.
- The detection and recovery algorithms of binary data is very complex.
- It is a non coherent reference signal.

MULTIPLEXING

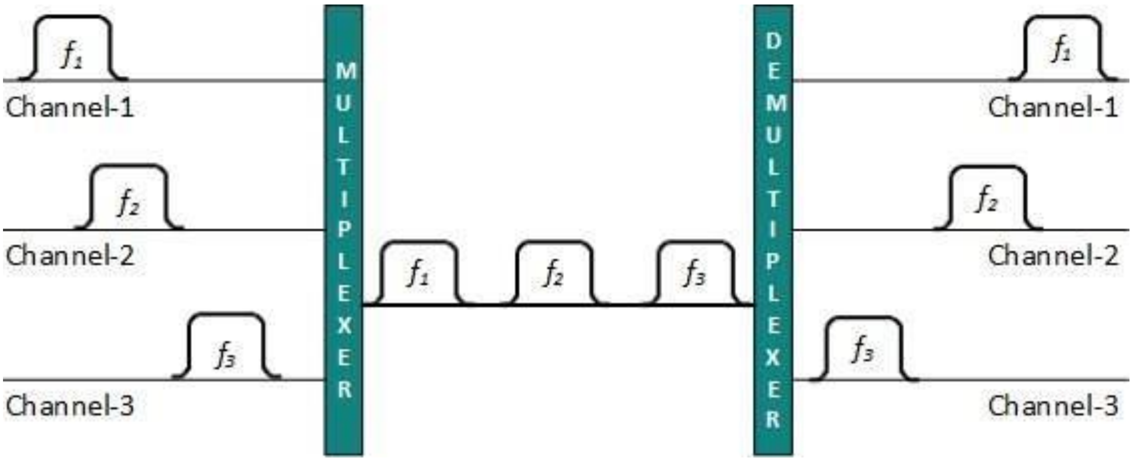
Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.

When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

FREQUENCY DIVISION MULTIPLEXING

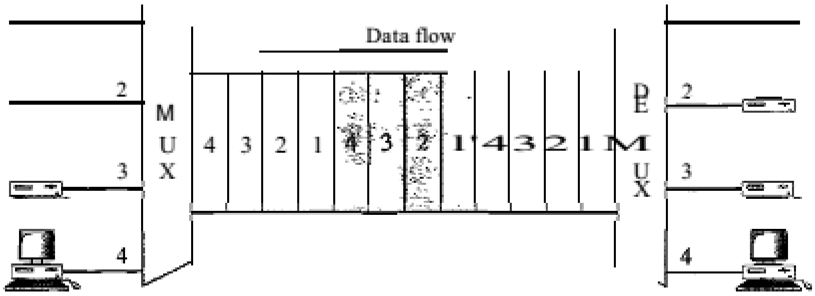
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



TIME DIVISION MULTIPLEXING

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a linle Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. Figure 6.12 gives a conceptual view of TDM. Note that the same link is used as in FDM; here, however, the link is shown sectioned by time rather than by frequency. In the figure, portions of signals 1,2,3, and 4 occupy the link sequentially.

Figure 6.12 *TDM*



Note that in Figure 6.12 we are concerned with only multiplexing, not switching. This means that all the data in a message from source 1 always go to one specific desti nation, be it 1, 2, 3, or 4. The delivery is fixed and unvarying, unlike switching.

We also need to remember that TDM is, in principle, a digital multiplexing technique. Digital data from different sources are combined into one timeshared link. However, this does not mean that the sources cannot produce analog data; analog data can be sampled, changed to digital data, and then multiplexed by using TDM.

TDM is a digital multiplexing technique for combining several low-rate channels into one high-rate one.

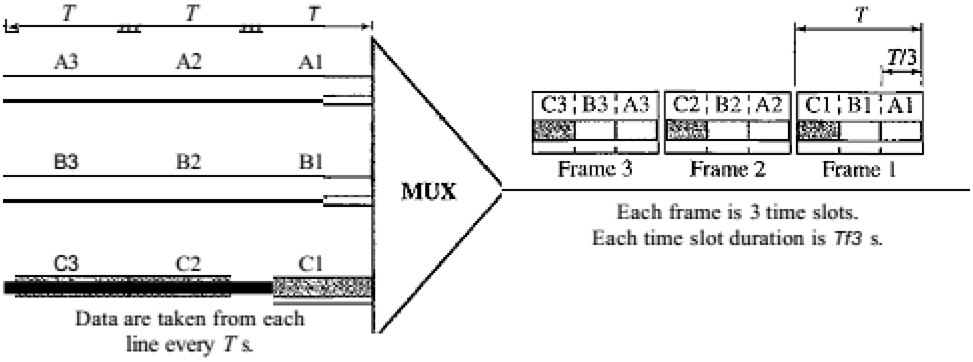
We can divide TDM into two different schemes: **synchronous and statistical.** We first discuss synchronous TDM and then show how statistical TDM differs.

Synchronous Time-Division Multiplexing

In synchronous TDM, each input connection has an allotment in the output even if it is not sending data.

Time Slots and Frames In synchronous TDM, the data flow of each input connection is divided into units, where each input occupies one input time slot. A unit can be 1 bit, one character, or one block of data. Each input unit becomes one output unit and occupies one output time slot. How ever, the duration of an output time slot is *n* times shorter than the duration of an input time slot. If an input time slot is *T* s, the output time slot is *Tin* s, where *n* is the number of connections. In other words, a unit in the output connection has a shorter duration; it travels faster. Figure 6.13 shows an example of synchronous TDM where *n* is 3.

Figure 6.13 *Synchronous time-division multiplexing*



In synchronous TDM, a round of data units from each input connection is collected into a frame (we will see the reason for this shortly). If we have *n* connections, a frame is divided into *n* time slots and one slot is allocated for each unit, one for each input line. If the duration of the input unit is *T*, the duration of each slot is *Tin* and the duration of each frame is *T* (unless a frame carries some other information, as we will see shortly).

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

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

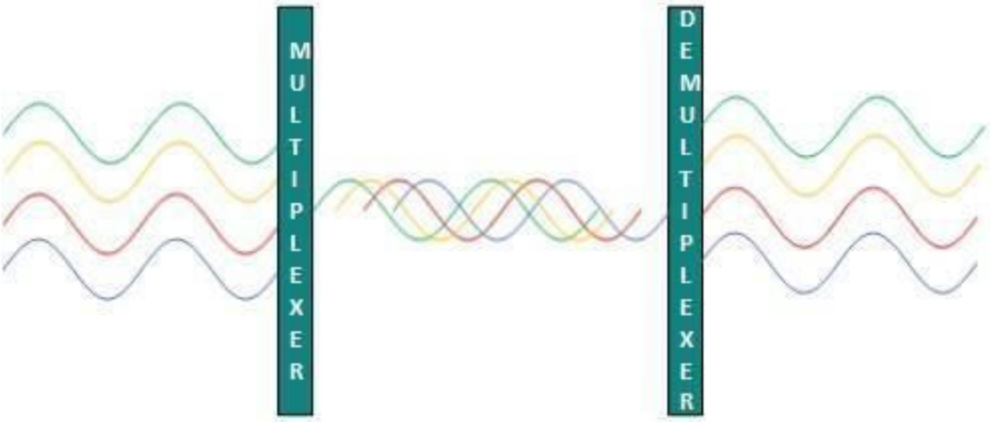
Time slots are grouped into frames. A frame consists of one complete cycle of time slots, with one slot dedicated to each sending device. In a system with *n* input lines, each frame has *n* slots, with each slot allocated to carrying data from a specific input line.

Statistical Time-Division Multiplexing

in synchronous TDM, each input has a reserved slot in the output frame. This can be inefficient if some input lines have no data to send. In statistical time-division multiplexing, slots are dynamically allocated to improve bandwidth efficiency. Only when an input line has a slot's worth of data to send is it given a slot in the output frame. In statistical multiplexing, the number of slots in each frame is less than the number of input lines. The multiplexer checks each input line in roundrobin fashion; it allocates a slot for an input line if the line has data to send; otherwise, it skips the line and checks the next line.

Wavelength Division Multiplexing

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.



Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

TRANSMISSION MEDIA

The transmission media is nothing but the physical media over which communication takes place in computer networks.

The medium over which the information between two computer systems is sent, called Transmission Media.

Transmission media comes in two forms.

Guided Media

All communication wires/cables comes into this type of media, such as UTP, Coaxial and Fiber Optics. In this media the sender and receiver are directly connected and the information is send (guided) through it.

- **Twisted Pair Cable**
- **Coaxial Cable**
- **Fiber Optics**

 Unguided Media

Wireless or open air space is said to be unguided media, because there is no connectivity between the sender and receiver. Information is spread over the air, and anyone including the actual recipient may collect the information.

- **Radio waves**
- **Micro waves**
- **Infrared waves**

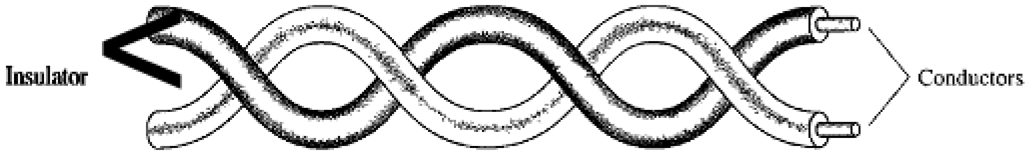
Twisted Pair Cable

A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires, only one carries actual signal and another is used for ground reference. The twists between wires are helpful in reducing noise (electro-magnetic interference) and crosstalk.

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

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

Figure 7.3 *Twisted-pair cable*

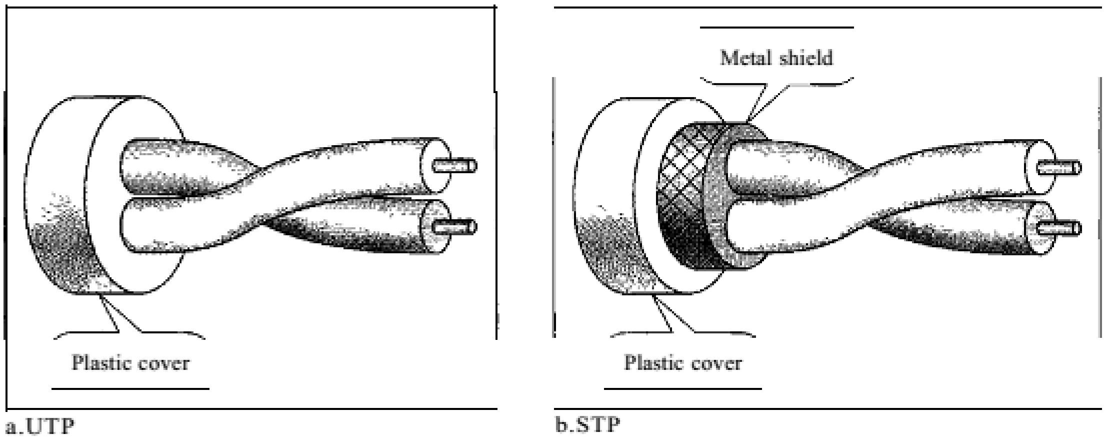


Applications Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office---commonly consists of unshielded twisted-pair cables

There are two types of twisted pair cables:

- Shielded Twisted Pair (STP) Cable
- Unshielded Twisted Pair (UTP) Cable

Figure 7.4 *UTP and STP cables*



STP cables comes with twisted wire pair covered in metal foil. This makes it more indifferent to noise and crosstalk.

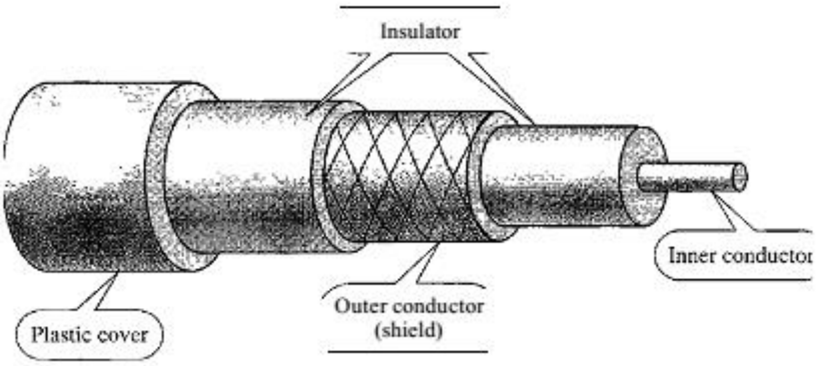
UTP has seven categories, each suitable for specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.

Coaxial Cable

Coaxial cable has two wires of copper. The core wire lies in the center and it is made of solid conductor. The core is enclosed in an insulating sheath. The second wire is wrapped around over the sheath and that too in turn encased by insulator sheath. This all is covered by plastic cover.

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

Figure 7.7 *Coaxial cable*



Because of its structure, the coax cable is capable of carrying high frequency signals than that of twisted pair cable. The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.

There are three categories of coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet), and RG-11 (Thick Ethernet). RG stands for Radio Government.

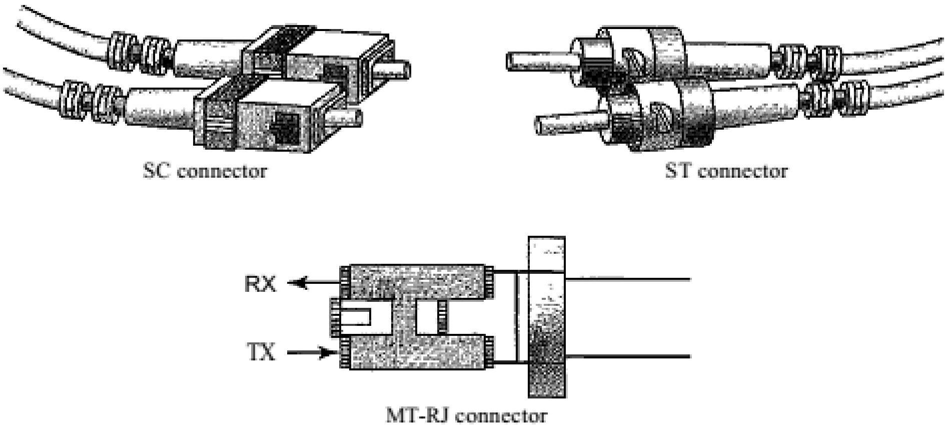
Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.

Fiber Optics

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.

Fiber Optic provides the highest mode of speed. It comes in two modes; one is single mode fiber and second is multimode fiber. Single mode fiber can carry a single ray of light whereas multimode is capable of carrying multiple beams of light.

Figure 7.15 *Fiber-optic cable connectors*



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

MT-RJ is a connector that is the same size as RJ45.

Fiber Optic also comes in unidirectional and bidirectional capabilities. To connect and access fiber optic special type of connectors are used. These can be Subscriber Channel (SC), Straight Tip (ST), or MT-RJ.

UnGuided Transmission Media

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

We can divide wireless transmission into three broad groups:

1. Radio waves
2. Micro waves
3. Infrared waves

Radio Waves

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.

Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

Radio waves, particularly with those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Omnidirectional Antenna for Radio Waves

Radio waves use omnidirectional antennas that send out signals in all directions.

Applications of Radio Waves

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

Micro Waves

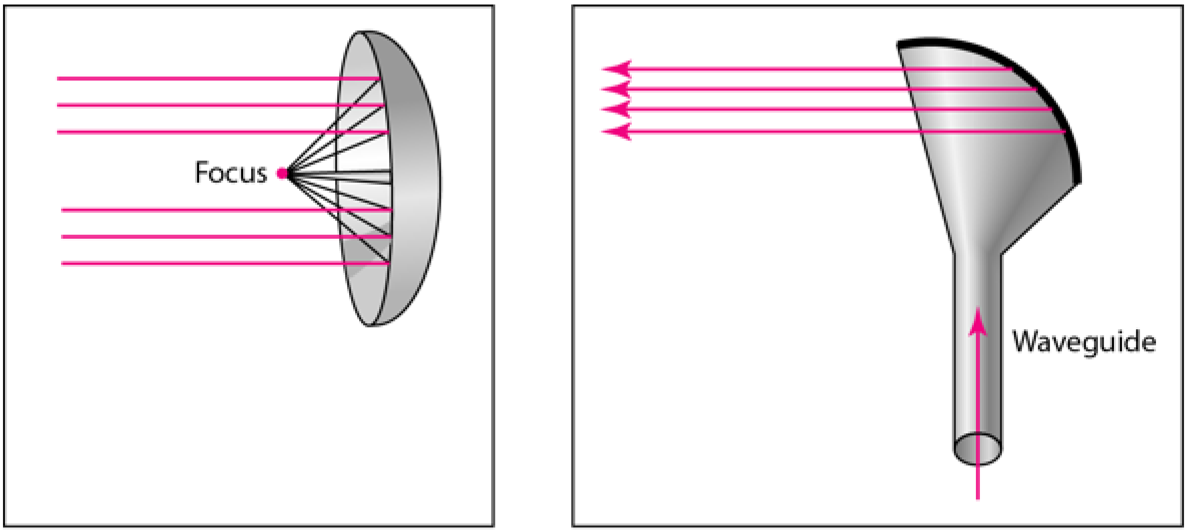
Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

The following describes some characteristics of microwaves propagation:

- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside the buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned and a high date rate is possible.
- Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna for Micro Waves

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: **Parabolic Dish** and **Horn**.



a. Dish antenna

b. Horn antenna

A parabolic antenna works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications of Micro Waves

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

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another, a short-range communication system in on room cannot be affected by another system in the next room.

When we use infrared remote control, we do not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications of Infrared Waves

- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.
- The Infrared Data Association(IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mouse, PCs and printers.
- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

POSSIBLE QUESTIONS

UNIT-I

PART-A (20 MARKS)

(Q.NO 1 TO 20 Online Examination)

PART-B (2 MARKS)

1. Define Network and Internet.
2. Mention the components of Data communication Systems.
3. What is protocol?
4. Define Simplex and Duplex Communication.
5. List out the network topologies.
6. What is UDP and SMTP?
7. Define analog and digital signal.
8. What is Modulation?
9. Mention the basic elements of PCM.
10. Define parallel and serial transmission.

PART-C (6 MARKS)

1. Explain about the network topologies with neat diagram.
2. Give a detailed description about the Network Classifications
3. Draw a neat sketch of OSI Reference Model and explain in detail.
4. Describe about TCP/IP protocol suite with neat diagram.
5. Explain Date Rate limits.
6. Discuss about Digital to Digital Line Encoding Schemes with neat sketch.
7. Illustrate PCM with neat diagram.
8. Explain about Parallel and Serial Transmission.

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CS Batch:2017

Subject:COMPUTER NETWORKS

SubCode:17CSU303

UNIT I

S.NO	QUESTION	CHOICE1	CHOICE2	CHOICE3	CHOICE4	ANS
1	Data communication means exchange of data between devices.	one	two	six	four	two
2	The combination of two or more networks are called _________	Internetwork	LAN	WAN	MAN	Internetwork
3	A______ is the set of rules.	protocols	transmission medium	networks	ip	protocols
4	In__________, the communication is unidirection.	duplex mode	full duplex mode	half duplex mode	simplex mode	simplex mode
5	A________is a set of devices connected by communication links.	protocols	networks	computer	printer	networks
6	A______connection provides a dedicated link between two devices.	point-to-point	multi-point	mesh	physical	point-to-point
7	One long cable acts as a ______to link all the devices in a network.	bus	mesh	hub	backbone	backbone
8	MAN stands for _________	metropolitician area network	metropolitan area network	metropolitical area network	macro area network	metropolitan area network
9	A ______ can be a device which is capable of sending or receiving data	node	data	bit	link	node
10	The multipoint topology is ________	Bus	Star	Mesh	Ring	Bus
11	In physical layer we can transfer data into ___________	frame	packet	bit	sp du	bit
12	A communication path way that transfers data from one point to another is called ______	Link	Node	Medium	Topology	Link
13	The __________layer is responsible for process to process delivery.	physical	presentation	networks	transport	transport

14	The ________layer is responsible for dialog control and synchronization.	transport	session	application	presentation	session
15	Tcp/Ip is a _______protocol.	hyper text	transfer	internet	hierarchical	internet
16	Ip is a_______protocol.	hop to hop	node to node	process to process	host to host	host to host
17	A set of devices connected by a __________links	data	networks	communicatio n	application	communication
18	In _______ topology every device is connected to a single cable	Bus	Star	Ring	Mesh	Bus
19	Periodic analog signals can be classified into ___________	simple	composite	simple or composite	simple and composite	simple or composite
20	Period and frequency has the following formula.	f=1/t and t=1/f	t=1/f or f=1/t	c=t/f	t=c/f	f=1/t and t=1/f
21	Wavelength is____________	propagation speed	propagation speed *	propagation speed/period	propagation speed/frequency	propagation speed/frequenc
22	ISP stands for _______	Internet Service Provider	Internet System	International Service	International System Program	Internet Service
23	The range of frequency contained in a ________ signal is its bandwidth.	simple	composite	periodic	non periodic	composite
24	The bandwidth of the composite signal is the difference between the	highest	highest or lowest	highest and lowest	lowest	highest and lowest
25	The _________is the number of bits sent in a second.	bit length	bandpass	bandwidth	bit rate	bit rate
26	Bit length is _________	propagation speed/period	propagation speed *	bit	propagation speed*bit	propagation speed*bit
27	A________signal is a composite analog signal with an infinite bandwidth	simple	composite	digital	analog	digital
28	Bus topology is also called as_____	Linear Bus Topology	Hybrid Bus Topology	Dual Ring topology	Non Linear Bus Topology	Linear Bus Topology
29	Transmission time=___________	message size/birate	distance/band width	message size/distance	message size/bandwidth	message size/bandwidth
30	________and star is a point to point device.	bus	ring	mesh	physical	mesh

31	_____ **and** _____ is an example of simplex communication	Keyboard and Monitor	Printer and fax	Mobile and Tab	Bus and ring	Keyboard and Monitor
32	___________is a basic key element.	protocols	standards	topology	protocols and standards	protocols and standards
33	Bit rate=_________	4*BW*log2L	2*BW*log2L	4*BW/L	2*BW*log 4L	2*BW*log2L
34	OSI stands for__________	open systems interconnection	open system internetworkin	open symantic interconnectio	open system internet	open systems interconnection
35	Net work layer delivers data in the form of_______	frame	bits	data	packet	packet
36	Session layer provides_________ services.	one	two	three	four	two
37	UDP stands for _________	user data protocol	user datagram protocol	user defined protocol	user dataframe protocol	user datagram protocol
38	FTP stands for ___________	file transmit protocol	file transmission	file transfer protocol	flip transfer protocol	file transfer protocol
39	SMTP stands for ____________	single mail transfer protocol	simple mail transfer	simple mail transmission	single mail transmit	simple mail transfer
40	Complete a cycle is called as ________	period	frequency	non periodic	periodic	period
41	_______ generally expands throughout a city such as cable TV network	LAN	WAN	MAN	PAN	MAN
42	__________is reliable and **connection oriented protocol.**	TCP	UDP	FTP	SMTP	TCP
43	Full duplex also called as__________	simple duplex	single duplex	multiple duplex	duplex	duplex
44	____________can be measured in transmit time and response time.	performance	frequency	period	non period	performance
45	A multipoint is also called as____________	multi line	multi drop	multi level	single level	multi drop
46	Mesh has __________ physical channels to link n devices	n(n-1)	n(n+1)	n(n+1)/2	n(n-1)/2	n(n-1)/2
47	A__________topology on the other hand is multipoint.	star	ring	bus	mesh	bus

48	Combination of two or more network topology is called _________	Mesh	Star	Ring	Hybrid	Hybrid
49	A MAN is a network with a size between a __________ and ____________ .	WAN and LAN	WAN or LAN	LAN	WAN	WAN and LAN
50	_________ refers to information that has discrete states.	Digital data	Analog data	bits	bytes	Digital data
51	The_________layer is responsible for providing services to the user.	presentation	datalink	application	network	application
52	The ________ layer is responsible for translation, compression encryption.	transport	data link	presentation	application	presentation
53	The____________layer is responsible for the delivery of a message from one process to another.	data link	transport	presentation	network	transport
54	A ______________layer is responsible for the delivery of packets from the source to destination.	physical	data link	network	session	network
55	The ____________layer is responsible for moving frames from one hop to the next.	data link	physical	network	presentation	data link
56	The _________layer is responsible for movements of bits from one hop to next.	data link	physical	transport	session	physical
57	RARP stands for _________	reverse address resolution	reverse address result protocol	reverse addess revolutinized	reverse addess research	reverse address resolution
58	In multicast communication, the relationship is	One to one	One to many	Many to one	many to many	One to many
59	The TCP/IP protocol suite was developed prior to the ___________ model.	OSI	ISO	TCP	IP	OSI
60	The __________layer is responsible for flow control.	session	presentation	application	transport	transport
61	The term ________ data refers to information continous	analog	digital	physical	analog and digital	analog
62	The sine wave is the most fundamental form of a __________ analog signal.	composite	single	periodic	non periodic	periodic

Unit – II

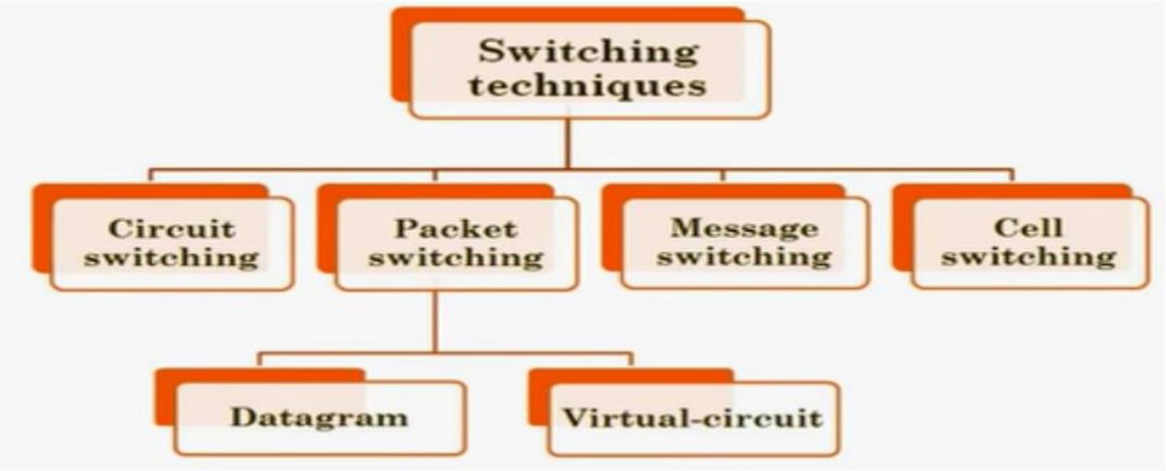
SYLLABUS

Networks Switching Techniques and ACSUess mechanisms: Circuit switching; packetswitching - connectionless datagram switching, connection-oriented virtual circuit switching; dial-up modems; digital subscriber line; cable TV for data transfer.

NETWORKS SWITCHING TECHNIQUES AND ACCESSES MECHANISMS:

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

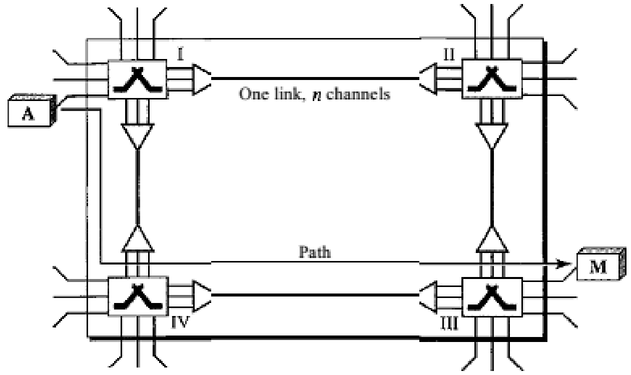


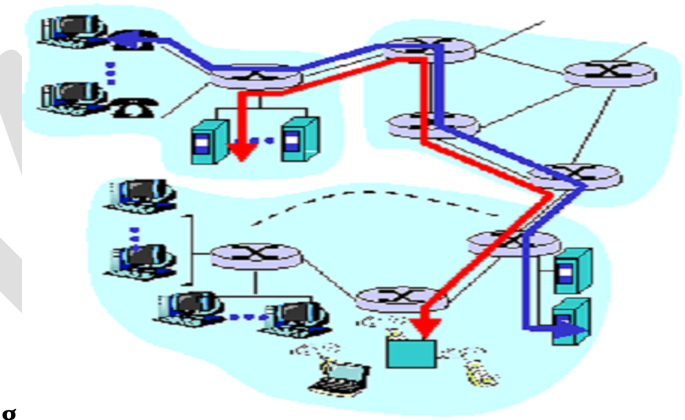
Circuit Switching

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the communication session. The circuit functions as if the nodes were physically connected as with an electrical circuit. The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

Figure 8.3 *A trivial circuit-switched network*





Packet Switching

Packet switching features delivery of variable bit rate data streams (sequences of packets) over a computer network which allocates transmission resources as needed using statistical multiplexing or dynamic bandwidth allocation techniques. When traversing network adapters, switches, routers, and other network nodes, packets are buffered and queued, resulting in variable delay and throughput depending on the network's capacity and the traffic load on the network. Packet switching is used to optimize the use of the channel capacity available in digital telecommunication networks such as computer networks.

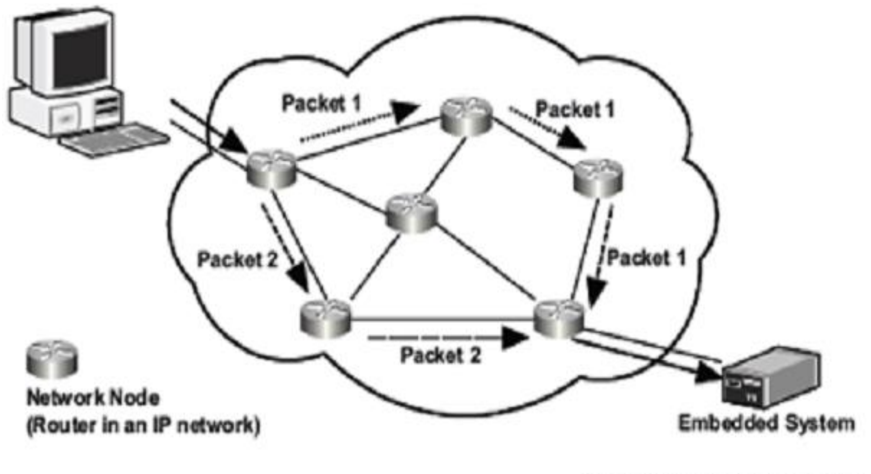
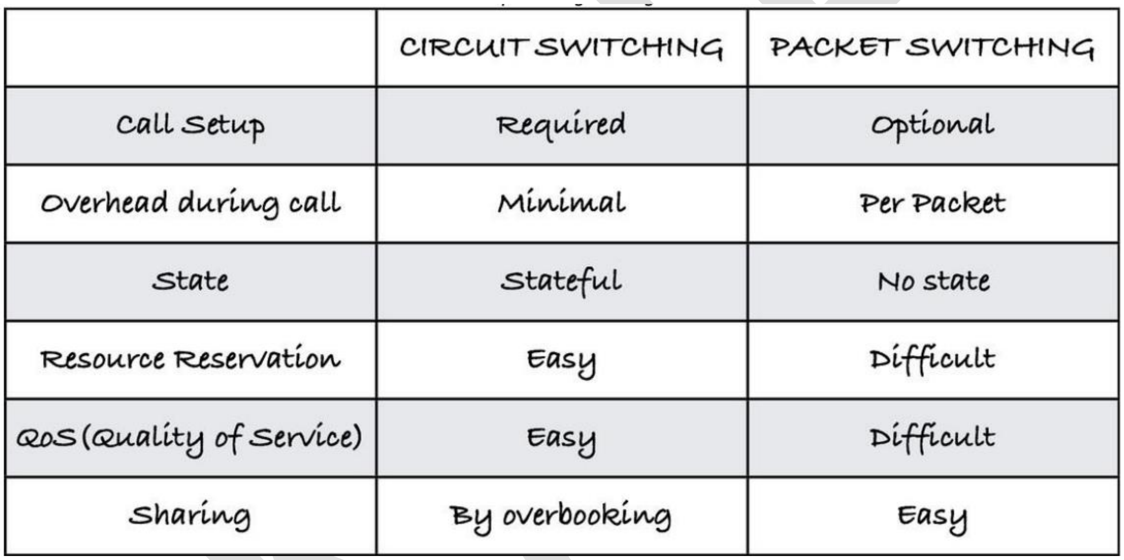


Figure 2-2 Packet Switched Network



	CIRCUIT SWITCHING	PACKET SWITCHING
Call Setup	Required	Optional
Overhead during call	Minimal	Per Packet
State	Stateful	No state
Resource Reservation	Easy	Difficult
QoS (Quality of Service)	Easy	Difficult
Sharing	By overbooking	Easy

Connectionless and connection-oriented packet switching
Two major packet switching modes exist:

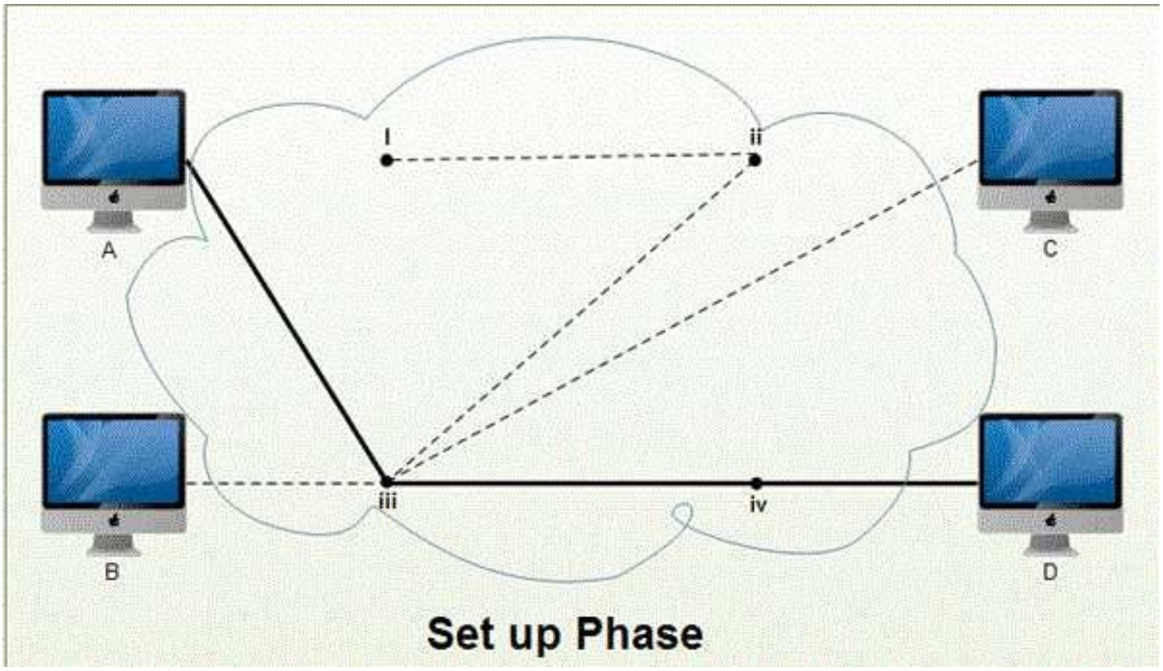
1. connectionless packet switching, also known as datagram switching; and
2. connection-oriented packet switching, also known as virtual circuit switching.

Types of Packet Switching

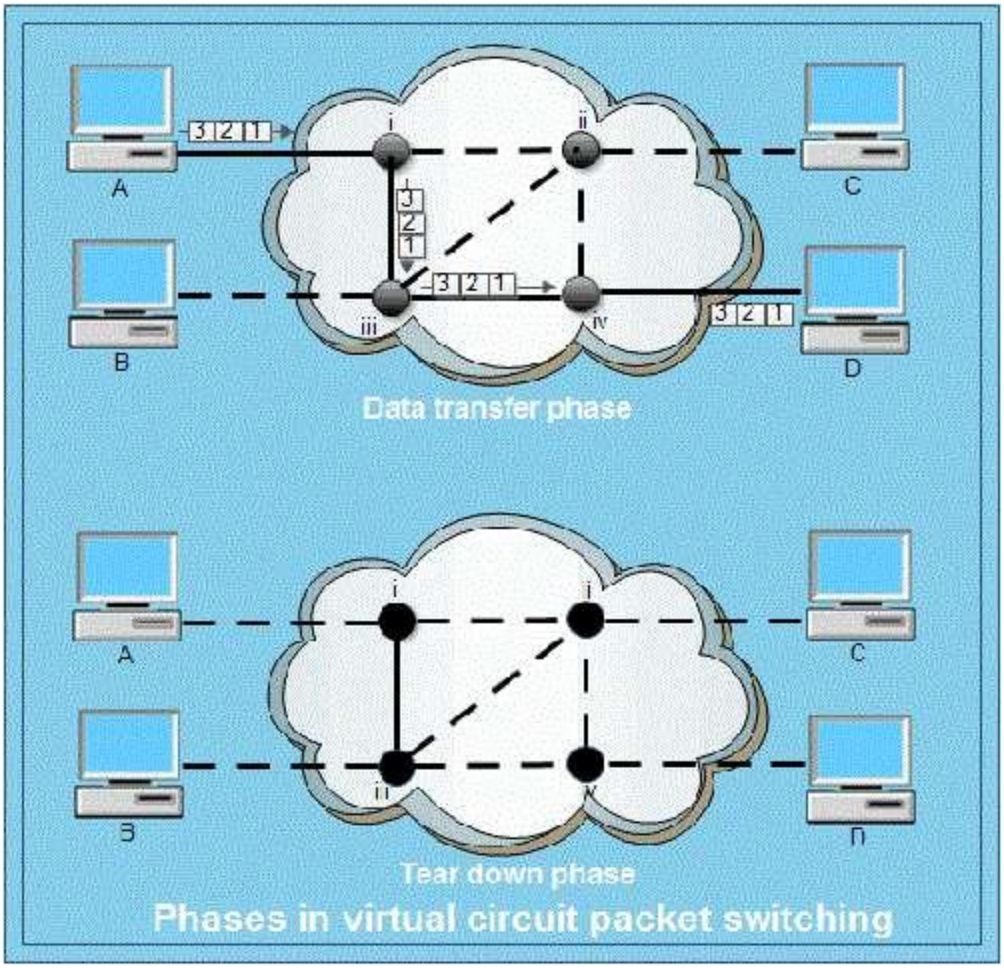
The packet switching has two approaches: Virtual Circuit approach and Datagram approach. WAN, ATM, frame relay and telephone networks use connection oriented virtual circuit approach; whereas internet relies on connectionless datagram based packet switching.

(i) **Virtual Circuit Packet Switching:**

In virtual circuit packet switching, a single route is chosen between the sender and receiver and all the packets are sent through this route. Every packet contains the virtual circuit number. As in circuit switching, virtual circuit needs call setup before actual transmission can be started. He routing is based on the virtual circuit number.

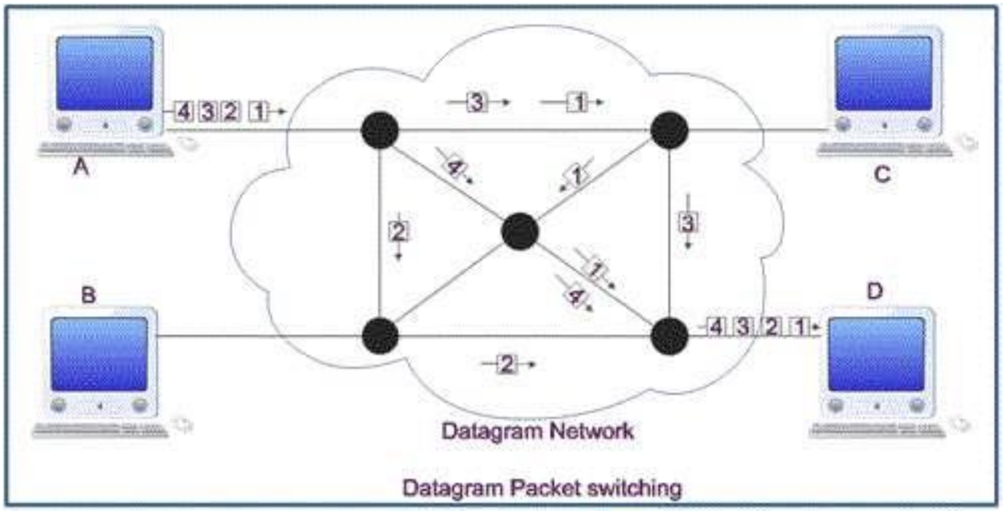


This approach preserves the relationship between all the packets belonging to a message. Just like circuit switching, virtual circuit approach has a set up, data transfer and tear down phases. Resources can be allocated during the set up phase, as in circuit switched networks or on demand, as in a datagram network. All the packets of a message follow the same path established during the connection. A virtual circuit network is normally implemented in the data link layer, while a circuit switched network is implemented in the physical layer and a datagram network in the network layer.



(ii) **Datagram Packet Switching:** In datagram packet switching each packet is transmitted without any regard to other packets. Every packet contain full packet of source and destination. Every packet is treated as individual, independent transmission.

Even if a packet is a part of multi-packet transmission the network treats it as though it existed alone. Packets in this approach are called **datagrams.** Datagram switching is done at the network layer. Figure show how a datagram approach is used to deliver four packets from station A to station D. All the four packets belong to same message but they may travel via different paths to reach the destination *i.e.* station D.



Datagram Packet switching

Datagram approach can cause the datagrams to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of lack of resources. The datagram networks are also referred as connectionless networks. Here connectionless means that the switch does not keep information about connection state. There are no connection establishment or tear down phases.

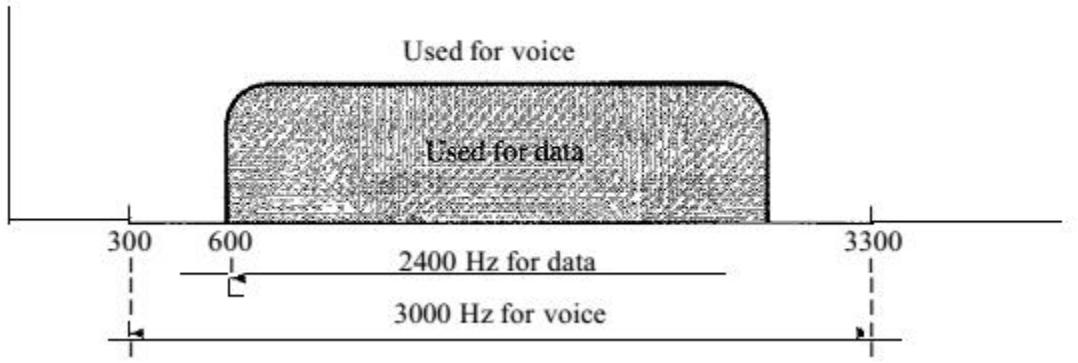
The datagram can arrive at the destination with a different order from the order in which they where sent. The source and destination address are used by the routers to decide the route for packets. Internet use datagram approach at the network layer.

In the first case, each packet includes complete addressing or routing information. The packets are routed individually, sometimes resulting in different paths and out-of-order delivery. In the second case, a connection is defined and pre-allocated in each involved node during a connection setup phase before any packet is transferred. The packets include a connection identifier rather than address information. Some connectionless protocols are Ethernet, IP, and UDP; connection oriented packet-switching protocols include X.25, Frame relay, Multiprotocol Label Switching (MPLS), and TCP.

Dial-Up Modems

Traditional telephone lines can carry frequencies between 300 and 3300 Hz, giving them a bandwidth of 3000 Hz. All this range is used for transmitting voice, where a great deal of interference and distortion can be accepted without loss of intelligibility. As we have seen, however, data signals require a higher degree of accuracy to ensure integrity. For safety's sake, therefore, the edges of this range are not used for data communications. In general, we can say that the signal bandwidth must be smaller than the cable bandwidth. The effective bandwidth of a telephone line being used for data transmission is 2400 Hz, covering the range from 600 to 3000 Hz. Note that today some telephone lines are capable of handling greater bandwidth than traditional lines. However, modem design is still based on traditional capability

Telephone line bandwidth



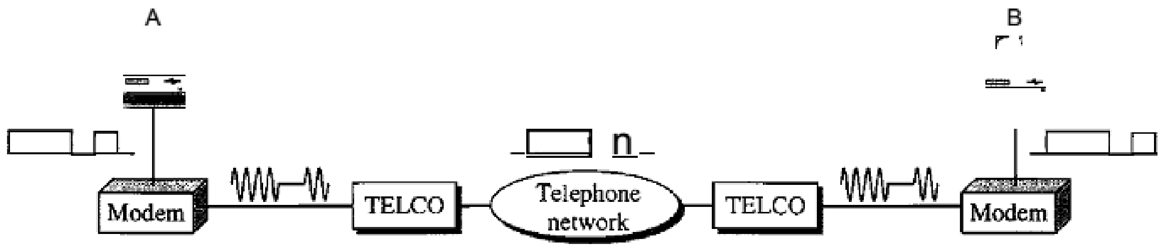
The term modem is a composite word that refers to the two functional entities that make up the device: a signal modulator and a signal demodulator. A modulator creates a band pass analog signal from binary data. A demodulator recovers the binary data from the modulated signal.

Modem stands for modulator/demodulator.

The computer on the left sends a digital signal to the modulator portion of the modem; the data are sent as an analog signal on the telephone lines. The modem on the right receives the analog signal,
demodulates it through its demodulator, and delivers data to the computer on the right. The communication can be bidirectional, which means the computer on the right can simultaneously send data to the computer on the left, using the same modulation/demodulation processes.

Modulation/demodulation

TELCO: Telephone company



Modem Standards

Today, many of the most popular modems available are based on the V-series standards published by the ITU-T.

V.32 and V.32bis

The V.32 modem uses a combined modulation and encoding technique called trelliscoded modulation.

V:90

b. Constellation and bandwidth for V.32bis Traditional modems have a data rate limitation of 33.6 kbps, as determined by the Shannon capacity (see Chapter 3). However, V.90 modems with a bit rate of 56,000 bps are available; these are called 56K modems.

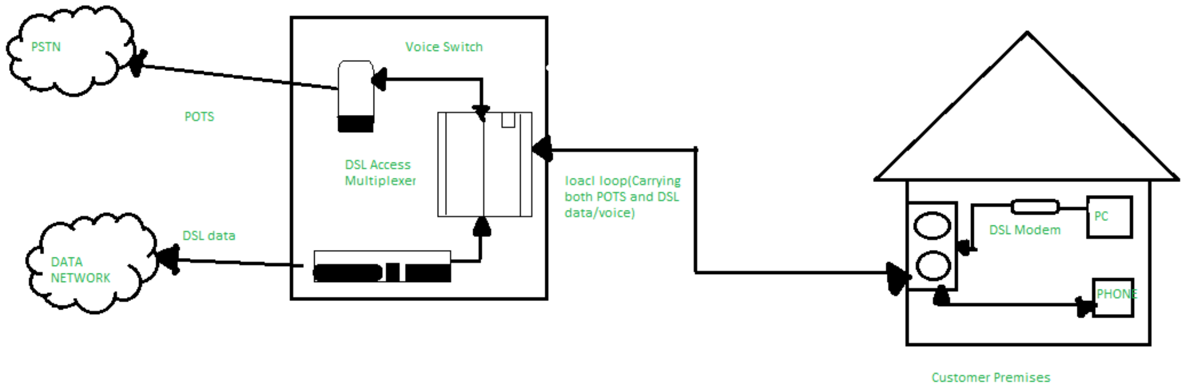
V:92

The standard above V90 is called ~92. These modems can adjust their speed, and if the noise allows, they can upload data at the rate of 48 kbps. The downloading rate is still 56 kbps. The modem has additional features. For example, the modem can interrupt the Internet connection when there is an incoming call if the line has call-waiting service.

DIGITAL SUBSCRIBER LINE:

Digital Subscriber Line (DSL, *originally*, **digital subscriber loop**) is a communication medium, which is used to transfer internet through copper wire telecommunication line.Along with cable internet, DSL is one of the most popular ways *ISPs* provide broadband internet access.

- Its aim is to maintain the high speed of the internet being transfered.
- If we ask that how we gonna achieve such thing i.e., both telephone and internet facility, then the answer is by using *splitters or DSL filters*(shown in below diagram).Basically, the use *splitter* is to splits the frequency and make sure that they can't get interrupted.



Types of DSL –

1. **Symmetric DSL** – SDSL, *splits* the upstream and downstream frequencies evenly, providing equal speeds to both uploading and downloading data transfer.This connection may provide *2 Mbps*upstream and downstream.it is mostly preferred by small organizations.
2. **Asymmetric DSL** – ADSL, provides a wider frequency range for downstream transfers, which offers several times faster downstream speeds.an ADSL connection may offer *20*

Mbps downstream and 1.5 Mbps upstream, it is because most users download more data than they upload.

Benefits –

- **No Additional Wiring** – A DSL connection makes use of your existing telephone wiring, so you will not have to pay for expensive upgrades to your phone system.
- **Cost Effective –** DSL internet is a very cost-effective method and is best in connectivity
- Availability of DSL modems by the service providers.
- User can use the both telephone line and internet at a same time.And it is because the voice is transferred on other frequency and digital signals are transferred on others.
- User can choose between different connection *speeds* and *pricing* from various providers.

DSL Internet service only works over a limited physical distance and remains unavailable in many areas where the local telephone infrastructure does not support DSL technology. The service is not available everywhere. The connection is faster for receiving data than it is for sending data over the Internet.

CABLE TV FOR DATA TRANSFER:

Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer. DSL technology provides high-data-rate connections for residential subscribers over the local loop.

1. Bandwidth

Even in an HFC system, the last part of the network, from the fiber node to the subscriber premises, is still a coaxial cable. This coaxial cable has a bandwidth that ranges from 5 to 750 MHz (approximately). To provide Internet access, the cable company has divided this bandwidth into three bands: video, downstream data, and upstream data.

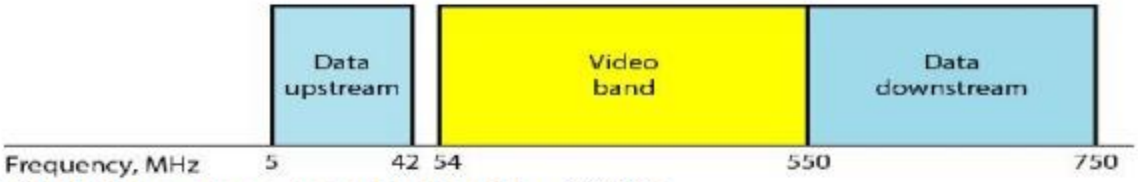


Figure 1.61 Division of coaxial cable band by CATV

Downstream Video Band

The downstream video band occupies frequencies from 54 to 550 MHz. Since each TV channel occupies 6 MHz, this can accommodate more than 80 channels.

Downstream Data Band

The downstream data (from the Internet to the subscriber premises) occupies the upper band, from 550 to 750 MHz. This band is also divided into 6-MHz channels. Modulation Downstream data band uses the 64-QAM (or possibly 256-QAM) modulation technique. Downstream data are modulated using the 64-QAM modulation technique.

Upstream Data Band

The upstream data (from the subscriber premises to the Internet) occupies the lower band, from 5 to 42 MHz. This band is also divided into 6-MHz channels. Modulation The upstream data band uses lower frequencies that are more susceptible to noise and interference. For this reason, the QAM technique is not suitable for this band.

2. CM and CMTS

To use a cable network for data transmission, we need two key devices: a cable modem (CM) and a cable modem transmission system (CMTS).

CM

The cable modem (CM) is installed on the subscriber premises. It is similar to an ADSL.

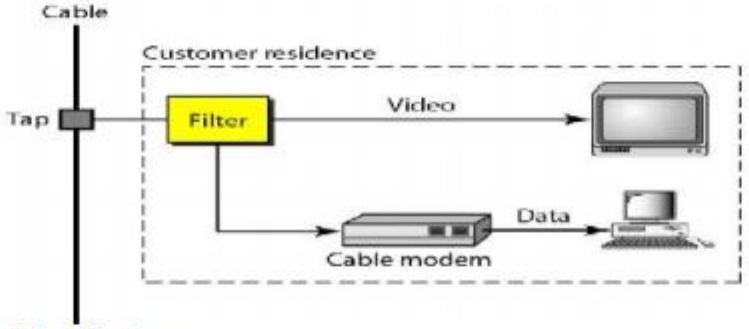


Figure 1.61 Cable Modem

CMTS

The cable modem transmission system (CMTS) is installed inside the distribution hub by the cable company. It receives data from the Internet and passes them to the combiner, which sends them to the subscriber. The CMTS also receives data from the subscriber and passes them to the Internet. Figure 1.77 shows the location of the CMTS.

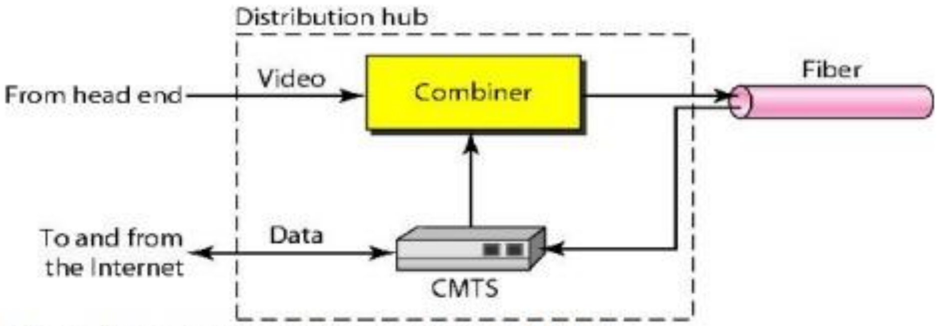


Figure 1.77 Cable modem transmission system (CMTS)

3. Data Transmission Schemes: DOCSIS

Several schemes have been designed for data transmission over an HFC network.

Upstream Communication

The following describes the steps that must be followed by a CM:

· The CM checks the downstream channels for a specific packet periodically sent by the CMTS. The packet asks any new CM to announce itself on a specific upstream channel.

· The CMTS sends a packet to the CM, defining its allocated downstream and upstream Channels.

· The CM then starts a process, called ranging, which determines the distance between the CM and CMTS. This process is required for synchronization between all CMs and CMTSs for the minislots used for timesharing of the upstream channels.
· The CM sends a packet to the ISP, asking for the Internet address.

· The CM and CMTS then exchange some packets to establish security parameters, which are needed for a public network such as cable TV.

· The CM sends its unique identifier to the CMTS.

· Upstream communication can start in the allocated upstream channel; the CM can contend for the minislots to send data.

Downstream Communication

In the downstream direction, the communication is much simpler. There is no contention because there is only one sender. The CMTS sends the packet with the address of the receiving CM, using the allocated downstream channel.

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CS Batch:2017

Subject:COMPUTER NETWORKS

SubCode:17CSU303

UNIT - II

S.No	Questions	choice 1	choice2	choice3	choice4	ANS
1	Before data can be transmitted, they must be transformed to______	periodic signals	electromagnetic signals	Aperiodic signals	low frequency sine waves	electromagnetic signals
2	Which of the following can be determined from a frequency_domain graph of a signal?	frequency	phase	power	all the above	frequency
3	Which of the following can be determined from a frequency_domain graph of a signal?	bandwidth	phase	power	all the above	bandwidth
4	In a frequency_domain plot, the vertical axis measures the______	peak amplitude	frequency	phase	slope	peak amplitude
5	In a frequency_domain plot, the horizontal axis measures the______	peak amplitude	frequency	phase	slope	frequency
6	As frequency increases, the period______	dereases	increases	remains the same	doubles	increases
7	The last step in Pulse Code Modulation (PCM) is____	Quantization	Sampling	Encoding	Modulation	Encoding
8	A sine wave is______	periodic and continuous	aperiodic and continuous	periodic and discrete	aperiodic and discrete	periodic and continuous
9	______is a type of transmission impairment in which the signal loses strength due to the resistance	attenuation	distortion	noise	decibel	attenuation
10	______is a type of transmission impairment in which the signal loses strength due to different	attenuation	distortion	noise	decibel	distortion
11	______is a type of transmission impairment in which an outside source such as crosstalk corrupts a	attenuation	distortion	noise	decibel	noise
12	Propogation time is_______ proportional to distance and_______ proportional to propogation	inversely; directly	directly; inversely	inversely; inversely	directly; directly	directly; inversely
13	The wavelength of a signal depend on the______	frequency of the signal	medium	phase of signal	(a) and (b)	(a) and (b)
14	Unipolar, bipolar and polar encoding are types of______ encoding	line	block	NRZ	manchester	line

15	Guided media provides a conduit from one device to another, includes __________	twisted pair cable	fiber optic cable	coaxial cable	All of the above	All of the above
16	______ encoding has a transition at the middle of each bit	RZ	manchester	differential manchester	all the above	RZ
17	Optical fibers use reflection to guide light through a ___________	channel	metal wire	light	plastic	channel
18	PCM is an example of______conversion	digital-to-digital	digital-to-anolog	anolog-to-analog	analog-to-digital	analog-to-digital
19	The nyquist theorem specifies the minimum sampling rate to be______	equal to the lowest frequency of signal	equal to the highest	twice the bandwidth of a	twice the highest	twice the highest frequency of
20	Which encoding type always has a nonzero average amplitude?	unipolar	polar	bipolar	all the above	unipolar
21	Which of the following encoding methods does not provide for synchronization?	NRZ-L	RZ	NRZ-I	manchester	NRZ-L
22	Which encoding method uses altering positive and negative voltage for bit 1?	NRZ-I	RZ	manchester	Biploar encoding	Biploar encoding
23	RZ encoding involves______ signal levels	two	three	four	five	three
24	Unguided medium is ________	twisted pair cable	coaxial cable	fiber optic cable	free space	free space
25	Block coding can help is______ at the receiver	synchronization	error detection	attenuation	(a) and (b)	synchronization
26	______ transmission, bits are transmitted simultaneously, each across the own wire	asynchronous serial	synchronous serial	parallel	(a) and (b)	parallel
27	In______ transmission, bits are transmitted over a single wire, one at a time	asynchronous serial	synchronous serial	parallel	(a) and (b)	(a) and (b)
28	In______ transmission, a start bit and a stop bit frame a character byte	asynchronous serial	synchronous serial	parallel	(a) and (b)	synchronous serial
29	In asynchronous transmission, the gap tim between bytes is______	fixed	variable	a function of the data rate	zero	fixed
30	synchronous transmission does not have______	a start bit	a stop bit	gaps between bytes	all the above	all the above
31	ASK, PSK, FSK and QAM are examples of______ modulation	digital-to-digital	digital-to-anolog	analog-to-analog	analog-to-digital	digital-to-anolog
32	AM and FM are examples of modulation	digital-to-digital	digital-to-anolog	analog-to-analog	analog-to-digital	anolog-to-analog

33	In QAM, both phase and______ of a carrier frequency are varied	amplitude	frequency	bit rate	baud rate	amplitude
34	Telephone companies implement ______ multiplexing	TDM	FDM	WDM	DWDM	TDM
35	The applications of Frequency-Division Multiplexing (FDM) are______	broadcasting	AM and FM radio stations	cellular telephones	All of the mentioned	All of the mentioned
36	The Time-Division multiplexing (TDM) is a digital technique of ________	Encoding	Decoding	Multiplexing	Demultiplexing	Multiplexing
37	Wavelength division multiplexing is same as_____	FDM	TDM	DWDM	SDM	FDM
38	The types of multiplexing techniques are _______	one	two	three	four	three
39	Switching in the Internet is done by using the datagram approach to packet switching at the _____	Network Layer	Application Layer	Data link Layer	physical Layer	Network Layer
40	A Circuit-Switched Network is made of a set of switches connected by physical ____	Links	media	nodes	limes	Links
41	A switch in a datagram network uses a ____	destination address	sender address	routing table	header	routing table
42	Time Division Multiplexing inside a switch, is used by ________	Space division switch	crossbar switch	packet switch	switch	switch
43	The identifier that is actually used for data transfer is called the _____	virtual-circuit identifier	global address	local address	header	virtual-circuit identifier
44	Global and local addressing are types of ______	WAN network	local area circuit network	virtual-circuit network	MAN network	virtual-circuit network
45	A modulator converts ______ signal to _______ signal	digital ; analog	analog; digital	PSK; FSK	FSK; PSK	analog; digital
46	In which conversion technique the amplitude of analog carrier signal is modified to reflect binary	FSK	ASK	PSK	TSK	ASK
47	The sharing of medium and its link by two or more devices is called______	decoding	encoding	line discipline	multiplexing	multiplexing
48	Which multiplexing technique transmits analog signals	FDM	TDM	WDM	(a) and ©	(a) and ©
49	Which multiplexing technique transmits digital signals?	FDM	TDM	WDM	none of the above	TDM
50	Which multi plexing technique shifts each signal to a different carrier frequency?	FDM	TDM	both(a) and (b)	none of the above	FDM

51	In TDM, for n signal sources of the same data rate, each frame contains______ slots	n	n+1	n-1	0 to n	n
52	Guard bands increases the bandwidth for______	FDM	TDM	both(a) and (b)	none of the above	FDM
53	Which multiplexing technique involves signals composed of light beams?	FDM	TDM	WDM	none of the above	WDM
54	Transmission media are usually categorized as______	fixed or unfixed	guided of unguided	determinate or indeterminate	metallic or non-metallic	guided of unguided
55	Transmission media are usually categorized as______	physical	network	transport	application	physical
56	Category 1 UTP cable is most often used in______ networks	fast ethernet	traditional ethernet	infrared	telephone	telephone
57	BNC connectors are used by______ cables	UTP	STP	coaxial	fiber-optic	coaxial
58	In fiber optics, the signal source is______ waves	light	radio	infrared	very low frequency	light
59	A parabolic dish Antenna is a(n)______ antenna	omni directional	bi directional	uni directional	horn	uni directional
60	A telephone network is an example of a______ network	packet switching	circuit switched	message switched	none of the above	circuit switched
61	Radio waves are _________.	omnidirectional	unidirectional	bidirectional	multidirectional	omnidirectional
62	Microwaves are _________.	omnidirectional	unidirectional	bidirectional	multidirectional	unidirectional
63	________ are used for short-range communications such as those between a PC and a peripheral device.	Radio waves	Microwaves	Miniwaves	Infrared waves	Infrared waves

Unit – III

Syllabus

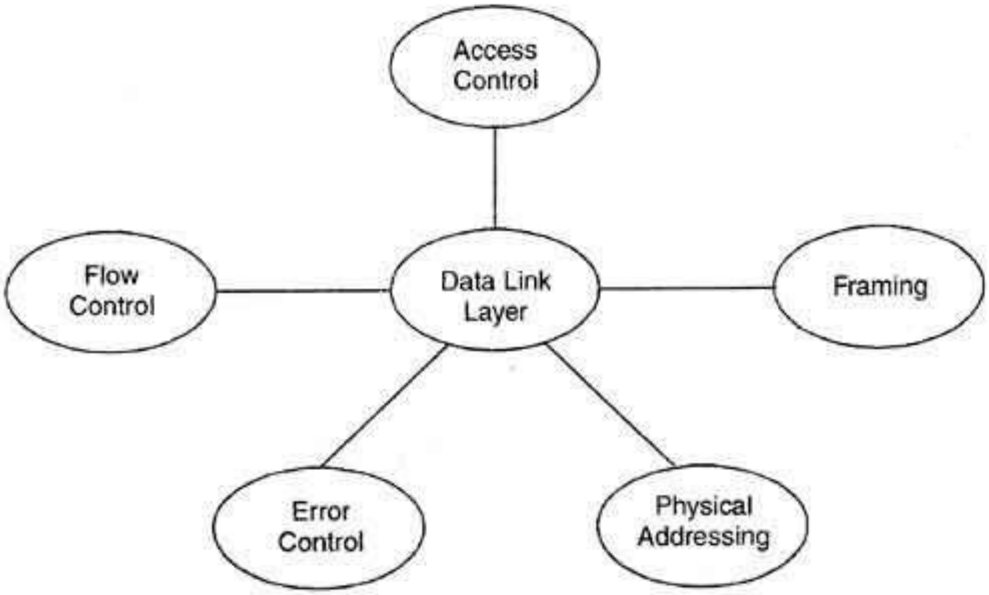
Data Link Layer Functions and Protocol: Error detection and error correction techniques; data-link control- framing and flow control; error recovery protocols- stop and wait ARQ, go-back-n ARQ; Point to Point Protocol on Internet.

DATA LINK LAYER FUNCTIONS AND PROTOCOL:

Data link layer is the second layer in OSI reference model and lies above the physical layer.

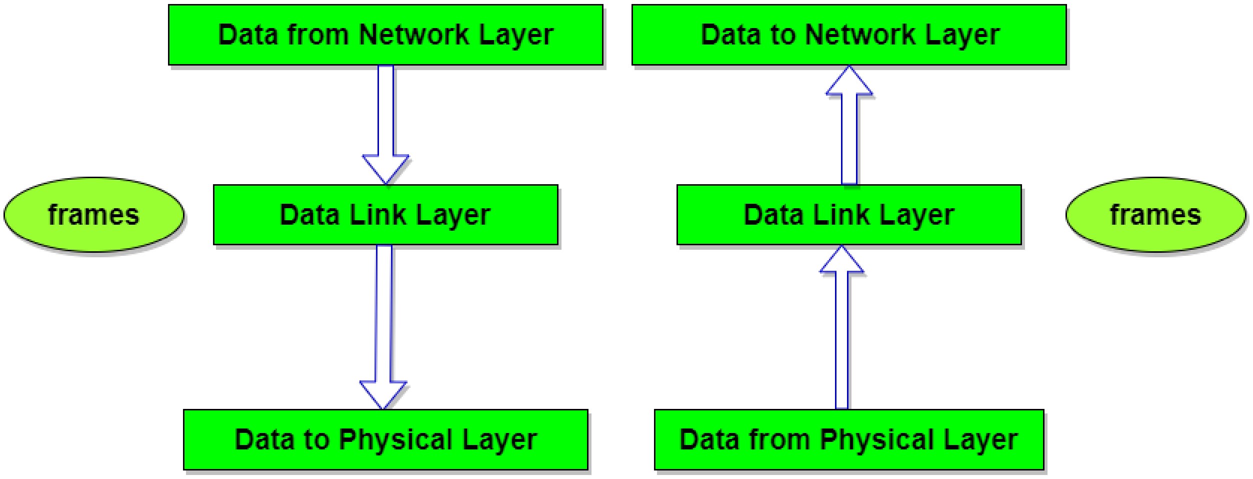
The data link layer performs the following functions.

1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.



Functions of data link layer

3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames is also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



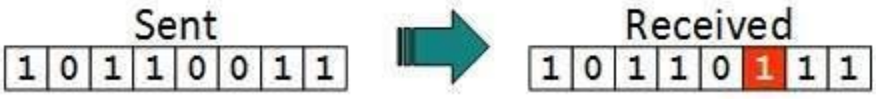
ERROR DETECTION AND ERROR CORRECTION TECHNIQUES:

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

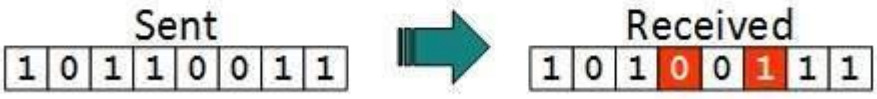
There may be three types of errors:

- **Single bit error**



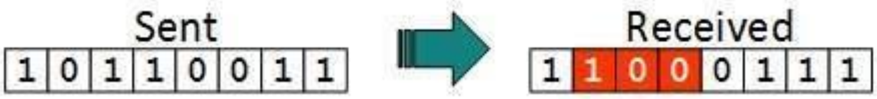
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bit in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

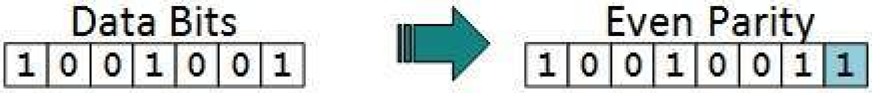
Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

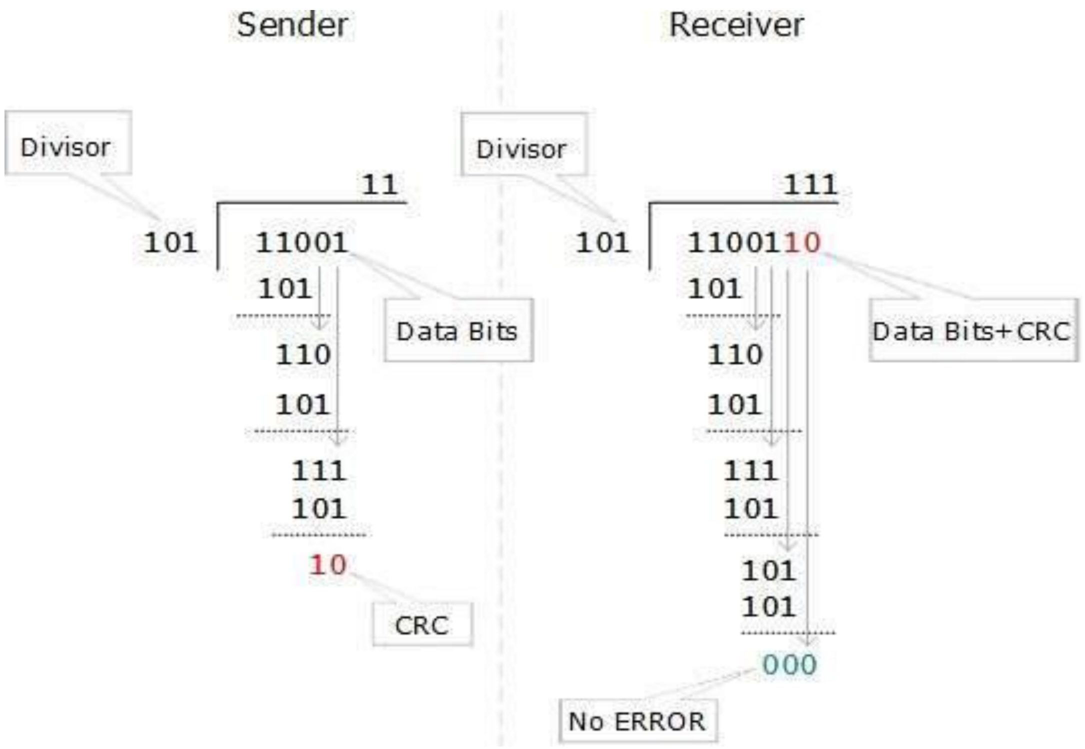


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bit is erroneous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

$$2^r >= m+r+1$$

DATA-LINK CONTROL- FRAMING AND FLOW CONTROL:

Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

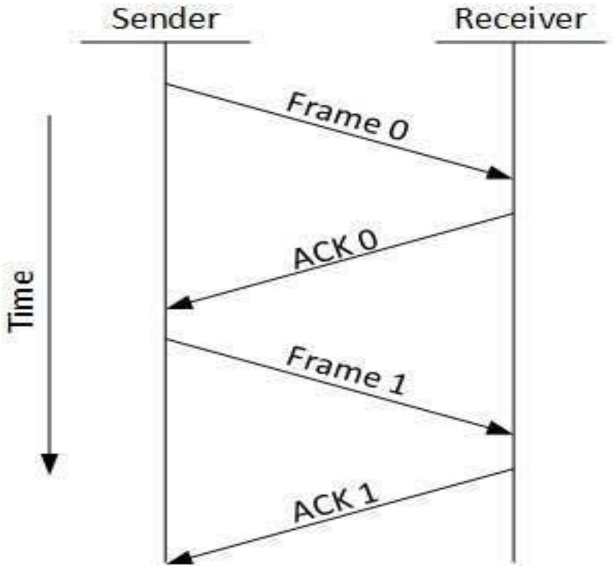
Flow Control

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- **Stop and Wait**

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



- **Sliding Window**

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which help them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

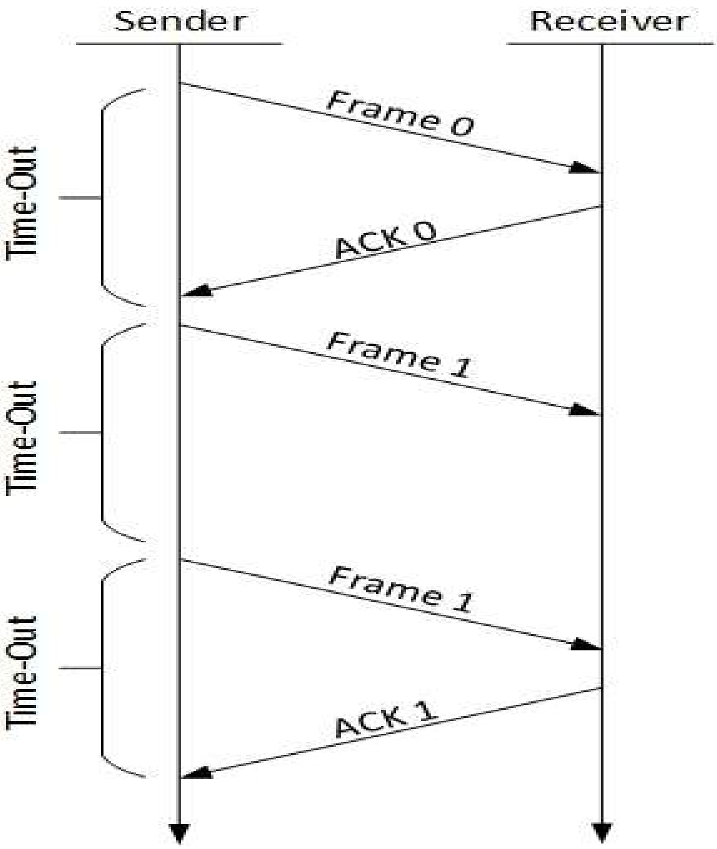
Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.

- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

- **Stop-and-wait ARQ**



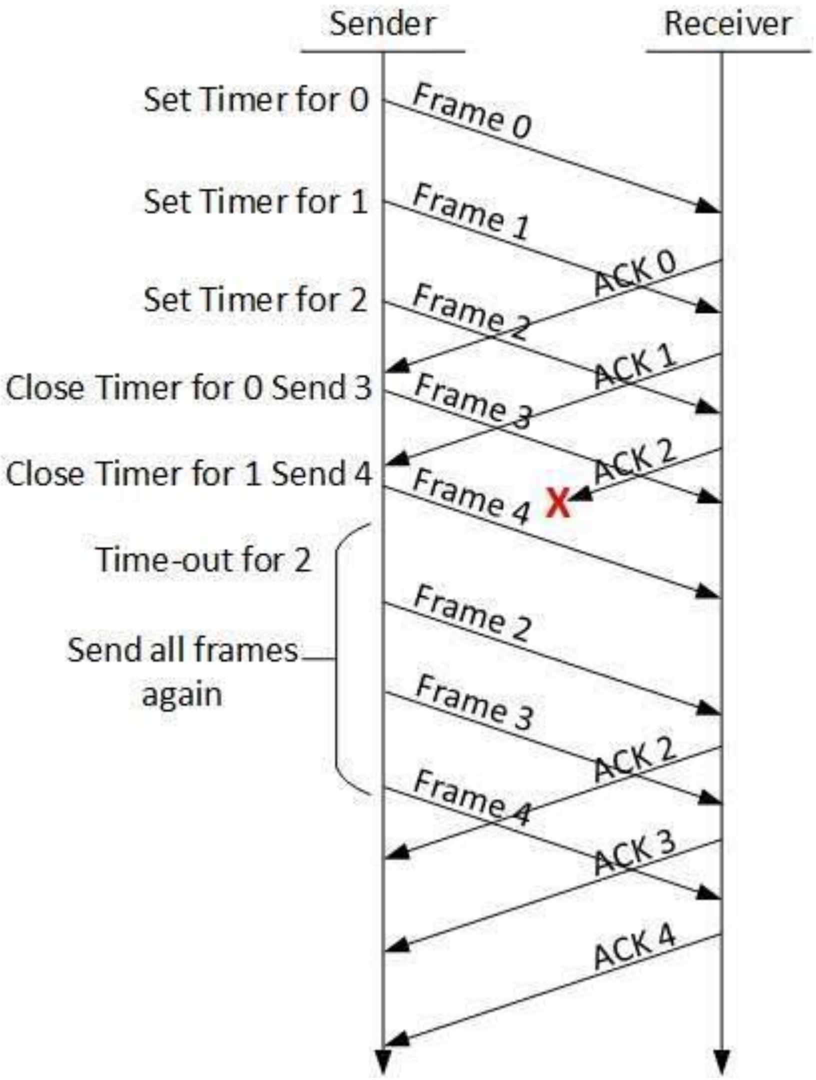
The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.

- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

- **Go-Back-N ARQ**

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

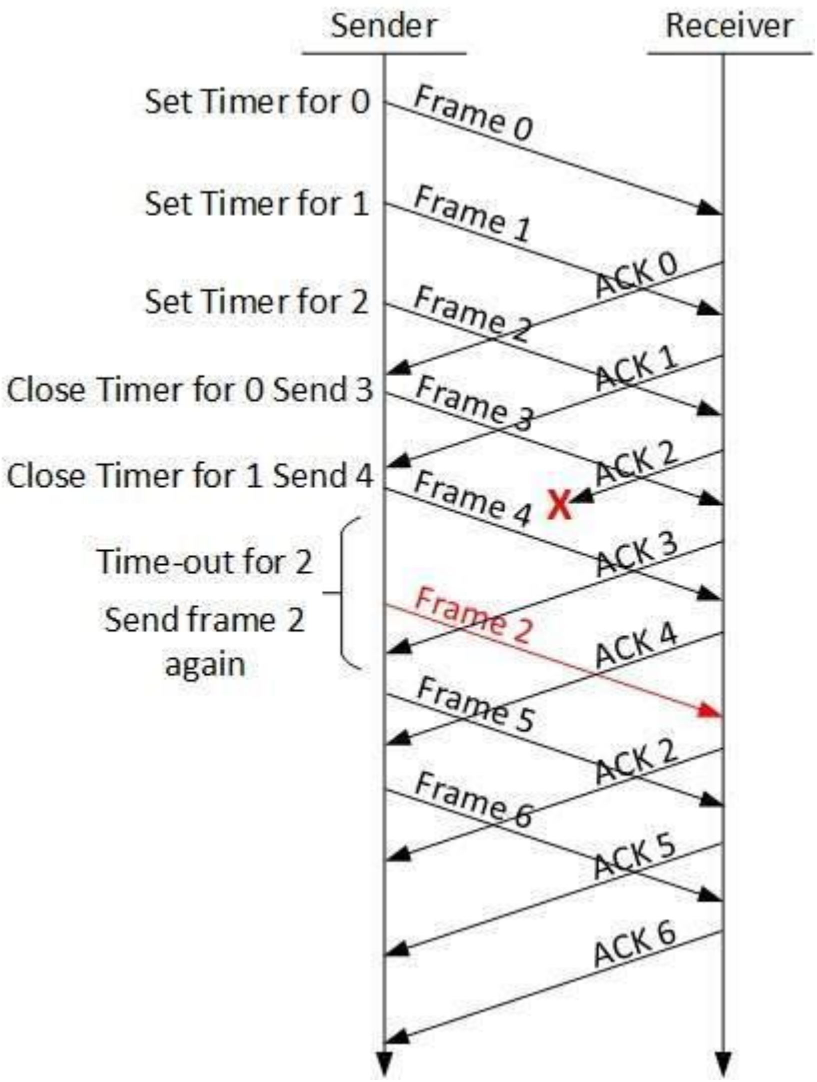


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not received any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

- Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.

Error Recovery Protocols:

It allows the receiver to inform the sender if a frame is lost or damaged during transmission and coordinates the retransmission of those frames by the sender. Error control in the data link layer is based on automatic repeat request (ARQ). Whenever an error is detected, specified frames are retransmitted.

STOP AND WAIT ARQ:

Characteristics

- Used in Connection-oriented communication.
- It offers error and flow control
- It is used in Data Link and Transport Layers
- Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1

Useful Terms:

1. **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.
   Propagation Delay = (Distance between routers) / (Velocity of propagation)
2. RoundTripTime (**RTT**) = 2* Propagation Delay
3. TimeOut (**TO**) = 2* RTT
4. Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 180 seconds)

Simple Stop and Wait

Sender:

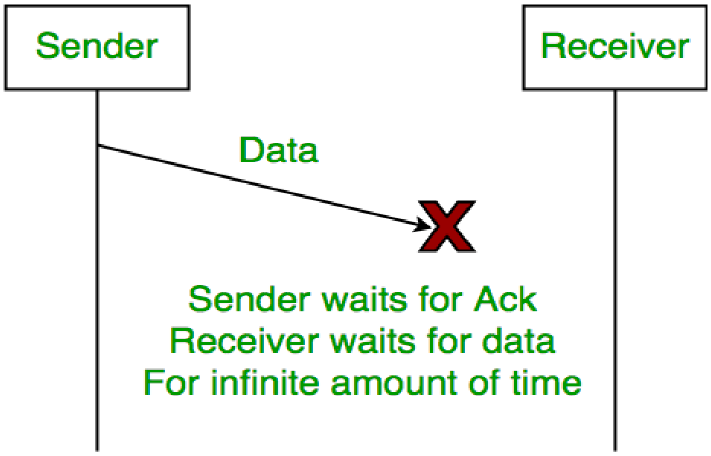
Rule 1) Send one data packet at a time.
Rule 2) send next packet only after receiving acknowledgement for previous.

Receiver:

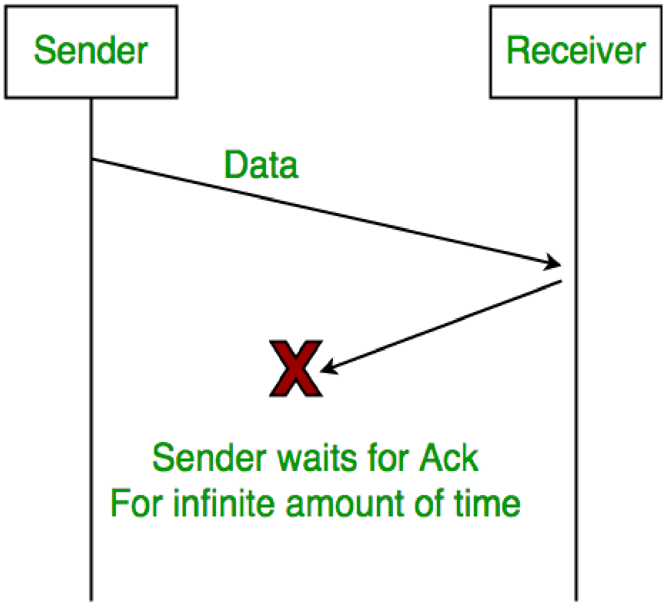
Rule 1) Send acknowledgement after receiving and consuming of data packet.
Rule 2) After consuming packet acknowledgement need to be sent (Flow Control)

Problems:

1. Lost Data



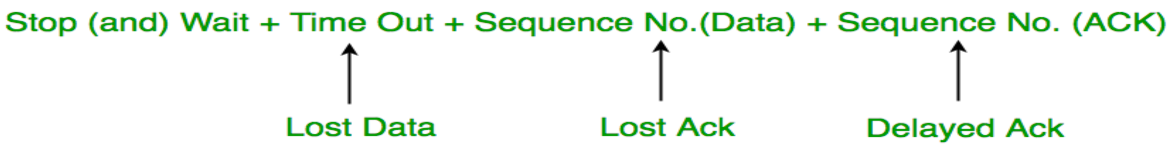
2. Lost Acknowledgement:



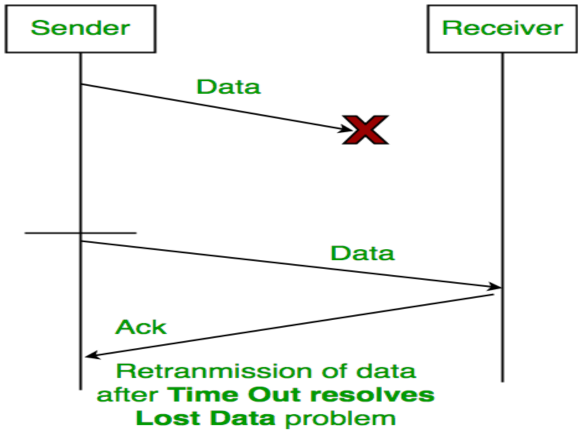
3. Delayed Acknowledgement/Data: After timeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

<u>Stop and Wait ARQ (Automatic Repeat Request)</u>

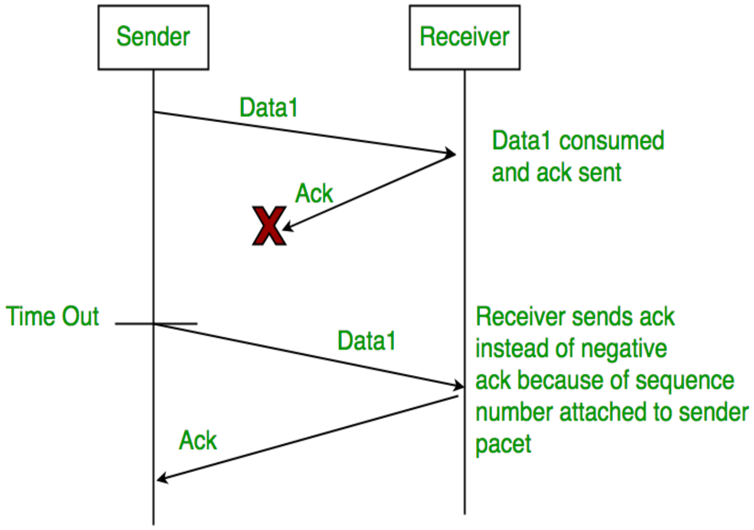
Above 3 problems are resolved by Stop and Wait ARQ (Automatic Repeat Request) that does both error control and flow control.


Stop (and) Wait + Time Out + Sequence No.(Data) + Sequence No. (ACK)
Lost Data
Lost Ack
Delayed Ack

1. Time Out:



2. Sequence Number (Data)

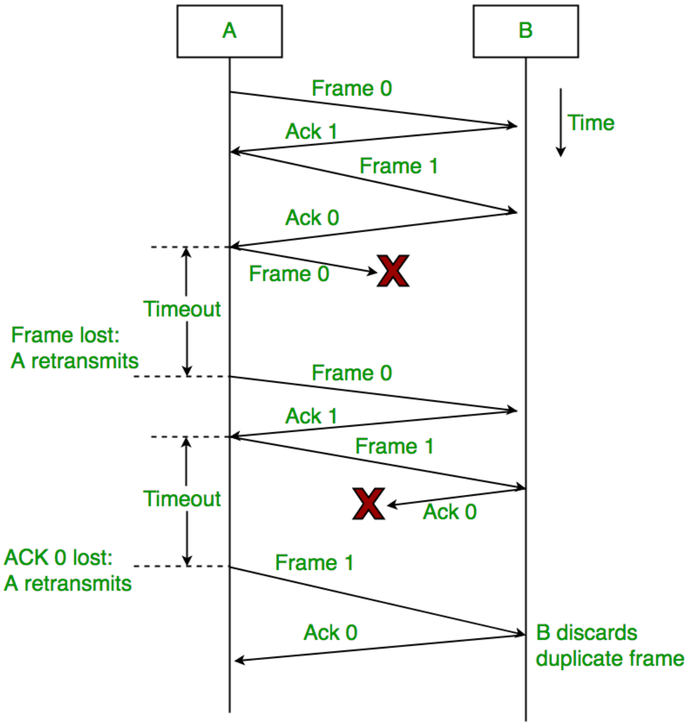


3. Delayed Acknowledgement:

This is resolved by introducing sequence number for acknowledgement also.

Working of Stop and Wait ARQ:

1) Sender A sends a data frame or packet with sequence number 0.
2) Receiver B, after receiving data frame, sends and acknowledgement with sequence number 1 (sequence number of next expected data frame or packet)
There is only one bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.



Characteristics of Stop and Wait ARQ:

- It uses link between sender and receiver as half duplex link
- Throughput = 1 Data packet/frame per RTT
- If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example for "**Closed Loop OR connection oriented** " protocols
- It is an special category of SWP where its window size is 1
- Irrespective of number of packets sender is having stop and wait protocol requires only 2 sequence numbers 0 and 1

The Stop and Wait ARQ solves main three problems, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country though a high speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence numbers. So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections, but performs badly for distant connections like satellite connection.

Sliding Window Protocol | Set 1 (Sender Side)

The Stop and Wait ARQ offers error and flow control, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country though a high speed connection); you can't use this full speed due to limitations of stop and wait.

Sliding Window protocol handles this efficiency issue by sending more than one packet at a time with a larger sequence numbers. The idea is same as pipelining in architectures.

Few Terminologies:

Transmission Delay (Tt) – Time to transmit the packet from host to the outgoing link. If B is the Bandwidth of the link and D is the Data Size to transmit

$$Tt = D/B$$

Propagation Delay (Tp) – It is the time taken by the first bit transferred by the host onto the outgoing link to reach the destination. It depends on the distance d and the wave propagation speed s (depends on the characteristics of the medium).

$$Tp = d/s$$

Efficiency – It is defined as the ratio of total useful time to the total cycle time of a packet. For stop and wait protocol,

Total cycle time = Tt(data) + Tp(data) +

Tt(acknowledgement) + Tp(acknowledgement)

= Tt(data) + Tp(data) + Tp(acknowledgement)

= Tt + 2*Tp

Since acknowledgements are very less in size, their transmission delay can be neglected.

Efficiency = Useful Time / Total Cycle Time

= Tt/(Tt + 2*Tp) (For Stop and Wait)

= 1/(1+2a) [Using a = Tp/Tt]

Effective Bandwidth(EB) or Throughput – Number of bits sent per second.

EB = Data Size(L) / Total Cycle time(Tt + 2*Tp)

Multiplying and dividing by Bandwidth (B),

= (1/(1+2a)) * B [Using a = Tp/Tt]

= Efficiency * Bandwidth

Capacity of link – If a channel is Full Duplex, then bits can be transferred in both the directions and without any collisions. Number of bits a channel/Link can hold at maximum is its capacity.
Capacity = Bandwidth(B) * Propagation(Tp)

For Full Duplex channels,

Capacity = 2*Bandwidth(B) * Propagation(Tp)

Concept of Pipelining

In Stop and Wait protocol, only 1 packet is transmitted onto the link and then sender waits for acknowledgement from the receiver. The problem in this setup is that efficiency is very less as we are not filling the channel with more packets after 1st packet has been put onto the link. Within the total cycle time of Tt + 2*Tp units, we will now calculate the maximum number of packets that sender can transmit on the link before getting an acknowledgement.

In Tt units ----> 1 packet is Transmitted.

In 1 units ----> 1/Tt packet can be Transmitted.

In Tt + 2*Tp units -----> (Tt + 2*Tp)/Tt

packets can be Transmitted

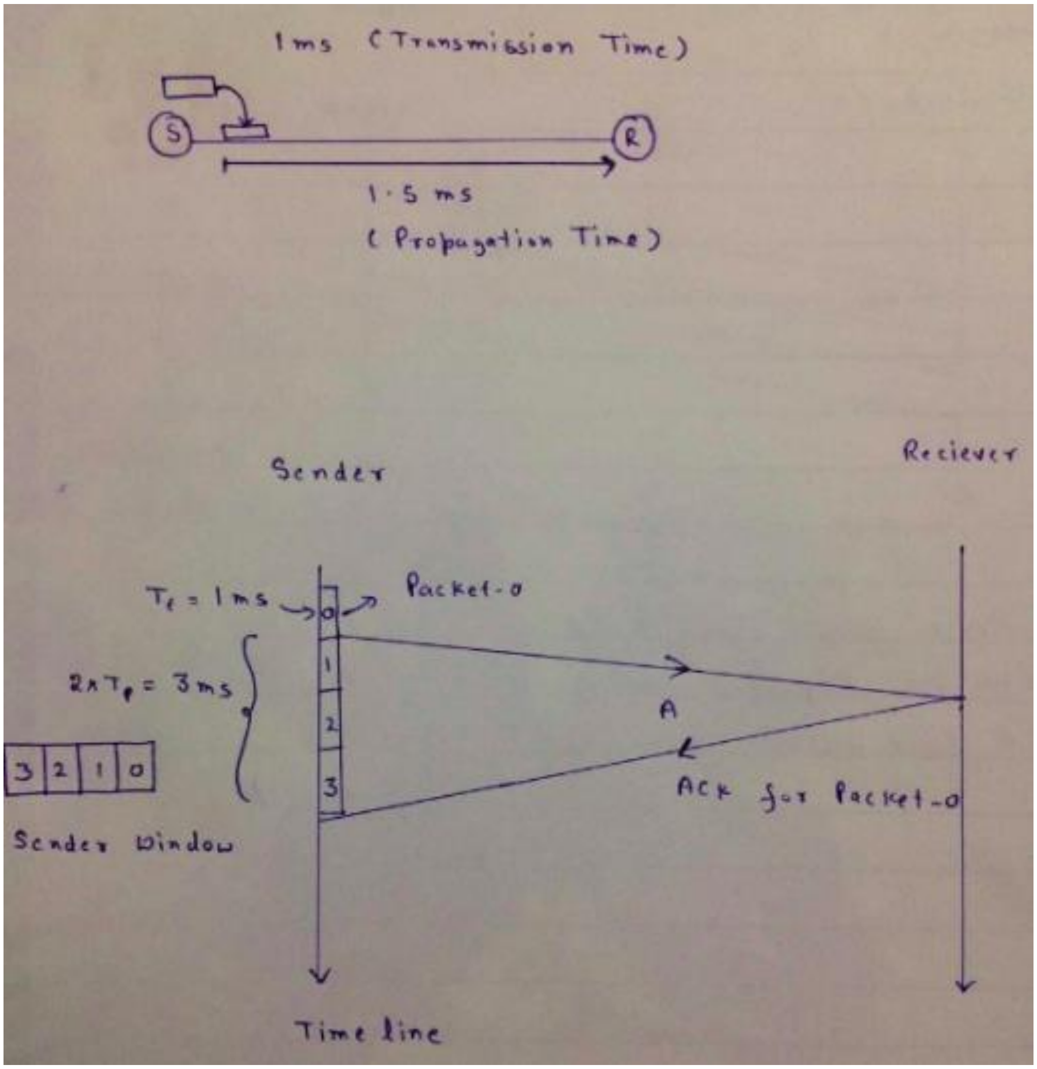
------> 1 + 2a [Using a = Tp/Tt]

Maximum packets That can be Transmitted in total cycle time = 1+2*a

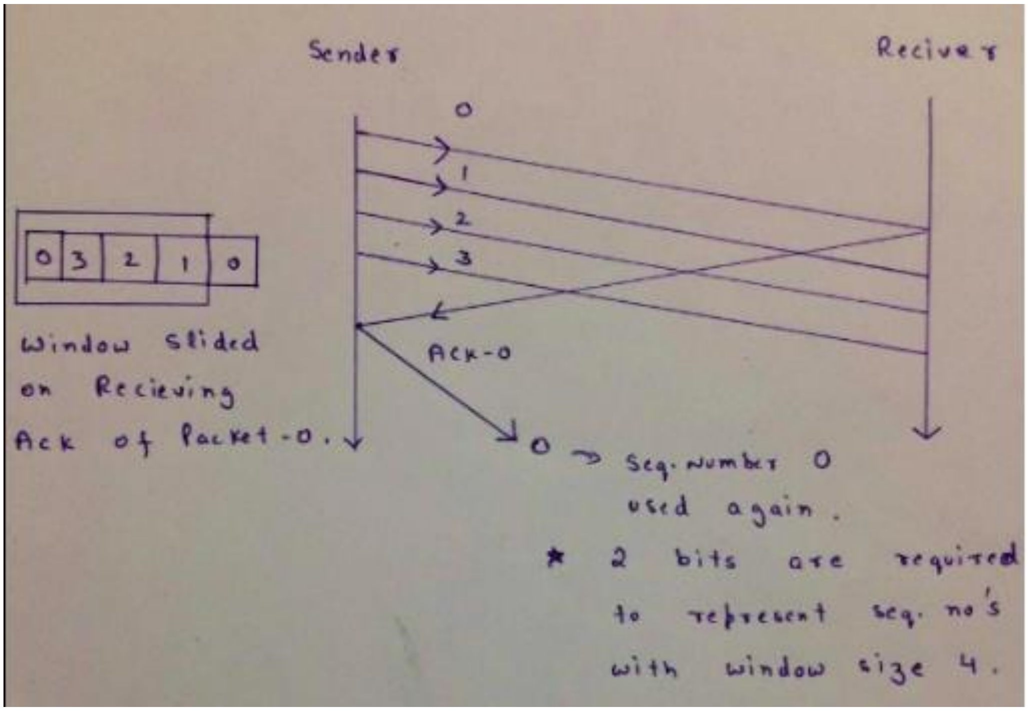
Let me explain now with the help of an example.

Consider Tt = 1ms, Tp = 1.5ms.

In the picture given below, after sender has transmitted packet 0, it will immediately transmit packets 1, 2, 3. Acknowledgement for 0 will arrive after 2*1.5 = 3ms. In Stop and Wait, in time 1 + 2*1.5 = 4ms, we were transferring one packet only. Here we keep a **window of packets which we have transmitted but not yet acknowledged**.



After we have received the Ack for packet 0, window slides and the next packet can be assigned sequence number 0. We reuse the sequence numbers which we have acknowledged so that header size can be kept minimum as shown in the diagram given below.


Sender
Reciver
0
1
2
3
Ack-0
0 3 2 1 0
Window Slided on Recieving Ack of Packet-0.
0 → Seq. number 0 used again.
★ 2 bits are required to represent seq. no's with window size 4.

Minimum Number of Bits for Sender window (Very Important For GATE)

As we have seen above,

Maximum window size = 1 + 2*a where a = Tp/Tt

Minimum sequence numbers required = 1 + 2*a.

All the packets in the current window will be given a sequence number. Number of bits required to represent the sender window = ceil(log2(1+2*a)).

But sometimes number of bits in the protocol headers is pre-defined. Size of sequence number field in header will also determine the maximum number of packets that we can send in total cycle time. If N is the size of sequence number field in the header in bits, then we can have 2^Nsequence numbers.

Window Size ws = min(1+2*a, 2^N)

If you want to calculate minimum bits required to represent sequence numbers/sender window, it will be **ceil(log2(ws))**.

SLIDING WINDOW PROTOCOL | SET 2 (RECEIVER SIDE):

Sliding Window Protocol is actually a theoretical concept in which we have only talked about what should be the sender window size (1+2a) in order to increase the efficiency of stop and wait arq. Now we will talk about the practical implementations in which we take care of what should be the size of receiver window. Practically it is implemented in two protocols namely :

1. Go Back N (GBN)
2. Selective Repeat (SR)

In this article, we will explain you about the first protocol which is GBN in terms of three main characteristic features and in the last part we will be discussing SR as well as comparison of both these protocols

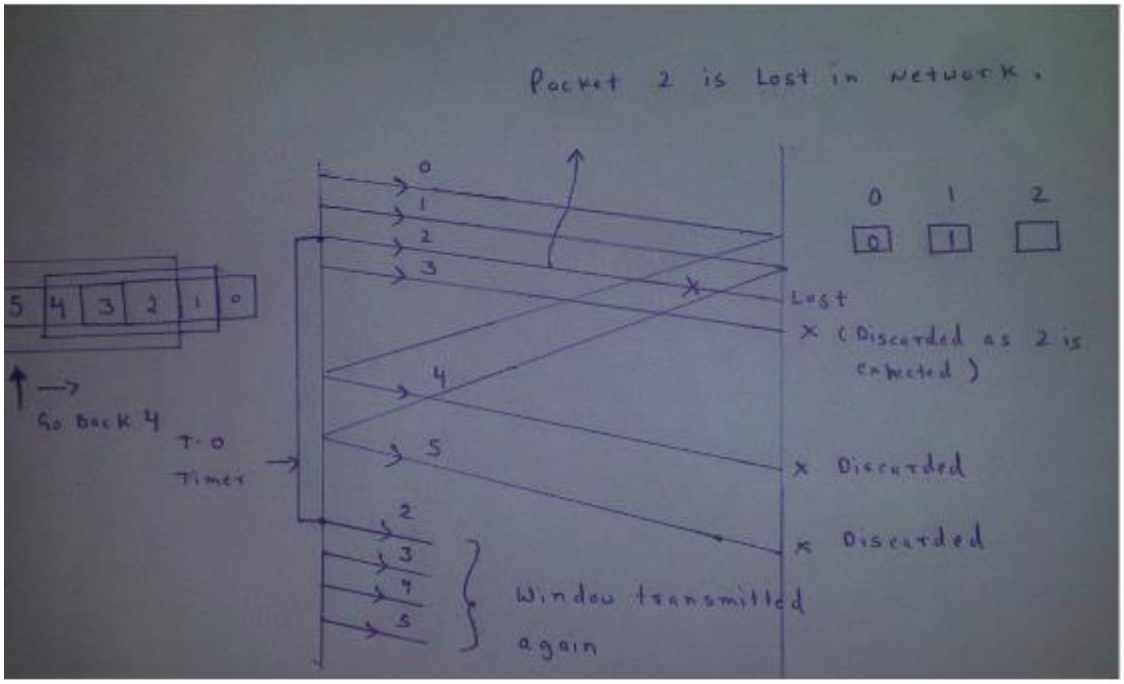
Sender Window Size (WS)
It is N itself. If we say protocol is GB10, then Ws = 10. N should be always greater than 1 in order to implement pipelining. For N = 1, it reduces to Stop and Wait protocol.

Efficiency Of GBN = N/(1+2a) Where a = Tp/Tt

If B is the bandwidth of the channel, then Effective Bandwidth or Throughput = Efficiency * Bandwidth = (N/(1+2a)) * B.

Receiver Window Size (WR)
WR is always 1 in GBN.

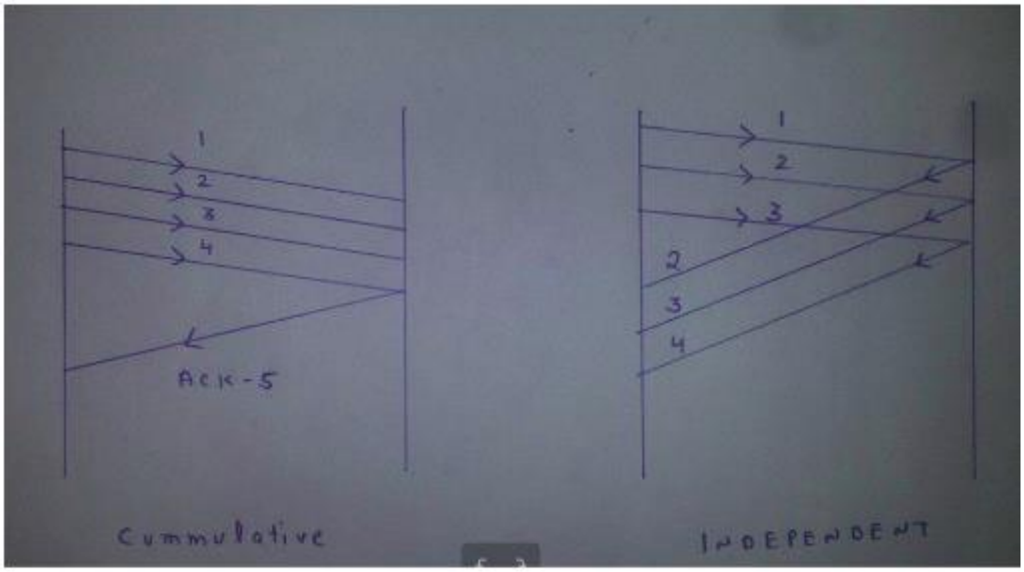
Now what exactly happens in GBN, we will explain with a help of example. Consider the diagram given below. We have sender window size of 4. Assume that we have lots of sequence numbers just for the sake of explanation. Now the sender has sent the packets 0, 1, 2 and 3. After acknowledging the packets 0 and 1, receiver is now expecting packet 2 and sender window has also slided to further transmit the packets 4 and 5. Now suppose the packet 2 is lost in the network, Receiver will discard all the packets which sender has transmitted after packet 2 as it is expecting sequence number of 2. On the sender side for every packet send there is a time out timer which will expire for packet number 2. Now from the last transmitted packet 5 senders will go back to the packet number 2 in the current window and transmit all the packets till packet number 5. That’s why it is called Go Back N. Go back means sender has to go back N places from the last transmitted packet in the unacknowledged window and not from the point where the packet is lost.



Acknowledgements

There are 2 kinds of acknowledgements namely:

- **Cumulative Ack** – One acknowledgement is used for many packets. Main advantage is traffic is less. Disadvantage is less reliability as if one ack is loss that would mean that all the packets sent are lost.
- **Independent Ack** – If every packet is going to get acknowledgement independently. Reliability is high here but disadvantage is that traffic is also high since for every packet we are receiving independent ack.



GBN uses Cumulative Acknowledgement. At the receiver side, it starts a acknowledgement timer whenever receiver receives any packet which is fixed and when it expires, it is going to send a cumulative Ack for the number of packets received in that interval of timer. If receiver has received N packets, then the Acknowledgement number will be N+1. Important point is Acknowledgement timer will not start after the expiry of first timer but after receiver has received a packet.
Time out timer at the sender side should be greater than Acknowledgement timer.

POINT TO POINT PROTOCOL ON INTERNET:

PPP is most commonly used data link protocol. It is used to connect the Home PC to the server of ISP via a modem.

- This protocol offers several facilities that were not present in SLIP. Some of these facilities are:

1. PPP defines the format of the frame to be exchanged between the devices.

2. It defines link control protocol (LCP) for:-

(a) Establishing the link between two devices.

(b) Maintaining this established link.

(c) Configuring this link.

(d) Terminating this link after the transfer.

3. It defines how network layer data are encapsulated in data link frame.

4. PPP provides error detection.

5. Unlike SLIP that supports only IP, PPP supports multiple protocols.

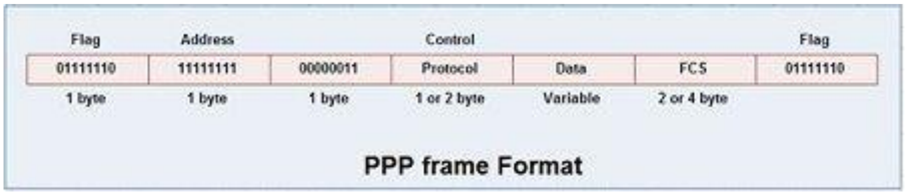
6. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

7. PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

8. It also defines how two devices can authenticate each other.

PPP Frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:



PPP frame Format

1. **Flag field**: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).

2. **Address field**: This field is of 1 byte and is always 11111111. This address is the broadcast address *i.e.* all the stations accept this frame.

3. **Control field**: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000011 to show that the frame does not contain any sequence numbers and there is no flow control or error control.

4. **Protocol field**: This field specifies the kind of packet in the data field *i.e.* what is being carried in data field.

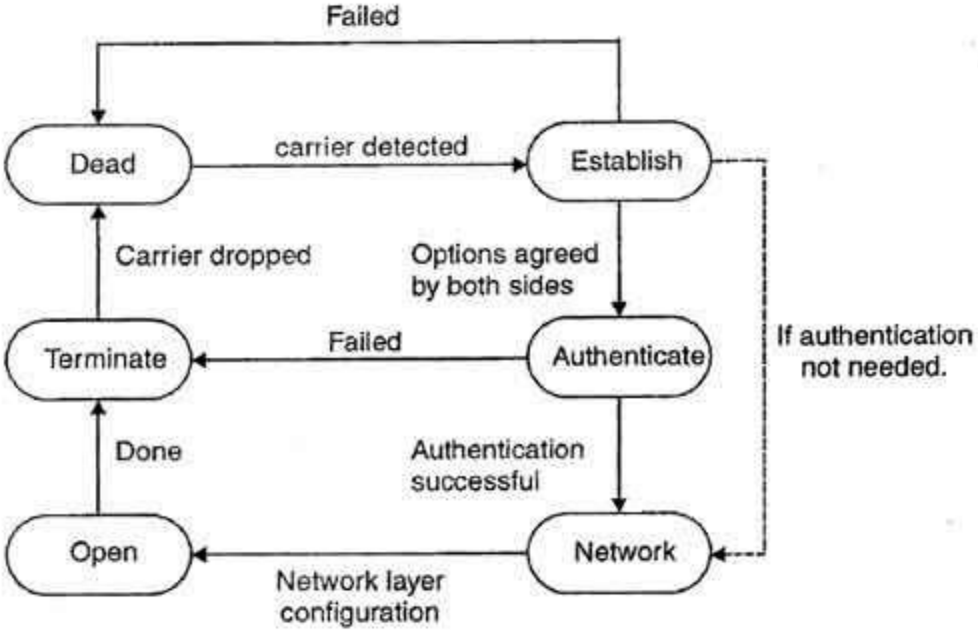
5. **Data field**: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.

6. **FCS field**: The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

Transition Phases in PPP

The PPP connection goes through different states as shown in fig.

1. **Dead**: In dead phase the link is not used. There is no active carrier and the line is quiet.


Failed
Dead
carrier detected
Establish
Carrier dropped
Options agreed by both sides
Terminate
Failed
Authenticate
If authentication not needed.
Done
Authentication successful
Open
Network
Network layer configuration

Transition phases

2. **Establish**: Connection goes into this phase when one of the nodes start communication. In this phase, two parties negotiate the options. If negotiation is successful, the system goes into authentication phase or directly to networking phase. LCP packets are used for this purpose.

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

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

5. **Open**: In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.

6. **Terminate**: In this phase connection is terminated.

Point-to-point protocol Stack

PPP uses several other protocols to establish link, authenticate users and to carry the network layer data.

The various protocols used are:

1. Link Control Protocol

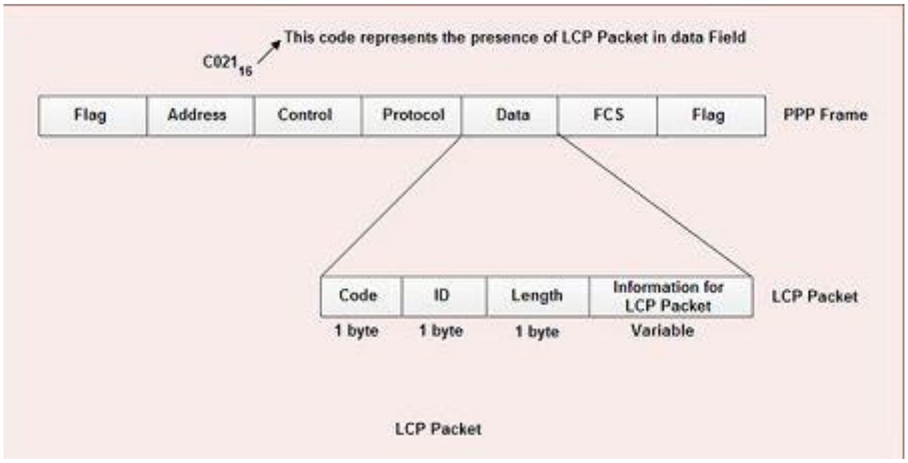
2. Authentication Protocol

3. Network Control Protocol

1. Link Control Protocol

- It is responsible for establishing, maintaining, configuring and terminating the link.

- It provides negotiation mechanism to set options between two endpoints.



LCP Packet

- All LCP packets are carried in the data field of the PPP frame.

- The presence of a value $C021_{16}$ in the protocol field of PPP frame indicates that LCP packet is present in the data field.

• The various fields present in LCP packet are:

1. **Code**: 1 byte-specifies the type of LCP packet.

2. I**D**: 1 byte-holds a value used to match a request with the reply.

3. **Length**: 2 byte-specifies the length of entire LCP packet.

4. **Information**: Contains extra information required for some LCP packet.

• There are eleven different type of LCP packets. These are categorized in three groups:

1. **Configuration packet**: These are used to negotiate options between the two ends. For example: configure-request, configure-ack, configure-nak, configure-reject are some configuration packets.

2. **Link termination packets**: These are used to disconnect the link between two end points. For example: terminate-request, terminate-ack, are some link termination packets.

3. **Link monitoring and debugging packets**: These are used to monitor and debug the links. For example: code-reject, protocol-reject, echo-request, echo-reply and discard-request are some link monitoring and debugging packets.

2. Authentication Protocol

Authentication protocols help to validate the identity of a user who needs to access the resources.

There are two authentication protocols:

1. Password Authentication Protocols (PAP)

2. Challenge Handshake Authentication Protocol (CHAP)

1. PAP (Password Authentication Protocol)

This protocol provides two step authentication procedures:

Step 1: User name and password is provided by the user who wants to access a system.

Step 2: The system checks the validity of user name and password and either accepts or denies the connection.

• PAP packets are also carried in the data field of PPP frames.

• The presence of PAP packet is identified by the value $C023_{16}$ in the protocol field of PPP frame.

• There are three PAP packets.

1. **Authenticate-request**: used to send user name & password.

2. **Authenticate-ack**: used by system to allow the access.

3. **Authenticate-nak**: used by system to deny the access.

2. CHAP (Challenge Handshake Authentication Protocol)

• It provides more security than PAP.

• In this method, password is kept secret, it is never sent on-line.

• It is a three-way handshaking authentication protocol:

1. System sends. a challenge packet to the user. This packet contains a value, usually a few bytes.

2. Using a predefined function, a user combines this challenge value with the user password and sends the resultant packet back to the system.

3. System then applies the same function to the password of the user and challenge value and creates a result. If result is same as the result sent in the response packet, access is granted, otherwise, it is denied.

• There are 4 types of CHAP packets:

1. Challenge-used by system to send challenge value.

2. Response-used by the user to return the result of the calculation.

3. Success-used by system to allow access to the system.

4. Failure-used by the system to deny access to the system.

3. Network Control Protocol (NCP)

• After establishing the link and authenticating the user, PPP connects to the network layer. This connection is established by NCP.

- Therefore NCP is a set of control protocols that allow the encapsulation of the data coming from network layer.

- After the network layer configuration is done by one of the NCP protocols, the users can exchange data from the network layer.

- PPP can carry a network layer data packet from protocols defined by the Internet, DECNET, Apple Talk, Novell, OSI, Xerox and so on.

- None of the NCP packets carry networks layer data. They just configure the link at the network layer for the incoming data.

POSSIBLE QUESTIONS

UNIT-I

PART-A (20 MARKS)

(Q.NO 1 TO 20 Online Examination)

PART-B (2 MARKS)

PART-C (6 MARKS)

Enable | Enlighten | Enrich
KARPAGAM
ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established Under Section 3 of UGC Act, 1956)

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CS Batch:2017

Subject:COMPUTER NETWORKS

SubCode:17CSU303

UNIT III

SL NO	QUESTIONS	OPTION A	OPTION B	OPTION C	OPTION D	ANS
1	Transmission errors are usually detected at the……….layer of OSI model	physical	datalink	network	transport	physical
2	Transmission errors are usually corrected at the……….layer of OSI model	network	transport	datalink	physical	transport
3	Datalink layer imposes a …………mechanism to avoid	flow control	error control	access control	none of the above	flow control
4	Error control mechanism of datalink layer is achieved through a ………..added to the end	header	trailer	adress	frames	trailer
5	The datalink layer is responsible for moving……from one hop to next	packets	frames	signals	message	frames
6	In a single_bit error,how many bits in a data unit are changed	one	two	four	five	one
7	In a burst error,how many bits in a data unit are changed	less than 2	2 or more than 2	2	3	2 or more than 2
8	The length of the burst error is measured from ………	first bit to last bit	first corrupted bit to last corrupted	two	three	first corrupted bit to last
9	Single bit error will least occur in………data transmissions	serial	parallel	synchronous	asynchronous	serial
10	To detect errors or correct errors,we need to send …… with data	address	frames	extra bits	packets	extra bits
11	Which of the following best describes a single bit error	a single bit is inverted	a single bit is inverted per data	a single bit is inverted per	any of the above	a single bit is inverted per

12	In block coding,we divide our message intp blocks,each of k bits,called	dataword	codeword	integers	none of the above	dataword
13	In block coding,the length of the block is ……….	k	r	k+r	k-r	k+r
14	Block coding can detect only …………error	single	burst	multiple	none of the above	single
15	We need ……..redundant bits for error correction than for error detection	less	more	equal	less than or equal to	more
16	The corresponding codeword for the dataword 01 is…..	011	000	101	110	011
17	The hamming distance can easily be found if we apply the …… operation	XOR	OR	AND	NAND	XOR
18	The ……… hamming distance is the smallest hamming distance between all	minimum	maximum	equal	none of the above	minimum
19	The hamming distance d(000,111) is …….	1	0	2	3	2
20	To guarantee correction of upto t errors in all cases,the minimum hamming distance in a	d(min)=2t+1	d(min)=2t-1	d(min)=2t	d(min)=t+1	d(min)=2t+1
21	To guarantee correction of upto s errors in all cases,the minimum hamming distance in	d(min)=s-1	d(min)=s+1	d(min)=s	none of the above	d(min)=s+1
22	A simple_parity check code is a single bit error detecting code in which n=……… with	K	K*1	K-1	K+1	K+1
23	The codeword corresponding to the dataword 1111 is	11110	11111	11101	11011	11110
24	A simple_parity check code can detect an ……. Number of errors	odd	even	prime	none of the above	odd
25	The hamming code is a method of …………..	error detection	error correcton	error encapsulation	A and B	error correcton
26	To make the hamming code respond to a burst error of size N,we neeed to make ……	N+1	N-1	N	0	N
27	CRC is used in network such as ……………	WAN	LAN and WAN	LAN	MAN	LAN and WAN
28	In CRC there is no error if the remainder at the receiver is……………..	equal to the remainder at the	all 0's	non zero	the quotient at the sender	all 0's

29	At the CRC checker,…….means that the dataunit is damaged.	string of 0's	string of 1's	a string of alternating 1's	a non-zero remainder	a non-zero remainder
30	………. Is a regulation of data transmission so that the receiver buffer do not become	flow control	error control	access control	none of the above	flow control
31	……..in the datalink layer separates a message from one source ti a destination or	packets	address	framing	none of the above	framing
32	…….is the process of adding 1 extra byte whenever there is a flag or escape character	byte stuffing	redundancy	bit_stuffing	none of the above	byte stuffing
33	…….is the process of adding 1 extra 0 whenever five consecutive 1's follows a 0 in	byte stuffing	redundancy	bit_stuffing	none of the above	bit_stuffing
34	……in the data link layer is based on automatic repeat request,which is the	error control	flow control	access control	none of the above	error control
35	At any time an error is detected in an exchange specified frames are retransmitted	ARQ	ACK	NAK	SEL	ARQ
36	The datalink layer at the sender side gets data from its……..layer	network	physical	application	transport	network
37	ARQ stands for …………..	acknowledge repeat request	automatic repeat request	automatic repeat	automatic retransmission	automatic repeat
38	Which of the following is a data link layer function	line discipline	error control	flow control	all the above	all the above
39	In protocols the flow and error control information such as ACK and NAK is	stop and wait	go_back	A and B	piggybacking	piggybacking
40	In stop and wait ARQ ,the sequence of numbers is based on……….	modulo-2-arithmetic	modulo-12-arithmetic	modulo-N-arithmetic	all the above	modulo-2-arithmetic
41	Error correction in ……….is done by keeping a copy of the send frames and	stop and wait ARQ	ARQ	ACK	NAQ	stop and wait ARQ
42	In the Go_Back N protocol,the sequence numbers are modulo……..	2^m	2^{m-1}	2^{m+1}	2	2m
43	In sliding window ,the range which is the concern of the sender is called………..	send sliding window	receive sliding window	piggybacking	none of the above	send sliding window
44	Piggypacking is used to improve the efficiency of the ………..protocols.	bidirectional	unidirectional	multidirectional	none of the above	bidirectional
45	The send window can slide …….slots when a valid acknowledgment arrive	one or more	one	two	two or more	one or more

46	The upper sublayer that is responsible for flow and error control is	logical	media access	A and B	all the above	logical
47	The MAC(media access control)sublayer co-ordinates the datalink task within a	LAN	MAN	WAN	LAN and MAN	LAN
48	The lower sublayer that is responsible for multiple access resolution is called	Logical	media access	A and B	all the above	media access
49	In the sliding window method or flow control several frame can be be ………..at a	transit	received	A and B	none of the above	transit
50	The sliding window of the sender expands to the ……..when acknowledgement are	left	middle	right	B and C	right
51	Error detecting codes require ………..nuber of redundant bits.	less	equal	more	less than or equal to	more
52	The datalink layer transforms the …………,a raw transmission facility to a	datalink	physical	network	transport	physical
53	Datalink layer divided into ………… functionality oriented sublayer.	one	zero	two	three	two
54	The send window in Go_Back N maximum size can be …………	2^m	2^{m+1}	2	2^{m-1}	2m-1
55	In stop and wait ARQ and Go_Back_N ARQ,the size of the send window	0	3	1	2	1
56	The relationship between m and n in hamming code is …………	n=2m-1	n=m	n=m-1	n=2m+1	n=2m-1
57	A simple parity_check code is a single_bit error detecting code in which n=k+1 with	3	1	0	2	2
58	……..mechanism of datalink layer is achieved through added to the trailer added	ARQ	ARC	Error control	Flow control	Error control
59	In …………,we divide our message into blocks	convolution coding	block coding	linear coding	A and C	block coding
60	The ………….layer at the sender site gets data from its network layer.	physical	datalink	application	transport	datalink
61	In the ……….protocol,the sequence numbers are modulo 2^m	Go_Back N	Simplest	Stop and wait	all the above	Go_Back N
62	_________ and encapsulates them into frames for transmission.	network layer	physical layer	transport layer	application layer	network layer

63	Which one of the following task is not done by data link layer?	framing	error control	flow control	channel coding	channel coding
64	CRC stands for________	cyclic redundancy check	code repeat check	redundancy check	cyclic repeat check	redundancy check

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2018 onwards)
DEPARTMENT OF COMPUTER SCIENCE,CA& IT

Unit IV - MULTIPLE ACCESS PROTOCOLANDNETWORKS

- CSMA/CD protocols
- Ethernet LANS
- connecting LAN back-bone networks
  - ✓ repeaters
  - ✓ hubs,
  - ✓ switches
  - ✓ bridges,
  - ✓ Router
  - ✓ gateways
- Networks Layer Function stand Protocols
  - ✓ Routing;
  - ✓ Routing algorithms;
- Network layer protocol of Internet-
  - ✓ IP protocol,
  - ✓ Internet control protocols.

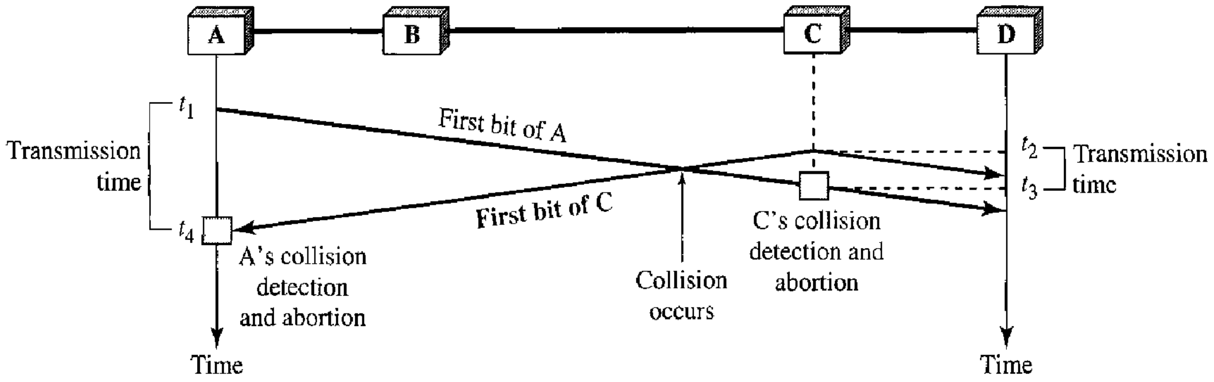
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

Figure 12.12, stations A and C are involved in the collision.

Figure 12.12 *Collision of the first bit in CSMA/CD*

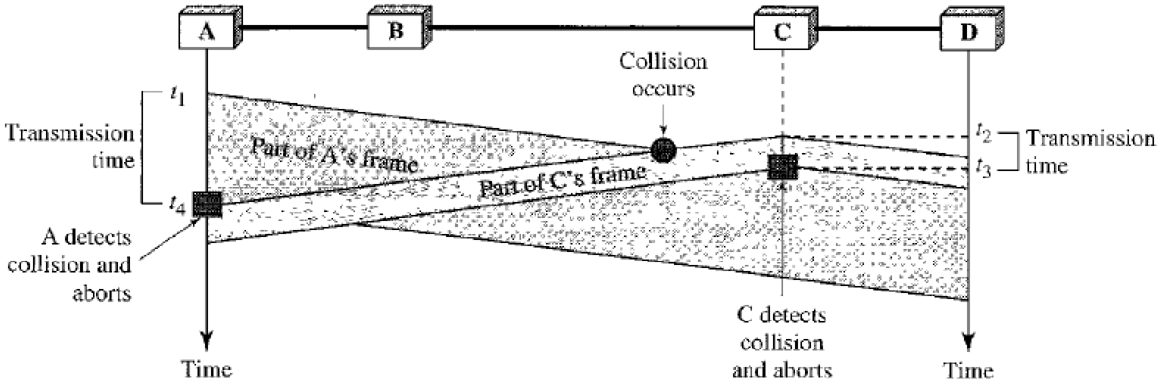


At time t_1, station A has executed its persistence procedure and starts sending the bits of its frame. At time t_2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t_2. Station C detects a collision at time t_3 when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time t_4 when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration $t_4 - t_1$; C transmits for the duration $t_3 - t_2$. Later we show that, for the protocol to work, the length of any frame divided by the bit rate in this protocol must be more than either of these durations. At time t_4, the transmission of A's frame, though incomplete, is aborted; at time t_3, the transmission of B's frame, though incomplete, is aborted.

Minimum Frame Size

For CSMA/CD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission. This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time T_{fr} must be at least two times the maximum propagation time T_p. To understand the reason, let us think about the worst-case scenario. If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time T_p to reach the second, and the effect of the collision takes another time T_p to reach the first. So the requirement is that the first station must still be transmitting after $2T_p$.

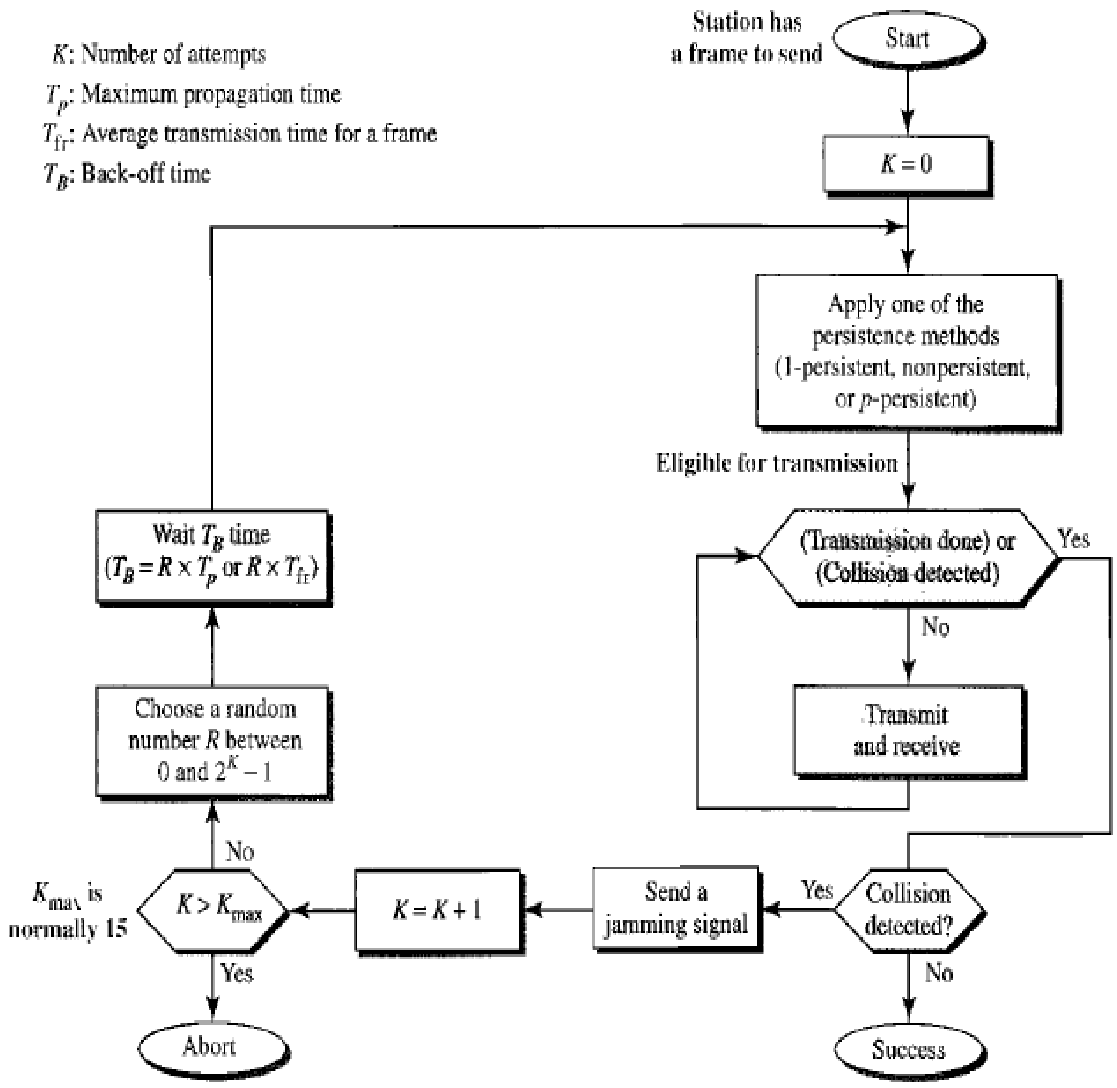
Figure 12.13 *Collision and abortion in CSMA/CD*



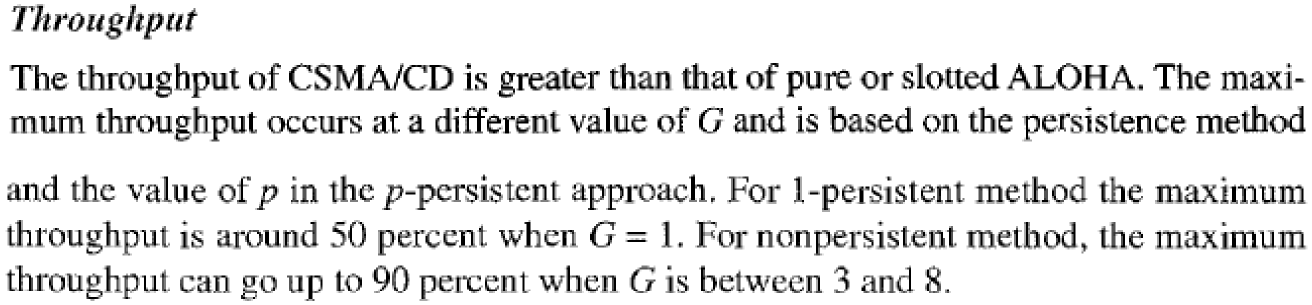
Energy Level

We can say that the level of energy in a channel can have three values: zero, normal, and abnormal. At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame. At the abnormal level, there is a collision and the level of the energy is twice the normal level. A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode. Figure 12.15 shows the situation.

Figure 12.14 *Flow diagram for the CSMA/CD*



K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Station has a frame to send
Start
$K = 0$
Apply one of the persistence methods (1-persistent, nonpersistent, or p-persistent)
Eligible for transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)
Choose a random number R between 0 and $2^K - 1$
No
K_{max} is normally 15
$K > K_{max}$
Yes
Abort
$K = K + 1$
Send a jamming signal
Yes
Collision detected?
No
Success



Throughput

The throughput of CSMA/CD is greater than that of pure or slotted ALOHA. The maximum throughput occurs at a different value of G and is based on the persistence method and the value of p in the p-persistent approach. For 1-persistent method the maximum throughput is around 50 percent when $G = 1$. For nonpersistent method, the maximum throughput can go up to 90 percent when G is between 3 and 8.

Connecting LAN OR Connecting Devices: Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter)

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

Active Hub :- These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.

Passive Hub :- These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend distance between nodes.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

Transparent Bridges :- These are the bridge in which the stations are completely unaware of the

bridge’s existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of

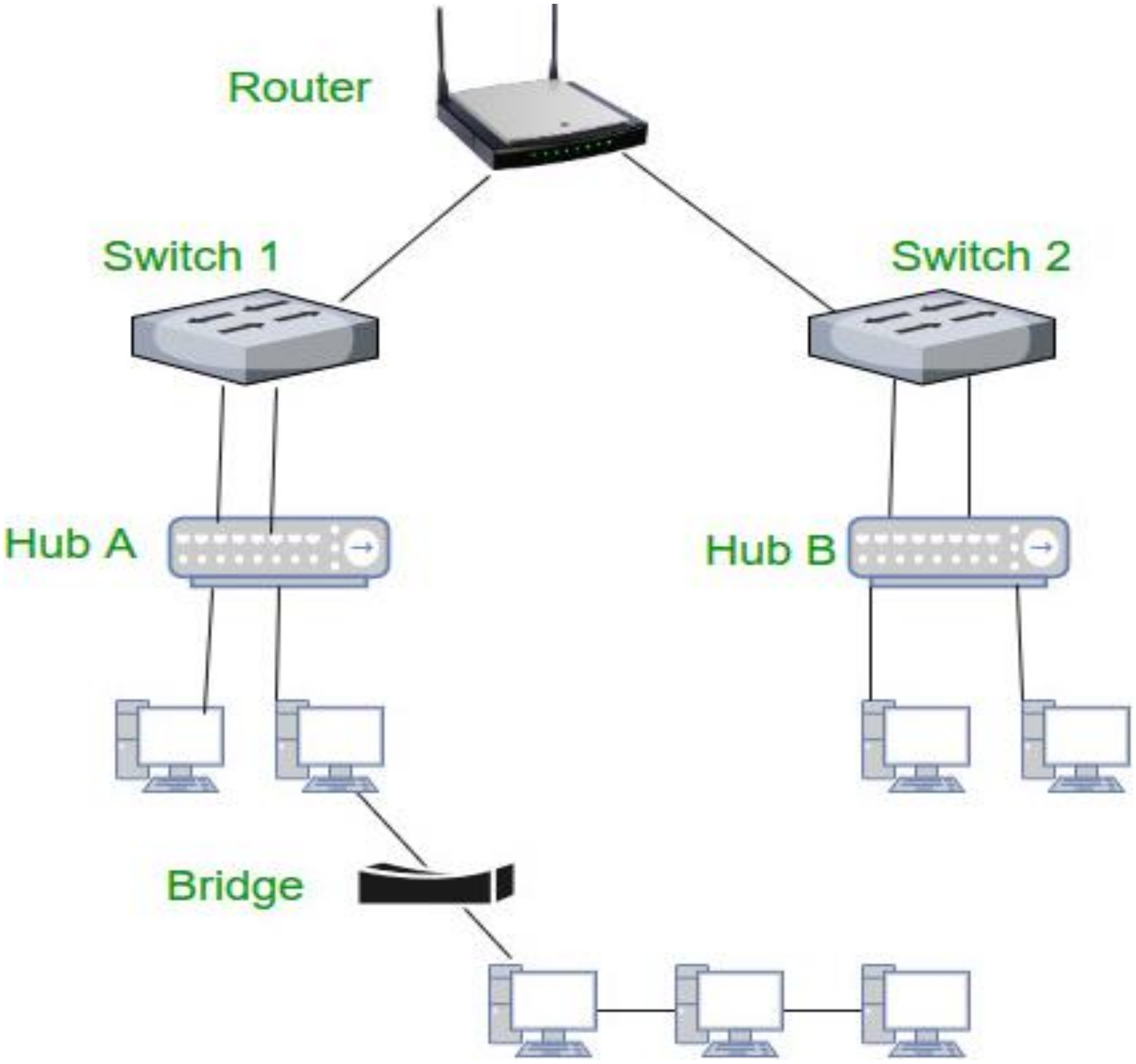
the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.

Source Routing Bridges :- In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have

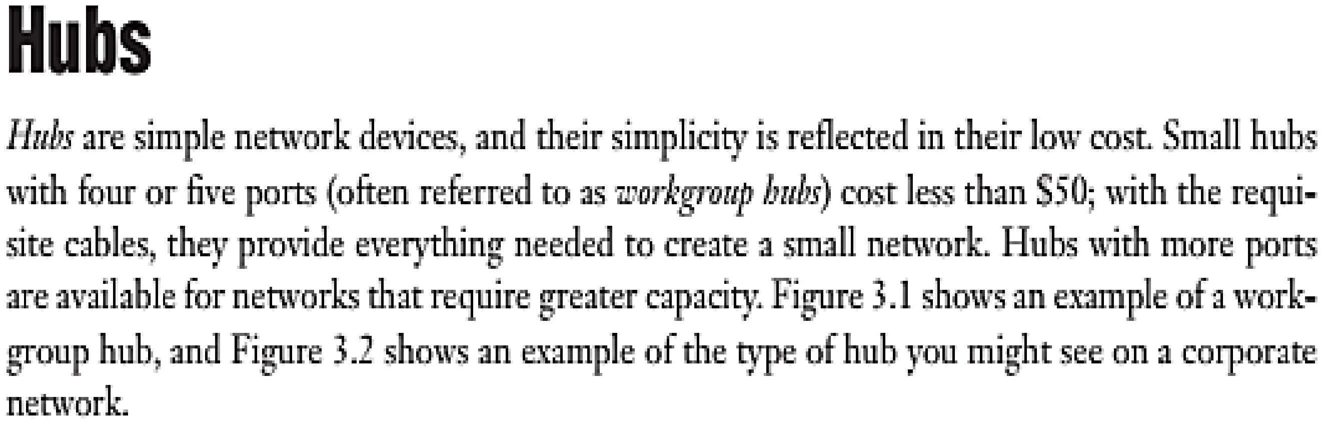
a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. Brouter – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as

bridge, it is capable of filtering local area network traffic.



Hubs

Hubs are simple network devices, and their simplicity is reflected in their low cost. Small hubs with four or five ports (often referred to as *workgroup hubs*) cost less than $50; with the requisite cables, they provide everything needed to create a small network. Hubs with more ports are available for networks that require greater capacity. Figure 3.1 shows an example of a workgroup hub, and Figure 3.2 shows an example of the type of hub you might see on a corporate network.

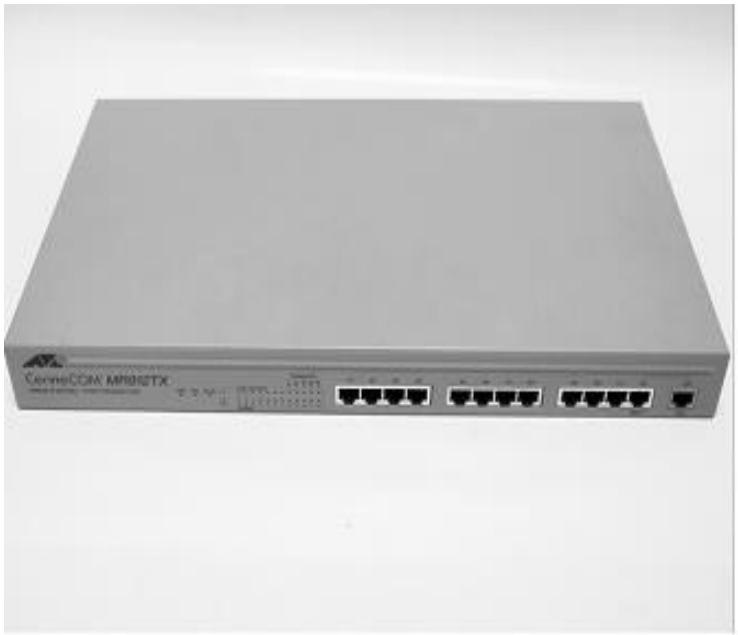


FIGURE 3.2 A high-capacity, or high-density, hub.

Computers connect to a hub via a length of twisted-pair cabling. In addition to ports for connecting computers, even an inexpensive hub generally has a port designated as an uplink port that enables the hub to be connected to another hub to create larger networks. The "Working

Most hubs are referred to as either active or passive. *Active* regenerate a signal before forwarding it to all the ports on the device and requires a power supply. Small workgroup hubs normally use an external power adapter, but on larger units the power supply is built in. *Passive* hubs, which today are seen only on older networks, do not need power and they don't regenerate the data signal.

Regeneration of the signal aside, the basic function of a hub is to take data from one of the connected devices and forward it to all the other ports on the hub. This method of operation is inefficient because, in most cases, the data is intended for only one of the connected devices. You can see a representation of how a hub works in Figure 3.3.

NOTE

Broadcasting The method of sending data to all systems regardless of the intended recipient is referred to as *broadcasting*. On busy networks, broadcast communications can have a significant impact on overall network performance.

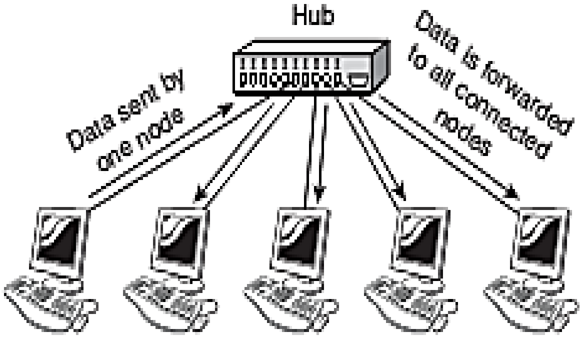


FIGURE 3.3 How a hub works.

Due to the inefficiencies of the hub system and the constantly increasing demand for more bandwidth, hubs are slowly but surely being replaced with switches. As you will see in the next section, switches offer distinct advantages over hubs.

Switches

On the surface, a *switch* looks much like a hub. Despite their similar appearance, switches are far more efficient than hubs and are far more desirable for today's network environments. Figure 3.4 shows an example of a 32-port Ethernet switch. If you refer to Figure 3.2, you'll notice few differences in the appearance of the high-density hub and this switch.

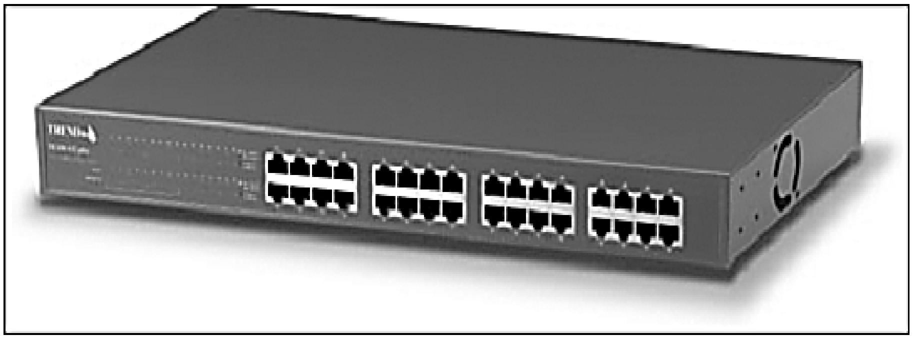


FIGURE 3.4 A 32-port Ethernet switch. (Photo courtesy TRENDware International, www.trendware.com.)

As with a hub, computers connect to a switch via a length of twisted-pair cable. Multiple switches are often interconnected to create larger networks. Despite their similarity in appearance and their identical physical connections to computers, switches offer significant operational advantages over hubs.

As discussed earlier in the chapter, a hub forwards data to all ports, regardless of whether the data is intended for the system connected to the port. This arrangement is inefficient; however, it requires little intelligence on the part of the hub, which is why hubs are inexpensive.

Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected. It looks at the Media Access Control (MAC) addresses of the devices connected to it to determine the correct port. A *MAC address* is a unique number that is stamped into every NIC. By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically. In effect, the switch literally channels (or *switches*, if you prefer) data between the ports. Figure 3.5 illustrates how a switch works.

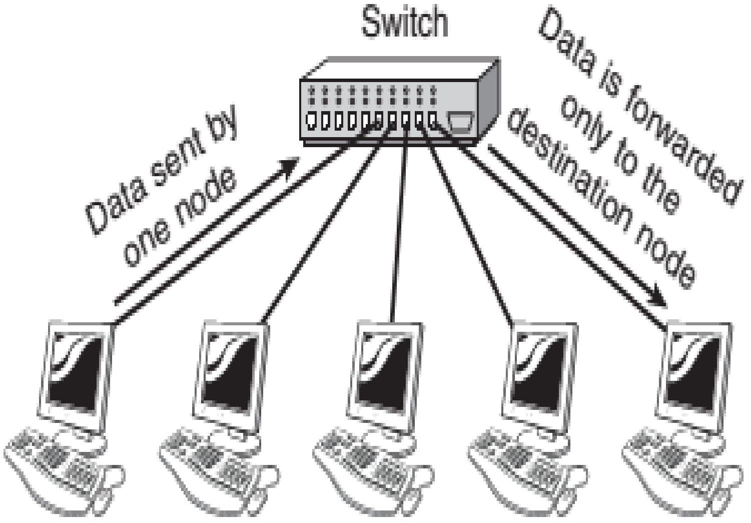


FIGURE 3.5 How a switch works.

Switches can also further improve performance over the performance of hubs by using a mechanism called *full-duplex*. On a standard network connection, the communication between the system and the switch or hub is said to be *half-duplex*. In a half-duplex connection, data can be either sent or received on the wire but not at the same time. Because switches manage the data flow on the connection, a switch can operate in full-duplex mode—it can send and receive data on the connection at the same time. In a full-duplex connection, the maximum data throughput is double that for a half-duplex connection—for example, 10Mbps becomes 20Mbps, and 100Mbps becomes 200Mbps. As you can imagine, the difference in performance between a 100Mbps network connection and a 200Mbps connection is considerable.

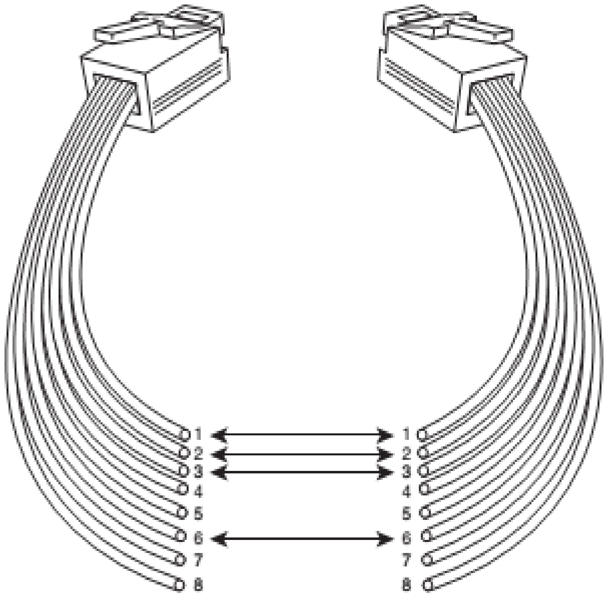


FIGURE 3.7 Pinouts for a straight-through twisted-pair cable.

Switching Methods

Switches use three methods to deal with data as it arrives:

- **Cut-through**—In a cut-through configuration, the switch begins to forward the packet as soon as it is received. No error checking is performed on the packet, so the packet is moved through quickly. The downside of cut-through is that because the integrity of the packet is not checked, the switch can propagate errors.
- **Store-and-forward**—In a store-and-forward configuration, the switch waits to receive the entire packet before beginning to forward it. It also performs basic error checking.
- **Fragment-free**—Building on the speed advantages of cut-through switching, fragment-free switching works by reading only the part of the packet that enables it to identify fragments of a transmission.

Bridges

Bridges are networking devices that connect networks. Sometimes it is necessary to divide networks into subnets to reduce the amount of traffic on each larger subnet or for security reasons. Once divided, the bridge connects the two subnets and manages the traffic flow between them. Today, network switches have largely replaced bridges.

A bridge functions by blocking or forwarding data, based on the destination MAC address written into each frame of data. If the bridge believes the destination address is on a network other than that from which the data was received, it can forward the data to the other networks to which it is connected. If the address is not on the other side of the bridge, the data is blocked from passing. Bridges "learn" the MAC addresses of devices on connected networks by "listening" to network traffic and recording the network from which the traffic originates. Figure 3.9 shows a representation of a bridge.

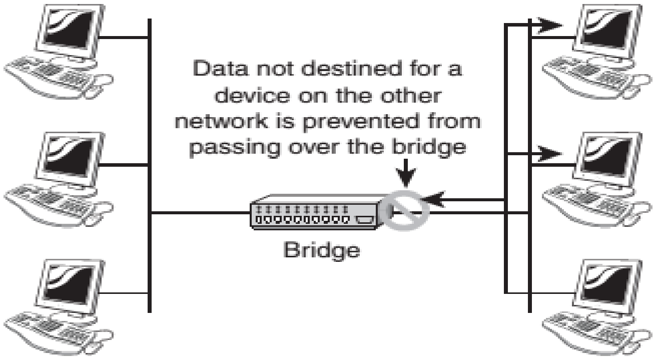

Data not destined for a device on the other network is prevented from passing over the bridge
Bridge

FIGURE 3.9 How a bridge works.

Types of Bridges

Three types of bridges are used in networks. You don't need detailed knowledge of how each bridge works, but you should have an overview:

- **Transparent bridge**—A transparent bridge is invisible to the other devices on the network. Transparent bridges perform only the function of blocking or forwarding data based on the MAC address; the devices on the network are oblivious to these bridges' existence. Transparent bridges are by far the most popular types of bridges.

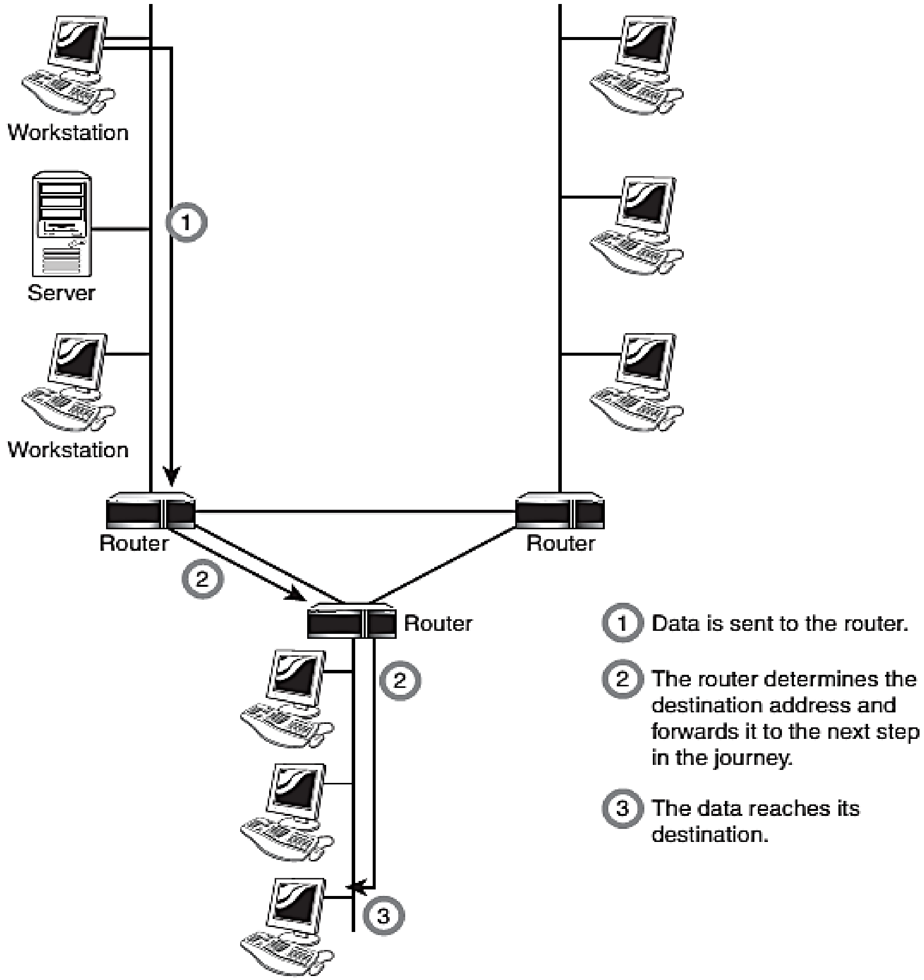
- **Translational bridge**—A translational bridge can convert from one networking system to another. As you might have guessed, it translates the data it receives. Translational bridges are useful for connecting two different networks, such as Ethernet and Token Ring networks. Depending on the direction of travel, a translational bridge can add or remove information and fields from the frame as needed.
- **Source-route bridge**—Source-route bridges were designed by IBM for use on Token Ring networks. The source-route bridge derives its name from the fact that the entire route of the frame is embedded within the frame. This allows the bridge to make specific decisions about how the frame should be forwarded through the network. The diminishing popularity of Token Ring makes the chances that you'll work with a source-route bridge very slim.

Routers

Routers are an increasingly common sight in any network environment, from a small home office that uses one to connect to an Internet service provider (ISP) to a corporate IT environment where racks of routers manage data communication with disparate remote sites. Routers make internetworking possible, and in view of this, they warrant detailed attention.

Routers are network devices that literally route data around the network. By examining data as it arrives, the router can determine the destination address for the data; then, by using tables of defined routes, the router determines the best way for the data to continue its journey. Unlike bridges and switches, which use the hardware-configured MAC address to determine the destination of the data, routers use the software-configured network address to make decisions. This approach makes routers more functional than bridges or switches, and it also makes them more complex because they have to work harder to determine the information. Figure 3.12 shows basically how a router functions.

The basic requirement for a router is that it must have at least two network interfaces. If they are LAN interfaces, the router can manage and route the information between two LAN segments. More commonly, a router is used to provide connectivity across wide area network (WAN) links. Figure 3.13 shows a router with two LAN ports (marked AUI 0 and AUI 1) and two WAN ports (marked Serial 0 and Serial 1). This router is capable of routing data between two LAN segments and two WAN segments.



1 Data is sent to the router.

2 The router determines the destination address and forwards it to the next step in the journey.

3 The data reaches its destination.

FIGURE 3.12 The basic function of a router.

The following are some of the disadvantages of dedicated hardware routers:

- More expensive than server-based router solutions; extra functionality may have to be purchased
- Often require specialized skills and knowledge to manage them
- Limited to a small range of possible uses

Gateways

The term *gateway* is applied to any device, system, or software application that can perform the function of translating data from one format to another. The key feature of a gateway is that it converts the format of the data, not the data itself.

You can use gateway functionality in many ways. For example, a router that can route data from an IPX network to an IP network is, technically, a gateway. The same can be said of a translational bridge that, as described earlier in this chapter, converts from an Ethernet network to a Token Ring network and back again.

Software gateways can be found everywhere. Many companies use an email system such as Microsoft Exchange or Novell GroupWise. These systems transmit mail internally in a certain format. When email needs to be sent across the Internet to users using a different email system, the email must be converted to another format, usually to Simple Mail Transfer Protocol (SMTP). This conversion process is performed by a software gateway.

Another good (and often used) example of a gateway involves the Systems Network Architecture (SNA) gateway, which converts the data format used on a PC to that used on an IBM mainframe or minicomputer. A system that acts as an SNA gateway sits between the client PC and the mainframe and translates requests and replies from both directions. Figure 3.15 shows how this would work in a practical implementation.

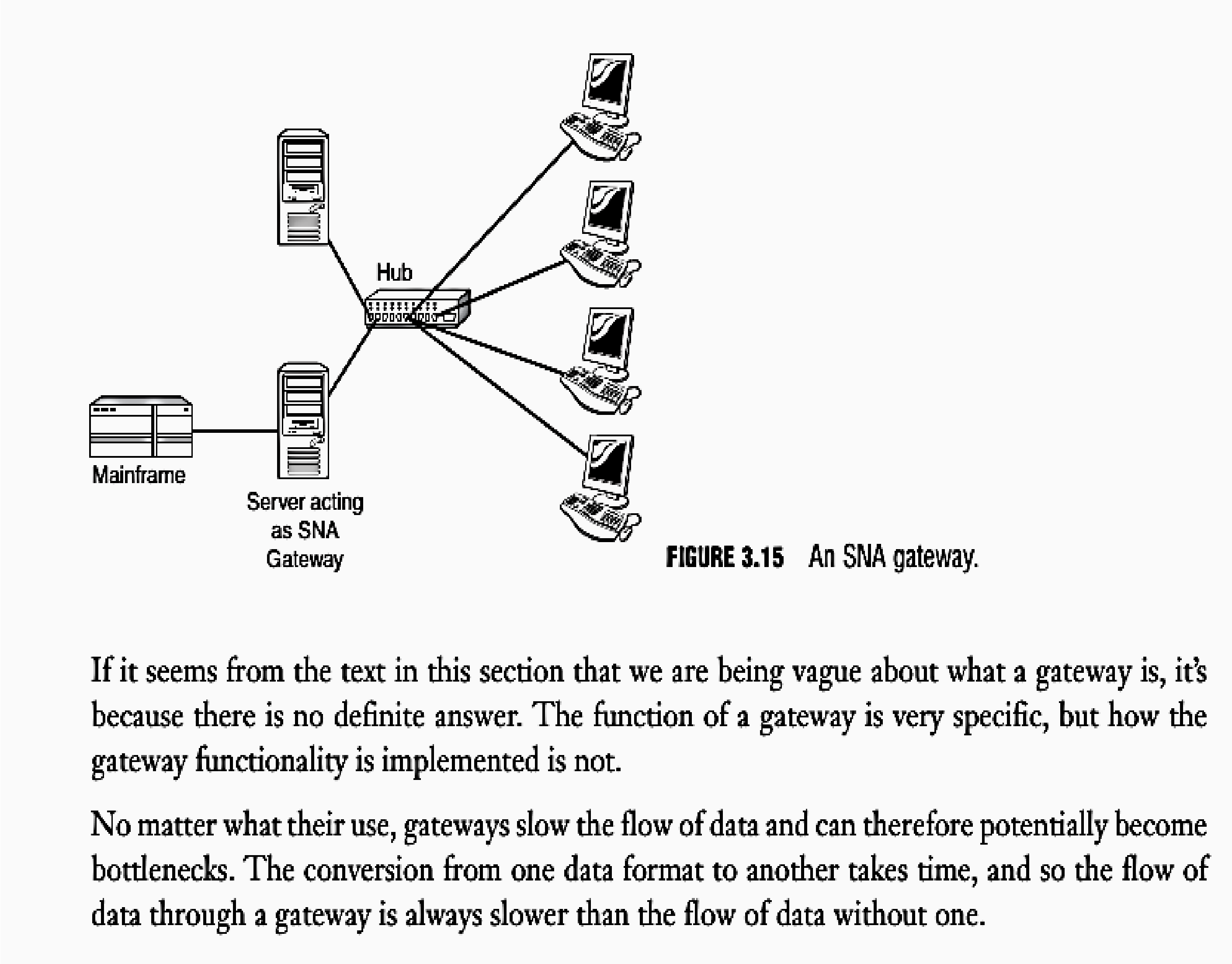

Hub
Mainframe
Server acting
as SNA
Gateway

FIGURE 3.15 An SNA gateway.

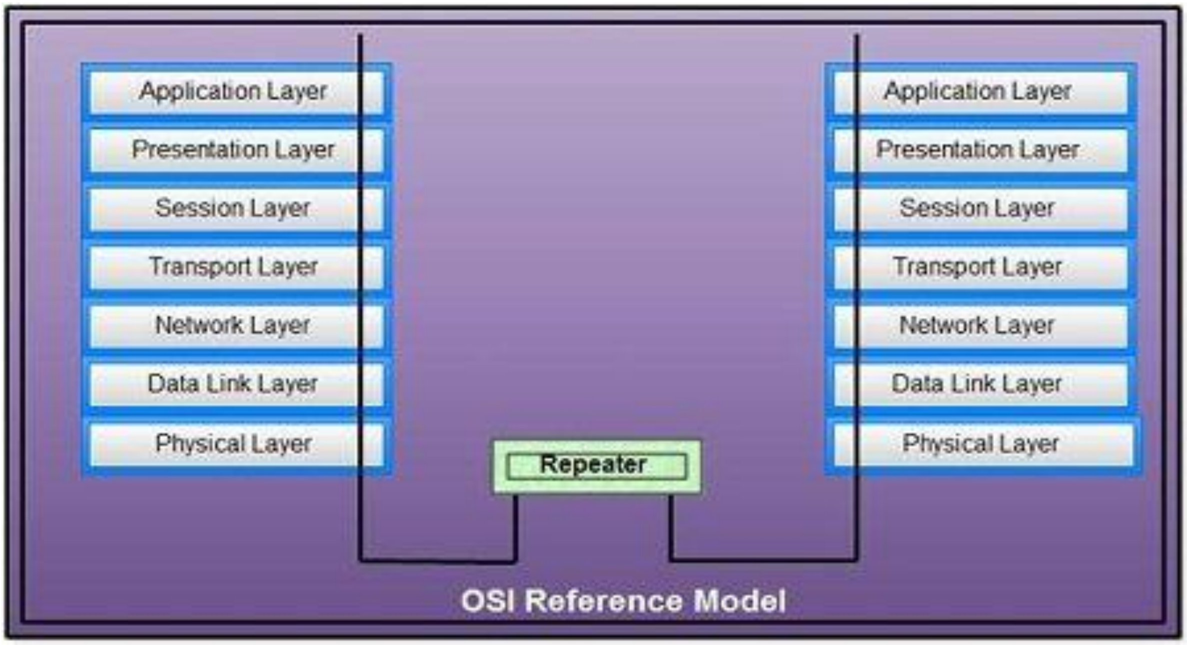
If it seems from the text in this section that we are being vague about what a gateway is, it's because there is no definite answer. The function of a gateway is very specific, but how the gateway functionality is implemented is not.

No matter what their use, gateways slow the flow of data and can therefore potentially become bottlenecks. The conversion from one data format to another takes time, and so the flow of data through a gateway is always slower than the flow of data without one.

Repeaters

The repeaters take the signal they receive from the network devices and regenerate it to keep it intact during its transmission through the physical environment. Since all components of the physical environment of a network (copper, fiber optic cables and wireless media) have to control the attenuation that limits the possible distance between the different nodes of the network, repeaters are an excellent way to extend the net physically.

When an electrical signal travels along a medium it gets attenuated depending upon the medium characteristics. That is why a LAN cannot send signal beyond a certain limit imposed by the different types of LAN technologies. To increase the length of the LAN, repeaters are frequently used. Repeaters in its simplest form relay analog electric signal. It means that they transmit the physical layer signals or data and therefore correspond to the bottom layer of OSI model.



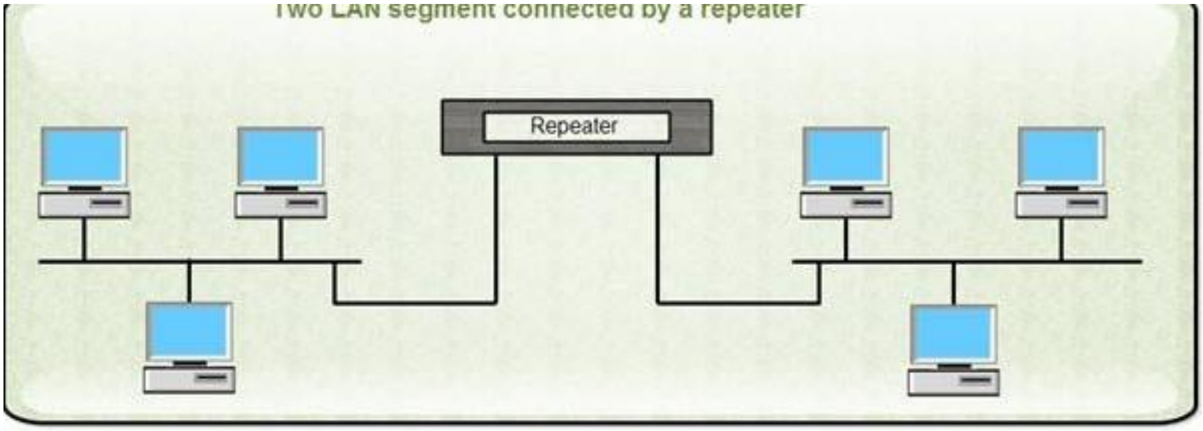
Repeater amplifies the signal, which has got attenuated during the course of transmission because of the physical conditions imposed by the transmission media. It also restores the signal to its original shape. The specific characteristic of repeater is that whatever it receives it transmits to the other LAN segment. This does not understand the frame format and also physical addresses. In other words, it is a transparent device. Therefore, multiple LANs connected by repeaters may be considered as a single LAN.

Since repeaters are devices that operate in the physical layer, they do not examine the data packets they receive, nor do they know any of the logical or physical addresses related to those packets. It means that the location of a repeater hardly affects the transmission speed of the information flow in the network. The repeater is limited to expanding the data signals received from a particular segment of the network and passing them to another segment of the network, as the data moves to its final destination.

The repeaters extend the data signal from one segment of the network and pass it to another segment of the network, thus expanding the size of the network.

Repeaters are also often called concentrators. Hubs that have the same functions as repeaters to amplify the signal are known as active hubs or multiport repeaters. All these devices (regardless of the term used to designate them) operate in the physical layer of the OSI model.

Two LAN connected Repeater

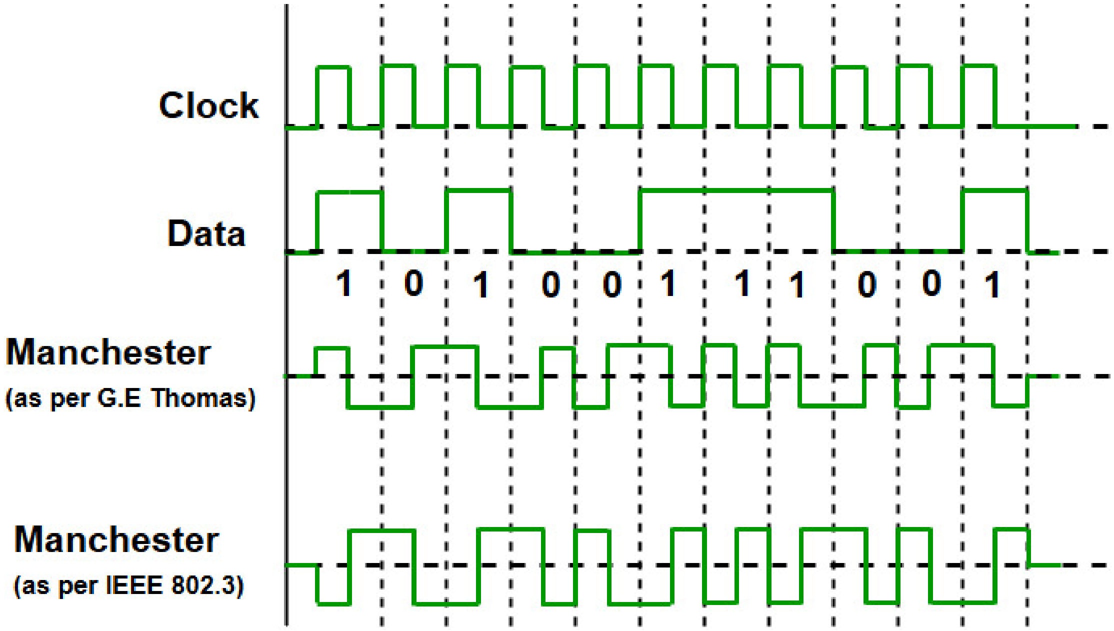


ETHERNET LAN Technologies and Connecting LAN

Local Area Network (LAN) is a data communication network connecting various terminals or computers within a building or limited geographical area. The connection among the devices could be wired or wireless. Ethernet, Token Ring and Wireless LAN using IEEE 802.11 are examples of standard LAN technologies.

Ethernet :-

Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3. The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of topologies which are allowed. Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer. For Ethernet, the protocol data unit is Frame since we mainly deal with DLL. In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.



Manchester Encoding Technique is used in Ethernet.

Since we are talking about IEEE 802.3 standard Ethernet therefore, 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition. In both Manchester Encoding and Differential Manchester, Encoding Baud rate is double of bit rate.

Baud rate = 2* Bit rate

Ethernet LANs consist of network nodes and interconnecting media or link. The network nodes can be of two types:

Data Terminal Equipment (DTE):-

Generally, DTEs are the end devices that convert the user information into signals or reconvert the received signals. DTEs devices are: personal computers, workstations, file servers or print servers also referred to as end stations. These devices are either the source or the destination of data frames. The data terminal equipment may be a single piece of equipment or multiple pieces of equipment that are interconnected and perform all the required functions to allow the user to communicate. A user can interact to DTE or DTE may be a user.

Data Communication Equipment (DCE):-

DCEs are the intermediate network devices that receive and forward frames across the network. They may be either standalone devices such as repeaters, network switches, routers or maybe communications interface units such as interface cards and modems. The DCE performs functions such as signal conversion, coding and may be a part of the DTE or intermediate equipment.

Currently, these data rates are defined for operation over optical fibers and twisted-pair cables:

i) Fast Ethernet

Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100 Mbit/s.

ii) Gigabit Ethernet

Gigabit Ethernet delivers a data rate of 1,000 Mbit/s (1 Gbit/s).

iii) 10 Gigabit Ethernet

10 Gigabit Ethernet is the recent generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s). It is generally used for backbones in high-end applications requiring high data rates.

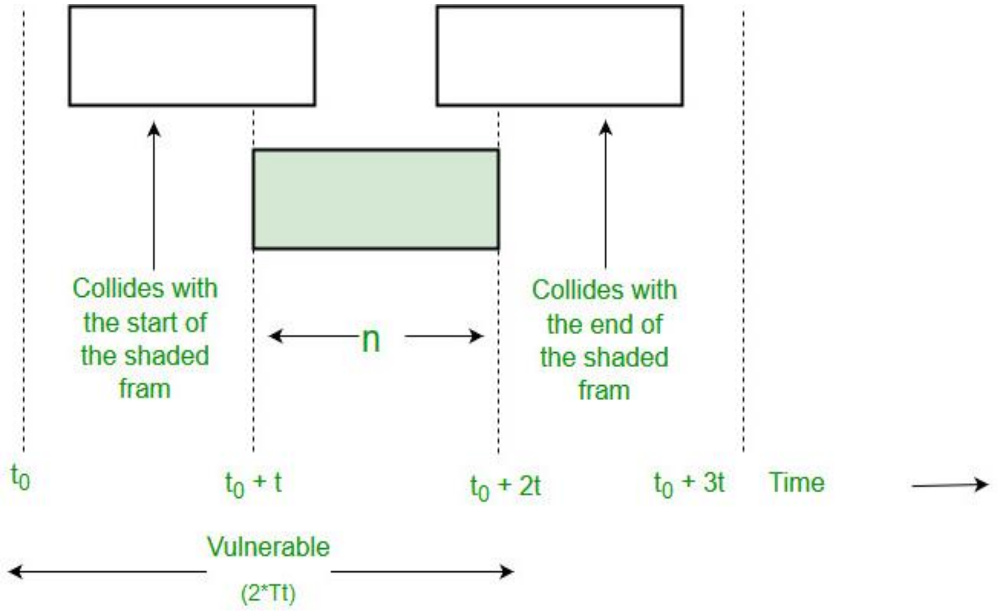
ALOHA

The Aloha protocol was designed as part of a project at the University of Hawaii. It provided data transmission between computers on several of the Hawaiian Islands involving packet radio networks. Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision.

There are two different versions of ALOHA:

1. Pure Aloha

Pure Aloha is an un-slotted, decentralized, and simple to implement a protocol. In pure ALOHA, the stations simply transmit frames whenever they want data to send. It does not check whether the channel is busy or not before transmitting. In case, two or more stations transmit simultaneously, the collision occurs and frames are destroyed. Whenever any station transmits a frame, it expects the acknowledgment from the receiver. If it is not received within a specified time, the station assumes that the frame or acknowledgment has been destroyed. Then, the station waits for a random amount of time and sends the frame again.


Collides with the start of the shaded fram
n
Collides with the end of the shaded fram
t_0
t_0 + t
t_0 + 2t
t_0 + 3t
Time
Vulnerable
(2*Tt)

To assure pure aloha: Its throughput and rate of transmission of the frame to be predicted.

For that to make some assumption:

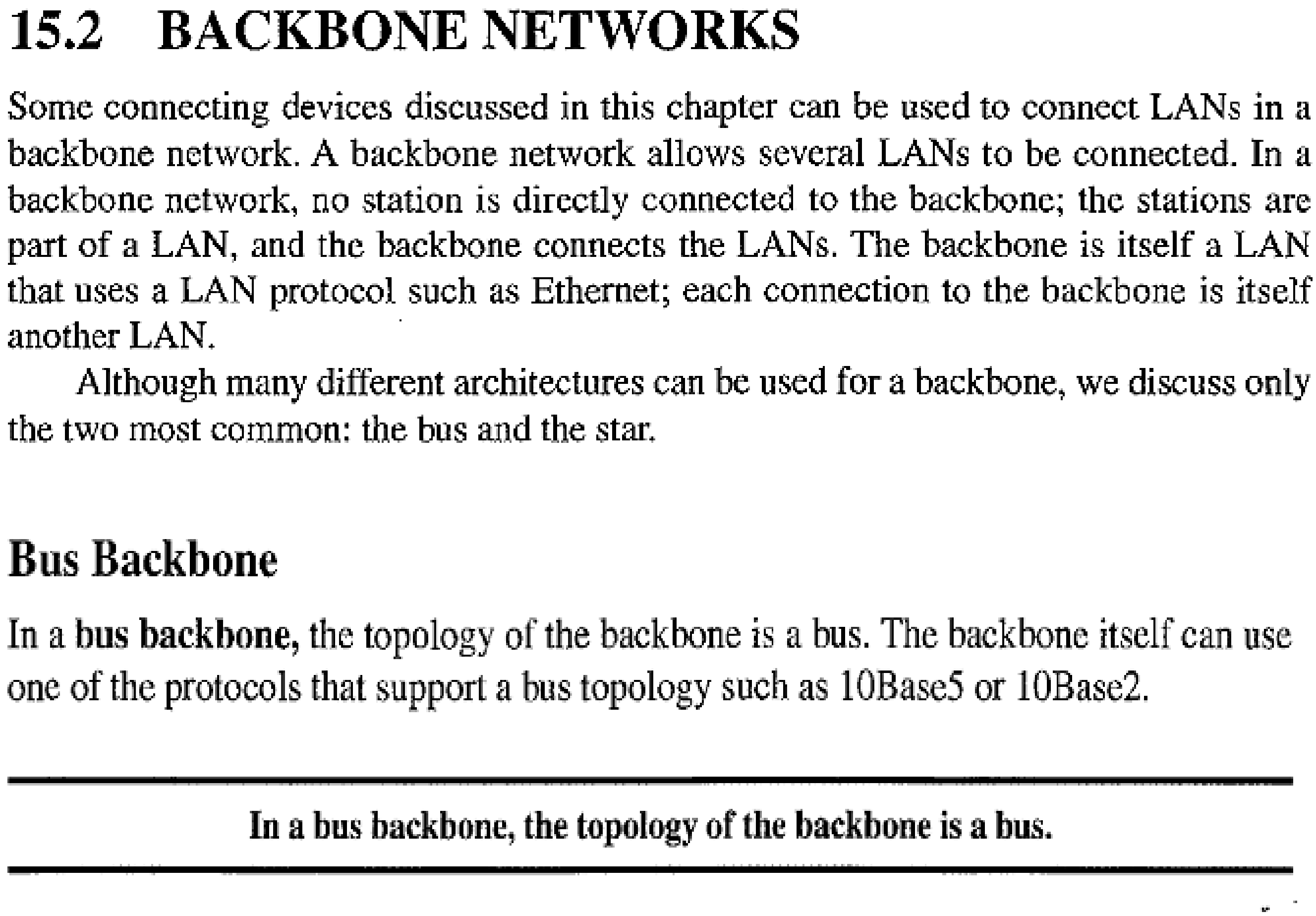
i) All the frames should be the same length.

ii) Stations can not generate frame while transmitting or trying to transmit frame.

iii)The population of stations attempts to transmit (both new frames and old frames that collided) according to a Poisson distribution.

2. Slotted Aloha

This is quite similar to Pure Aloha, differing only in the way transmissions take place. Instead of transmitting right at demand time, the sender waits for some time. In slotted ALOHA, the time of the shared channel is divided into discrete intervals called Slots. The stations are eligible to send a frame only at the beginning of the slot and only one frame per slot is sent. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the beginning of the next time slot. There is still a possibility of collision if two stations try to send at the beginning of the same time slot. But still the number of collisions that can possibly take place is reduced by a large margin and the performance becomes much well compared to Pure Aloha.



15.2 BACKBONE NETWORKS

Some connecting devices discussed in this chapter can be used to connect LANs in a backbone network. A backbone network allows several LANs to be connected. In a backbone network, no station is directly connected to the backbone; the stations are part of a LAN, and the backbone connects the LANs. The backbone is itself a LAN that uses a LAN protocol such as Ethernet; each connection to the backbone is itself another LAN.

Although many different architectures can be used for a backbone, we discuss only the two most common: the bus and the star.

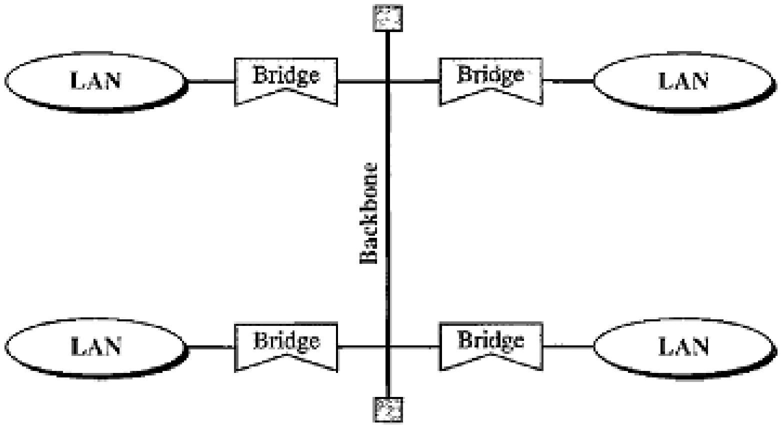
Bus Backbone

In a **bus backbone,** the topology of the backbone is a bus. The backbone itself can use one of the protocols that support a bus topology such as 10Base5 or 10Base2.

In a bus backbone, the topology of the backbone is a bus.

Bus backbones are normally used as a distribution backbone to connect different buildings in an organization. Each building can comprise either a single LAN or another backbone (normally a star backbone). A good example of a bus backbone is one that connects single- or multiple-floor buildings on a campus. Each single-floor building usually has a single LAN. Each multiple-floor building has a backbone (usually a star) that connects each LAN on a floor. A bus backbone can interconnect these LANs and backbones. Figure 15.12 shows an example of a bridge-based backbone with four LANs.

Figure 15.12 *Bus backbone*



In Figure 15.12, if a station in a LAN needs to send a frame to another station in the same LAN, the corresponding bridge blocks the frame; the frame never reaches the backbone. However, if a station needs to send a frame to a station in another LAN, the bridge passes the frame to the backbone, which is received by the appropriate bridge and is delivered to the destination LAN. Each bridge connected to the backbone has a table that shows the stations on the LAN side of the bridge. The blocking or delivery of a frame is based on the contents of this table.

Star Backbone

In a **star backbone,** sometimes called a collapsed or switched backbone, the topology of the backbone is a star. In this configuration, the backbone is just one switch (that is why it is called, erroneously, a collapsed backbone) that connects the LANs.

In a star backbone, the topology of the backbone is a star; the backbone is just one switch.

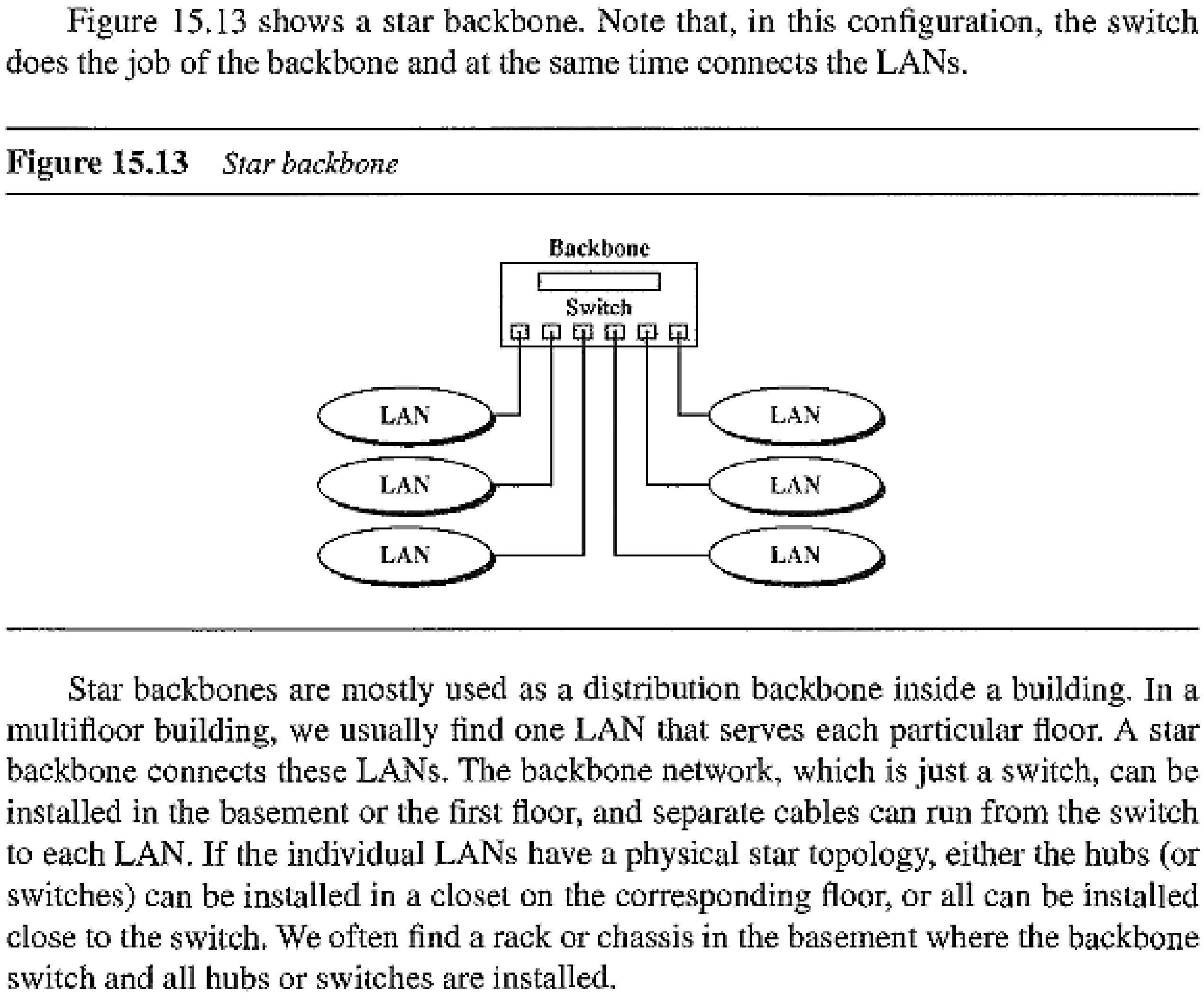


Figure 15.13 shows a star backbone. Note that, in this configuration, the switch does the job of the backbone and at the same time connects the LANs.

Figure 15.13 *Star backbone*

Backbone
Switch
LAN
LAN
LAN
LAN
LAN
LAN

Star backbones are mostly used as a distribution backbone inside a building. In a multifloor building, we usually find one LAN that serves each particular floor. A star backbone connects these LANs. The backbone network, which is just a switch, can be installed in the basement or the first floor, and separate cables can run from the switch to each LAN. If the individual LANs have a physical star topology, either the hubs (or switches) can be installed in a closet on the corresponding floor, or all can be installed close to the switch. We often find a rack or chassis in the basement where the backbone switch and all hubs or switches are installed.

Network Layer Functions and Protocols

- Routing
- Routing Algorithm

Functions of the network layer

The primary function of the network layer is to permit different networks to be interconnected. It does this by forwarding packets to network routers, which rely on algorithms to determine the best paths for the data to travel. These paths are known as virtual circuits. The network layer relies on the Internet Control Message Protocol (ICMP) for error handling and diagnostics to ensure packets are sent correctly. Quality of service (QoS) is also available to permit certain traffic to be prioritized over other traffic. The network layer can support either connection-oriented or connectionless networks, but such a network can only be of one type and not both.

Routing

The process of transferring these packets of information from their source node to the destination node with one or more hops in between along the most optimum path is called as ‘Routing’. Routers and switches are the devices that are used for the purpose which work on the routing protocols and algorithms they are configured with. The routing of packets is taken care of by the L3 layer or the network layer of the OSI Reference Model.

How does it take place?

When a packet is introduced in the network and received by one of the routers, it reads the headers of the packet to understand the destination and checks its routing table marked with routing metrics to see what would be the next best hope for the packet to optimally reach the destination. Then, it pushes the packet to the next node and the above process repeats at the new node too until the packet reaches the destination node.

Routing metrics –

Routing tables have the information based on which packet switching takes place in the most optimal path. And this information is different metrics or variables which the routing algorithms look for and then decide their path. The standard metrics include –

Path Length – In this, the administrator will assign costs to each path (between two nodes). The path length will be the sum of all the path costs. The path with the less path length will be chosen as the most optimal one.

Delay – This is the measure of time it takes for the packet to route from source to destination. This depends on many factors like network bandwidth, the number of intermediate nodes, congestion at nodes, etc. Sooner the transfer, better the Quality of Service (QoS).

Bandwidth – This refers to the amount of data a link can transfer through it. Usually, the enterprise lease the network line to achieve a higher link and bandwidth.

Load – Load refers to the traffic which a router or a link is handling. The unbalanced or unhandled load might cause congestion and a lower rate of transmission packet losses.

Communication Cost – This is the operational expense which the company incurs by sending the packets on the leased line between the nodes.

Resilience and Reliability – This refers to the error handling capacity of the router and the routing algorithms. If some nodes in the network fail then the resilience and reliability measure will show us how well the other nodes can handle the traffic.

Types of Routing

There are two types–

Static Routing – This is the type of routing in which the optimal path between all possible pairs of sources & destinations in the given network is pre-defined and fed into the routing table of the routers of the network.

Advantages –

There is no CPU overhead for the routers to decide the next hop for the packet as the paths are predefined.

This offers higher security as the administrator has autonomy over the permissions for packet flow along a defined path.

Between the routers, no bandwidth would be used (for tasks like updating the routing table, etc.)

Disadvantages

For a larger network topology, it will be difficult for the administrator to identify and pre-define an optimal path from all possible combinations of source & destination nodes. The administrator would be expected to be thorough in the concepts of networks and topology. Transition to a new administrator would consume time so as understand the topology and policies that are defined.

Dynamic Routing – This type gives the router the ability to discover the network by protocols like OSPF (Open Shortest Path First) and RIP (Routing Information Protocol), updates the routing table by itself and effectively decides upon the path that the incoming packet must follow to reach its destination.

Advantages

This is easy to configure.

It would be efficient in order to discover some remote network and execute routing there.

Disadvantages –

When one of the routers in the network implementing dynamic routings discovers change or generates an update, it broadcasts it to all the nodes. Thus, consuming a higher amount of bandwidth.

It is relatively less secure than static.

Types of Routing Algorithms

There are two types of algorithms –

Adaptive – The routes are decided dynamically based on the changes in the network topology.

Distance Vector Routing – In this algorithm, each router maintains a routing table containing an entry for each router in the network. These entries are updated periodically. This is also called as the Bellman-Ford Algorithm. Originally, this was the ARPANET algorithm.

Link State Routing – LSR discovers the neighbors, measures the cost to each neighbor, then constructs the packets and sends it along the computed shortest path.

Routing Algorithm

There are two types of algorithms –

Adaptive – The routes are decided dynamically based on the changes in the network topology.

Distance Vector Routing – In this algorithm, each router maintains a routing table containing an entry for each router in the network. These entries are updated periodically. This is also called as the Bellman-Ford Algorithm. Originally, this was the ARPANET algorithm.

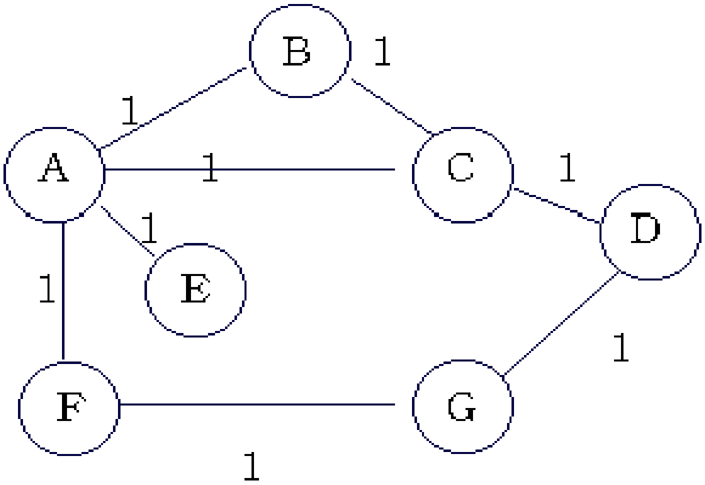
Link State Routing – LSR discovers the neighbors, measures the cost to each neighbor, then constructs the packets and sends it along the computed shortest path.

Distance-Vector Routing

Each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.

1. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.
2. A link that is down is assigned an infinite cost.

Example.



Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	�	1	1	�
B	1	0	1	�	�	�	�
C	1	1	0	1	�	�	�
D	�	�	1	0	�	�	1
E	1	�	�	�	0	�	�
F	1	�	�	�	�	0	1
G	�	�	�	1	�	1	0

Table 1. Initial distances stored at each node(global view).

We can represent each node's knowledge about the distances to all other nodes as a table like the one given in Table 1.

Note that each node only knows the information in one row of the table.

1. Every node sends a message to its directly connected neighbors containing its personal list of distance. (for example, A sends its information to its neighbors B,C,E, and F.)
2. If any of the recipients of the information from A find that A is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through A. (node B learns from A that node E can be reached at a cost of 1; B also knows it can

reach A at a cost of 1, so it adds these to get the cost of reaching E by means of A. B records that it can reach E at a cost of 2 by going through A.)

3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.
4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table. (for example, B knows that it was A who said " I can reach E in one hop" and so B puts an entry in its table that says " To reach E, use the link to A.)

Information	Distance to

Stored at Node	Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Table 2. final distances stored at each node (global view).

In practice, each node's forwarding table consists of a set of triples of the form:

(Destination, Cost, NextHop).

For example, Table 3 shows the complete routing table maintained at node B for the network in figure1.

Destination	Cost	NextHop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

Table 3. Routing table maintained at node B.

Link State Routing

Every node knows how to reach its directly connected neighbors, and if we make sure that the totality of this knowledge is disseminated to every node, then every node will have enough knowledge of the network to determine correct routes to any destination.

Reliable Flooding is the process of making sure that all the nodes participating in the routing protocol get a copy of the link-state information from all the other nodes. As the term " flooding" suggests, the basic idea is for a node to send its link-state information out on all of its directly connected links, with each node that receives this information forwarding it out on all of its link. This process continues until the information has reached all the nodes in the network.

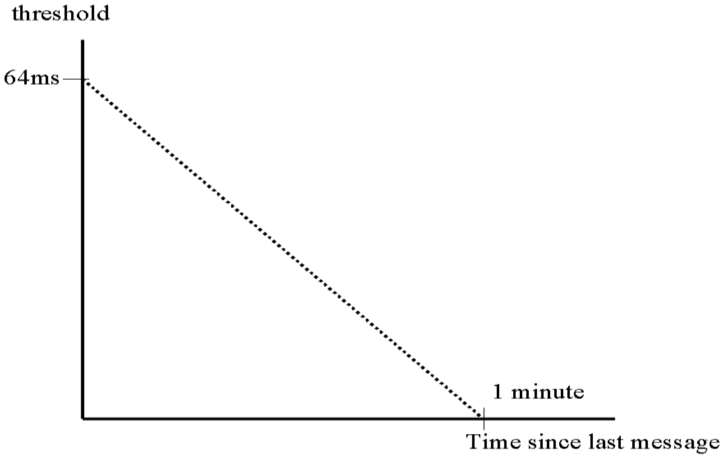
Link State Packet(LSP) contains the following information:

1. The ID of the node that created the LSP;
2. A list of directly connected neighbors of that node, with the cost of the link to each one;
3. A sequence number;
4. A time to live(TTL) for this packet.

Flooding works in the following way. When a node X receives a copy of an LSP that originated at some other node Y, it checks to see if it has already stored a copy of an LSP from Y. If not, it stores the LSP. If it already has a copy, it compares the sequence numbers; if the new LSP has a larger sequence number, it is assumed to be the more recent, and that LSP is stored, replacing the old one. The new LSP is then forwarded on to all neighbors of X except the neighbor from which the LSP was just received.

Each switch computes its routing table directly from the LSPs it has collected using a realization of Dijkstra's algorithm.

Delay Measurement(MRR Page 714)



- Every 10 S the average delay of all packets is computed.

  (A longer measurement period = less adaptive routing if conditions actually change.

A shorter measurement period = less optimal routing because of inaccurate measurement.)

- The delay is considered to have changed "by a significant amount" whenever the absolute value of the change exceeds a certain thershold.
- Threshold is a decreasing function of time.
- Threshold is decreased by 12.8 ms.

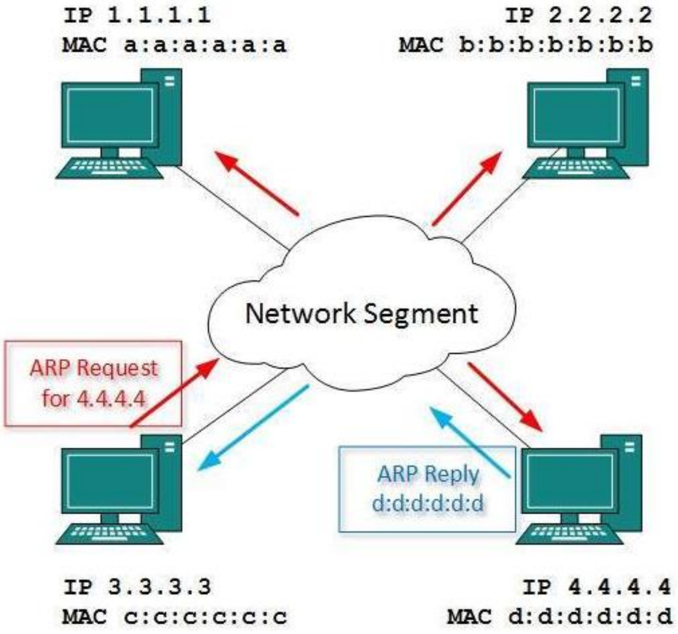
When the delay changes by only a small amount, it is not important routing changes. However, whenever a change in delay is long lasting, it is important that it should be reported eventually, even if it is small; otherwise, additive effects can introduce large inaccuracies into routing. A threshold value which is initially high but which decreases to zero over a period time has this effect.

NETWORK LAYER PROTOCOLS

Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.

Address Resolution Protocol(ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.



On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.

ARP Mechanism

To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, “Who has this IP address?” Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Internet Control Message Protocol (ICMP)

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of

ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

Class A - it uses first octet for network addresses and last three octets for host addressing

Class B - it uses first two octets for network addresses and last two for host addressing

Class C - it uses first three octets for network addresses and last one for host addressing

Class D - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.

Class E - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides ‘Best-Effort-Delivery’ mechanism.

Internet Protocol Version 6 (IPv6)

The IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

- Dual stack implementation
- Tunneling
- NAT-PT

INTERNET PROTOCOLS (IP)

Transmission Control Protocol (TCP)

TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection.It exhibits the following key features:

Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.

TCP is a reliable and connection oriented protocol.

TCP offers:

- Stream Data Transfer.
- Reliability.
- Efficient Flow Control

- Full-duplex operation.
- Multiplexing.
- TCP offers connection oriented end-to-end packet delivery.
- TCP ensures reliability by sequencing bytes with a forwarding acknowledgement number that indicates to the destination the next byte the source expect to receive.
- It retransmits the bytes not acknowledged with in specified time period.

TCP Services

- TCP offers following services to the processes at the application layer:
- Stream Delivery Service
- Sending and Receiving Buffers
- Bytes and Segments
- Full Duplex Service
- Connection Oriented Service
- Reliable Service

- Stream Deliver Service

TCP protocol is stream oriented because it allows the sending process to send data as stream of bytes and the receiving process to obtain data as stream of bytes.

Sending and Receiving Buffers

It may not be possible for sending and receiving process to produce and obtain data at same speed, therefore, TCP needs buffers for storage at sending and receiving ends.

Bytes and Segments

The Transmission Control Protocol (TCP), at transport layer groups the bytes into a packet. This packet is called segment. Before transmission of these packets, these segments are encapsulated into an IP datagram.

Full Duplex Service

Transmitting the data in duplex mode means flow of data in both the directions at the same time.

Connection Oriented Service

TCP offers connection oriented service in the following manner:

- TCP of process-1 informs TCP of process – 2 and gets its approval.

- TCP of process – 1 and TCP of process – 2 and exchange data in both the two directions.

After completing the data exchange, when buffers on both sides are empty, the two TCP’s destroy their buffers.

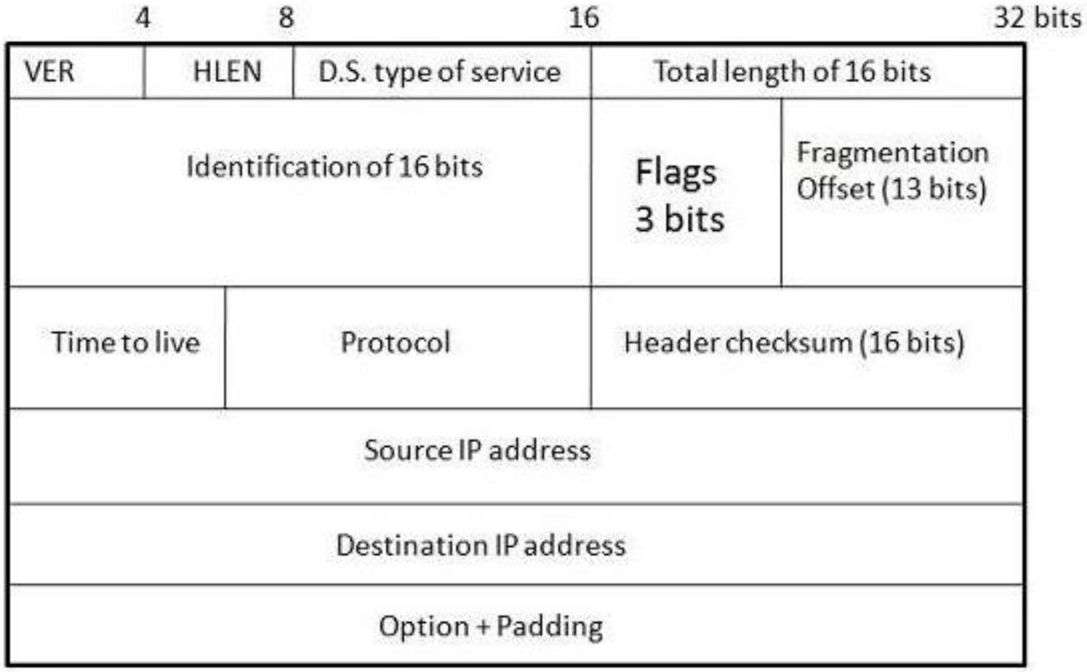
Reliable Service

For sake of reliability, TCP uses acknowledgement mechanism.

Internet Protocol (IP)

Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data. In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

Internet protocol transmits the data in form of a datagram as shown in the following diagram:



4	8	16		32 bits
VER	HLEN	D.S. type of service	Total length of 16 bits	
Identification of 16 bits			Flags 3 bits	Fragmentation Offset (13 bits)
Time to live		Protocol	Header checksum (16 bits)	
Source IP address				
Destination IP address				
Option + Padding				

Points to remember:

- The length of datagram is variable.
- The Datagram is divided into two parts: header and data.
- The length of header is 20 to 60 bytes.
- The header contains information for routing and delivery of the packet.

User Datagram Protocol (UDP)

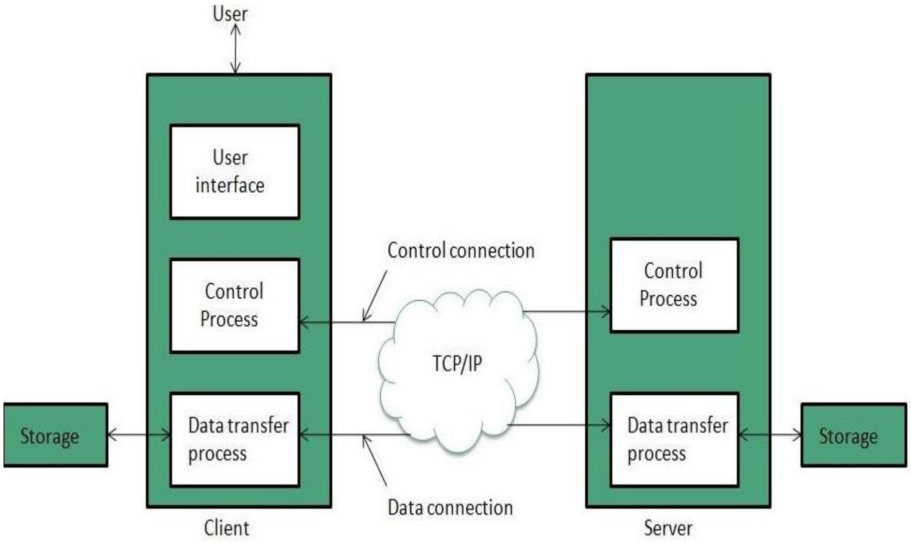
Like IP, UDP is connectionless and unreliable protocol. It doesn’t require making a connection with the host to exchange data. Since UDP is unreliable protocol, there is no mechanism for ensuring that data sent is received.

UDP transmits the data in form of a datagram. The UDP datagram consists of five parts as shown in the following diagram:

UDP is used by the application that typically transmit small amount of data at one time.UDP provides protocol port used i.e. UDP message contains both source and destination port number, that makes it possible for UDP software at the destination to deliver the message to correct application program.

File Transfer Protocol (FTP)

- FTP is used to copy files from one host to another. FTP offers the mechanism for the same in following manner:
- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.
- Control connection is made between control processes while Data Connection is made between
- FTP uses port 21 for the control connection and Port 20 for the data connection.



Hyper Text Transfer Protocol (HTTP)

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

HTTP Request

HTTP request comprises of lines which contains:

- Request line
- Header Fields
- Message body
- Key Points

The first line i.e. the Request line specifies the request method i.e. Get or Post.

The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

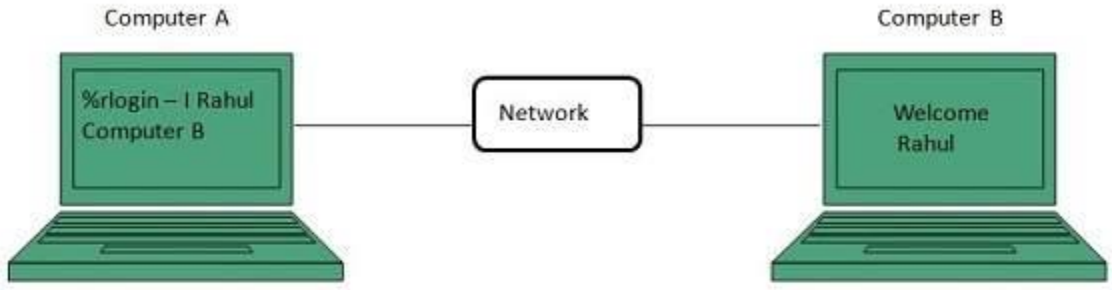
HTTP Response
Like HTTP request, HTTP response also has certain structure. HTTP response contains:

- Status line

- Headers
- Message body

Telnet

Telnet is a protocol used to log in to remote computer on the internet. There are a number of Telnet clients having user friendly user interface. The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.

- 

Internet Control Protocols

IP packets use logical (host to host) addresses and need to be encapsulated in a frame with the help of physical (node-to-node) addresses.

Some protocols are needed to create mapping between physical and logical addresses.

Static Mapping

It creates a table that associates a logical address with a physical address.

This address is stored on each machine in the network.

Each machine has an IP address of another machine but not its physical address. Hence, physical addresses are usually seen in the table.

Dynamic Mapping

In this mapping, each machine knows one of the two addresses (logical or physical address) and tries to find the other one.

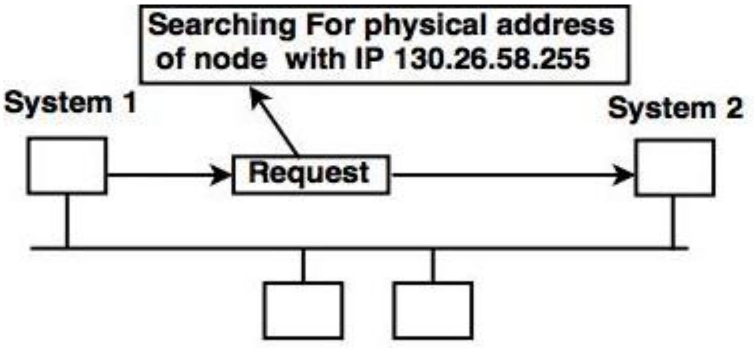
Address Resolution Protocol (ARP)

- Host or router has an IP address and needs to send another host or router (it has the logical (IP) address of the receiver).

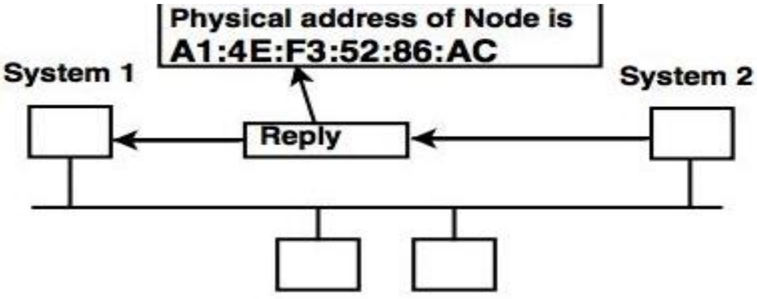
- The logical address is obtained from the routing table, if the sender is a router.
- But, the IP datagram is encapsulated in a frame, which is able to pass through the physical network. This means that the sender needs the physical address of the receiver.
- The host or the router sends an ARP query packet (packet contains the physical and IP addresses of the sender and the IP address of the receiver).
- Considering that, the sender does not know the physical address of the receiver, the query is broadcast over the network.
- Every host or router on the network receives and processes the ARP query packet, but only the desired recipient

recognizes its IP address and sends back ARP response (response packet contains the recipients IP and physical addresses).

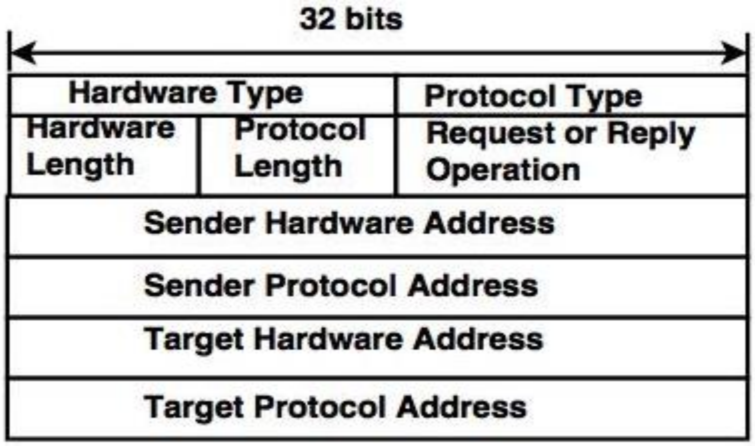
- The packet is unicasted directly to the inquirer by using the physical address which is received in the query packet.



ARP Request Broadcast.



ARP Reply Unicast.



ARP Packet

1. Hardware type

This is 16 bit field used to define the type of the network on which ARP is running.

2. Protocol Length

This is 16 bit length used to define the protocol. For example, the value of this field in IPv4 is 0800H.

3. Hardware length

This is 8 bit field used to define the length of physical address in bytes. This value is 6 for ethernet.

4. Protocol Length

This is 8 bit field used to define the length of logical address in bytes. This value is 4 for IPv4.

5. Operation

This is 16 bit field used to define a type of packet; ARP reply or request.

6. Sender Hardware Length

This is a variable length field used to define the physical address of the sender.

7. Sender Protocol Address

This is a variable length field used to define the logical address of the sender. This field is 4 bytes long for IP protocol.

8. Target Hardware Address

This is a variable length field used to define the physical address of the target. This field is 6 bytes long for ethernet. For ARP request message, this field is '0' because the sender does not know the physical address of the target.

9. Target Protocol Address

This is a variable length used to define the logical address of the target. This is 4 byte long for the IPv4 protocol.

Internetwork is made of_______networks.	3 LANs and 2 WANs	2 LANs and 3 WANs	.4 LANs and 1 WAN	1 LAN and 4 WANs	**.4 LANs and 1 WAN**
Internet at the network layer is a______network.	packet-switched	.LAN	connection	connetionless	**packet-switched**
Internet has chosen the datagram approach to______in network layer	routers	packets	switching	protocol	**protocol**
Internet is made of so many______networks.	homogenous	hetrogeneous	MAN	multipoint	**hetrogeneous**
Communication at network layer in the internet is_______.	connectionless	point-to-point	connection oriented	packet-switched	**connection less**
What is the abbrevation for IPV4_______.	Inter Protocol Versus 4	Inter Position Version 4	Internet protocol version 4	Internet Position Versus 4	**Internet protocol version 4**
IPV4 provides the term 'best-effort' means that________.	no error control	error control	error detection	datagram	**no error control**
Packets in the IPV4 layer are called______.	frames	datagroup	switching	datagrams	**datagrams**
A datagram is a variable length packet consisting of______parts.	one	six	two	three	**two**
The total length field defines the total length of the datagram including_______.	footer	header	flags	frames	**header**

Abbravation for MTU_______.	Minimum Transfer Unit	Maximum Transfer Unit	Maximum Travel Unit	Minimum Travel Unit	**Maximum Transfer Unit**
________in the IPV4 packet covers only header,not the data.	Check subtract	Check sum	options	Check product	**Check sum**
Options can be used for network testings and_________.	checking	packets	types	debugging	**debugging**
A no-operation option is a _____ byte used as a filler between option.	three	six	one	four	**one**
_______can only used as the last option.	end-of-option	first-of-option	options	no options	**end-of-option**
Record route can list up to________router address.	fifteen	sixty	nine	ten	**nine**
_________route has less rigid.	loose source	strict source	no route	record	**loose source**
_________is expressed in millisecond,from midnight.	time stand	time stamp	time shot	time start	**time stamp**
IPv4 also known as_______.	IPNg	IPNG	ipNG	Ipng	**Ipng**
The adoption of IPv6 has been_______.	fast	slow	neuter	quick	**slow**
An IPv6 address is_______bits long.	128	126	125	127	**128**

IPv6 has_______options to allow for additional functionalities.	old	first	new	last	**new**
In packet format,the extension headers and data from the upper layer conains upto_____bytes of information.	65.033	65.535	65.536	65.035	**65.535**
Base header with________fields.	eight	ten	five	six	**eight**
The 4bit field defines the______number of the IP.	versus	header	.footer	version	**version**
Delivery has_____types.	3	4	5	2	**2**
Source and destination of the packet are located on the same physical network called_______.	Indirect delivery	Inward delivery	Direct delivery	Outward delivery	**Direct delivery**
One technique to reduce the content of a routing table is_______.	before-hop	next-hop	first hop	last hop	**next-hop**
The Routing table holds only the address of the next hop______.	next hop	route method	network method	host method	**route method**
A second technique to reduce the routing table________.	next hop	default	forward	network specific	**network specific**
All hosts connected to the same network as one single entity_______.	route	next-hop	host specific	network specific	**host specific**
In classless addressing,atleast_______columns in a routing table.	5	6	3	4	**4**

In an address aggregation,the network for each organization is_______.	independent	dependent	network specific	host specific	**independent**
The routing table can be either_______.	static	static and dynamic	static or dynamic	dynamic	**static or dynamic**
A static routing table can be used in a______internet.	big	small	multi	LAN	**small**
Dynamic routing protocols such as________.	RIP	OSPF	BGP	RIP, OSPF and BGP	**RIP, OSPF and BGP**
The flags are_________.	U,G,H,D,M	G,H,S,S,D	U,G,H	U	**U,G,H,D, M**
The one of the flag is not present,the router is down______.	G	U	H	D	**U**
D means__________.	added by direction	added	added by redirection	subtracted by direction	**added by redirection**
Routing inside an autonomous system____	Intra	Inter	Inside	Outside	**Inside**
Abbrevation for BGP_________.	Border Gateway Process	Bit Gateway Process	Border Gateway Protocol	Byte Gateway Protocol	**Border Gateway Protocol**
A node sends its routing table,at every______in a periodic update.	33s	30s	31s	35s	**30s**
__________algorithm creates a shortest path tree from a graph.	data	dakstra	define	dijkstra	**dijkstra**

An area is a collection of___________.	networks	hosts	route	networks, hosts and route	**networks, hosts and route**
___________link is a network and is connected to only one router.	stub	point-to-point	transient	route	**stub**
Multicasting of the relationship is_________.	one-to-one	many-to-one	one-to-many	many-to-many	**one-to-many**
_________layer is responsible for process-to-process delivery.	transport	physical	application	network	**transport**
Internet has decided to use universal port numbers for severs called_______.	well-unknown port	well-known port	well-known protocol	well-unknown process	**well-known port**
IANA has divided the port numbers into_______ranges.	six	four	five	three	**three**
_______a connection,is first established between the sender and receiver.	connection-oriented	connectionless	token	dialog	**connection-oriented**
UDP is called___________.	connection-oriented	check point	token	connetionless	**connetionless**
UDP length = IP length - ________.	IP length	IP breadth	IP header's length	IP header's breadth	**IP header's length**
UDP is a suitable transport protocol for________.	unicasting	multicasting	nocasting	bicasting	**multicasting**
TCP groups a number of bytes together into a packet called_______.	segment	encapsulation	datagram	data binding	**segment**

The acknowledgement number is ________.	natural	whole	integers	cumulative	**cumulative**
_________ flag is used to terminate the connection.	TER	FIN	URG	PSH	**FIN**
________ protocol is used to remote procedure call.	DNS	PRC	RPC	RPCC	**RPC**
An ACK segment,if carrying ________data consumes no sequence number.	no	2	3	5	**no**
In TCP,one end can stop sending data while still receiving data is ______.	full-close	full-open	half-close	half- open	**half-close**
The value of RTO is dynamic in TCP and is updated based on _______segment.	RTO	RTT	ACK	ARQ	**RTT**

Unit-V

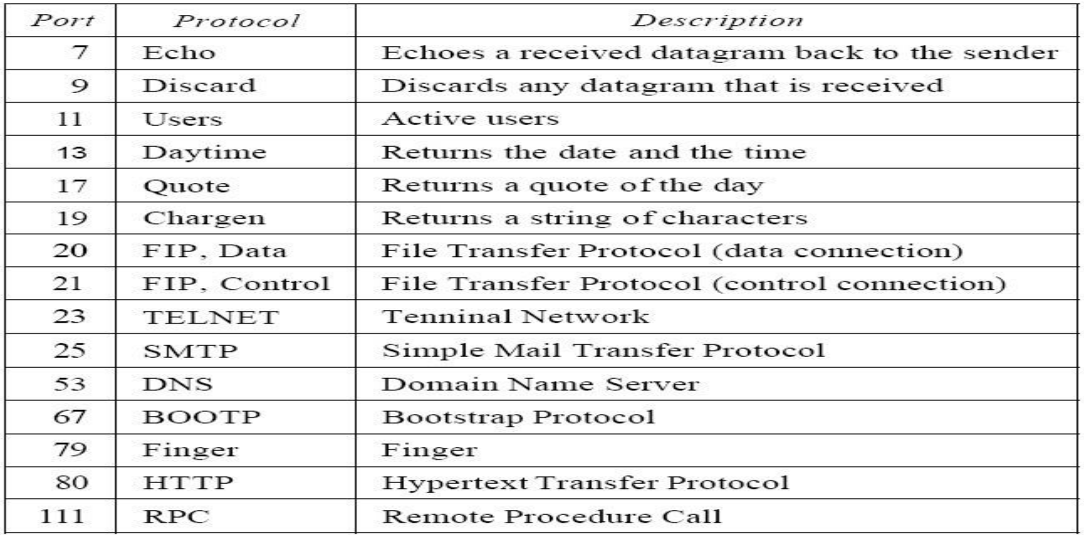
Transmission Control Protocol (TCP). TCP

Transmission Control Protocol (TCP). TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.In brief, TCP is called a *connection-oriented, reliable* transport protocol. It adds connection-oriented and reliability features to the services of IP.

TCP Services

Process-to-Process Communication

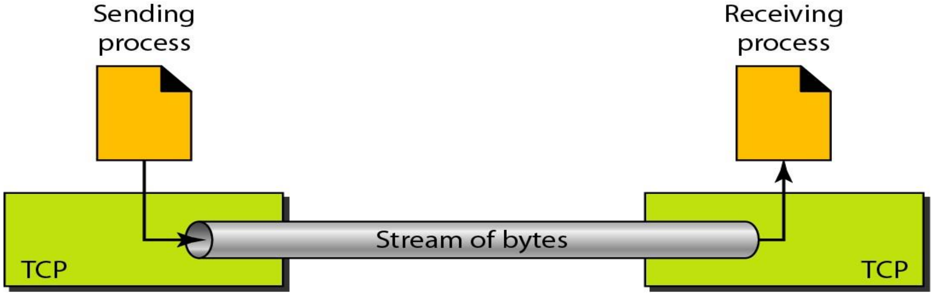
The Transmission Control Protocol (TCP) is one of the main transport layer protocols used with IP. It is a connection oriented protocol based on the connectionless IP protocol..



Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FIP, Data	File Transfer Protocol (data connection)
21	FIP, Control	File Transfer Protocol (control connection)
23	TELNET	Tenninal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Stream Delivery Service

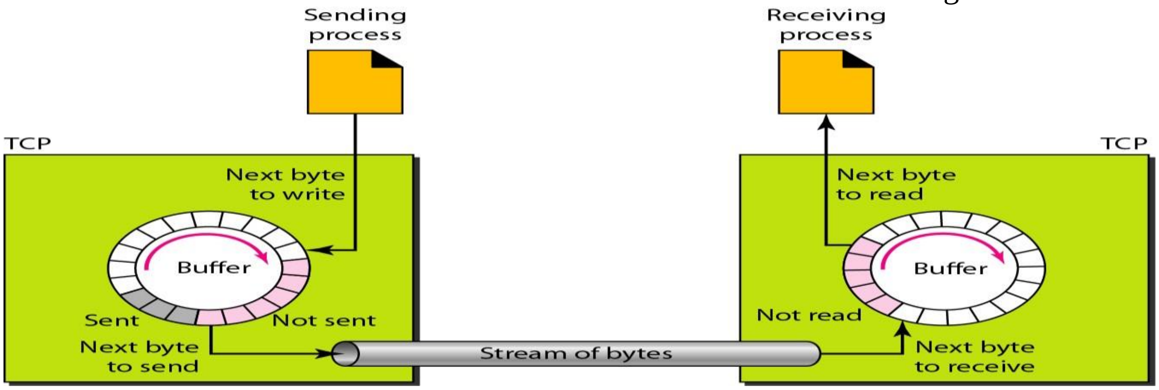
TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the Internet.



The sending process produces (writes to) the stream of bytes, and the receiving process consumes (reads from) them.

Sending and Receiving Buffers:

Because the sending and the receiving processes may not write or read data at the same speed, TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction. One way to implement a buffer is to use a circular array of 1-byte locations as shown in Figure below.

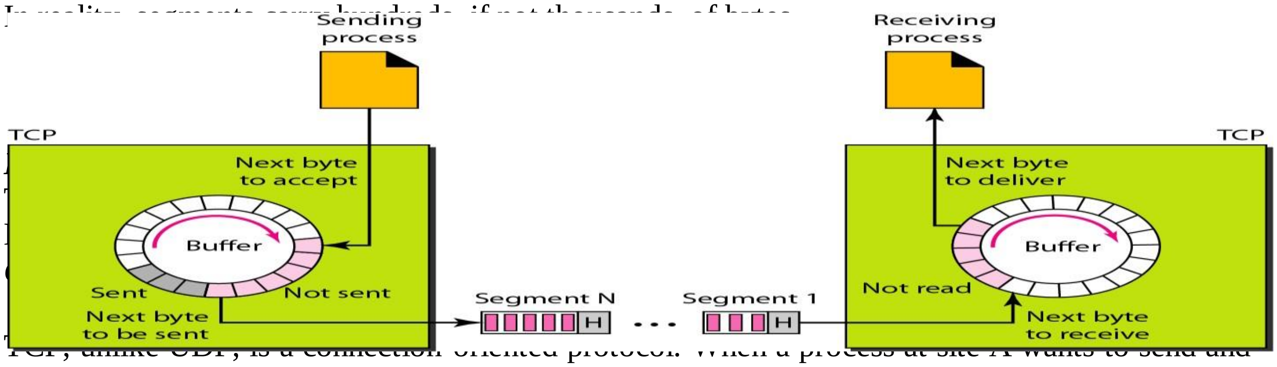


At the sending site, the buffer has three types of chambers. The white section contains empty chambers that can be filled by the sending process (producer). The gray area holds bytes that have been sent but not yet acknowledged. TCP keeps these bytes in the buffer until it receives an acknowledgment. The colored area contains bytes to be sent by the sending TCP.

The circular buffer is divided into two areas (shown as white and colored). The white area contains empty chambers to be filled by bytes received from the network. The colored sections contain received bytes that can be read by the receiving process. When a byte is read by the receiving process, the chamber is recycled and added to the pool of empty chambers.

Segments. At the transport layer, TCP groups a number of bytes together into a packet called a segment. TCP adds a header to each segment (for control purposes) and delivers the segment to the IP layer for transmission. The segments are encapsulated in IP datagrams and transmitted.

In reality, segments carry hundreds, if not thousands, of bytes.



TCP, unlike UDP, is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:

1. The two TCPs establish a connection between them.
2. Data are exchanged in both directions.
3. The connection is terminated.

Note that this is a virtual connection, not a physical connection. The TCP segment is encapsulated in an IP datagram and can be sent out of order, or lost, or corrupted, and then resent. Each may use a different path to reach the destination. There is no physical connection.

TCP creates a stream-oriented environment in which it accepts the responsibility of delivering the bytes in order to the other site. The situation is similar to creating a bridge that spans multiple islands and passing all the bytes from one island to another in one single connection.

Reliable Service

TCP is a reliable transport protocol. It uses an acknowledgment mechanism to check the safe and sound arrival of data. We will discuss this feature further in the section on error control.

TCP Features

To provide the services mentioned in the previous section, TCP has several features that are briefly summarized in this section.

Numbering System

Although the TCP software keeps track of the segments being transmitted or received, there is no field for a segment number value in the segment header. Instead, there are two fields called the sequence number and the acknowledgment number. These two fields refer to the byte number and not the segment number.

Byte Number: TCP numbers all data bytes that are transmitted in a connection. Numbering is independent in each direction. When TCP receives bytes of data from a process, it stores them in the sending buffer and numbers them. The numbering does not necessarily start from O. Instead, TCP generates a random number between 0 and 232 - 1 for the number of the first byte. For example, if the random number happens to be 1057 and the total data to be sent are 6000 bytes, the bytes are numbered from 1057 to 7056. The bytes of data being transferred in each connection are numbered by TCP. The numbering starts with a randomly generated number. **Sequence Number** After the bytes have been numbered, TCP assigns a sequence number to each segment that is being sent. The sequence number for each segment is the number of the first byte carried in that segment.

The **acknowledgment number** defines the number of the next byte that the party expects to receive. In addition, the acknowledgment number is cumulative, which means that the party takes the number of the last byte that it has received, safe and sound, adds 1 to it, and announces this sum as the acknowledgment number.

Flow Control

TCP, unlike UDP, provides *flow control*. The receiver of the data controls the amount of data that are to be sent by the sender. This is done to prevent the receiver from being overwhelmed with data. The numbering system allows TCP to use a byte-oriented flow control.

Error Control

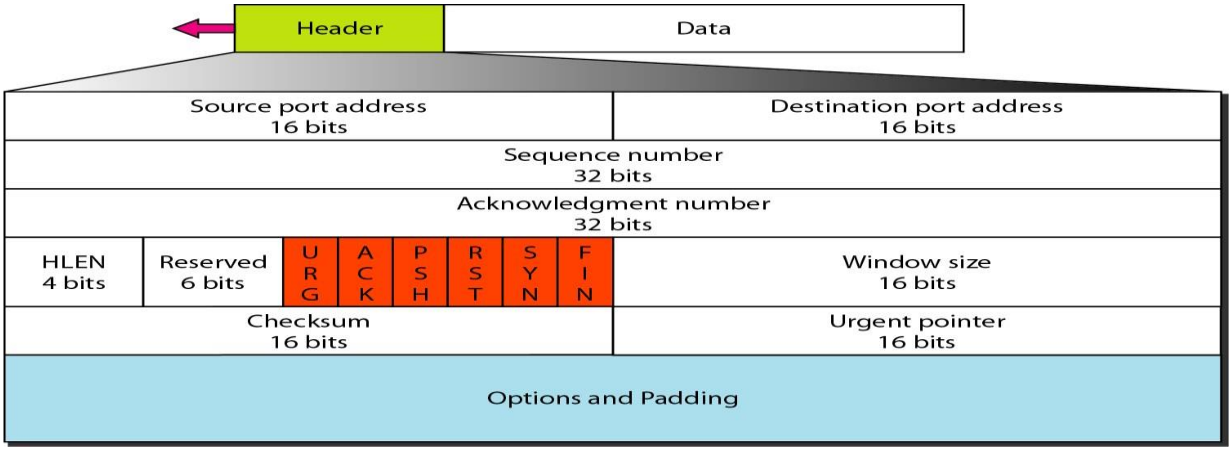
To provide reliable service, TCP implements an error control mechanism. Although error control considers a segment as the unit of data for error detection (loss or corrupted segments), error control is byte-oriented.

Congestion Control

TCP, unlike UDP, takes into account congestion in the network. The amount of data sent by a sender is not only controlled by the receiver (flow control), but is also detennined by the level of congestion in the network.

Segment

A packet in TCP is called a segment. The format of a TCP segment header is shown in figure below.



S

Source port: The source port is simply the number of the outgoing connection from the source host.

Destination port: Similarly, this is the number of the incoming connection on the destination host.

Sequence number: This is the sequence number of this packet and is incremented by the number of bytes in this packet for the next message. In other words, it counts the number of bytes transmitted rather than the number of packets.

acknowledgement number .This is the sequence number of the last byte being acknowledged. This is a piggy-backed acknowledgement. This field is the offset in the packet of the beginning of the data field

flags: This field contains several flags relating to the transfer of the packet.

Window: This field is used in conjunction with the acknowledgement number field. TCP uses a sliding window protocol with a variable window size (often depending on the amount of buffer space available. This field contains the number of bytes which the host is willing to accept from the remote host.

Checksum: This field contains a checksum of the header. It actually uses a modified form of the header which includes some of the information from the IP header to detect some unusual types of errors.

Urgent pointer: There is provision in TCP for some urgent data messages to be sent bypassing the normal sequence number system. This field is used to indicate where such data is stored in the packet.

Options: As with IP, various options may be set.

Padding: Padding is added to make the header a multiple of 32 bits long. This is only necessary when options are used.

Data: The data field is passed intact to the program which is receiving packets addressed to this port.

A TCP Connection

TCP is connection-oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All the segments belonging to a message are then sent over this virtual path. Using a single virtual pathway for the entire message facilitates the acknowledgment process as well as retransmission of damaged or lost frames. The point is that a TCP connection is virtual, not physical. TCP operates at a higher level. TCP uses the services of

IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted. If a segment arrives out of order, TCP holds it until the missing segments arrive. In TCP, connection-oriented transmission requires three phases: connection establishment, data transfer, and connection termination.

Flow Control

TCP uses a sliding window to handle flow control. The sliding window protocol used by TCP, however, is something between the *Go-Back-N* and Selective Repeat sliding window. The sliding window protocol in TCP looks like the Go-Back-N protocol because it does not use NAKs; it looks like Selective Repeat because the receiver holds the out-of-order segments until the missing ones arrive. There are two big differences between this sliding window and the one we used at the data link layer. First, the sliding window of TCP is byte-oriented; the one we discussed in the data link layer is frame-oriented. Second, the TCP's sliding window is of variable size; the one we discussed in the data link layer was of fixed size.

Figure below shows the sliding window in TCP. The window spans a portion of the buffer containing bytes received from the process. The bytes inside the window are the bytes that can be in transit; they can be sent without worrying about acknowledgment.

The imaginary window has two walls: one left and one right.

The window is *opened, closed,* or *shrunk.* These three activities are in the control of the receiver (and depend on congestion in the network), not the sender. The sender must obey the commands of the receiver in this matter.

Opening a window means moving the right wall to the right. This allows more new bytes in the buffer that are eligible for sending. Closing the window means moving the left wall to the right. This means that some bytes have been acknowledged and the sender need not worry about them anymore. Sluinking the window means moving the right wall to the left. This is strongly discouraged and not allowed in some implementations because it means revoking the eligibility of some bytes for sending. This is a problem if the sender has already sent these bytes. Note that the left wall cannot move to the left because this would revoke some of the previously sent acknowledgments. The size of the window at one end is determined by the lesser of two values: *receiver window (rwnd)* or *congestion window (cwnd).* The *receiver window* is the value advertised by the opposite end in a segment containing acknowledgment. It is the number of bytes the other end can accept before its buffer overflows and data are discarded. The congestion window is a value determined by the network to avoid congestion.

Error Control

TCP is a reliable transport layer protocol. This means that an application program that delivers a stream of data to TCP relies on TCP to deliver the entire stream to the application program on the other end in order, without error, and without any part lost or duplicated. TCP provides reliability using error control. Error control includes mechanisms for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments. Error control also includes a mechanism for correcting errors after they are detected. Error detection and correction in TCP is achieved through the use of three simple tools: checksum, acknowledgment, and time-out.

Checksum

Each segment includes a checksum field which is used to check for a corrupted segment.

If the segment is corrupted, it is discarded by the destination TCP and is considered as lost. TCP uses a 16-bit checksum that is mandatory in every segment.

Acknowledgment

TCP uses acknowledgments to confirm the receipt of data segments. Control segments that carry no data but consume a sequence number are also acknowledged. ACK segments are never acknowledged.

ACK segments do not consume sequence numbers and are not acknowledged layer, SCTP. However, it cannot be changed for TCP because this would involve reconfigurationof the entire header format.

Retransmission

The heart of the error control mechanism is the retransmission of segments. When a segment is corrupted, lost, or delayed, it is retransmitted. In modern implementations, a segment is retransmitted on two occasions: when a retransmission timer expires or when the sender receives three duplicate ACKs.

In modern implementations, a retransmission occurs if the retransmission timer expires or three duplicate ACK segments have arrived. Note that no retransmission occurs for segments that do not consume sequence numbers. In particular, there is no transmission for an ACK segment.

No retransmission timer is set for an ACK segment.

Retransmission After RTO A recent implementation of TCP maintains one retransmission time-out (RTO) timer for all outstanding (sent, but not acknowledged) segments.

When the timer matures, the earliest outstanding segment is retransmitted even though lack of a received ACK can be due to a delayed segment, a delayed ACK, or a lost acknowledgment. Note that no time-out timer is set for a segment that carries only an acknowledgment, which means that no such segment is resent. The value of RTO is dynamic in TCP and is updated based on the round-trip time (RTT) of segments. An RTI is the time needed for a segment to reach a destination and for an acknowledgment to be received.

Retransmission After Three Duplicate ACK Segments The previous rule about retransmission of a segment is sufficient if the value ofRTO is not very large. Sometimes, however, one segment is lost and the receiver receives so many out-of-order segments that they cannot be saved (limited buffer size). To alleviate this situation, most implementations today follow the three-duplicate-ACKs rule and retransmit the missing segment immediately. This feature is referred to as fast retransmission, which we will see in an example shortly.

Out-of-Order Segments

When a segment is delayed, lost, or discarded, the segments following that segment arrive out of order. Originally, TCP was designed to discard all out-of-order segments, resulting in the retransmission of the missing segment and the following segments. Most implementations today do not discard the out-of-order segments. They store them temporarily and flag them as out-of-order segments until the missing segment arrives. Note, however, that the out-of-order segments are not delivered to the process. TCP guarantees that data are delivered to the process in order.

Fast Retransmission

When the receiver receives the fourth, fifth, and sixth segments, it triggers an acknowledgment. The sender receives four acknowledgments with the same value (three duplicates). Although the timer for segment 3 has not matured yet, the fast transmission requires that segment 3, the segment that is expected by all these acknowledgments, be resent immediately.

Note that only one segment is retransmitted although four segments are not acknowledged. When the sender receives the retransmitted ACK, it knows that the four segments are safe and sound because acknowledgment is cumulative.

Connection Establishment

TCP transmits data in full-duplex mode. When two TCPs in two machines are connected, they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred.

Three-Way Handshaking

The connection establishment in TCP is called threeway handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.

The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a *passive open.* Although the server TCP is ready to accept any connection from any machine in the world, it cannot make the connection itself.

The client program issues a request for an *active open.* A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process as shown in Figure below

The three steps in this phase are as follows.

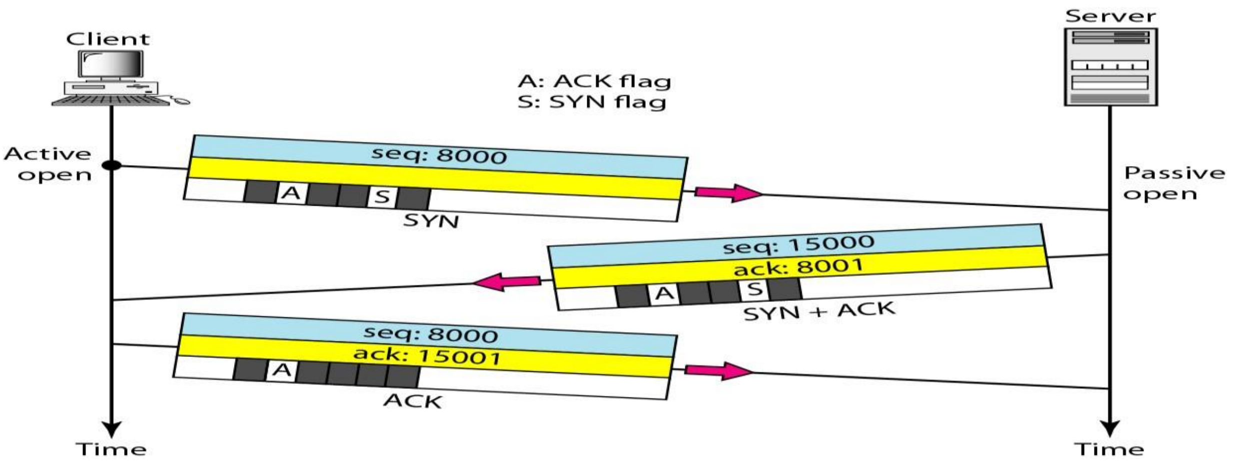
1. The client sends the first segment, a SYN segment, in which only the SYN flag is set.

This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing 1 imaginary byte. A SYN segment cannot carry data, but it consumes one sequence number.

2. The server sends the second segment, a SYN +ACK segment, with 2 flag bits set: SYN and ACK. This segment has a dual purpose. It is a SYN segment for communication in the other direction and serves as the acknowledgment for the SYN segment. It consumes one sequence number. A SYN +ACK segment cannot carry data, but does consume one sequence number.

3. The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers. An ACK segment, if carrying no data, consumes no sequence number.

Simultaneous Open A rare situation, called a simultaneous open, may occur when both processes issue an active open. In this case, both TCPs transmit a SYN + ACK segment to each other, and one single connection is established between them.



SYN Flooding Attack The connection establishment procedure in TCP is susceptible to a serious security problem called the SYN flooding attack. This happens when a malicious attacker sends a large number of SYN segments to a server, pretending that each of them is corning from a different client by faking the source IP addresses in the datagrams.

The server, assuming that the clients are issuing an active open, allocates the necessary resources, such as creating communication tables and setting timers. The TCP server then sends the SYN +ACK segments to the fake clients, which are lost. During this time, however, a lot of resources are occupied without being used. If, during this short time, the number of SYN segments is large, the server eventually runs out of resources and may crash. This SYN flooding attack belongs to a type of security attack known as a denial-of-service attack, in which an attacker monopolizes a system with so many service requests that the system collapses and denies service to every request.

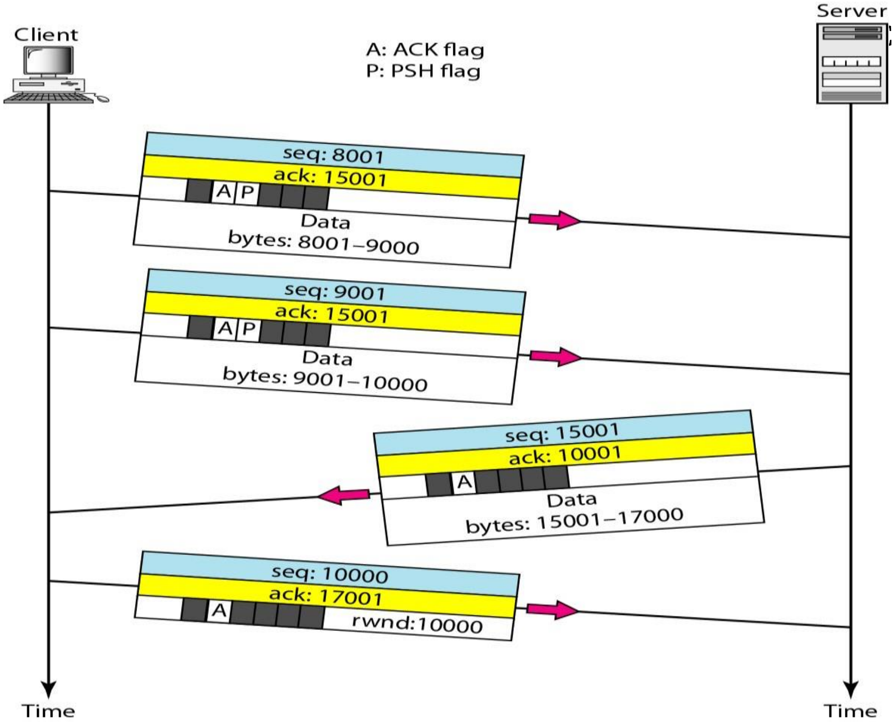
Some implementations of TCP have strategies to alleviate the effects of a SYN attack. Some have imposed a limit on connection requests during a specified period of time. Others filter out datagrams coming from unwanted source addresses. One recent strategy is to postpone resource allocation until the entire connection is set up, using what is called a cookie. SCTP, the new transport layer protocol that we discuss in the next section, uses this strategy.

Data Transfer

After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgments. We will study the rules of acknowledgment later in the chapter; for the moment, it is enough to know that data traveling in the same direction as an acknowledgment are carried on the same segment.

The acknowledgment is piggybacked with the data. Figure Shows an example. In this example, after connection is established (not shown in the figure), the client sends 2000 bytes of data in two segments. The server then sends 2000 bytes in one segment.

The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgment because there are no more data to be sent. Note the values of the sequence and acknowledgment numbers. The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received.



The segment from the server, on the other hand, does not set the push flag.

Pushing Data We saw that the sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size. The receiving TCP also buffers the data when they arrive and delivers them to the application program when the application program is ready or when it is convenient for the receiving TCP. This type of flexibility increases the efficiency of TCP.

Delayed transmission and delayed delivery of data may not be acceptable by the application program.

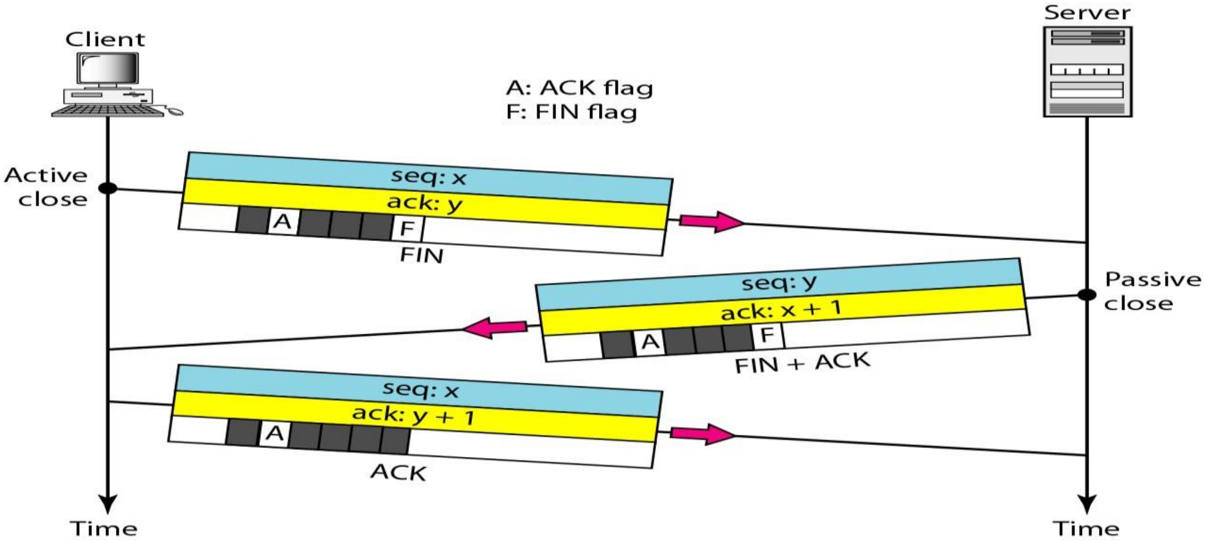
TCP can handle such a situation. The application program at the sending site can request a *push* operation. This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. The sending TCP must also set the push bit (PSH) to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come. Although the push operation can be requested by the application program, most current implementations ignore such requests. TCP can choose whether or not to use this feature.

Urgent Data

TCP is a stream-oriented protocol. This means that the data are presented from the application program to TCP as a stream of bytes. Each byte of data has a position in the stream. However, on occasion an application program needs to send *urgent* bytes. This means that the sending application program wants a piece of data to be read out of order by the receiving application program.

Connection Termination

Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option. Three-Way Handshaking Most implementations today allow *three-way handshaking* for connection termination as shown in Figure below.



1. In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set.

Note that a FIN segment can include the last chunk of data sent by the client, or itcan be just a control segment as shown in Figure below. If it is only a control segment, it consumes only one sequence number.

The FIN segment consumes one sequence number ifit does not carry data

2. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN +ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.

The FIN +ACK segment consumes one sequence number if it does not carry data.

3. The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers. In TCP, one end can stop sending data while still receiving data. This is called a half-close.

Overview of the DNS protocol operation

The Domain Name System (DNS) protocol is used primarily **to find out the IP address of a computer, given its domain or host name**. It is because of the DNS protocol, human beings are able to associate meaningful names to computers, instead of remembering the IP address of each computer.

DNS can also be used for other purposes like getting the domain name of a computer from its IP address (**reverse lookup**), getting the IP address of the mail server corresponding to a domain name (MX record parameter of a DNS message), getting the actual canonical host name of a machine, given its alias address (CNAME parameter), load balancing among a set of web servers serving the same domain etc. DNS is used by many application layer protocols like HTTP, SMTP, FTP etc. for translating domain names into IP addresses.

Basic Principle of Operation of DNS

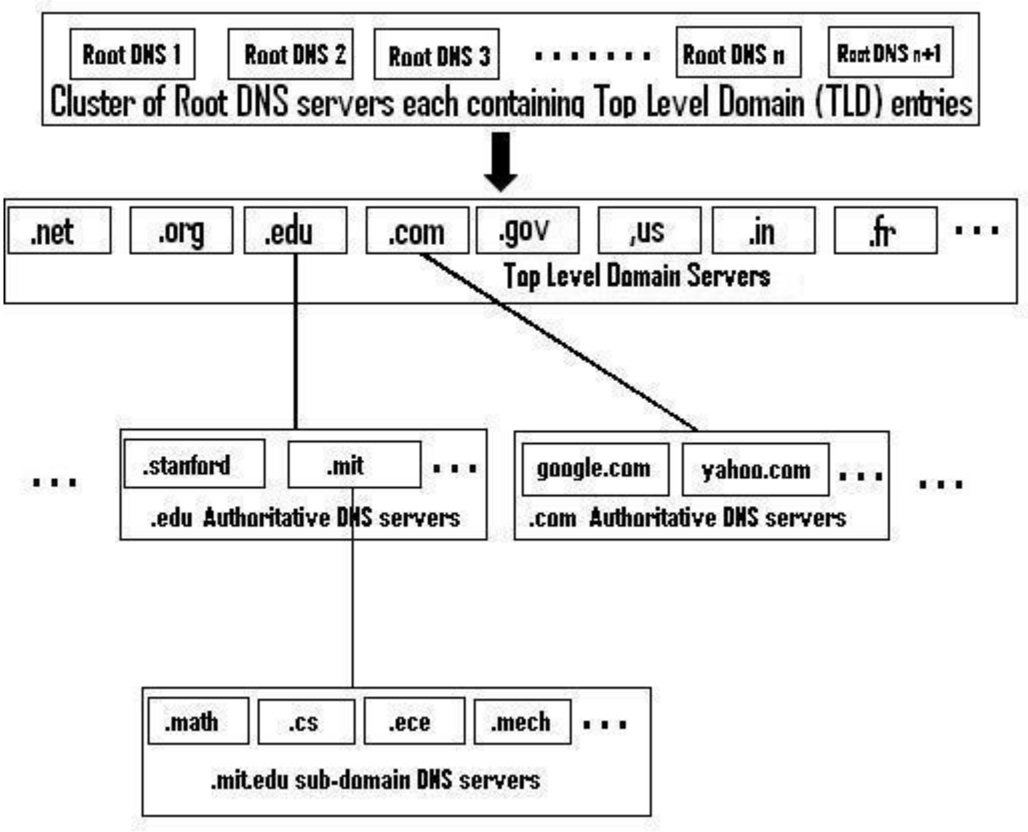
DNS is a simple, UDP based client-server application layer protocol, based on a hierarchical and distributed data base. DNS clients send DNS query messages using UDP, to remote DNS servers, to resolve hostnames into IP addresses.

Organization of DNS Servers and DNS DataBase

The DNS data base, containing the mapping of domain name to IP address, of millions of computers, is distributed across a huge number of distributed DNS servers, organized in a hierarchical fashion. The DNS server hierarchy consists primarily of four levels of servers, namely

1. **Root DNS servers**
2. **Top level Domain (TLD) servers**
3. **Authoritative DNS servers**
4. **Authoritative sub-domain DNS servers**

The DNS server hierarchy is shown in the diagram given below:



Root DNS 1
Root DNS 2
Root DNS 3
Root DNS n
Root DNS n+1
Cluster of Root DNS servers each containing Top Level Domain (TLD) entries
.net
.org
.edu
.com
.gov
.us
.in
.fr
Top Level Domain Servers
.stanford
.mit
.edu Authoritative DNS servers
google.com
yahoo.com
.com Authoritative DNS servers
.math
.cs
.ece
.mech
.mit.edu sub-domain DNS servers

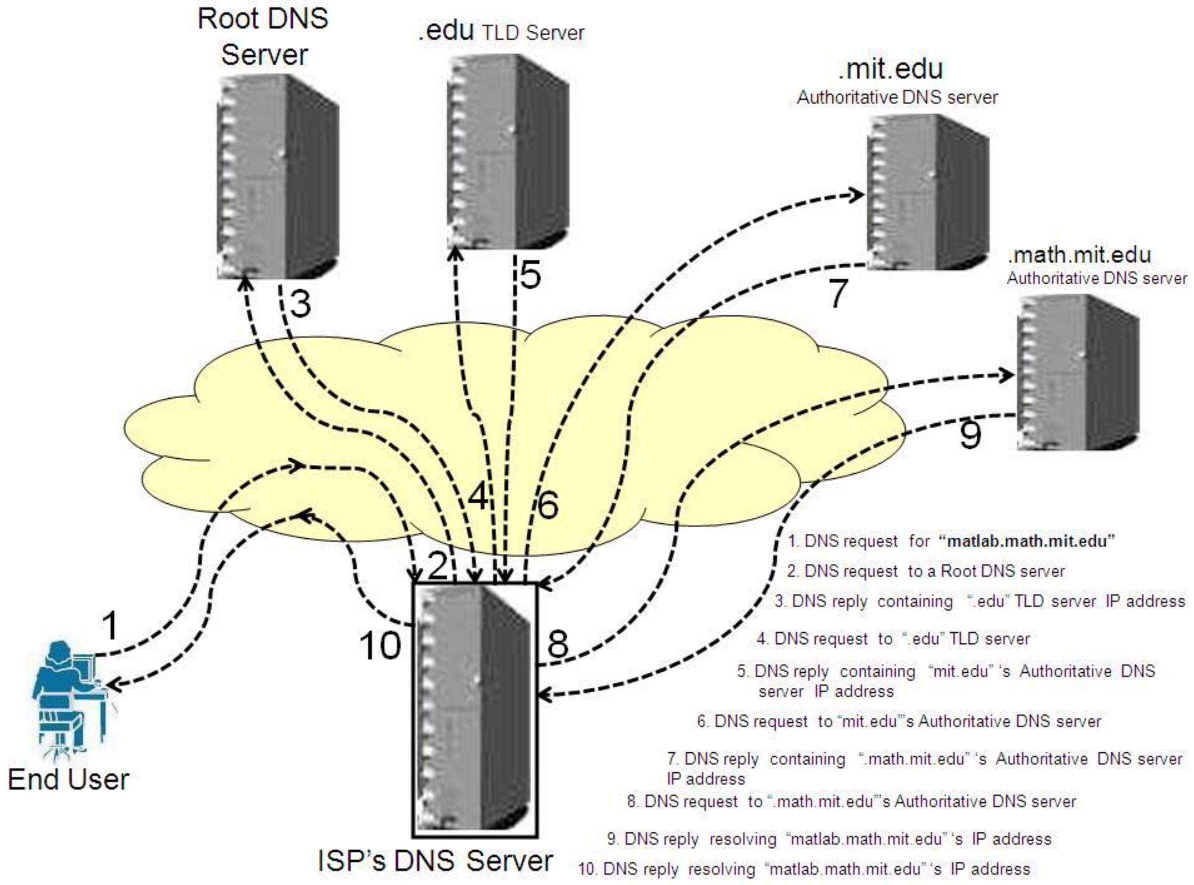
Hierarchy of DNS server and DNS databases

As shown in the diagram above,

- At the **highest** level, **Root DNS servers** contain DNS records pertaining to the DNS servers of all the TLDs like **.com, .edu, .org** etc.
- At the **second** level, TLD servers contain the DNS records of all the Authoritative DNS servers for a specific TLD. For e.g. .com TLD server contains the records of all the authoritative DNS servers of the .com domain (e.g. google.com authoritative DNS server details, yahoo.com authoritative DNS server details etc.).
- The third level in the DNS data base hierarchy consists of individual domain level **authoritative DNS servers**, that are responsible for resolving the DNS entries corresponding to a specific domain (e.g. google.com, yahoo.com, stanford.edu domains).

- The fourth level in the DNS data base hierarchy consists of sub-domain level authoritative DNS servers, that are responsible for resolving the DNS entries corresponding to specific sub-domains (e.g. cs.stanford.edu authoritative DNS server is responsible for resolving the host names of all computers belonging to the computer science department of stanford university). Also, at the sub-domain level, there can be further hierarchy and DNS protocol is flexible enough to allow any level of further hierarchy. For e.g. there could be a further sub-domain like research.cs.stanford.edu pertaining to the research wing of the computer science department of stanford university.

For reliability, load balancing and redundancy purposes, each DNS server is replicated by at least one more machine. For example, there are more than 13 Root DNS servers distributed across different geographical locations across the globe.


Root DNS Server
.edu TLD Server
.mit.edu
Authoritative DNS server
.math.mit.edu
Authoritative DNS server
End User
ISP's DNS Server
1
2
3
4
5
6
7
8
9
10
1. DNS request for "matlab.math.mit.edu"
2. DNS request to a Root DNS server
3. DNS reply containing ".edu" TLD server IP address
4. DNS request to ".edu" TLD server
5. DNS reply containing "mit.edu" 's Authoritative DNS server IP address
6. DNS request to "mit.edu"'s Authoritative DNS server
7. DNS reply containing ".math.mit.edu" 's Authoritative DNS server IP address
8. DNS request to ".math.mit.edu"'s Authoritative DNS server
9. DNS reply resolving "matlab.math.mit.edu" 's IP address
10. DNS reply resolving "matlab.math.mit.edu" 's IP address

DNS Message Exchange

When an application in the end computer wants to resolve a host name, it contacts the DNS client software in the computer to resolve the host name. The DNS client software then sends a DNS query message to its configured local DNS server (ISP's DNS server), using UDP as the underlying transport protocol. DNS servers usually wait on UDP port number 53.

If the local DNS server has the resolved entry already in its cache and if that entry is recent (not an outdated stale entry), then the local DNS server replies back with a DNS reply message, that contains the IP address corresponding to the queried host name.

If the local DNS server does not have the entry in its local cache, then it queries one of the root DNS servers. Based on the queried domain, the root DNS server sends back the IP address of the next level TLD server to the local DNS server. For e.g. if the query is for the host name google.com, then the root server returns back the IP address of the TLD server corresponding to the .com domain. The local DNS server then sends a new DNS query to the .com TLD server.

The .com TLD server then sends back the IP address of the Authoritative DNS server of google.com, to the local DNS server. The local DNS server then sends the DNS query to the Authoritative DNS server of google.com and gets the IP address of the google.com hostname resolved.

Once it get the hostname resolved, the local DNS server replies back to the DNS client with the resolved name.

An example DNS query

The figure given below illustrates the typical steps involved in resolving a hostname named “matlab.math.mit.edu”.

Sequence of steps involved in resolving the hostname matlab.math.mit.edu

As indicated in the figure, the process of resolving the hostname “research.math.mit.edu” by an end user, involves a total of 10 DNS messages, with DNS messages being sent to DNS servers distributed at different places. At each level, the query is redirected back to the corresponding domain/sub-domain server, till it finally reaches the actual DNS server responsible for resolving the complete hostname.

In the above example, the first DNS query sent by the end computer to the local DNS server is an example of a **recursive DNS query,** because the end computer requests the local DNS server to resolve the hostname on its behalf, by asking the local DNS server to recursively query other DNS servers to resolve the hostname. Rest of the DNS queries are all sent by the local DNS server and they are examples of **iterative DNS queries**, because they are all sent by the same local DNS server, one after the other. The type of the DNS query (recursive/iterative) is a parameter that can be specified in the DNS query message.

Since DNS uses the unreliable UDP as the underlying transport layer protocol, if DNS messages are lost, then it is the responsibility of the DNS protocol or applications that use the DNS protocol to retransmit DNS messages.

As for the message formats, DNS messages are based on standard TLV (Type, Length, Value), with the type specifying the different types of DNS messages like query, reply etc. and the value containing the actual IP address, CNAME, MX record etc.

NS Protocol Overview

Part of the confusion associated with the DNS protocol is that it lacks a special name. Thus DNS can refer either to the entire system, or to the protocol that makes it work. This page documents the protocol, which operates in one of two basic modes - lookups or zone transfers.

DNS Lookups

Normal resource records lookups are done with UDP. An "intelligent retransmission" is to be used, though one is not specified in the protocol, resulting in a mix of poor strategies with good ones. The protocol itself is stateless; all the information needed is contained in a single message, fully documented in RFC 1035 §4.1, and having the following format:

```
    +---------------------+
    |        Header       |
    +---------------------+
    |       Question      | the question for the name server
    +---------------------+
    |        Answer       | RRs answering the question
    +---------------------+
    |      Authority      | RRs pointing toward an authority
    +---------------------+
    |      Additional      | RRs holding additional information
    +---------------------+
```

- **Questions** are always Name, Type, Class tuples. For Internet applications, the Class is IN, the Type is a valid RR type, and the Name is a fully-qualified domain name, stored in a standard format. Names can't be wildcarded, but Types and Classes can be. In addition, special Types exist to wildcard mail records and to trigger zone transfers. The question is the only section included in a query message; the remaining sections being used for replies.
- **Answers** are RRs that match the Name, Type, Class tuple. If any of the matching records are CNAME pointers leading to other records, the target records should also be included in the answer. There may be multiple answers, since there may be multiple RRs with the same labels.
- **Authority** RRs are type NS records pointing to name servers closer to the target name in the naming hierarchy. This field is completely optional, but clients are encouraged to cache this information if further requests may be made in the same name hierarchy.
- **Additional** RRs are records that the name server believes may be useful to the client. The most common use for this field is to supply A (address) records for the name servers listed in the Authority section.

However, more clever name servers are feasible. For example, if the question is for an MX record for FreeSoft.org, the answer will currently point to mail.adnc.com. The name server can infer that the client's next request will be an A query for mail.adnc.com, which will be answered by with a CNAME record, the DNS equivalent of a symbolic link, and the target of that link, an A record for gemini.adnc.com. The name server can avoid all this extra traffic by just including the CNAME and A records as additional RRs in the original reply. Not all name servers do this, however. Use the Dig program to watch what really happens.

Zone Transfers

Sometimes, it is necessary to efficiently transfer the resource records of an entire DNS zone. This is most commonly done by a secondary name server having determined the need to update its database.

The operation of a zone transfer is almost identical to a normal DNS query, except that TCP is used (due to large quantity of reply records) and a special Class exists to trigger a zone transfer. A DNS query with Name=FreeSoft.org, Class=IN, Type=AXFR will trigger a zone transfer for FreeSoft.org. The end of a zone transfer is marked by duplicating the SOA RR that started the zone.

Zone transfers are discussed in more detail in RFC 1034 §4.3.5.

Lower-Level Transport

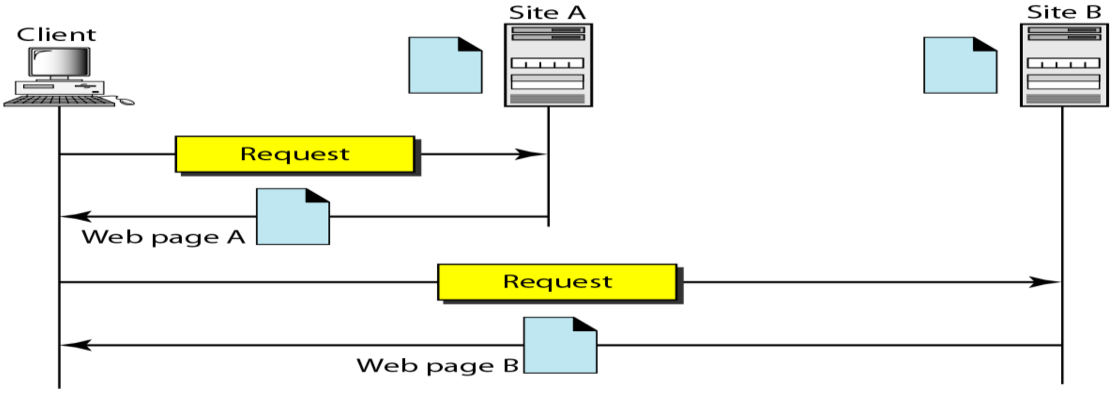
Either TCP or UDP can be used to transport DNS protocol messages, connecting to server port 53 for either. Ordinary DNS requests can be made with TCP, though convention dictates the use of UDP for normal operation. TCP *must* be used for zone transfers, however, because of the danger of dropping records with an unreliable delivery protocol such as UDP.

WWW and HTTP

The **World Wide Web** (WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet. The WWW project was initiated by CERN (European Laboratory for Particle Physics) to create a system to handle distributed resources necessary for scientific research

ARCHITECTURE

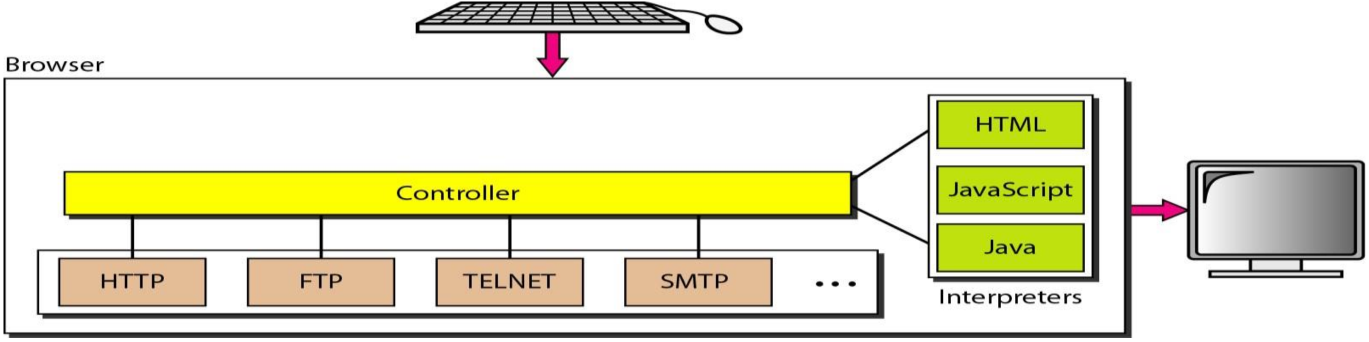
The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called *sites*, as shown in Figure



Each site holds one or more documents, referred to as *Web pages*. Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browsers.

Client (Browser)

A variety of vendors offer commercial browsers that interpret and display a Web document, and all use nearly the same architecture. Each browser usually consists of three parts: a controller, client protocol, and interpreters. The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols described previously such as FTP or HTIP. The interpreter can be HTML, Java, or JavaScript, depending on the type of document.

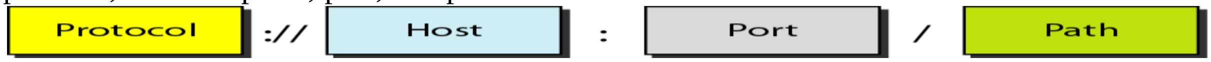


Server

The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. A server can also become more efficient through multithreading or multiprocessing.

Uniform Resource Locator

A client that wants to access a Web page needs the address. To facilitate the access of documents distributed throughout the world, HTTP uses locators. The uniform resource locator (URL) is a standard for specifying any kind of information on the Internet. The URL defines four things: protocol, host computer, port, and path.



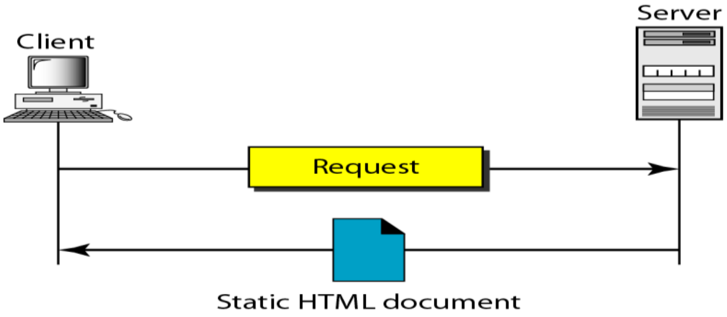
The protocol is the client/server program used to retrieve the document. Many different protocols can retrieve a document; among them are FTP or HTTP. The most common today is HTTP. The host is the computer on which the information is located The URL can optionally contain the port number of the server. If the port is included, it is inserted between the host and the path, and it is separated from the host by a colon. Path is the pathname of the file where the information is located.

WEB DOCUMENTS

The documents in the WWW can be grouped into three broad categories: static, dynamic, and active. The category is based on the time at which the contents of the document are determined.

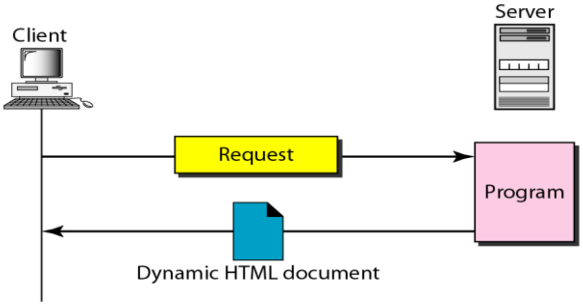
Static Documents

Static documents are fixed-content documents that are created and stored in a server. The client can get only a copy of the document. In other words, the contents of the file are determined when the file is created, not when it is used. Of course, the contents in the server can be changed, but the user cannot change them. When a client accesses the document, a copy of the document is sent. The user can then use a browsing program to display the document



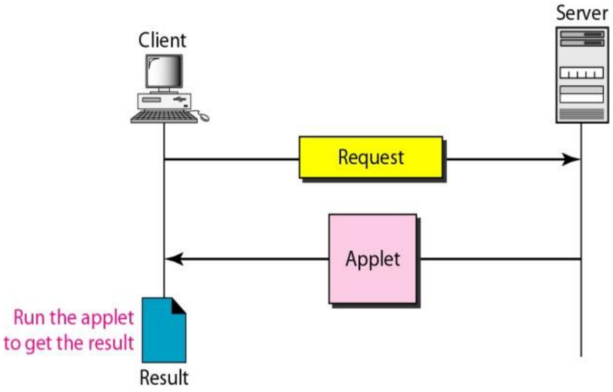
Dynamic Documents

A **dynamic document** is created by a Web server whenever a browser requests the document. When a request arrives, the Web server runs an application program or a script that creates the dynamic document. The server returns the output of the program or script as a response to the browser that requested the document. Because a fresh document is created for each request, the contents of a dynamic document can vary from one request to another.



Active Documents

For many applications, we need a program or a script to be run at the client site. These are called active documents. For example, suppose we want to run a program that creates animated graphics on the screen or a program that interacts with the user. The program definitely needs to be run at the client site where the animation or interaction takes place. When a browser requests an active document, the server sends a copy of the document or a script. The document is then run at the client (browser) site.



HTTP

The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. The contents of the requested file or other information are embedded in a response message. HTTP uses the services of TCP on well-known port 80.

HTTP Transaction

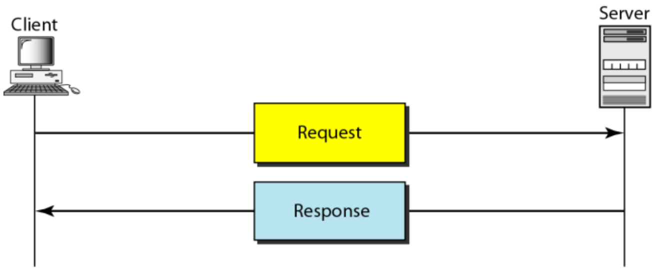
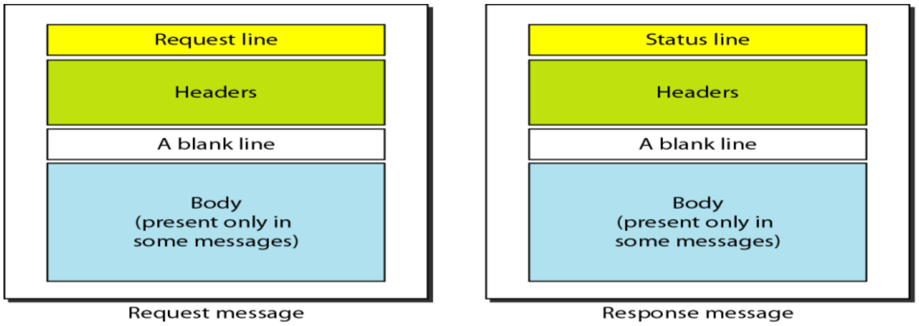


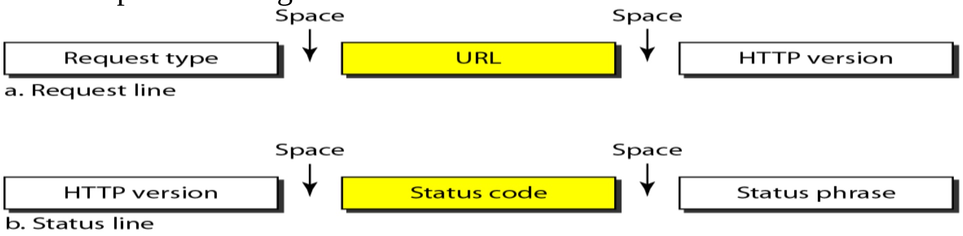
Figure illustrates the HTTP transaction between the client and server. Although HTTP uses the services of TCP, HTTP itself is a stateless protocol. The client initializes the transaction by sending a request message. The server replies by sending a response.

Messages: Request and response messages

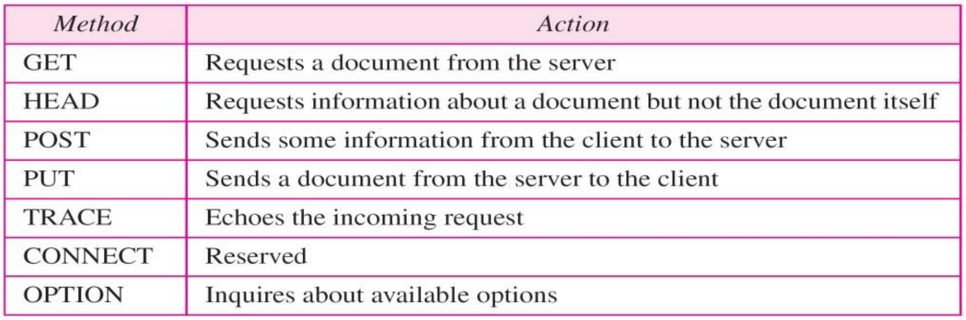
The formats of the request and response messages are similar; both are shown in Figure. A request message consists of a request line, a header, and sometimes a body. A response message consists of a status line, a header, and sometimes a body.



Request and Status Lines The first line in a request message is called a request line; the first line in the response message is called the status line. There is one common field, as shown in Figure

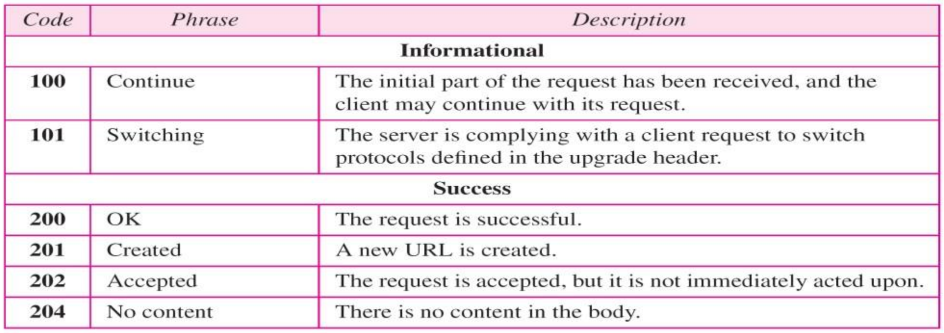


Request type. This field is used in the request message. In version 1.1 of HTTP, several request types are defined. The request type is categorized into methods as defined in Table below.

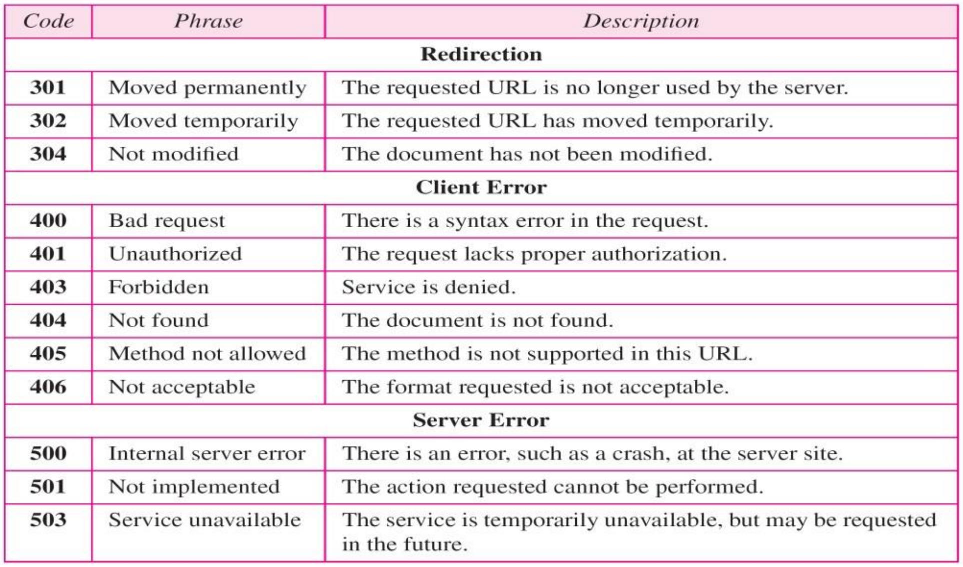


Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
OPTION	Inquires about available options

- URL. We discussed the URL earlier in the chapter.
- Version. The most current version of HTTP.
- Status code. This field is used in the response message. The status code field is similar to those in the FTP and the SMTP protocols. It consists of three digits. Whereas the codes in the 100 range are only informational, the codes in the 200 range indicate a successful request. The codes in the 300 range redirect the client to another URL, and the codes in the 400 range indicate an error at the client site. Finally, the codes in the 500 range indicate an error at the server site. We list the most common codes in Table.
- Status phrase. This field is used in the response message. It explains the status code in text form. Table also gives the status phrase.

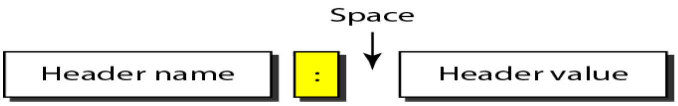


Code	*Phrase*	*Description*
	Informational	
100	Continue	The initial part of the request has been received, and the client may continue with its request.
101	Switching	The server is complying with a client request to switch protocols defined in the upgrade header.
	Success	
200	OK	The request is successful.
201	Created	A new URL is created.
202	Accepted	The request is accepted, but it is not immediately acted upon.
204	No content	There is no content in the body.

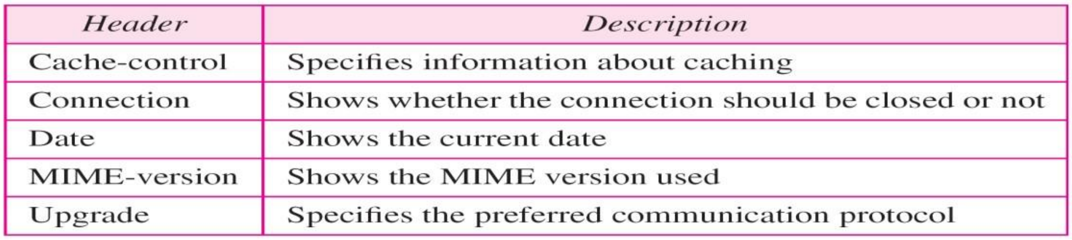


Code	*Phrase*	*Description*
	Redirection	
301	Moved permanently	The requested URL is no longer used by the server.
302	Moved temporarily	The requested URL has moved temporarily.
304	Not modified	The document has not been modified.
	Client Error	
400	Bad request	There is a syntax error in the request.
401	Unauthorized	The request lacks proper authorization.
403	Forbidden	Service is denied.
404	Not found	The document is not found.
405	Method not allowed	The method is not supported in this URL.
406	Not acceptable	The format requested is not acceptable.
	Server Error	
500	Internal server error	There is an error, such as a crash, at the server site.
501	Not implemented	The action requested cannot be performed.
503	Service unavailable	The service is temporarily unavailable, but may be requested in the future.

Header The header exchanges additional information between the client and the server. For example, the client can request that the document be sent in a special format, or the server can send extra information about the document. The header can consist of one or more header lines. Each header line has a header name, a colon, a space, and a header value. A header line belongs to one of four categories: general header, request header, response header, and entity header. A request message can contain only general, request, and entity headers. A response message, on the other hand, can contain only general, response, and entity headers.

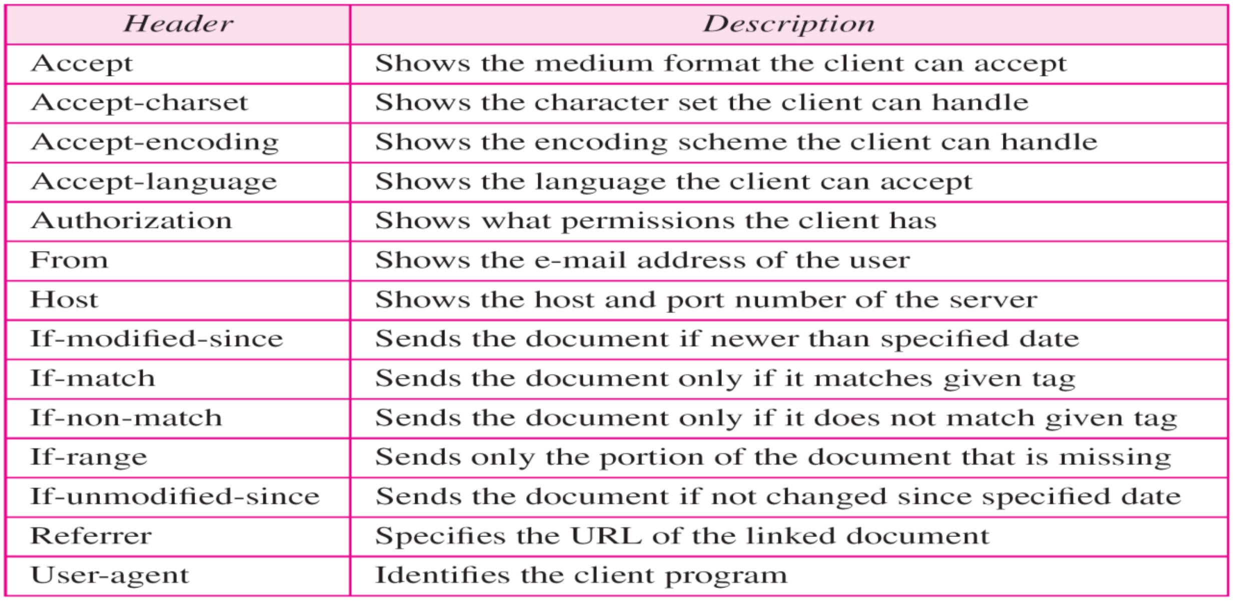


General header: The general header gives general information about the message and can be present in both a request and a response.



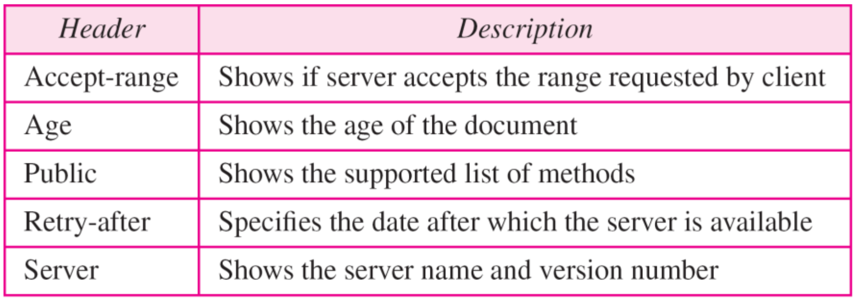
Header	*Description*
Cache-control	Specifies information about caching
Connection	Shows whether the connection should be closed or not
Date	Shows the current date
MIME-version	Shows the MIME version used
Upgrade	Specifies the preferred communication protocol

Request header: The request header can be present only in a request message. It specifies the client's configuration and the client's preferred document format



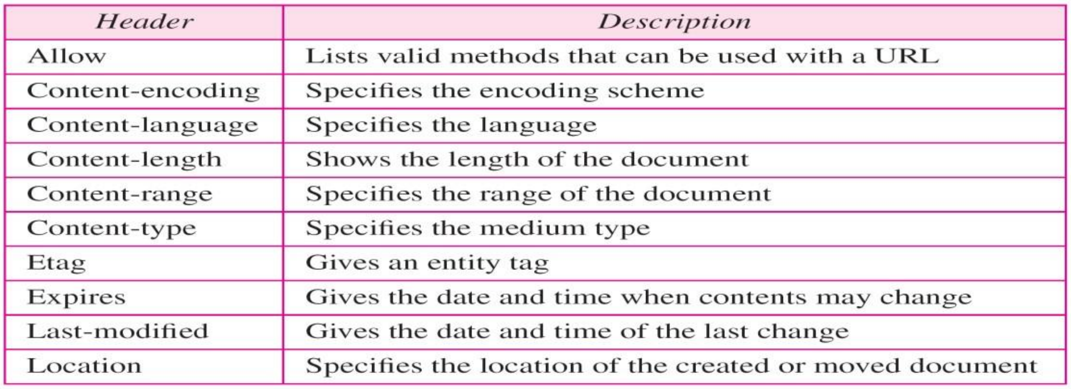
Header	*Description*
Accept	Shows the medium format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
From	Shows the e-mail address of the user
Host	Shows the host and port number of the server
If-modified-since	Sends the document if newer than specified date
If-match	Sends the document only if it matches given tag
If-non-match	Sends the document only if it does not match given tag
If-range	Sends only the portion of the document that is missing
If-unmodified-since	Sends the document if not changed since specified date
Referrer	Specifies the URL of the linked document
User-agent	Identifies the client program

Response header: The response header can be present only in a response message. It specifies the server's configuration and special information about the request.



Header	*Description*
Accept-range	Shows if server accepts the range requested by client
Age	Shows the age of the document
Public	Shows the supported list of methods
Retry-after	Specifies the date after which the server is available
Server	Shows the server name and version number

Entity header: The entity header gives information about the body of the document. Although it is mostly present in response messages, some request messages, such as POST or PUT methods, that contain a body also use this type of header.



Header	*Description*
Allow	Lists valid methods that can be used with a URL
Content-encoding	Specifies the encoding scheme
Content-language	Specifies the language
Content-length	Shows the length of the document
Content-range	Specifies the range of the document
Content-type	Specifies the medium type
Etag	Gives an entity tag
Expires	Gives the date and time when contents may change
Last-modified	Gives the date and time of the last change
Location	Specifies the location of the created or moved document

Body The body can be present in a request or response message. Usually, it contains the document to be sent or received.

Nonpersistent Connection

In a nonpersistent connection, one TCP connection is made for each request/response. The following lists the steps in this strategy:

1. The client opens a TCP connection and sends a request.
2. The server sends the response and closes the connection.
3. The client reads the data until it encounters an end-of-file marker; it then closes the connection.

In this strategy, for N different pictures in different files, the connection must be opened and closed N times. The nonpersistent strategy imposes high overhead on the server because the server needs N different buffers and requires a slow start procedure each time a connection is opened.

Persistent Connection

HTTP version 1.1 specifies a persistent connection by default. In a persistent connection, the server leaves the connection open for more requests after sending a response. The server can close the connection at the request of a client or if a time-out has been reached. The sender usually sends the length of the data with each response. However, there are some occasions when the sender does not know the length of the data. This is the case when a document is created dynamically or actively. In these cases, the server informs the client that the length is not known and closes the connection after sending the data so the client knows that the end of the data has been reached.

Proxy Server

HTTP supports proxy servers. A proxy server is a computer that keeps copies of responses to recent requests. The HTTP client sends a request to the proxy server. The proxy server checks its

cache. If the response is not stored in the cache, the proxy server sends the request to the corresponding server. Incoming responses are sent to the proxy server and stored for future requests from other clients. The proxy server reduces the load on the original server, decreases traffic, and improves latency.

QUESTION	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWER
------------------ are qualitative values that represent a flow data	data traffic	data descriptor	data traffic and data descriptor	traffic data	data descriptor
the----- define the maximum data rate of the traffic	peak data rate	maximum burst size	bandwith	effective bandwith	peak data rate
the----- define the maximum length of time the traffic is generated in the peak rate	effective bandwith	constant rate	peak data rate	maximum burst size	maximum burst size
the------- is the bandwith that the network needs to allocate for the flow of traffic	effective bandwith	peak data rate	maximum burst size	data descriptor	effective bandwith
a constant-bit-rate is also called as -------	fixed rate	nonfixed rate	definite rate	indefinte rate	fixed rate
data flow changes in time, whith the change smooth instead of sudden and sharp	constant-bit-rate	variable-bit-rate	both a & b	bit rate	variable-bit-rate
in the ---------------the data rate changes suddenly in a very short times	variable-bit-rate	constant-bit-rate	bursty data	constant-bit-rate	bursty data
congestion control is divided into--------types	1	2	3	4	2
a ------------------is mechanism that can prevent before and after it happens	open-loop	closed-loop	congestion control	Congestion avoidance	congestion control

in----------- control ,policies are applied to prevent congestion before it happens	open-loop congestion	closed-loop congestion	Congestion avoidance	congestion control	open-loop congestion
if the sender feels that a sent packets is lost ,the packet needs to -------------------	transmission	delete	retransmission	open	retransmission
the type of ---------------- at the sender may also affect congestion	closed-loop	window	control	discarding	window
the -------- policy imposed by the receiver may also effect	acknowledgment	discarding	admission	window	acknowledgment
routers may prevent congestion and the same time may not harm the integrity network	admission	window	discarding	acknowledgment	discarding
an----------- policy , which is a quality of service mechanism	acknowledgment	window	daiscarding	admission	admission
a ------------------is mechanism try to alleviate congestion after it happens	open-loop	closed-loop	congestion control	Congestion avoidance	closed-loop
to congestion control mechanism in which a congestion node stops	choke packet	control	window	backpressure	backpressure
in---------- is anodeto node congestion control that start with a node and propagates	backpressure	choke packet	none	window	backpressure
a------------ is apacket sent by anode to the source to inform it of congestion	control	choke packet	admission	backpressure	choke packet

in -----------there is no communication between the congested nodes and source	explict signaling	left side	implicit signaling	right side	implicit signaling
lack of reliablity means losing a ------------------	packet	control	data flow	admission	packet
a ----------- in a file transfer or E-mail is less important	jitter	delay	reliablity	speed	delay
a ----------- in the variation in delay for packets belonging to the same flow	jitter	reliablity	delay	speed	jitter
different application need different -------------	maximum burst size	effective bandwith	bandwith	peak data rate	bandwith
packets from different flows arrive at ------------------	scheduling	fifo	bandwith	switch	switch
a good ---------------- technique treats the different flows in apair in appropriate manner	bandwith	scheduling	admission	window	scheduling
several scheduling are designed to improve ------------	quality of service	quality of data	quality of control	quality of data flow	quality of service
wait in a buffer(queue) until the node is ready to process them	lifo	linked	fifo	circular	fifo
in --------- queuing , packets are first assigned to a priorety class	fifo	lifo	circular	priority	priority

in priority the packets in a------------ priority queue are processed first	lowest	highest	medium	topest	highest
------------ queuing, in this ,the packets are still assigned to different classes	weighted fair	priority	both a & b	fair queuing	weighted fair
the-------- is amechanism to control the amount and rate of traffic sent to the network	priority	data descriptor	traffic shaping	weighted fair	traffic shaping
the ----------------- does not credit an idle host	token bucket	leak bucket	both a & b	empty bucket	leak bucket
shapes bursty traffic into fixed-rete traffic by averaging the data rate	leak bucket	token bucket	empty bucket	bus	leak bucket
the ------- bucket allows the bursty traffic at aregulated maximum rate	empty bucket	leak bucket	token bucket	star	token bucket
combained to credit an idle host and at the same time regulate the traffic	leak bucket	token bucket	empty bucket	leak and token bucket	both a & b
____________allows us to send message include text,auido and video .	mail	internet	E-mail	WWW	E-mail
the____________client established a connection with MTA server on the system	MTA	alice	UA	system server	MTA
the first component of an electrionic mail system is the_________	alice	server	user agent	services provider	user agent

__________________is the example of user agents are mail,pine,and elm	user agent	command driven	GUI-based	E-mail	command driven
________________ define the names of aspecial files	local part	domain name	mime	local and domain	local part
the second part of address is___________	system server	internet	domain name	local part	domain name
MIME is__________________________	multiple internet mail extensions	multipurpose interface mail extensions	e internet mail exchange	e internet mail extensions	se internet mail extensions
_______ has delete and keep mode	pop	pop2	pop3	pop1	pop3
mechanism provided by TCP/IP for copying a file from one host to another	FTP	MIME	UA	pop3	FTP
____________ is the default formate for transferring text files	image	ASCII	data structure	record structure	ASCII
____________ is the default formate for transferring binary files	image	data structure	record structure	ASCII	image
in the _______________ formate, the file is a continuous stream of byte	file structure	record structure	data structure	image	file structure
the service provider is distrubuted over many location called __________	internet	sites	www	http	sites

theweb page store at the __________	hard disk	disk	client	server	server
the _________ is the computer on which the information is located	path	sites	host	cookies	host
_______________is the pathname of the file where the information is located	host	path	server	sites	path
_______________ is language for creating web pages	HTML	C	C++	java	HTML
a_____________ is created by a web server whenever a browser request the document	common gate way	dynamic document	script	static script	dynamic document
____________ is the protocol used mainly to access data on the world wide web	communicatio	network	WWW	HTTP	HTTP
a_____________ replaces one symbol with another	substitution cipher	monoalphabetic ciphet	traditional cipher	ceasar cipher	substitution cipher
a____________ reorders (permutes) symbols in a block of symbols	traditional cipher	substitution cipher	transposition cipher	monoalphabetic cipher	transposition cipher
the __________ is sometimes referred to as the caesar cipher	monoalphabetic ciphet	shift cipher	traditional cipher	transposition cipher	shift cipher
techique that emplys the morden block ciphers such as DES and AES	modes	modes of operation	operating server	OS	modes of operation

the most common public key algorithm is _______	RSA	RSSA	RSS	ARQ	RSA
data can must arrive at the receiver axactly as they were sent	integrity	message integrity	authentication	message authentication	message integrity
_________________ is the service beyond message integrity	message authentication	message integrity	integrity	authentication	message authentication
a digital signature needs a _____________ system	private-key	primary-key	public-key	secondary-key	public-key
a digital signature today provides _______________	message authentication	integrity	message integrity	authentication	message integrity
a___________________ keys between two parties is used only once	session	primary-key	private-key	public-key	session