Computer Networks

Chapter1

Introduction to Computer Network

Definition

- A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

- In information technology, a computer network, also called a data network, is a series of points, or nodes, interconnected by communication paths for the purpose of transmitting, receiving and exchanging data, voice and video traffic.

- Computer Networking is simply a group of computers that are connected to each other in some way (eg. wired (LAN), wireless or internet) for the purpose of communicating to each other.

Uses of the computer Network

- Exchange of information between different computers. (File sharing).
- Interconnected small computers in place of large computers.
- Communication tools (voice , video)
- Some applications and technologies are examples of Distributed system. (Railway reservation system, Distributed databases etc).

Advantages of Computer Network

- **It enhances communication and availability of information**

  Networking, especially with full access to the web, allows ways of communication that would simply be impossible before it was developed. Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world, which is a huge boon for businesses. Also, it allows access to a vast amount of useful information, including traditional reference materials and timely facts, such as news and current events.

- **It allows for more convenient resource sharing**

  This benefit is very important, particularly for larger companies that really need to produce huge numbers of resources to be shared to all the people. Since the technology involves computer-based work, it is assured that the resources they wanted to get across would be completely shared by connecting to a computer network which their audience is also using.

- **It makes file sharing easier**

  Computer networking allows easier accessibility for people to share their files, which greatly helps them with saving more time and effort, since they could do file sharing more accordingly and effectively.

- **It is highly flexible.**

  This technology is known to be very flexible, as it gives users the opportunity to explore everything about essential things, such as software without affecting their functionality. Plus, people will have the accessibility to all information they need to get and share.

- **It is an inexpensive system.**

  Installing networking software on your device would not cost too much, as you are assured that it lasts and can effectively share information to your peers. Also, there is no need to change the software regularly, as mostly it is not required to do so.

- **It increases cost efficiency.**

  With computer networking, you can use a lot of software products available on the market which can just be stored or installed in your system or server, and can then be used by various workstations.

- **It boosts storage capacity.**

  Since you are going to share information, files and resources to other people, you have to ensure all data and content are properly stored in the system. With this networking technology, you can do all of this without any hassle, while having all the space you need for storage.

Disadvantages of Computer Network

- **It lacks independence.**

  Computer networking involves a process that is operated using computers, so people will be relying more of computer work, instead of exerting an effort for their tasks at hand. Aside from this, they will be dependent on the main file server, which means that, if it breaks down, the system would become useless, making users idle.

- **It poses security difficulties.**

  Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.

- **It lacks robustness.**

  As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To deal with these problems, huge networks should have a powerful computer to serve as file server to make setting up and maintaining the network easier.

- **It allows for more presence of computer viruses and malware.**

  There would be instances that stored files are corrupt due to computer viruses. Thus, network administrators should conduct regular check-ups on the system, and the stored files at the same time.

- **Its light policing usage promotes negative acts.**

  It has been observed that providing users with internet connectivity has fostered undesirable behavior among them. Considering that the web is a minefield of distractions—online games, humor sites and even porn sites—workers could be tempted during their work hours. The huge network of machines could also encourage them to engage in illicit practices, such as instant messaging and file sharing, instead of working on work-related matters. While many organizations draw up certain policies on this, they have proven difficult to enforce and even engendered resentment from employees

- **It requires an efficient handler.**

  For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

- **It requires an expensive set-up.**

  Though computer networks are said to be an inexpensive system when it is already running, its initial set up cost can still be high depending on the number of computers to be connected. Expensive devices, such as routers, switches, hubs, etc., can add up to the cost. Aside from these, it would also need network interface cards (NICs) for workstations in case they are not built in.

Network Models

There are several classifications for networks

- Classification based on Scale(size)
- Classification based on Topology
- Classification based on Architecture

Based on Scale

Based on the scale (size), networks are classified into following

I. PAN (Personal Area Network)
II. LAN (Local Area Network)
III. CAN (Campus Area Network)
IV. MAN (Metropolitan Area Network)
V. DAN (Desert Area Network)
VI. CAN* (Country Area Network)
VII. WAN (Wide Area Network)
VIII. GAN (Global Area Network)

Personal Area Network (PAN)

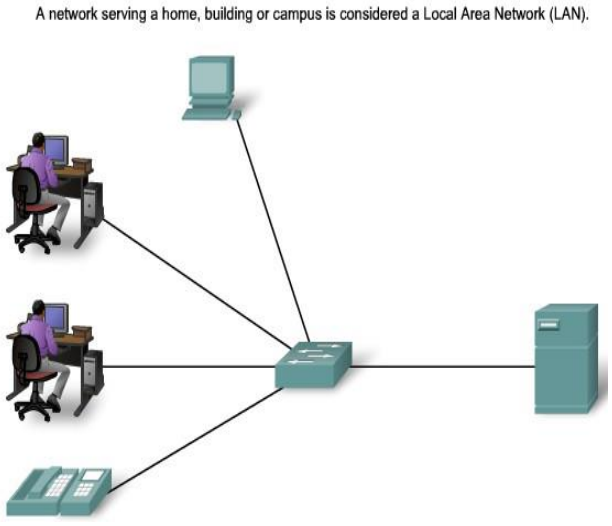
- Used for data transmission among devices such as computers, mobile phones, PDA etc.
- Within few meters like 10 meters only
- Medium : Bluetooth, Infrared
- Only very few connections will be available

Local Area Network (LAN)

The term LAN refers to a local network or a group of interconnected network that are under the same administrative control. In the early days of networking, LANS are defined as small networks that existed in a single physical location. While LANs can be a single network installed in a home or small office, the definition of LAN has evolved to include interconnected local networks consisting of many hundreds of hosts, installed in multiple buildings and locations. LANs are designed to Operate within a limited geographic area. Allow Multi-access to high bandwidth media.

LANs consist of the following components:

- Computers
- Network interface cards
- Peripheral devices
- Networking media
- Network devices

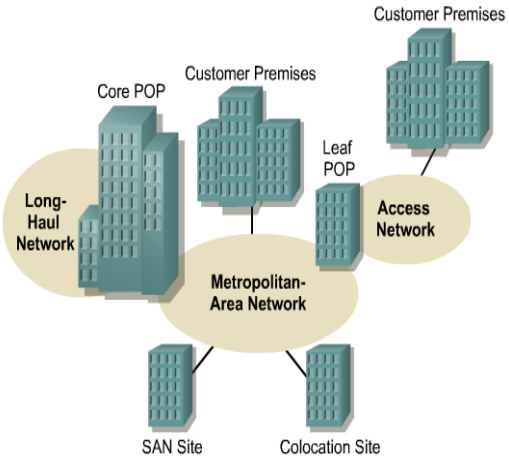

A network serving a home, building or campus is considered a Local Area Network (LAN).

LANs allow businesses to locally sharecompute make internal communications possible. A good example of this technology is email. LANs manage data, local communications, and computing equipment. Some common LAN technologies include the following:

· Ethernet
· Token Ring
· FDDI

Metropolitan Area Network (MAN)

- Metropolitan Area Network, are data networks designed for a town In terms of geographic breadth
- MANs are larger than local area networks (LANs), but smaller than wide-area networks s)
- MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media
- Generally covers towns and cities (50 kms)
- Medium: optical fibers, cables.
- Data rates adequate for distributed computing applications.



Country Area Network (CAN*)

- It's wide area network which is limited to country
- It consist of more than one MAN
- It may be extended up to thousands kms
- It is more public network owned by some public organization or governments
- Example: In Nepal NTC have CAN*

Wide Area Network (WAN)

A network that spans broader geographical area than a local area network over public communication network. WANs interconnect LANs, which then provide access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs provide instant communications across large geographic areas. Collaboration software provides access to real-time information and resources and allows meetings to be held remotely. WANs have created a new class of workers called telecommuters. These people never have to leave their homes to go to work.

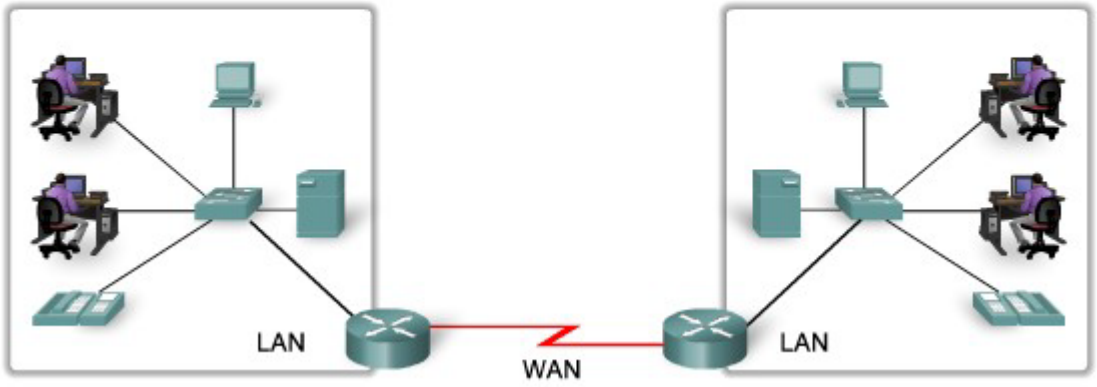
WANs are designed to do the following:

- Operate over a large and geographically separated area
- Allow users to have real-time communication capabilities with other users
- Provide full-time remote resources connected to local services
- Provide e-mail, Internet, file transfer, and e-commerce services

Some common WAN technologies include the following:

- Modems
- Integrated Services Digital Network (ISDN)
- Digital subscriber line (DSL)
- Frame Relay
- T1, E1, T3, and E3
- Synchronous Optical Network (SONET)

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



LAN	WAN
Connects host within a relatively small geographic area. • Same Building • Same room • Same Campus	Hosts may be widely dispersed. • Across Campuses • Across Cities/ Countries/ Continents
Faster	Slower
Cheaper	Expensive
Under a control of single ownership	Not under a control of a single person
Typical Speed: 10 Mbps to 10 Gbps	Typical Speed: 64 Kbps to 8 Mbps

Modes of communication:

Simplex:

The simplest signal flow technique is the simplex configuration. In Simplex transmission, one of the communicating devices can only send data, whereas the other can only receive it. Here, communication is only in one direction (unidirectional) where one party is the transmitter and the other is the receiver. Examples of simplex communication are the simple radio, and Public broadcast television where, you can receive data from stations but can't transmit data back. The television station sends out electromagnetic signals. The station does not expect and does not monitor for a return signal from the television set. This type of channel design is easy and inexpensive to set up.

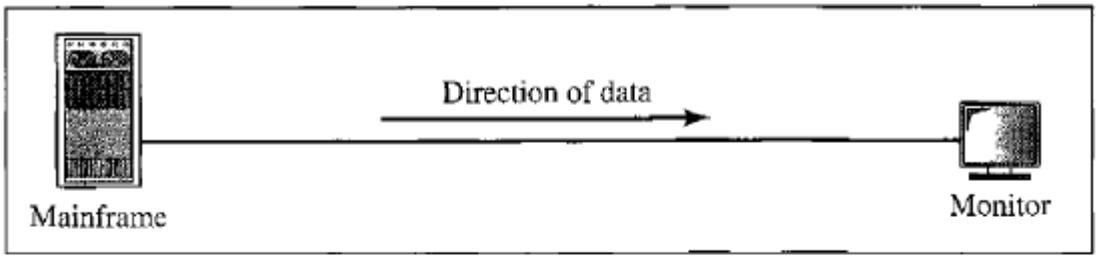
Half-Duplex

Half duplex refers to two-way communication where, only one party can transmit data at a time. Unlike, the Simplex mode here, both devices can transmit data though, not at the same time, that is Half duplex provides Simplex communication in both directions in a single channel. When one device is sending data, the other device must only receive it and vice versa. Thus, both sides take turns at sending data. This requires a definite turnaround time during which, the device changes from the receiving mode to the transmitting mode. Due to this delay, half duplex communication is slower than simplex communication. However, it is

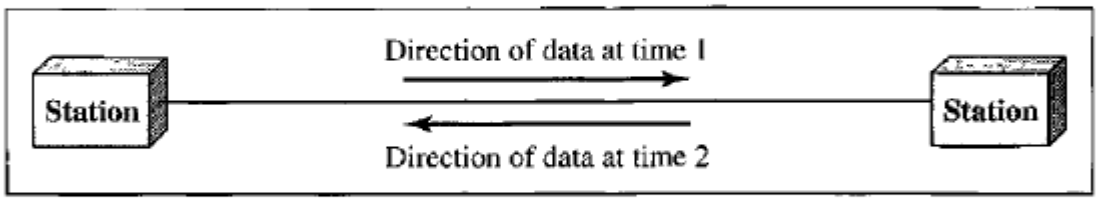
more convenient than simplex communication as both the devices can send and receive data. For example, a walkie-talkie is a half-duplex device because only one party can talk at a time.

Full Duplex

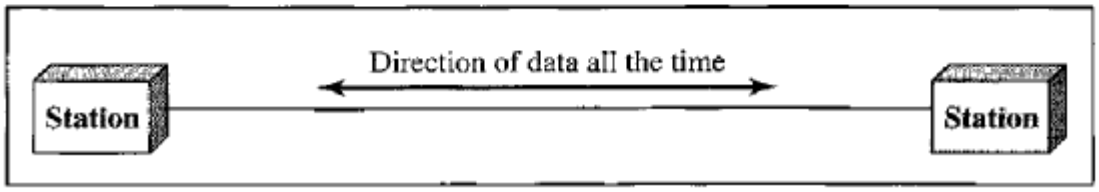
Full duplex refers to the transmission of data in two directions simultaneously. Here, both the devices are capable of sending as well as receiving data at the same time as. Sharing the same channel and moving signals in both directions increases the channel throughput without increasing its bandwidth. For example, a telephone is a full-duplex device because both parties can talk to each other simultaneously.



a. Simplex



b. Half-duplex

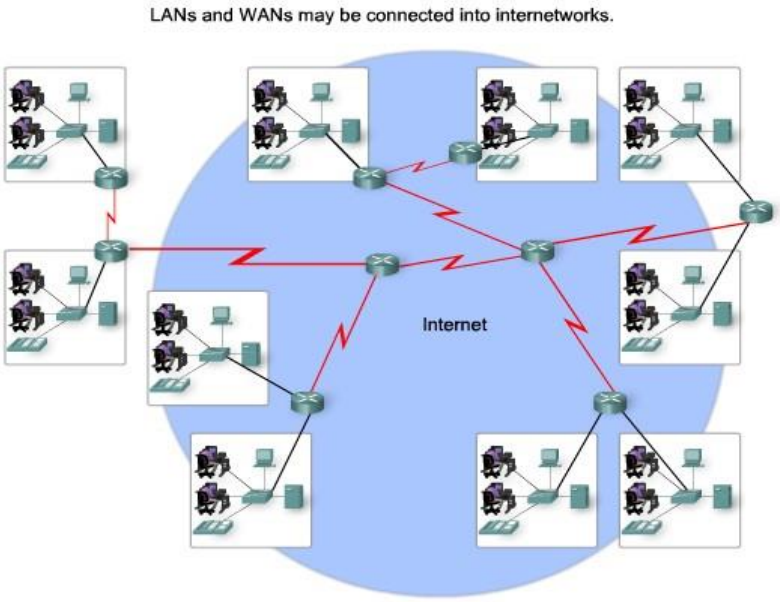


c. Full-duplex

Internet:

The network formed by the co-operative interconnection of a large number of computer networks.

- Network of Networks
- No one owns the Internet
- Every person who makes a connection owns a slice of the Internet.
- There is no central administration of the Internet.



Internet is comprises of :
A community of people: who use and develop the network.
A collection of resources: that can be reached from those networks.
A setup to facilitate collaboration: Among the members of the research and educational communities worldwide.
The connected networks use the TCP/IP protocols:

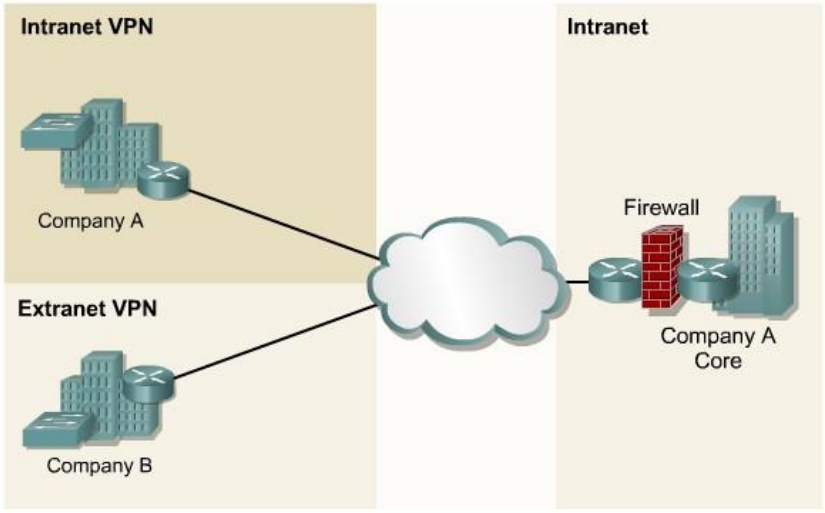
Important Internet applications:
world wide web(WWW)
File Transfer Protocol(FTP)
Electronic Mail
Internet Relay Chat

Intranet:

A private TCP/IP internetwork within an organization that uses Internet technologies such as Web servers and Web browsers for sharing information and collaborating. Intranets can be used to publish company policies and newsletters, provide sales and marketing staff with product information, provide technical support and tutorials, and just about anything else you can think of that fits within the standard Web server/Web browser environment.

Intranet Web servers differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization. Intranets are designed to

permit users who have access privileges to the internal LAN of the organization. Within an intranet, Web servers are installed in the network. Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data.



Extranet:

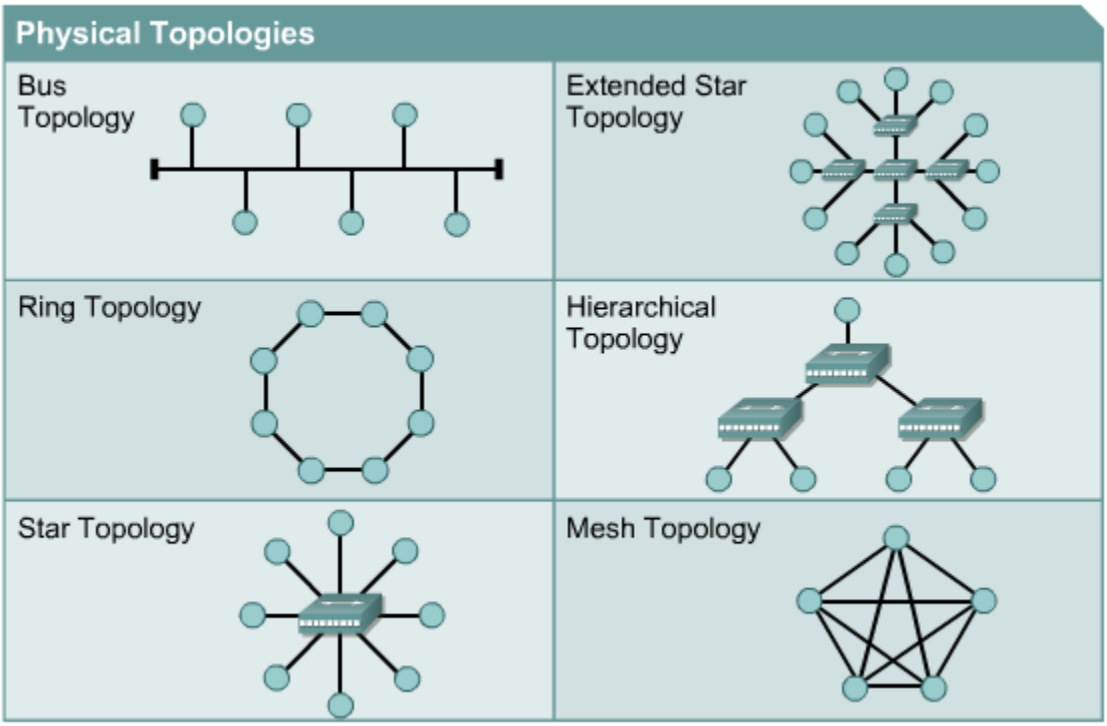
Extranets refer to applications and services that are Intranet based, and use extended, secure access to external users or enterprises. This access is usually accomplished through passwords, user IDs, and other application-level security. An extranet is the extension of two or more intranet strategies with a secure interaction between participant enterprises and their respective intranets.

Part of a Company's Intranet that is extended to users outside the company (eg Normally over the Internet). In its simplest form, a private TCP/IP network that securely shares information using Hypertext Transfer Protocol (HTTP) and other Internet protocols with business partners such as vendors, suppliers, and wholesale customers. An extranet is thus a corporate intranet that is exposed over the Internet to certain specific groups that need access to it. Extranets built in this fashion follow the client/server paradigm, with Web servers such as Apache.

Extranets are a powerful tool because they let businesses share resources on their own private networks over the Internet with suppliers, vendors, business partners, or customers. Extranets are typically used for supporting real-time supply chains, for enabling business partners to work together, or to share information such as catalogs with customers. The power of the extranet is that it leverages the existing technology of the Internet to increase the power, flexibility, and competitiveness of businesses utilizing well-known and easily used tools such as Web servers and Web browsers. Extranets also save companies money by allowing them to establish business-to-business connectivity over the Internet instead of using expensive, dedicated leased lines. Extranets can also save money by reducing phone and fax costs.

Physical Topology and Logical Topology:

Physical Topology: The term physical topology refers to the way in which a network is laid out physically. The actual layout of the wire or media. Two or more devices connect to a link; two or more links form a topology.
Logical Topology: Defines how the hosts access the media to send data. Shows the flow of data on a network.



Bus Topology:

A networking topology that connects networking components along a single cable or that uses a series of cable segments that are connected linearly. A network that uses a bus topology is referred to as a "bus network." Bus networks were the original form of Ethernet networks, using the 10Base5 cabling standard. Bus topology is used for:

- Small work-group local area networks (LANs) whose computers are connected using a thinnet cable
- Trunk cables connecting hubs or switches of departmental LANs to form a larger LAN
- Backboning, by joining switches and routers to form campus-wide networks

Advantages:

- Easy to install
- Costs are usually low
- Easy to add systems to network
- Great for small networks

Disadvantages:

- Out of date technology.
- Include difficult reconnection and fault isolation

- Can be difficult to troubleshoot.
- Unmanageable in a large network
- If cable breaks, whole network is down

Ring Topology

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

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

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

Advantages:

- Very orderly network where every device has access to the token and the opportunity to transmit.
- Performs better than a bus topology under heavy network load
- Does not require network server to manage the connectivity between the computers

Disadvantage:

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Network adapter cards and MAU's a Multistation Access Unit are much more expensive than Ethernet cards and hubs
- Much slower than an Ethernet network under normal load

Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To connect n nodes in Mesh topology, we require n(n-1)/2 duplex mode links.

Advantages:

- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

- Robust: If one link becomes unusable, it does not incapacitate the entire system.
- Advantage of privacy or security.
- point-to-point links make fault identification and fault isolation easy , Traffic can be routed to avoid links with suspected problems.

Disadvantage:

- Required high amount of cabling and the number of I/O ports.
- The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

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

Star Topology:

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

Advantages:

- Less Expensive than Mesh topology.
- In a star topology, each device needs only one link and one I/O port to connect it to any number of other devices. This factor also makes it easy to install and reconfigure.
- Less Cabling, Addition and Deletion involves only one connection between the devices and the Hub or Switch.
- Easy for Fault identification and fault isolation. If one link fails, only that link is affected. All other links remain active.

Disadvantage:

- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

An extended star topology links individual stars together by connecting the hubs or switches.

A hierarchical topology is similar to an extended star. However, instead of linking the hubs or switches together, the system is linked to a computer that controls the traffic on the topology.

Logical Topology:

The logical topology of a network determines how the hosts communicate across the medium. The two most common types of logical topologies are **broadcast** and **token passing**.

The use of a **broadcast topology** indicates that each host sends its data to all other

hosts on the network medium. There is no order that the stations must follow to use the network. It is first come, first serve. Ethernet works this way as will be explained later in the course.

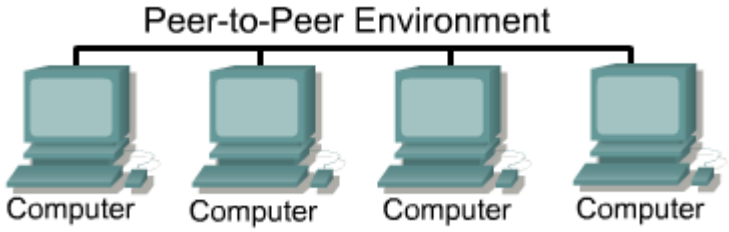
The second logical topology is **token passing**. In this type of topology, an electronic token is passed sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself. Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface(FDDI). A variation of Token Ring and FDDI is Arcnet. Arcnet is token passing on a bus topology.

Network Architecture:

Two types of Network Architecture:
I. Peer-to-Peer Model
II. Client-server Model

Peer-to-Peer Model:

In a peer-to-peer network, networked computers act as equal partners, or peers. As peers, each computer can take on the client function or the server function. Computer A may request for a file from Computer B, which then sends the file to Computer A. Computer A acts like the client and Computer B acts like the server. At a later time, Computers A and B can reverse roles.



In a peer-to-peer network, individual users control their own resources. The users may decide to share certain files with other users. The users may also require passwords before they allow others to access their resources. Since individual users make these decisions, there is no central point of control or administration in the network. In addition, individual users must back up their own systems to be able to recover from data loss in case of failures. When a computer acts as a server, the user of that machine may experience reduced performance as the machine serves the requests made by other systems.

As networks grow, peer-to-peer relationships become increasingly difficult to coordinate. A peer-to-peer network works well with ten or fewer computers. Since peer-to-peer networks do not scale well, their efficiency decreases rapidly as the number of computers on the network increases. Also, individual users control access to the resources on their computers, which means security may be difficult to maintain. The client/server model of networking can be used to overcome the limitations of the peer-to-peer network.

Peer-to-peer networks are relatively easy to install and operate. No additional equipment is necessary beyond a suitable operating system installed on each computer. Since users control their own resources, no dedicated administrators are needed.

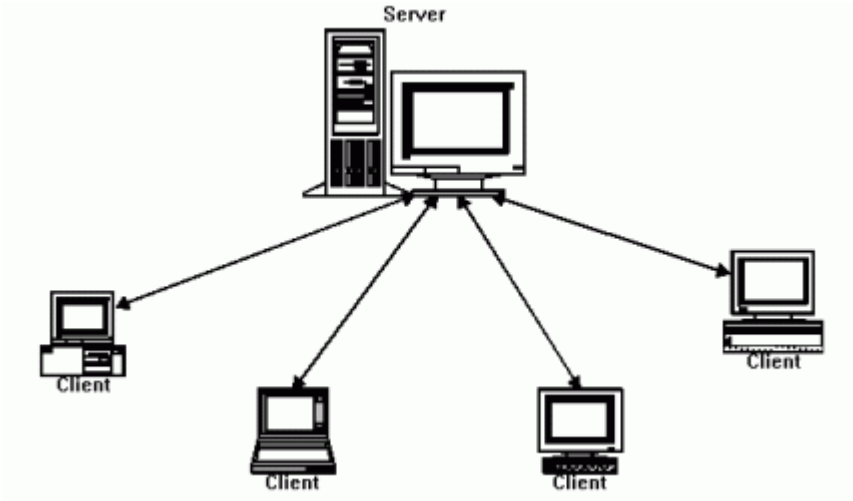
The advantages of peer-to-peer:

- No need for a network administrator.
- Network is fast/inexpensive to setup & maintain
- Each PC can make backup copies of its data to other PCs for security.
- Easiest type of network to build, peer-to-peer is perfect for both home and office use.

Client-server Model:

The term client-server refers to a popular model for computer networking that utilizes client and server devices each designed for specific purposes. The client-server model can be used on the Internet as well as local area networks (LANs). Examples of client-server systems on the Internet include Web browsers and Web servers, FTP clients and servers, and DNS.

In a client/server arrangement, network services are located on a dedicated computer called a server. The server responds to the requests of clients. The server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services. Most network operating systems adopt the form of a client/server relationship. Typically, desktop computers function as clients and one or more computers with additional processing power, memory, and specialized software function as servers.



Servers are designed to handle requests from many clients simultaneously. Before a client can access the server resources, the client must be identified and be authorized to use the resource. Each client is assigned an account name and password that is verified by an authentication service. The authentication service guards access to the network. With the centralization of user accounts, security, and access control, server-based networks simplify the administration of large networks. The concentration of network resources such as files, printers, and applications on servers also makes it easier to back-up and maintain the data. Resources can be located on specialized, dedicated servers for easier access. Most client/server systems also include ways to enhance the network with new services that extend the usefulness of the network.

The centralized functions in a client/server network has substantial advantages and some disadvantages. Although a centralized server enhances security, ease of access, and control, it introduces a single point of failure into the network. Without an operational server, the

network cannot function at all. Servers require a trained, expert staff member to administer and maintain. Server systems also require additional hardware and specialized software that add to the cost.

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfill the request. Although programs within a single computer can use the client/server idea, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank. That program might in turn forward the request to its own client program that sends a request to a database server at another bank computer to retrieve your account balance. The balance is returned back to the bank data client, which in turn serves it back to the client in your personal computer, which displays the information for you.

Advantages: Flexibility of the system, scalability, cost saving, centralized control and implementation of business rules, increase of developers productivity, portability, improved network and resource utilization.

Client-server Vs Peer-to-Peer Network:

Advantages of a Peer-to-Peer Network	Advantages of a client-server Network
Less Expensive to implementation	Provides of better security
Does not require additional specialized network administration software.	Easier to administer when the network is large because administration is centralized
Does not require a dedicated network administrator.	All date can be backed up on one central location.
Disadvantages of a Peer-to-Peer Network	Disadvantage of a Client-server Network
Does not scale well to large network and administration become unmanageable.	Requires expensive, specialized network administrative and operational software.
Less Secure	Requires a professional administrator.
All machine sharing the resources negatively impact the performance.	a single point of failure. User data is unavailable if the server is down.
Each user must be trained to perform administrative tasks.	Requires more expensive, more powerful hardware for the server machine.

Chapter 2:
Reference Model

Network Software

Network Software is a set of primitives that define the protocol between two machines. The network software resolves an ambiguity among different types of network making it possible for all the machines in the network to connect and communicate with one another and share information.

Network Software is the information, data or programming used to make it possible for computers to communicate or connect to one another.

Network software is used to efficiently share information among computers. It encloses the information to be sent in a "package" that contains a "header" and a "trailer". The header and trailer contain information for the receiving computer, such as the address of that computer and how the information package is coded. Information is transferred between computers as either electrical signals in electric wires, as light signals in fiber-optic cables, or as electromagnetic waves through space.

Protocols

A protocol is used for communication between entities in different systems. The terms 'entity' and 'system' are used in a very general sense. Examples of entities are user application programs, file transfer package, database management systems, electronic mail facilities, and terminals. Examples of systems are computers, terminals, and remote sensors. Note that in some cases the entity and the system in which it resides are coextensive (*e.g.* terminal).

In general, an entity is anything capable of sending or receiving information, and a system is physically distinct object that contains one or more entities. For two entities to communicate successfully, they must 'speak the same language'. What is communicated? How it is communicated and when it is communicated? Must conform to some mutually acceptable conventions between the entities involved. The conventions are referred to as a protocol.

Protocol may be defined as a set of rules governing the exchange of data between two entities. It also may be conceived as a set of agreement between two communicating processes. The key elements of protocol are:

- **Syntax:** Includes such things as data format and signal levels.
- **Semantics:** Includes control information for co-ordination and error handling.
- **Timing:** Includes speed matching and sequencing, create new paragraph.

Functions of protocols

Some of the numerous functions served by network protocol are as follows:

- Orderly exchange of data messages.
- Management of priorities at both the network entry and transmission levels within the network.
- Process synchronization.
- Session establishment between network users
- Session termination between network users.

- Means for protocol validation.
- Routing establishment and assignment of message routes and routing information.
- Flow control and congestion prevention.
- Sequencing—sequenced transmission and delivery of messages.
- Addressing of network components and users.
- Efficient network resources utilization.
- Resource management, monitoring and protection.
- Layered transparency between networks users and nodes.
- Reliable message transmission, including error, control and recovery.
- Testing of network resources, such as links and routes.
- Security and privacy.
- Optional packet switching through message segmenting and pipelining.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufactures and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communication. Data communication standards fall into two categories: by fact and by law.

Layered Approach

Some of the key design issues that occur in computer networking are present in several layers.

I. Every layer needs a mechanism for identifying senders and receivers. Since network normally has many computers, some of which have multiple processors means is needed for a process on one machine to specify with whom it wants to talk. As a consequence having multiple destinations, some form of addressing is needed in order to specify a Specific destination.

II. Another set of design decision concerns the rules for data transfer, such as. Simplex, Half duplex, Full duplex.

III. Error control is an important issue because physical communication circuits are not perfect. Many error-detecting and error-correcting codes are known, but both ends of the connection must agree on which one is being used. Also the receiver must have some way of telling the sender which messages have been correctly received and which has not.

IV. Not all communication channels preserve the order of messages sent on them. To deal with a possible loss of sequencing the protocol must make explicit provision for the receiver to allow the pieces to be put back together properly.

V. An issue that occurs at every level is how to keep a fast sender from swamping a slow receiver with data.

VI. Another problem that must be solved at several levels is the inability of all processes to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting and then reassembling messages.

When there are multiple paths between source and destination, a route must be chosen sometimes this decision must be split over two or more layers.

Services

Layers offer two types of services.

I. **Connection Oriented Service**

This is modeled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk and then hang up. Similarly, to use a connection oriented network services, the services user first establishes a connection, uses the connection and then releases the connection. The essential aspect of connection is that it acts like a tube. The sender pushes objects (bits) in at one end and the receiver takes them out in the same order at the other end.

Connection oriented services are of following:

- Reliable message stream service.
  e.g. sequence of pages.
- Reliable byte stream.
  e.g. remote login.
- Unreliable connection.
  e.g. Digitized voice.

II. **Connectionless Services**

This is modeled after the postal system. Each message carries the full destination address and each one is routed through the system independent of all the (users) others. Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive. However, it is possible that the first one sent, can be delayed so that the second one arrives first. With connection oriented service this is impossible.

Connectionless services are of the following:

- Unreliable datagram.
  e.g. Electronic junk mail.
- Acknowledged datagram.
  e.g. Registered mail.
- Request reply service.
  e.g. Database query.

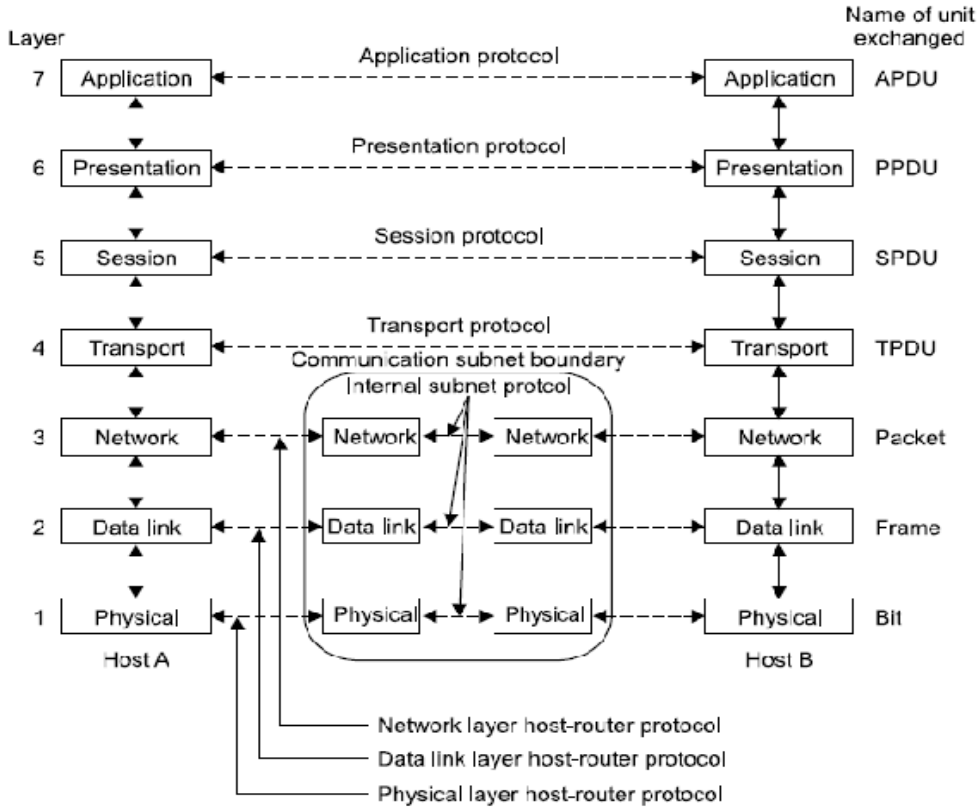
The OSI Reference Model

The OSI model is shown in the figure. This model is based on a proposal developed by the **International Standards Organization (ISO)** as a first step towards international standardization of the protocols used in the various layers, (Day & Zimmerman, 1983). The model is called the **ISO OSI (Open Systems Interconnection)** Reference Model because it deals with connecting open systems, *i.e.*, the systems that are open for communication with other systems.

The OSI Model has seven layers. The **principles that were** applied to arrive at the seven layers are as follows.

I. A layer should be created where a different level of abstraction is needed.
II. Each layer should perform a well defined function.
III. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
IV. The layer boundaries should be chosen to minimize the information flow across the interfaces.

V. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become widely.



Benefits of OSI Model:

- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

1. Physical Layer:

Physical layer is the bottom layer of the OSI reference model. The physical layer has four important characteristics.

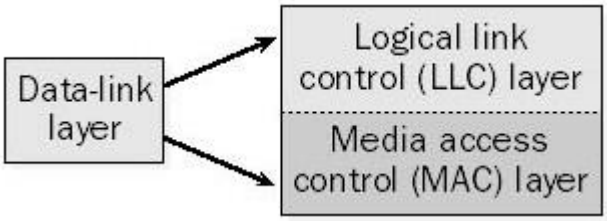
Mechanical: Relates to the physical properties of the interface to a transmission medium. Typically, the specification is of a pluggable connector that joins one or more signal conductors, called circuits.

Electrical: Relates to the representation of bits (e.g., in terms of voltage levels) and the data transmission rate of bits. It defines the voltage, current, modulation, bit synchronization, connection activation and deactivation, and various electrical characteristics for the transmission media (such as unshielded or shielded twisted-pair cabling, coaxial cabling, and fiber-optic cabling).

Functional: Specifies the functions performed by individual circuits of the physical interface between a system and the transmission medium.
Procedural: Specifies the sequence of events by which bit streams are exchanged across the physical medium.

2. Data Link Layer:

The physical layer provides only a raw bit-stream service, the data link layer attempts to make the physical link reliable while providing the means to activate, maintain, and deactivate the link . For LANs, the Project 802 standards of the Institute of Electrical and Electronics Engineers (IEEE) separate the data-link layer into two sub layers:



- The logical link control (LLC) layer, the upper of the two layers, which is responsible for flow control, error correction, and resequencing functions for connection-oriented communication, but which also supports connectionless communication
- The media access control (MAC) layer, the lower of the two layers, which is responsible for providing a method for stations to gain access to the medium

Functions:

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

Examples of data-link protocols for local area networking include the following:

- IEEE 802.3, which provides the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method for baseband Ethernet networks

- IEEE 802.5, which provides the token-passing access method for baseband token ring implementations

For WANs, data-link layer protocols encapsulate LAN traffic into frames suitable for transmission over WAN links. Common data-link encapsulation methods for WAN transmission include the following:

- Point-to-point technologies such as Point-to-Point Protocol (PPP) and High-level Data Link Control (HDLC) protocol
- Multipoint technologies such as frame relay, Asynchronous Transfer Mode (ATM), Switched Multimegabit Data Services (SMDS), and X.25

3. Network Layer:

The network layer is responsible for functions such as the following:

- Logical addressing and routing of packets over the network
- Establishing and releasing connections and paths between two nodes on a network
- Transferring data, generating and confirming receipts, and resetting connections

The network layer also supplies connectionless and connection-oriented services to the transport layer above it. The network layer functions closely with the physical layer (layer 1) and data-link layer (layer 2) in most real-world network protocol implementations.

On TCP/IP-based networks, IP addresses and network numbers are used at the network layer, and IP routers perform their routing functions at this layer. An example of an OSI model network layer protocol is the X.25 packet-switching network layer protocol, which is built on the X.21 physical layer protocol.

4. Transport Layer:

The transport layer is responsible for providing reliable transport services to the upper-layer protocols. These services include the following:

- Flow control to ensure that the transmitting device does not send more data than the receiving device can handle. Packet sequencing for segmentation of data packets and remote reassembly.
- Error handling and acknowledgments to ensure that data is retransmitted when required.
- Multiplexing for combining data from several sources for transmission over one data path.
- Virtual circuits for establishing sessions between communicating stations.

The Transmission Control Protocol (TCP) of the TCP/IP protocol suite resides at the transport layer

The connection between two devices that acts as though it's a direct connection even though it may physically be circuitous. The term is used most frequently to describe connections between two hosts in a packet-switching network. In this case, the two hosts can communicate as though they have a dedicated connection even though the packets might actually travel very different routes before arriving at their destination. An X.25 connection is an example of a virtual circuit. Virtual circuits can be either permanent (called PVCs) or temporary (called SVCs).

5. Session Layer:

Layer 5 of the Open Systems Interconnection (OSI) reference model, which enables sessions between computers on a network to be established and terminated. The session layer does not concern itself with issues such as the reliability and efficiency of data transfer between stations because these functions are provided by the first four layers of the OSI reference model.

Functions:

Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half- duplex (one way at a time) or full-duplex (two ways at a time) mode.
Synchronization: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

6. Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems .
Specific responsibilities of the presentation layer include the following:

Translation: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption: To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7. Application layer:

Layer 7 of the Open Systems Interconnection (OSI) reference model, in which network-aware, user-controlled software is implemented—for example, e-mail, file transfer utilities, and terminal access. The application layer represents the window between the user and the network. Examples of protocols that run at the application layer include File

Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), telnet, and similar protocols that can be implemented as utilities the user can interface with.

File transfer, access, and management: This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
Mail services: This application provides the basis for e-mail forwarding and storage.
Directory services: This application provides distributed database sources and access for global information about various objects and services.

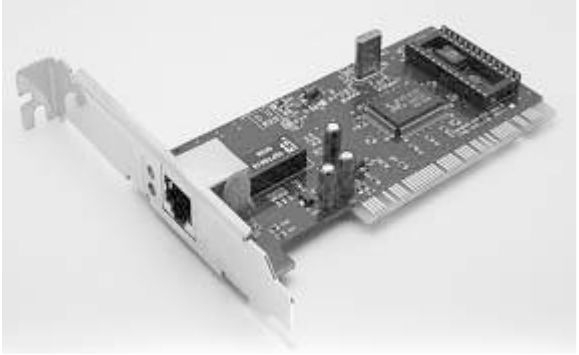
Comparison between OSI model and TCP/IP model

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical mode
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard
Protocols are not strictly defined	Stricter boundaries for the protocols

Networking Hardware:

NIC (Network Interface Card)

A NIC is a hardware board or card that you put into an empty slot in the back of your client computer or server. NIC is the interface between the PC and the physical network connection. This card physically connects to the cable that links network.



In addition to providing the physical connection to the networks, they also perform the following:

- **Prepare data**
  NIC prepare data so that it can transmit through the cable. The card translates data bit back and forth as they go from the computer to the cable and back again.
- **Address data**
  Each NIC has its own unique address that it imparts to the data stream. The card provides the data with an identifier. When it goes out on to the net and enables data seeking a particular computer to know where to exit the cable.
- **Control data flow**
  The card has RAM on it to help it, place the data so that it doesn't overwhelm the receiving computer on the cable.
- **Make (and agree on) the connection to another computer**
  Before it actually sends data, the NIC an electronic dialog with the other PC on the network that wants to communicate. They agree on thing like the maximum size of data groups to be sent. The total maximum size of data (amount), the time interval between data checks the amount of time that will elapse before confirmation that the data has arrived successfully and how much data each card hold before it overflows. NIC is an especially useful place to implement IP sec. technology. This is the place where end station data is turned into useful security management information where data can be queued in order of priority before transport and where hardware acceleration can be used to the greatest advantage to help facilitate encryption. An encrypted audio/video stream from a server to its clients provides a good example of the benefits of hardware acceleration. Users would experience much better network performance, if the stream were decrypted on an IP. (see enabled NIC). Instead of via decryption software only hardware acceleration in the NIC can help to improve network performance by accelerating the many math cycle required by encryption and decryption algorithms by offloading the process onto a NIC problems are avoided. Data transfers between the interfaces or nodes takes using this hardware address.

Hub

Hub is a basic networking component used in traditional 10-Mbps Ethernet networks to connect network stations to form a local area network (LAN). Hubs can be used for

- Connecting about a dozen computers to form a work-group or departmental LAN
- Connecting other hubs in a cascaded star topology to form a larger LAN of up to roughly a hundred computers

How It Works

Hubs are the foundation of traditional 10BaseT Ethernet networks. The hub receives signals from each station and repeats the signals to all other stations connected to the hub. In active hubs (which all of today's hubs are), the signal received from one port is regenerated (amplified) and retransmitted to the other ports on the hub. Hubs thus perform the function of a repeater and are sometimes called multiport repeaters. From a logical cabling point of view, stations wired into a hub form a star topology.

Hubs generally have RJ-45 ports for unshielded twisted-pair (UTP) cabling, and they range in size from 4 to 24 or more ports for connecting stations to the hub, plus one or more uplink ports for connecting the hub to other hubs in a cascaded star topology. Hubs generally have various light-emitting diode (LED) indicator lights to indicate the status of each port, link status, collisions, and so on. Hubs with several different types of LAN connectors such as RJ-45, BNC, and AUI are commonly called combo hubs.

Repeater

Networking components that extend a network by boosting the signal so that it can travel farther along the cabling.

How It Works

Digital signals traveling on cables weaken with distance—a phenomenon known as attenuation. A repeater is a form of digital amplifier that works at the physical layer (layer 1) of the Open Systems Interconnection (OSI) reference model for networking to regenerate (amplify) the signal so that it can travel farther. Repeaters also perform other functions such as filtering out noise caused by electromagnetic interference (EMI), reshaping the signal, and correcting timing to remove signal jitter so that the signal can travel farther. Repeaters can also be used to join dissimilar media such as unshielded twisted-pair (UTP) cabling and thinnet, but they cannot be used to join dissimilar network architectures such as Ethernet and Token Ring. Repeaters are an inexpensive way to extend a network.

Repeaters can be used in Ethernet and Token Ring local area networks (LANs) to extend signal transmission to remote nodes and over long fiber-optic cabling runs to connect LANs. Repeaters can also be used in mainframe environments for boosting signals for serial transmission to remote terminals.

Other uses for repeaters include the following:

- Joining two 16-Mbps Token Ring networks in different buildings over distances up to 3000 meters over multimode fiber-optic cabling or up to 20 kilometers over single-mode fiber
- Increasing the lobe length between a Token Ring main ring and a remote node
- Joining dissimilar 10Base2 and 10Base5 segments to form a single Ethernet LAN
- Boosting signals from mainframe controllers to 3270 terminals over coaxial or UTP cabling to support distances up to 2500 meters
- Extending the operating distance of T1 lines by placing G.703 repeaters at 2.2-kilometer intervals
- Extending backbone fiber-optic cable runs in campus wide LANs or metropolitan area networks (MANs)

Repeaters are also used in fiber-optic networks to amplify and regenerate light signals for long-distance cable runs. Repeaters come in various types for different network architectures and data communication technologies.

Bridge:

A networking component used either to extend or to segment networks. Bridges work at the OSI data-link layer. They can be used both to join dissimilar media such as unshielded twisted-pair (UTP) cabling and fiber-optic cabling, and to join different network architectures such as Token Ring and Ethernet. Bridges regenerate signals but do not perform any protocol conversion, so the same networking protocol (such as TCP/IP) must be running on both network segments connected to the bridge. Bridges can also support Simple Network Management Protocol (SNMP), and they can have other diagnostic features.

How it works?

Bridges operate by sensing the source MAC addresses of the transmitting nodes on the network and automatically building an internal routing table. This table is used to determine which connected segment to route packets to, and it provides the filtering capability that bridges are known for. If the bridge knows which segment a packet is intended for, it forwards the packet directly to that segment. If the bridge doesn't recognize the packet's

destination address, it forwards the packet to all connected segments except the one it originated on. And if the destination address is in the same segment as the source address, the bridge drops the packet. Bridges also forward broadcast packets to all segments except the originating one.

Switch:

Switch is essentially a multi-port bridge. Switches allow the segmentation of the LAN into separate collision domains. Each port of the switch represents a separate collision domain and provides the full media bandwidth to the node or nodes connected on that port. With fewer nodes in each collision domain, there is an increase in the average bandwidth available to each node, and collisions are reduced.

Why Switches:

In a LAN where all nodes are connected directly to the switch, the throughput of the network increases dramatically. The three primary reasons for this increase are:

- Dedicated bandwidth to each port
- Collision-free environment
- Full-duplex operation

Routers

Routers are internetwork connectivity devices. An internetwork may consists of two ormore physical connected independent network. These networks can be of different type. For example, they can be Ethernet and Token ring network. Each network is logically separate and is assigned an address. Routers can use network address to assists efficient delivery of message. Delivering packets according to logical network address is called routing. Routers perform routing. Routing is the process of finding a path from a source to every destination in the network. Routers are intelligent. They can use algorithms to determine most efficient path for sending a packet to any given network. Routers can also be used to divide large busy LANs into smaller segments. The protocols like IP, IPX and DDP are used to support routing functions. Routers are also employed to connect LAN to wide area network (WAN).

Routers are of two types.

1. *Static routers:* Static routers do not determine paths, but need to specify them.
2. *Dynamic routers:* Dynamic routers have capacity to determine routes.

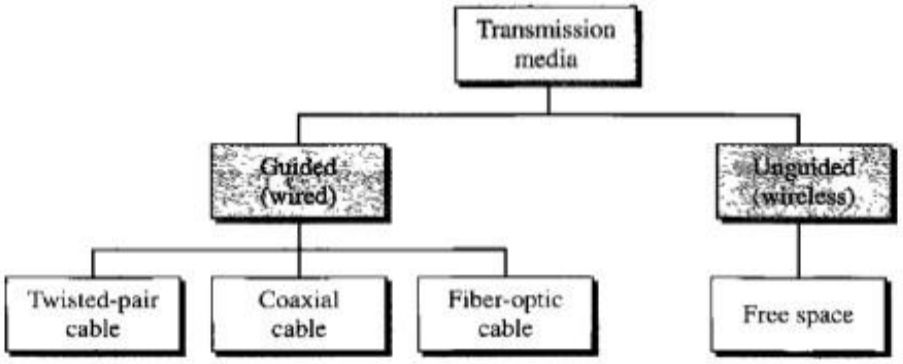
Chapter 3

Physical layer

Transmission Medium:

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane.

In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

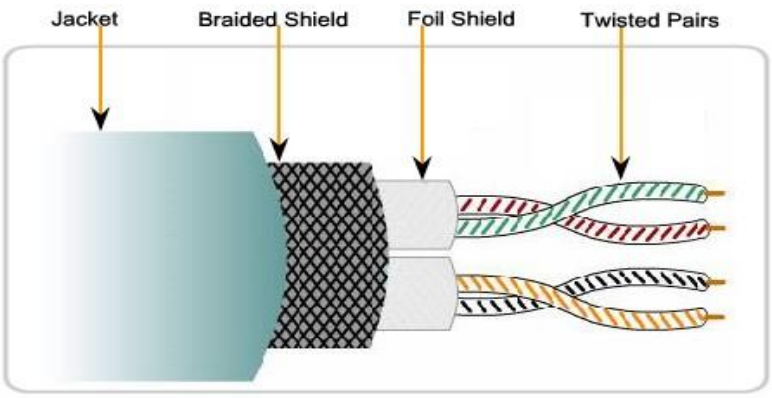


Guided Media:

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

Shielded Twisted-Pair (STP) Cable

Another type of cabling used in networking is shielded twisted-pair (STP). As shown in the figure, STP uses two pairs of wires that are wrapped in an overall metallic braid or foil. STP cable shields the entire bundle of wires within the cable as well as the individual wire pairs. STP provides better noise protection than UTP cabling, however at a significantly higher price.
For many years, STP was the cabling structure specified for use in Token Ring network installations. With the use of Token Ring declining, the demand for shielded twisted-pair cabling has also waned. The new 10 GB standard for Ethernet has a provision for the use of STP cabling. This may provide a renewed interest in shielded twisted-pair cabling.

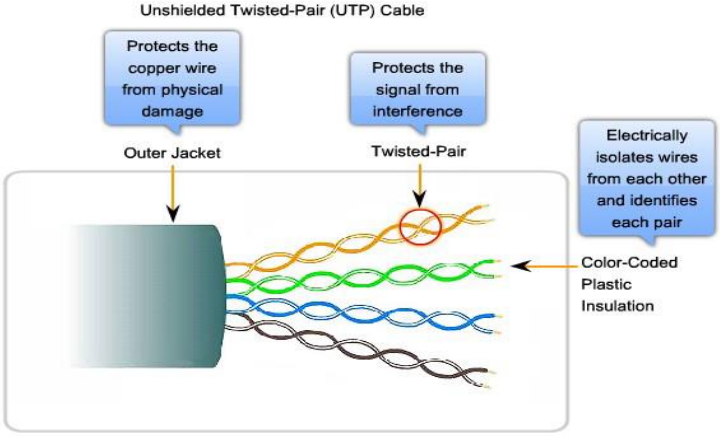


Unshielded twisted-pair (UTP)

Unshielded twisted-pair (UTP) cabling, as it is used in Ethernet LANs, consists of four pairs of color-coded wires that have been twisted together and then encased in a flexible plastic sheath. As seen in the figure, the color codes identify the individual pairs and wires in the pairs and aid in cable termination.

The twisting has the effect of canceling unwanted signals. When two wires in an electrical circuit are placed close together, external electromagnetic fields create the same interference in each wire. The pairs are twisted to keep the wires in as close proximity as is physically possible. When this common interference is present on the wires in a twisted pair, the receiver processes it in equal yet opposite ways. As a result, the signals caused by electromagnetic interference from external sources are effectively cancelled.

This cancellation effect also helps avoid interference from internal sources called crosstalk. Crosstalk is the interference caused by the magnetic field around the adjacent pairs of wires in the cable. When electrical current flows through a wire, it creates a circular magnetic field around the wire. With the current flowing in opposite directions in the two wires in a pair, the magnetic fields - as equal but opposite forces - have a cancellation effect on each other. Additionally, the different pairs of wires that are twisted in the cable use different number of twists per meter to help protect the cable from crosstalk between pairs.



UTP Cabling Standards

The UTP cabling commonly found in workplaces, schools, and homes conforms to the standards established jointly by the Telecommunications Industry Association (TIA) and the Electronics Industries Alliance (EIA). TIA/EIA-568A stipulates the commercial cabling standards for LAN installations and is the standard most commonly used in LAN cabling environments. Some of the elements defined are:

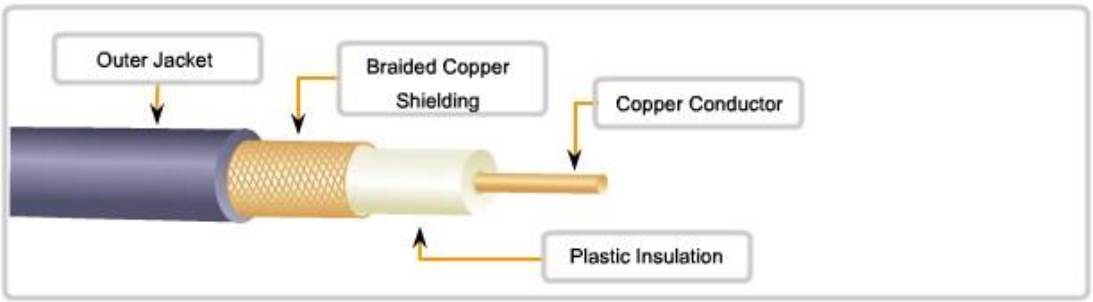
- Cable types
- Cable lengths
- Connectors
- Cable termination
- Methods of testing cable

The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE). IEEE rates UTP cabling according to its performance. Cables are placed into categories according to their ability to carry higher bandwidth rates. For example, Category 5 (Cat5) cable is used commonly in 100BASE-TX FastEthernet installations. Other categories include Enhanced Category 5 (Cat5e) cable and Category 6 (Cat6).

Cables in higher categories are designed and constructed to support higher data rates. As new gigabit speed Ethernet technologies are being developed and adopted, Cat5e is now the minimally acceptable cable type, with Cat6 being the recommended type for new building installations.

Co-axial Cable:

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted-pair 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



All the elements of the coaxial cable encircle the center conductor. Because they all share the same axis, this construction is called coaxial, or coax for short.

Uses of Coaxial Cable

The coaxial cable design has been adapted for different purposes. Coax is an important type of cable that is used in wireless and cable access technologies. Coax cables are used to attach

antennas to wireless devices. The coaxial cable carries radio frequency (RF) energy between the antennas and the radio equipment.

Coax is also the most widely used media for transporting high radio frequency signals over wire, especially cable television signals. Traditional cable television, exclusively transmitting in one direction, was composed completely of coax cable.

Cable service providers are currently converting their one-way systems to two-way systems to provide Internet connectivity to their customers. To provide these services, portions of the coaxial cable and supporting amplification elements are replaced with multi-fiber-optic cable. However, the final connection to the customer's location and the wiring inside the customer's premises is still coax cable. This combined use of fiber and coax is referred to as hybrid fiber coax (HFC).

In the past, coaxial cable was used in Ethernet installations. Today UTP offers lower costs and higher bandwidth than coaxial and has replaced it as the standard for all Ethernet installations.

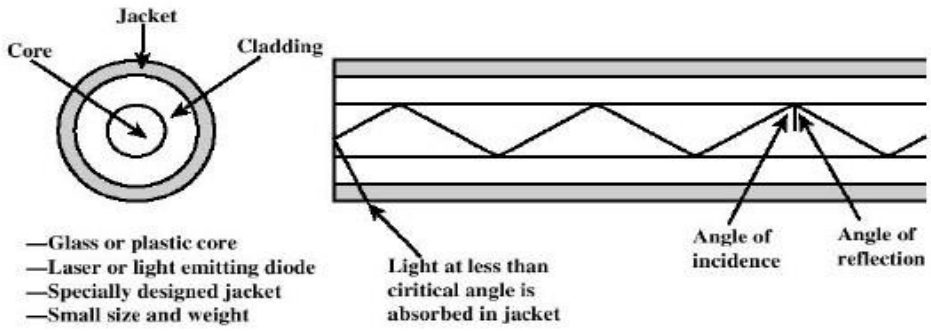
Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNC), connector. Three types of connectors: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks o branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

Fiber-optics

Fiber-optic cabling uses either glass or plastic fibers to guide light impulses from source to destination. The bits are encoded on the fiber as light impulses. Optical fiber cabling is capable of very large raw data bandwidth rates. Most current transmission standards have yet to approach the potential bandwidth of this media.

Principle of Fiber-optics:
It is based on the principle of Total internal Reflection.



(c) Optical fiber

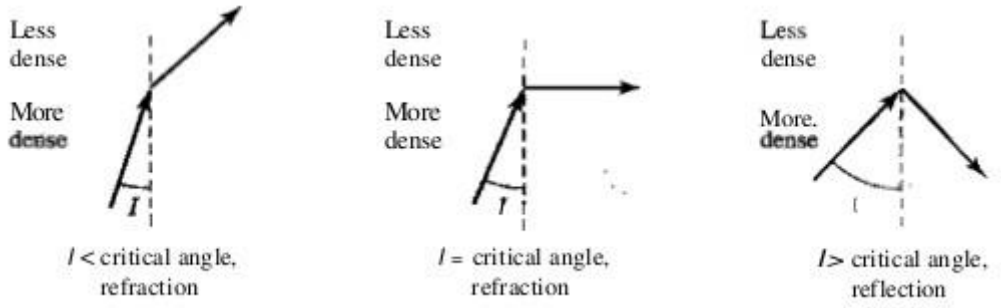
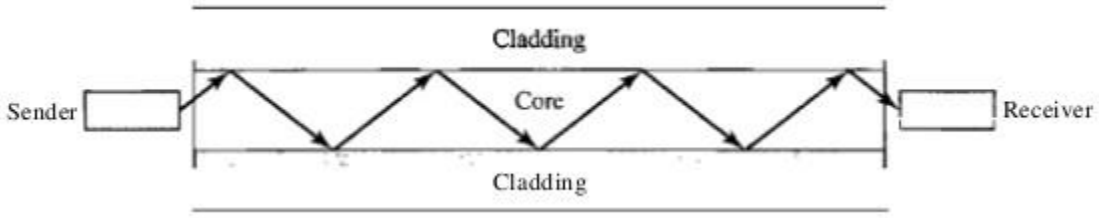


Figure: Bending of Light Ray

Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it as shown in fig below.



Fiber Compared to Copper Cabling:

Given that the fibers used in fiber-optic media are not electrical conductors, the media is immune to electromagnetic interference and will not conduct unwanted electrical currents due to grounding issues. Because optical fibers are thin and have relatively low signal loss, they can be operated at much greater lengths than copper media, without the need for signal regeneration. Some optical fiber Physical layer specifications allow lengths that can reach multiple kilometers.

Optical fiber media implementation issues include:

- More expensive (usually) than copper media over the same distance (but for a higher capacity)
- Different skills and equipment required to terminate and splice the cable infrastructure
- More careful handling than copper media.

At present, in most enterprise environments, optical fiber is primarily used as backbone cabling for high-traffic point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses. Because optical fiber does not conduct electricity and has low signal loss, it is well suited for these uses.

Propagation modes:

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical

characteristics. Multi- mode can be implemented in two forms: step-index or graded-index.

Single-mode optical fiber carries a single ray of light, usually emitted from a laser. Because the laser light is uni-directional and travels down the center of the fiber, this type of fiber can transmit optical pulses for very long distances.

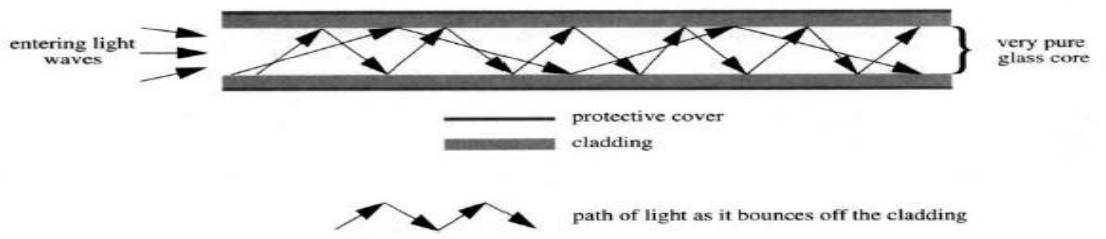
- Single mode
  - The diameter of the core is reduced to the order of wavelength s.t. only a single angle or mode can pass
  - Superior performance

Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single- mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction). The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible. All the beams arrive at the destination "together" and can be recombined with little distortion to the signal

Multimode fiber typically uses LED emitters that do not create a single coherent light wave. Instead, light from an LED enters the multimode fiber at different angles. Because light entering the fiber at different angles takes different amounts of time to travel down the fiber, long fiber runs may result in the pulses becoming blurred on reception at the receiving end. This effect, known as modal dispersion, limits the length of multimode fiber segments.

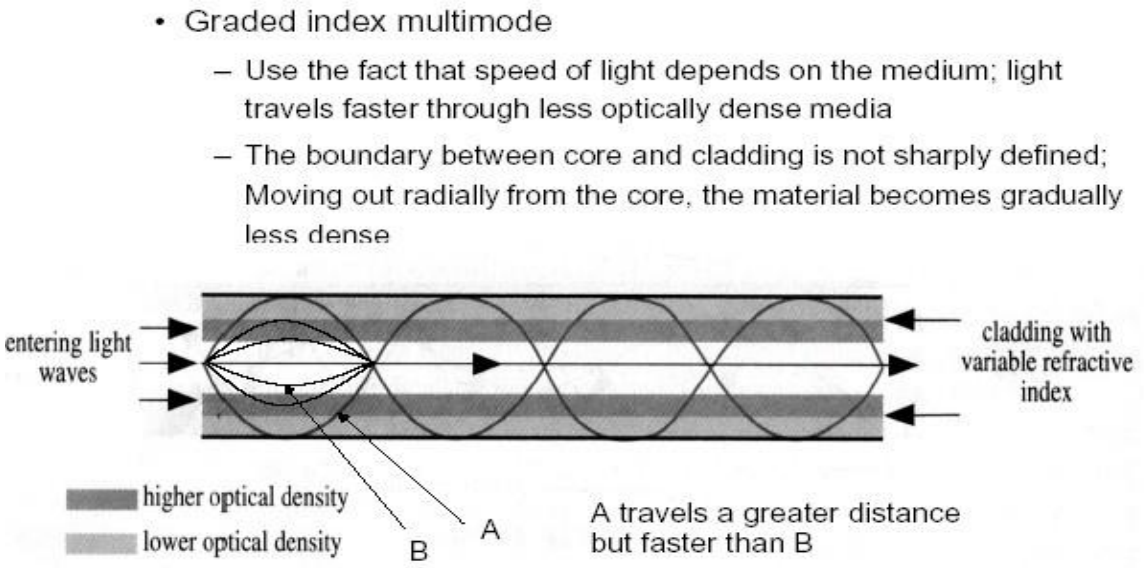
Multimode Step-index:
In multimode step-index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber .

- Three types of fiber transmission
  - Step index multimode
    - Variety of angles that reflect. Each angle defines a path or a mode
    - Limited data rate due to the different path lengths



Multimode Graded-Index

Multimode graded-index fiber, decreases this distortion of the signal through the cable. The word index here refers to the index of refraction. As we saw above, the index of refraction is related to density. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge



Advantages and Disadvantages of Optical Fiber

Advantages

Fiber-optic cable has several advantages over metallic cable (twisted- pair or coaxial).

- **Higher bandwidth:** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.
- **Less signal attenuation:** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- **Immunity to electromagnetic interference:** Electromagnetic noise cannot affect fiber-optic cables.
- **Resistance to corrosive materials**: Glass is more resistant to corrosive materials than copper.
- **Light weight:** Fiber-optic cables are much lighter than copper cables.
- **Greater immunity to tapping**: Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages

There are some disadvantages in the use of optical fiber.

- **Installation and maintenance**: Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- **Unidirectional light propagation**: Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

- **Cost:** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

Wireless Networking

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

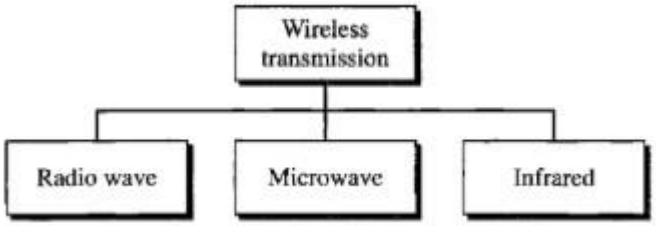


Figure: Wireless Transmission Waves

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure

Figure: Propagation Method

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3-30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30-300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz-3 MHz	Sky	AM radio
HF (high frequency)	3-30 MHz	Sky	Citizens band (CB), shi*p*/aircraft communication
VHF (very high frequency)	30-300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz-3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3-30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30-300 GHz	Line-of-sight	Radar, satellite

Radio Waves

Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves. However, the behavior of the waves, rather than the frequencies, is a better criterion for classification. Radio waves, for the most part, 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 sends waves that can be received by any receiving antenna. The omnidirectional property has a disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band. Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio. Radio waves, particularly those of low and medium frequencies, can penetrate walls.

This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, 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. The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into subbands, the subbands are also narrow, leading to allow data rate for digital communications.

Omnidirectional Antenna
Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas.

Applications
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.

Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, 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 microwave 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. The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for long-distance communication.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.

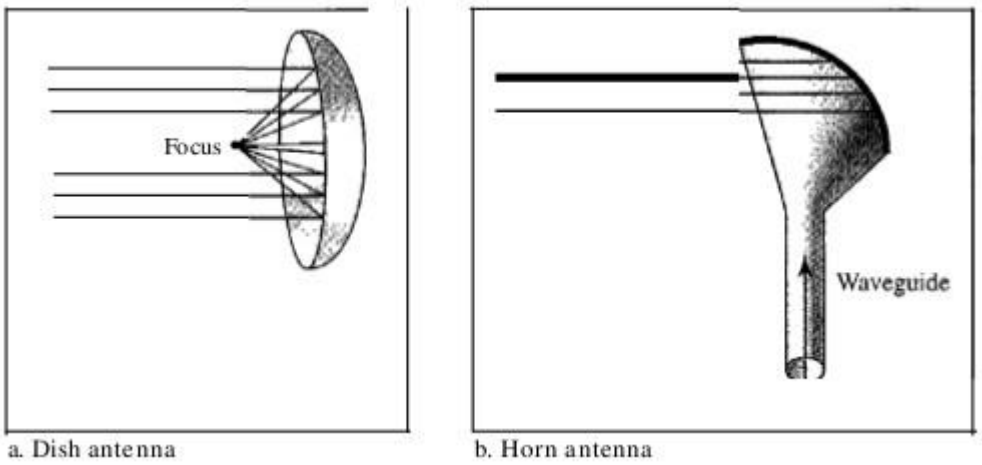
- The microwave band is relatively wide, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities.

Applications

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

Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn.



a. Dish antenna b. Horn antenna

A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus. The parabolic dish 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 (resembling a handle) 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.

Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), 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 one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. 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.

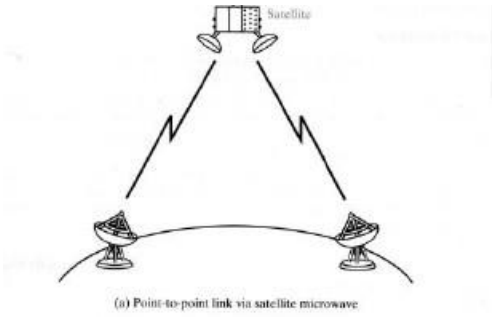
Applications

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, mice, PCs, and printers. For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC. The standard originally defined a data rate of 75 kbps for a distance up to 8 m. The recent standard defines a data rate of 4 Mbps. Infrared signals defined by IrDA transmit through line of sight; the IrDA port on the keyboard needs to point to the PC for transmission to occur.

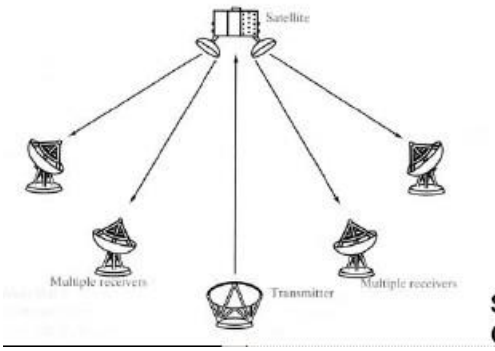
Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Satellite Communication:

- Uses satellite in geostationary (geosynchronous) orbit (36,000 km).
- Source transmits signal to satellite which amplifies or repeats it, and retransmits down to destinations.
- Optimum transmission in 1 - 10 GHz range; Bandwidth of 100'sMHz.
- Significant propagation delay 270ms.
- Total propagation delay is independent of distance between sender and receiver.
- Applications:
  - Long-distance telephones.
  - Television distribution
  - Private business networks.



(a) Point-to-point link via satellite microwave



Satellite Communications Configuration

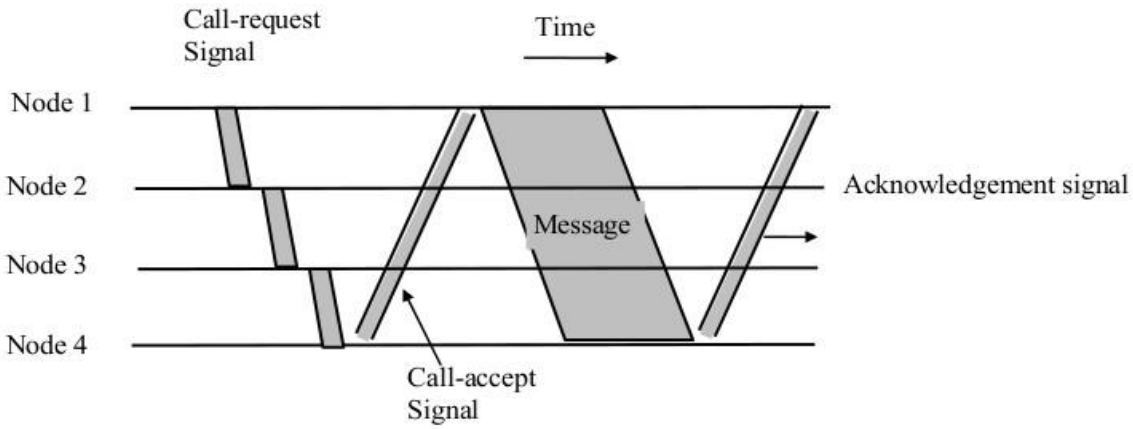
VSAT (Very Small Aperture System)

- For business data applications requiring high data rates for short periods of time.
- National Weather Service, news services, credit card verification, automatic tellers, car rental agencies.
- Commonly connects a central location with many remote ones.
- Communication between two sites is via a satellite and allows a low-cost small antenna dishes (5 ft).

Circuit Switching:

A dedicated path between the source node and the destination node is set up for the duration of communication session to transfer data. That path is a connected sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection. Communication via circuit switching involves three phases,

I. **Circuit Establishment:** Before any signals can be transmitted, an end-to-end (station-to-station) circuit must be established.
II. **Data Transfer:** The data may be analog or digital, depending on the nature of the network
III. **Circuit Disconnect:** After some period of data transfer, the connection is terminated, usually by the action of one of the two stations

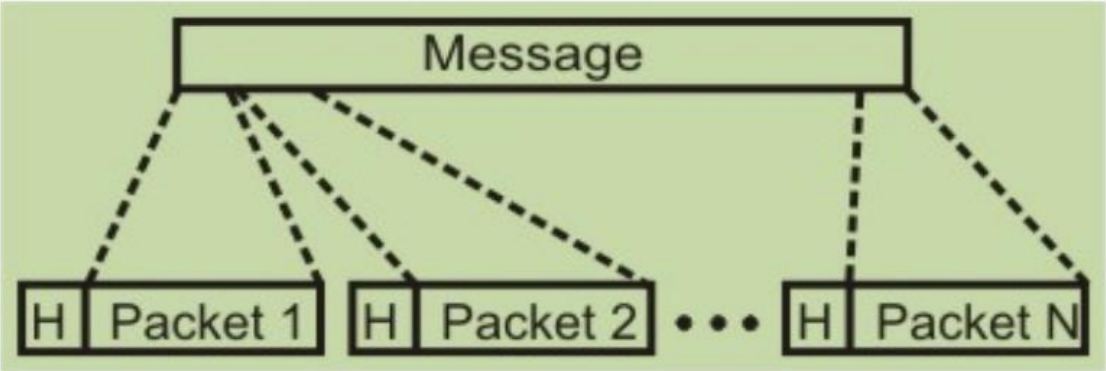


Circuit switching telecommunication networks was originally designed to handle voice traffic, and the majority of the traffic on these networks continues to be voice. A key characteristic of the circuit switching is that resources within the network are dedicated to a particular call. For voice communication the resulting circuit will enjoy the high percentage of utilization because most of the time one party or the other is talking. However, as the circuit-switching network began to be used increasingly for data connections, two shortcomings became apparent:

I. In a typical user host data connection (e.g., personal computer user logged on to a database server), much of the time the line is idle. Thus, with data connections, a circuit-switching approach is inefficient.
II. In a circuit-switching network, the connection provides for transmission at constant data rate. Thus, each of the two devices that are connected must transmit and receive at the same data rate as the other; this limits the utility of the network in interconnecting a variety of host computers and terminals.

Packet Switching:

Messages are divided into subsets of equal length called packets. In packet switching approach, data are transmitted in short packets (few Kbytes). A long message is broken up into a series of packets as shown in Figure. Every packet contains some control information in its header, which is required for routing and other purposes.

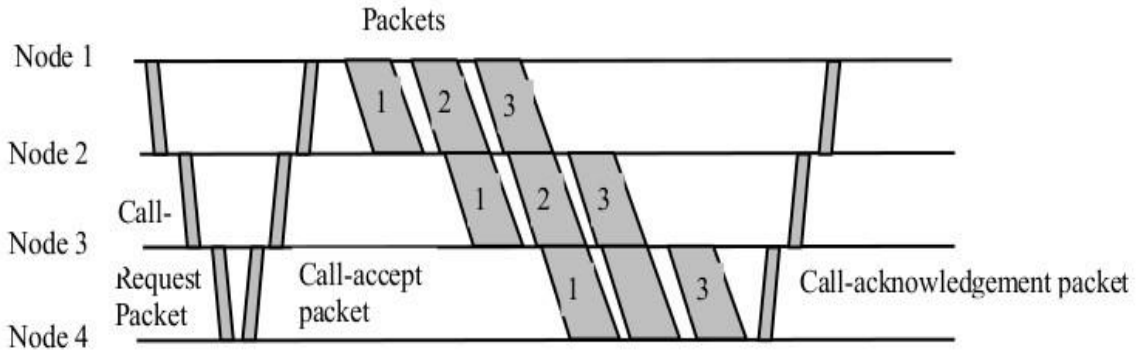


Main difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing messages from the source to the destination. In Packet Switching, different messages (and even different packets) can pass through different routes, and when there is a "dead time" in the communication between the source and the destination, the lines can be used by other sources.

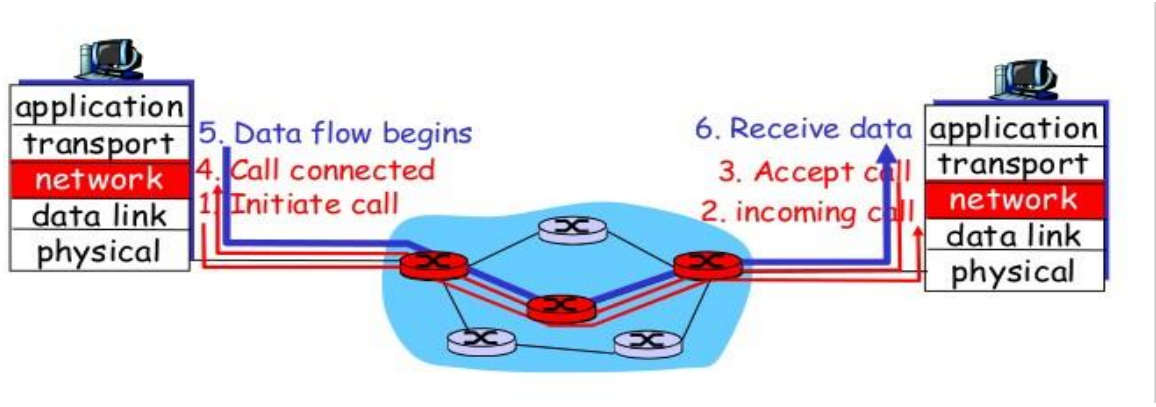
There are two basic approaches commonly used to packet Switching: virtual circuit packet switching and datagram packet switching. In virtual-circuit packet switching a virtual circuit is made before actual data is transmitted, but it is different from circuit switching in a sense that in circuit switching the call accept signal comes only from the final destination to the source while in case of virtual-packet switching this call accept signal is transmitted between each adjacent intermediate node as shown in Fig. Other features of virtual circuit packet switching are discussed in the following subsection.

Virtual Circuit:

An initial setup phase is used to set up a route between the intermediate nodes for all the packets passed during the session between the two end nodes. In each intermediate node, an entry is registered in a table to indicate the route for the connection that has been set up. Thus, packets passed through this route, can have short headers, containing only a virtual circuit identifier (VCI), and not their destination. Each intermediate node passes the packets according to the information that was stored in it, in the setup phase. In this way, packets arrive at the destination in the correct sequence, and it is guaranteed that essentially there will not be errors. This approach is slower than Circuit Switching, since different virtual circuits may compete over the same resources, and an initial setup phase is needed to initiate the circuit. As in Circuit Switching, if an intermediate node fails, all virtual circuits that pass through it are lost. The most common forms of Virtual Circuit networks are X.25 and Frame Relay, which are commonly used for public data networks (PDN).



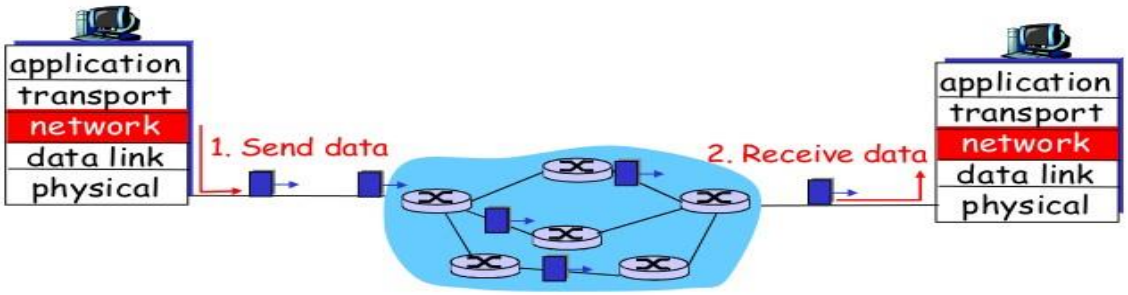
Virtual circuit packet switching techniques



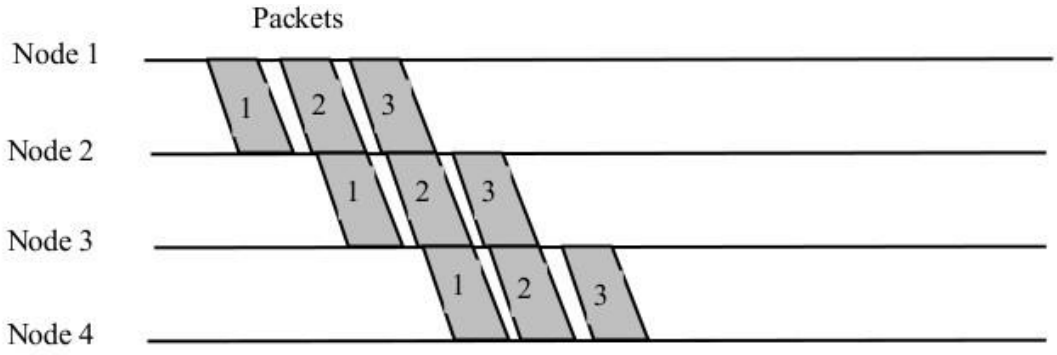
Virtual Circuit

Datagram:

This approach uses a different, more dynamic scheme, to determine the route through the network links. Each packet is treated as an independent entity, and its header contains full information about the destination of the packet. The intermediate nodes examine the header of the packet, and decide to which node to send the packet so that it will reach its destination.



In this method, the packets don't follow a pre-established route, and the intermediate nodes (the routers) don't have pre-defined knowledge of the routes that the packets should be passed through. Packets can follow different routes to the destination, and delivery is not guaranteed. Due to the nature of this method, the packets can reach the destination in a different order than they were sent, thus they must be sorted at the destination to form the original message. This approach is time consuming since every router has to decide where to send each packet. The main implementation of Datagram Switching network is the Internet, which uses the IP network protocol.



Datagram packet switching

Datagram Packet Switching Vs Virtual-circuit Packet Switching:

S.No	Datagram Packet Switching	Virtual-Circuit Packet Switching
1	Two packets of the same user pair can travel along different routes.	All packets of the same virtual circuit travel along the same path.
2	The packets can arrive out of sequence.	Packet sequencing is guaranteed.
3	Packets contain full source and destination address.	Packets contain short VC Id. (VCI).
4	Each host occupies routine table entries.	Each VC occupies routing table entries.
5	Requires no connection setup.	Requires VC setup. First packet has large delay.
6	Also called Connection less	Also called connection oriented.
7	Examples: X.25 and Frame Relay	Eg. Internet which uses IP Network protocol.

Virtual Circuit:

Virtual Circuits is a connection between two network devices appearing like a direct and dedicated connection but it but is actually a group of logic circuit resources from which specific circuits are allocated as needed to meet traffic requirements in a packet switched network. In this case, the two network devices can communicate as though they have a dedicated physical connection. Examples of networks with virtual circuit capabilities include X.25 connections, Frame Relay and ATM networks.

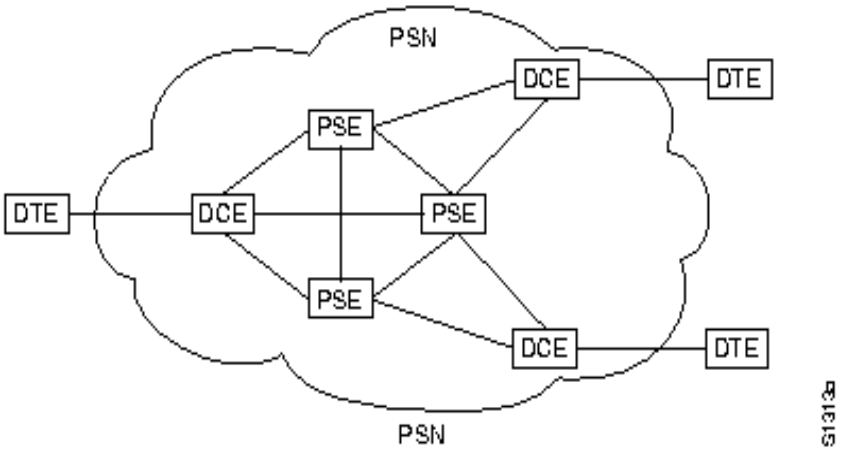
Virtual circuits can be either permanent, called Permanent virtual Circuits (PVC), or temporary, called Switched Virtual Circuits (SVCs).

A Permanent Virtual Circuit (PVC) is a virtual circuit that is permanently available to the user. A PVC is defined in advance by a network manager. A PVC is used on a circuit that includes routers that must maintain a constant connection in order to transfer routing information in a dynamic network environment. Carriers assign PVCs to customers to reduce overhead and improve performance on their networks.
A switched virtual circuit (SVC) is a virtual circuit in which a connection session is set up dynamically between individual nodes temporarily only for the duration of a session. Once a communication session is complete, the virtual circuit is disabled.

X.25:

A packet-switching protocol for wide area network (WAN) connectivity that uses a public data network (PDN) that parallels the voice network of the Public Switched Telephone Network (PSTN). The current X.25 standard supports synchronous, full-duplex communication at speeds up to 2 Mbps over two pairs of wires, but most implementations are 64-Kbps connections via a standard DS0 link.

X.25 defines a telephone network for data communications. To begin communication, one computer calls another to request a communication session. The called computer can accept or refuse the connection. If the call is accepted, the two systems can begin full-duplex information transfer. Either side can terminate the connection at any time.
The X.25 specification defines a point-to-point interaction between data terminal equipment (DTE) and data communication equipment (DCE). DTEs (terminals and hosts in the user's facilities) connect to DCEs (modems, packet switches, and other ports into the PDN, generally located in the carrier's facilities), which connect to packet switching exchanges (PSEs, or simply switches) and other DCEs inside a PSN and, ultimately, to another DTE. The relationship between the entities in an X.25 network is shown in Figure.



Because X.25 was designed when analog telephone transmission over copper wire was the norm, X.25 packets have a relatively large overhead of error-correction information, resulting in comparatively low overall bandwidth. Newer WAN technologies such as frame relay, Integrated Services Digital Network (ISDN), and T-carrier services are now generally preferred over X.25. However, X.25 networks still have applications in areas such as credit card verification, automatic teller machine transactions, and other dedicated business and financial uses.

How It Works
The X.25 standard corresponds in functionality to the first three layers of the Open Systems Interconnection (OSI) reference model for networking. Specifically, X.25 defines the following:

- The physical layer interface for connecting data terminal equipment (DTE), such as computers and terminals at the customer premises, with the data communications equipment (DCE), such as X.25 packet switches at the X.25 carrier's facilities. The physical layer interface of X.25 is called X.21bis and was derived from the RS-232 interface for serial transmission.

- The data-link layer protocol called Link Access Procedure, Balanced (LAPB), which defines encapsulation (framing) and error-correction methods. LAPB also enables the DTE or the DCE to initiate or terminate a communication session or initiate data transfer. LAPB is derived from the High-level Data Link Control (HDLC) protocol.
- The network layer protocol called the Packet Layer Protocol (PLP), which defines how to address and deliver X.25 packets between end nodes and switches on an X.25 network using permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). This layer is responsible for call setup and termination and for managing transfer of packets.

An X.25 network consists of a backbone of X.25 switches that are called packet switching exchanges (PSEs). These switches provide packet-switching services that connect DCEs at the local facilities of X.25 carriers. DTEs at customer premises connect to DCEs at X.25 carrier facilities by using a device called a packet assembler/disassembler (PAD). You can connect several DTEs to a single DCE by using the multiplexing methods inherent in the X.25 protocol. Similarly, a single X.25 end node can establish several virtual circuits simultaneously with remote nodes.

An end node (DTE) can initiate a communication session with another end node by dialing its X.121 address and establishing a virtual circuit that can be either permanent or switched, depending on the level of service required. Packets are routed through the X.25 backbone network by using the ID number of the virtual circuit established for the particular communication session. This ID number is called the logical channel identifier (LCI) and is a 12-bit address that identifies the virtual circuit. Packets are generally up to 128 bytes in size, although maximum packet sizes range from 64 to 4096 bytes, depending on the system.

Disadvantages of X.25

Prior to Frame Relay, some organizations were using a virtual-circuit switching network called X.25 that performed switching at the network layer. For example, the Internet, which needs wide-area networks to carry its packets from one place to another, used X.25. And X.25 is still being used by the Internet, but it is being replaced by other WANs. However, X.25 has several drawbacks:

- X.25 has a low 64-kbps data rate. By the 1990s, there was a need for higher- data-rate WANs.
- X.25 has extensive flow and error control at both the data link layer and the network layer. This was so because X.25 was designed in the 1970s, when the available transmission media were more prone to errors. Flow and error control at both layers create a large overhead and slow down transmissions. X.25 requires acknowledgments for both data link layer frames and network layer packets that are sent between nodes and between source and destination.
- Originally X.25 was designed for private lise, not for the Internet. X.25 has its own network layer. This means that the user's data are encapsulated in the network layer packets of X.25. The Internet, however, has its own network layer, which means if the Internet wants to use X.25, the Internet must deliver its network layer packet, called a datagram, to X.25 for encapsulation in the X.25 packet. This doubles the overhead.

Frame Relay:

Frame Relay is a high-performance WAN protocol that operates at the physical and Data Link layers of the OSI reference model. X.25 has several disadvantages so Frame Relay was invented. Frame Relay is a wide-area network with the following features:

I. Frame Relay operates at a higher speed (1.544 Mbps and recently 44.376 Mbps). This means that it can easily be used instead of a mesh of T-I or T-3 lines.
II. Frame Relay operates in just the physical and data link layers. This means it can easily be used as a backbone network to provide services to protocols that already have a network layer protocol, such as the Internet.
III. Frame Relay allows bursty data.
IV. Frame Relay allows a frame size of 9000 bytes, which can accommodate all local-area network frame sizes.
V. Frame Relay is less expensive than other traditional WANs.
VI. Frame Relay has error detection at the data link layer only. There is no flow control or error control. There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame Relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers.

Frame Relay Operation:

When carriers use Frame Relay to interconnect LANs, a router on each LAN is the DTE. A serial connection, such as a T1/E1 leased line, connects the router to the Frame Relay switch of the carrier at the nearest point-of-presence (POP) for the carrier. The Frame Relay switch is a DCE device. Network switches move frames from one DTE across the network and deliver frames to other DTEs by way of DCEs.

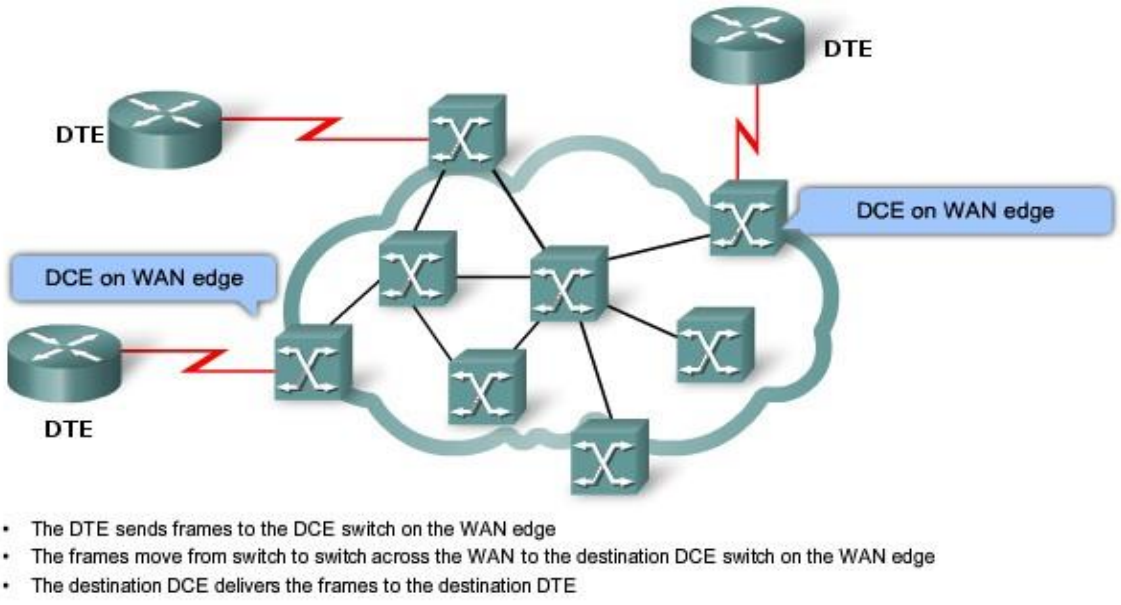


Figure: Frame Relay Operation

Virtual Circuits

The connection through a Frame Relay network between two DTEs is called a virtual circuit (VC). The circuits are virtual because there is no direct electrical connection from end to end. The connection is logical, and data moves from end to end, without a direct electrical circuit.

With VCs, Frame Relay shares the bandwidth among multiple users and any single site can communicate with any other single site without using multiple dedicated physical lines.

There are two ways to establish VCs:

Permanent Virtual Circuit (PVC):

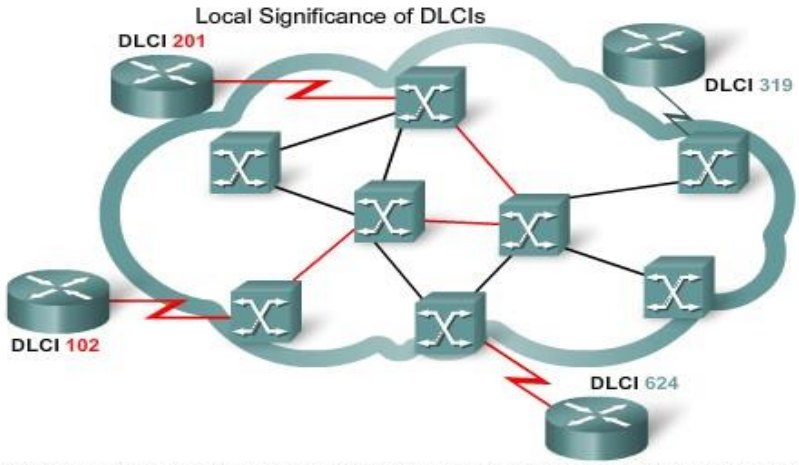
A source and a destination may choose to have a permanent virtual circuit (PVC). In this case, the connection setup is simple. The corresponding table entry is recorded for all switches by the administrator (remotely and electronically, of course). An outgoing DLCI is given to the source, and an incoming DLCI is given to the destination. PVC connections have two drawbacks. First, they are costly because two parties pay for the connection all the time even when it is not in use. Second, a connection is created from one source to one single destination. If a source needs connections with several destinations, it needs a PVC for each connection PVCs, permanent virtual circuits, are preconfigured by the carrier, and after they are set up, only operate in DATA TRANSFER and IDLE modes. Note that some publications refer to PVCs as private Vcs.

Switched Virtual-circuit (SVC):

An alternate approach is the switched virtual circuit (SVC). The SVC creates a temporary, short connection that exists only when data are being transferred between source and destination. SVCs, switched virtual circuits, are established dynamically by sending signaling messages to the network (CALL SETUP, DATA TRANSFER, IDLE, CALL TERMINATION).

DLCI (Data link connection identifier):

Frame Relay is a virtual circuit network. A virtual circuit in Frame Relay is identified by a number called a data link connection identifier (DLCI). DLCI values typically are assigned by the Frame Relay service provider (for example, the telephone company). Usually, DLCIs 0 to 15 and 1008 to 1023 are reserved for special purposes. Therefore, service providers typically assign DLCIs in the range of 16 to 1007. Frame Relay DLCIs have local significance, which means that the values themselves are not unique in the Frame Relay WAN. A DLCI identifies a VC to the equipment at an endpoint. A DLCI has no significance beyond the single link. Two devices connected by a VC may use a different DLCI value to refer to the same connection.



DLCI values have local significance, which means that they are unique only to the physical channel on which they reside. Therefore, devices at opposite ends of a connection can use the same DLCI values to refer to different virtual circuits.

Frame Relay Layers:
Frame Relay operates at the physical layer and the Data link layer.

Physical Layer
No specific protocol is defined for the physical layer in Frame Relay. Instead, it is left to the implementer to use whatever is available. Frame Relay supports any of the protocols recognized by ANSI.

Data Link Layer
At the data link layer, Frame Relay uses a simple protocol that does not support flow or error control. It only has an error detection mechanism. Figure blow shows the format of a Frame Relay frame. The address field defines the DLCI as well as some bits used to control congestion.

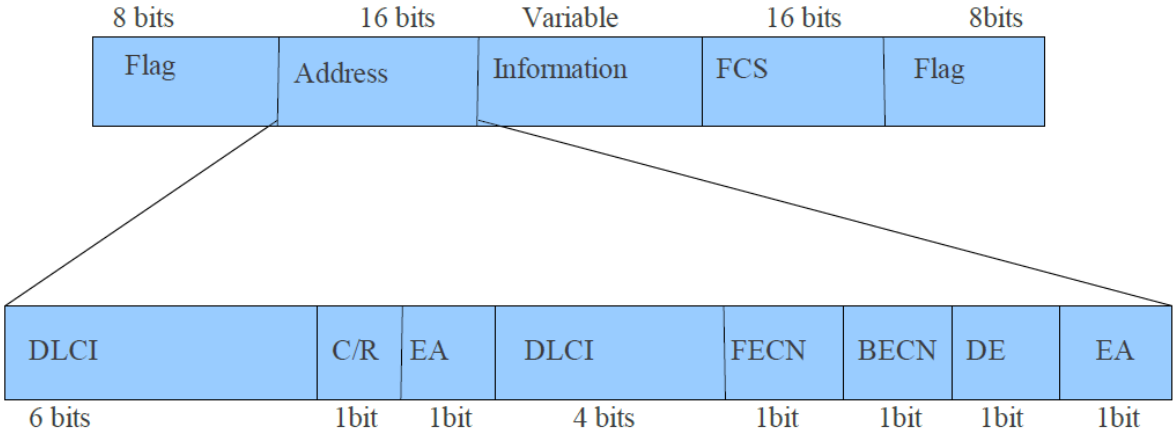


Figure Frame Relay Frame Format

C/R: Command/response
EA: Extended address
FECN: Forward explicit congestion notification
BECN: Backward explicit congestion notification
DE: Discard eligibility
DLCI: Data link connection identifier

Address (DLCI) field: The first 6 bits of the first byte makes up the first part of the DLCI. The second part of the DLCI uses the first 4 bits of the second byte. These bits are part of the10-bit data link connection identifier defined by the standard.

Command/response (CIR): The command/response (C/R) bit is provided to allow upper layers to identify a frame as either a command or a response. It is not used by the Frame Relay protocol.

Extended address (EA): The extended address (EA) bit indicates whether the current byte is the final byte of the address. An EA of 0 means that another address byte is to follow. An EA of 1 means that the current byte is the final one.

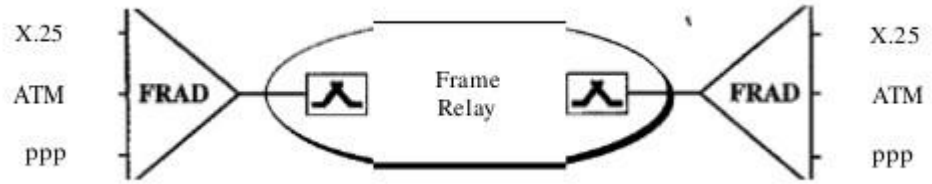
Forward explicit congestion notification (FECN): The forward explicit congestion notification (FECN) bit can be set by any switch to indicate that traffic is congested. This bit informs the destination that congestion has occurred. In this way, the destination knows that it should expect delay or a loss of packets.

Backward explicit congestion notification (BECN): The backward explicit congestion notification (BECN) bit is set (in frames that travel in the other direction) to indicate a congestion problem in the network. This bit informs the sender that congestion has occurred. In this way, the source knows it needs to slow down to prevent the loss of packets.

Discard eligibility (DE): The discard eligibility (DE) bit indicates the priority level of the frame. In emergency situations, switches may have to discard frames to relieve bottlenecks and keep the network from collapsing due to overload. When set (DE 1), this bit tells the network to discard this frame if there is congestion. This bit can be set either by the sender of the frames (user) or by any switch in the network.

FRADs

To handle frames arriving from other protocols, Frame Relay uses a device called a Frame Relay assembler/disassembler (FRAD). A FRAD assembles and disassembles frames coming from other protocols to allow them to be carried by Frame Relay frames. A FRAD can be implemented as a separate device or as part of a switch.



VOFR

Frame Relay networks offer an option called Voice Over Frame Relay (VOFR) that sends voice through the network. Voice is digitized using PCM and then compressed. The result is sent as data frames over the network. This feature allows the inexpensive sending of voice over long distances. However, note that the quality of voice is not as good as voice over a circuit-switched network such as the telephone network. Also, the varying delay mentioned earlier sometimes corrupts real-time voice.

Local Management Information (LMI)

Frame Relay was originally designed to provide PVC connections. There was not, therefore, a provision for controlling or managing interfaces. Local Management Information (LMI) is a protocol added recently to the Frame Relay protocol to provide more management features. In particular, LMI can provide:

- A keep-alive mechanism to check if data are flowing.
- A multicast mechanism to allow a local end system to send frames to more than one remote end system.
- A mechanism to allow an end system to check the status of a switch (e.g., to see if the switch is congested).

Asynchronous Transfer Mode (ATM)

Asynchronous transfer mode (ATM), also known as cell relay, is similar in concept to frame relay. Both frame relay and ATM take advantage of the reliability and fidelity of modern digital facilities to provide faster packet switching than X.25. ATM is even more streamlined than frame relay in its functionality, and can support data rates several orders of magnitude greater than frame relay.

The “asynchronous” in ATM means ATM devices do not send and receive information at fixed speeds or using a timer, but instead negotiate transmission speeds based on hardware and information flow reliability. The “transfer mode” in ATM refers to the

fixed-size cell structure used for packaging information.

ATM transfers information in fixed-size units called cells. Each cell consists of 53 octets, or bytes as shown in Figure.

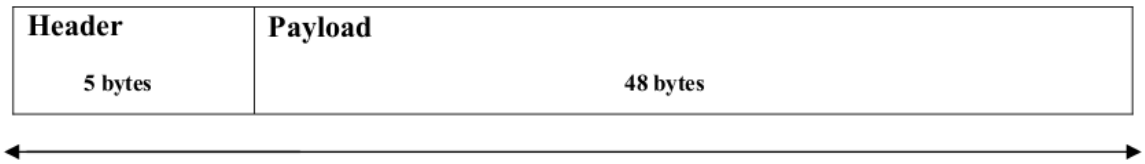


Figure: ATM cell Format

- Transmits all information in fixed size blocks called cells.
- Cells are transmitted asynchronously.
- The network is connection oriented.
- Each cell is 53 bytes long – 5 bytes header and 48 bytes payload.
- Making an ATM call requires first sending a message to set up a connection. Subsequently all cells follow the same path to the destination.
- ATM was envisioned as the technology for providing B-ISDN services.
- It can handle both constant rate traffic and variable-length traffic. Thus, it can carry multiple types of traffic with end-to-end quality of service.
- ATM is independent of transmission medium. It doesn't prescribe any particular rule.
- They may be sent on a wire or Fiber by themselves or they may be also packaged inside the payload of the other carrier system.
- Delivery of the system is not guaranteed but the order is.

When the virtual circuit is established, what really happens is that a route is chosen from source to destination. All the switches along the way make table entries for the virtual circuit and have the opportunity to reserve resources for the new circuit. The cells are sent from one switch to the next (stored and forwarded) until they reach the destination. When a cell comes along, the switch inspects its header to find out which virtual circuit it belongs to.

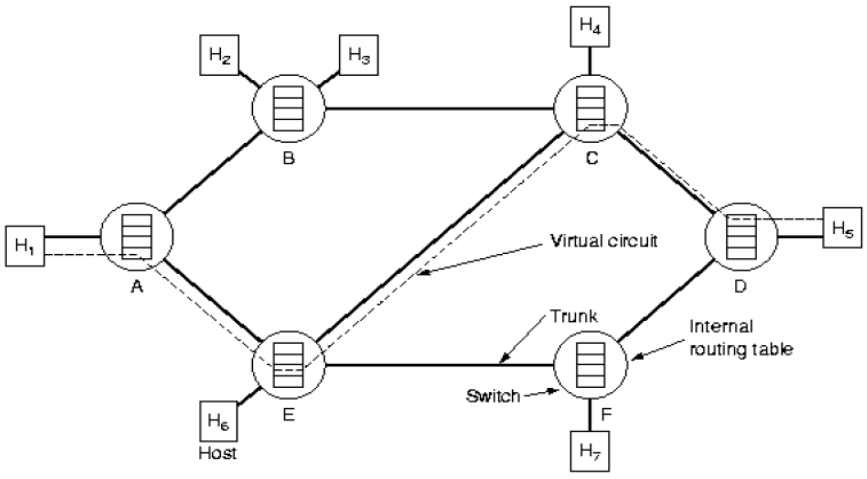


Figure: Cells travelling from Host 1 to Host 5

ATM Network Interfaces:

An ATM network consists of a set of ATM switches interconnected by point-to-point ATM links or interfaces. ATM switches support two primary types of interfaces: UNI and NNI as shown in Figure below. The UNI (User-Network Interface) connects ATM end systems (such as hosts and routers) to an ATM switch. The NNI (Network-Network Interface) connects two ATM switches. Depending on whether the switch is owned and located at the customer's premises or is publicly owned and operated by the telephone company, UNI and NNI can be further subdivided into public and private UNIs and NNIs. A private UNI connects an ATM endpoint and a private ATM switch. Its public counterpart connects an ATM endpoint or private switch to a public switch. A private NNI connects two ATM switches within the same private organization. A public one connects two ATM switches within the same public organization.

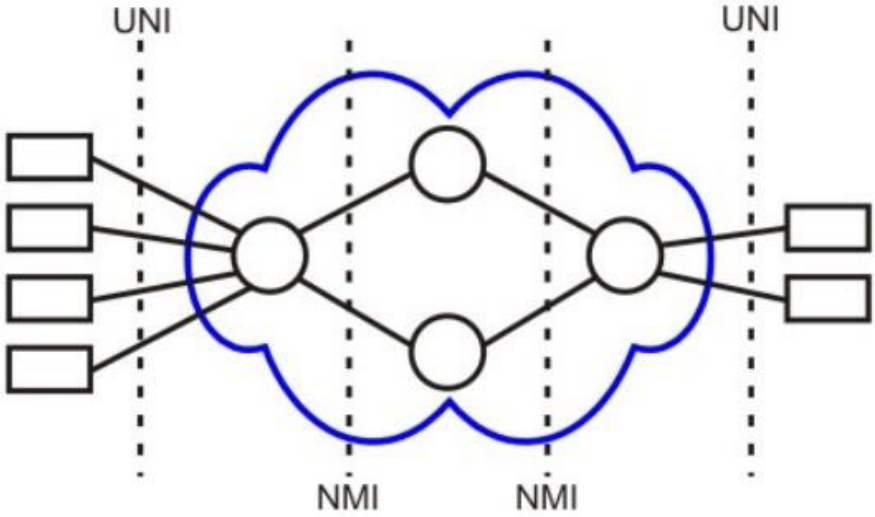


Figure: UNI and NNI interfaces of the ATM

ATM Virtual Connections

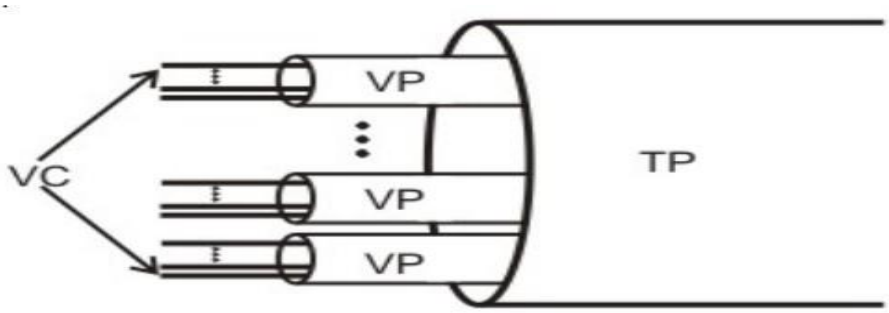
ATM operates as a channel-based transport layer; using Virtual circuits (VCs). This is encompassed in the concept of the Virtual Paths (VP) and Virtual Channels. Every ATM cell has an 8- or 12-bit Virtual Path Identifier (VPI) and 16-bit Virtual Channel Identifier (VCI) pair defined in its header. Together, these identify the virtual circuit used by the connection. The length of the VPI varies according to whether the cell is sent on the user-network interface (on the edge of the network), or if it is sent on the network-network interface (inside the network).

As these cells traverse an ATM network, switching takes place by changing the VPI/VCI values (label swapping). Although the VPI/VCI values are not necessarily consistent from one end of the connection to the other, the concept of a circuit is consistent (unlike IP, where any given packet could get to its destination by a different route than the others).

Another advantage of the use of virtual circuits comes with the ability to use them as a multiplexing layer, allowing different services (such as voice, Frame Relay, n* 64 channels, IP).

A virtual path connection (VPC) is a bundle of VCCs that have the same endpoints. Thus, all

of the cells flowing over all of the VCCs in a single VPC are switched together



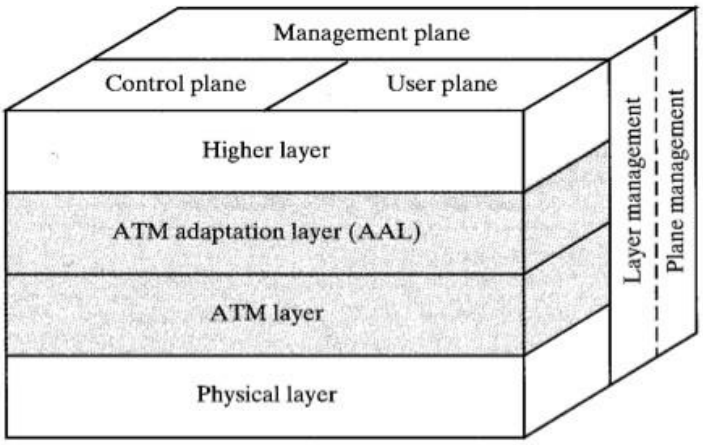
VC- Virtual Circuit
VP- Virtual Path
TP- Transmission Path

ATM Reference Model:
The protocol reference model makes reference to three separate planes:

User Plane: Provides for user information transfer, along with associated controls (e.g, flow control, error control).

Control Plane: Performs call control and connection control functions.

Management Plane: Includes plane management, which performs management functions related to a system as a whole and provides coordination between all the planes, and layer management, which performs management functions relating to resources and parameters residing in its protocol entities.



Physical layer: Analogous to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission.

ATM layer: Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model. The ATM layer is responsible for the simultaneous sharing of virtual circuits over a physical link (cell multiplexing) and passing cells through the ATM network (cell relay). To do this, it uses the VPI and VCI information in the header of each ATM cell.

ATM adaptation layer (AAL): Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model. The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes. The adaptation layer prepares user data for conversion into cells and segments the data into 48-byte cell payloads.

ATM Advantages:

- ATM supports voice, video and data allowing multimedia and mixed services over a single network.
- Provides the best multiple service support
- Supports delay close to that of dedicated services
- Supports the broadest range of burstiness, delay tolerance and loss performance through the implementation of multiple QoS classes
- Provides the capability to support both connection-oriented and connectionless traffic using AALs
- Able to use all common physical transmission paths (such as DS1, SONET).
- Cable can be twisted-pair, coaxial or fiber-optic
- Ability to connect LAN to WAN
- Legacy LAN emulation
- Efficient bandwidth use by statistical multiplexing
- Scalability
- Higher aggregate bandwidth
- High speed Mbps and possibly Gbps

ATM disadvantages

- Flexible to efficiency's expense, at present, for any one application it is usually possible to find a more optimized technology
- Cost, although it will decrease with time
- New customer premises hardware and software are required
- Competition from other technologies -100 Mbps FDDI, 100 Mbps Ethernet and fast Ethernet

Integrated Service Digital Network: (ISDN)

Integrated Services Digital Network (ISDN) is a network that provides end-to-end digital connectivity to support a wide range of services including voice and data services. ISDN allows multiple digital channels to operate simultaneously through the same regular phone wiring used for analog lines, but ISDN transmits a digital signal rather than analog. Latency is much lower on an ISDN line than on an analog line.

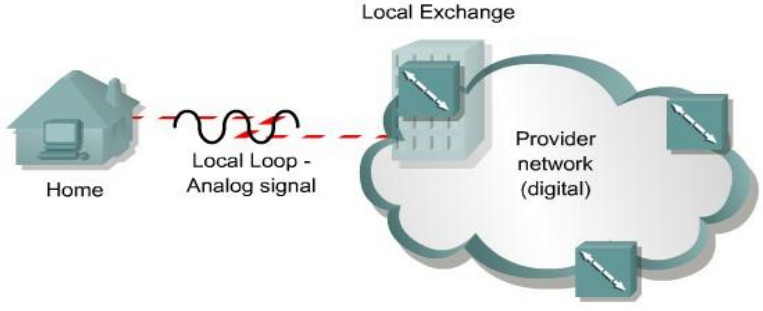


Figure: Analog communication without ISDN

The traditional PSTN was based on an analog connection between the customer premises and the local exchange, also called the local loop. The analog circuits introduce limitations on the bandwidth that can be obtained on the local loop. Circuit restrictions do not permit analog bandwidths greater than approximately 3000 Hz. ISDN technology permits the use of digital data on the local loop, providing better access speeds for the remote users.

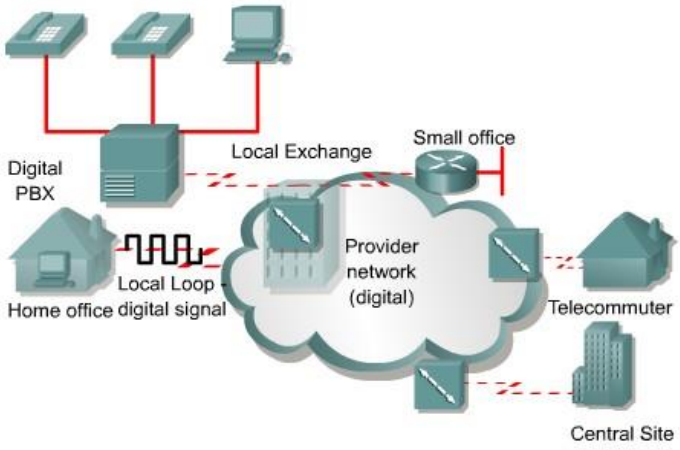
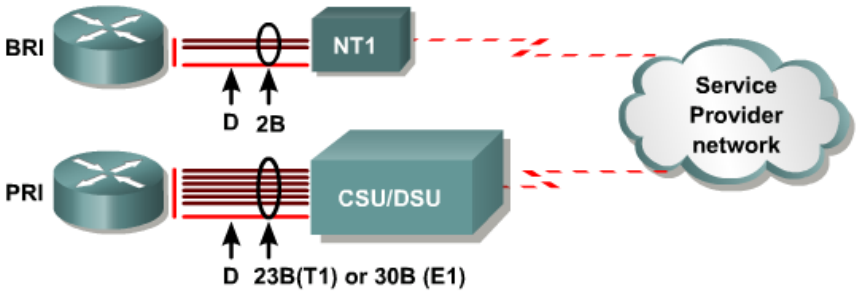


Figure: Digital communication with ISDN

ISDN standards define two main channel types, each with a different transmission rate.

The bearer channel or B channel: B channel is defined as a clear digital path of 64 kbps for voice or up to 64 Kbps of data. It is said to be clear because it can be used to transmit any type of digitized data in full-duplex mode. For example, a digitized voice call can be transmitted on a single B channel.

Delta channel or D channel: The D channel carries signaling messages, such as call setup and teardown, to control calls on B channels. Traffic over the D channel employs the Link Access Procedure on the D Channel (LAPD) protocol. LAPD is a data link layer protocol based on HDLC. There can either be 16 kbps for the Basic Rate Interface (BRI) or 64 kbps for the Primary Rate Interface (PRI). The D channel is used to carry control information for the B channel.



Channel	Capacity	Mostly Used for
B	64 kbps	Circuit-switched data (HDLC, PPP)
D	16/64 kbps	Signaling information (LAPD)

ISDN specifies two standard access methods, BRI and PRI. A single BRI or PRI interface provides a multiplexed bundle of B and D channels.

Basic Rate Interface (BRI)

The ISDN BRI structure consists of two B-channels at 64Kbps and one D-channel for control at 16Kbps. The B-channel can carry either voice or data while the D-channel is used for signaling and can be used for packet data.

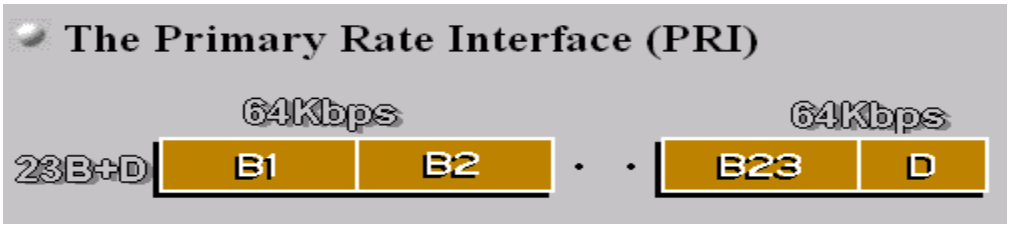
The capacity of the BRI is therefore:

- two voice, two high-speed data or
- one voice and one high-speed data plus 16kbps packet data

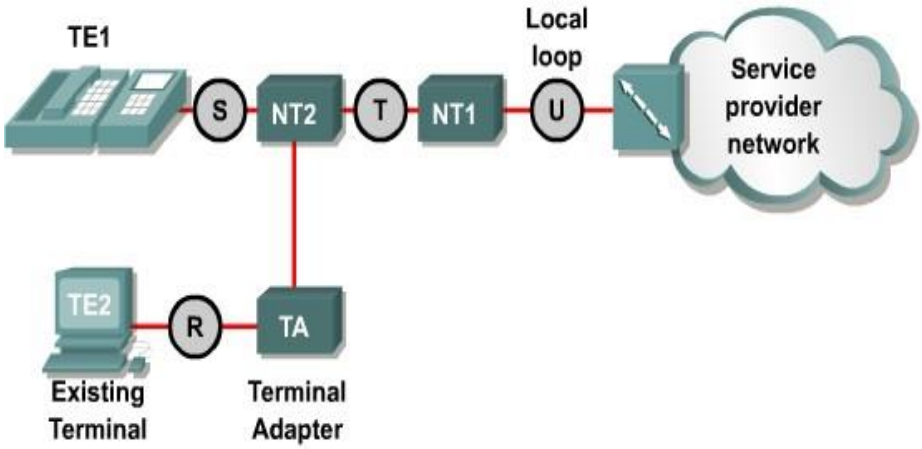
BRI can carry a wide and flexible range of communications. A single BRI, for example, can carry two simultaneous voice or data conversations (to the same or different locations). The D-channel can also be used for packet communications to a third location, also simultaneously.

PRI (Primary Rate Interface)

In North America and Japan, PRI offers twenty-three 64 kbps B channels and one 64 kbps D channel. A PRI offers the same service as a T1 or DS1 connection. In Europe and much of the rest of the world, PRI offers 30 B channels and one D channel in order to offer the same level of service as an E1 circuit. PRI uses a Data Service Unit/Channel Service Unit (DSU/CSU) for T1/E1 connections.



ISDN Reference Points



R: References the connection between a non-ISDN compatible device Terminal Equipment type 2 (TE2) and a Terminal Adapter (TA), for example an RS-232 serial interface.

S: References the points that connect into the customer switching device Network Termination type 2 (NT2) and enables calls between the various types of customer premises equipment.

T: Electrically identical to the S interface, it references the outbound connection from the NT2 to the ISDN network or Network Termination type 1 (NT1).

U: References the connection between the NT1 and the ISDN network owned by the telephone company.

Device	Device Type	Device Function
TE1	Terminal Equipment 1	Designates a device with a native ISDN interface, such as an ISDN router or ISDN telephone.
TE2	Terminal Equipment 2	Designates a non-ISDN device, such as a workstation or router, that requires a TA to connect to an ISDN service provider.
TA	Terminal Adapter	Converts EIA/TIA-232, V.35, and other signals into BRI signals.
NT2	Network Termination 2	The point at which all ISDN lines at a customer site are aggregated and switched using a customer switching device.
NT1	Network Termination 1	Controls the physical and electrical termination of the ISDN at the customer's premises. Converts the four-wire BRI signals into two-wire signals used by the ISDN digital line.

Public Switched Telephone Network (PSTN)

PSTN(Circuit Switch): PSTN is a circuit switched network is one where a dedicated connection (circuit or channel) must be set up between two nodes before they may communicate. For the duration of the communication, that connection may only be used by the same two nodes, and when the communication has ceased, the connection must be explicitly cancelled.

The basic digital circuit in the PSTN is a 64-kilobits-per-second channel, originally designed by Bell Labs, called a "DS0" or Digital Signal 0. To carry a typical phone call from a calling party to a called party, the audio sound is digitized at an 8 kHz sample rate using 8-bit pulse code modulation. The call is then transmitted from one end to another via telephone exchanges. The call is switched using a signaling protocol (SS7) between the telephone exchanges under an overall routing strategy.

PSTN, the Public Switched Telephone Network, is a circuit-switched network that is used primarily for voice communications worldwide, with more than 800 million subscribers. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital and also includes mobile as well as fixed telephones. The basic digital circuit in the PSTN is a 64-kilobit-per-second channel, known as "DS0" or Digital Signal 0. DS0's are also known as timeslots because they are multiplexed together in a time-division fashion. To carry a typical phone call from a calling party to a called party, the audio sound is digitized at an 8 kHz sample rate using 8-bit pulse code modulation. Multiple DS0's can be multiplexed together on higher capacity circuits, such that 24 DS0's make a DS1 signal or T1 (the European equivalent is an E1, containing 32 64 kbit/s channels). For more than a hundred years, the PSTN was the only bearer network available for telephony. Today, the mobile

telephone over wireless access network, which is carried through the PSTN trunking network, is becoming increasingly popular. Other bearer networks for voice transmission include integrated service digital network (ISDN), Digital Subscriber Line (DSL), Asynchronous Transfer Mode (ATM), frame relay and the Internet VOIP.

T-1 & E-1 Circuit:

T-1 is a digital circuit that uses the DS-1 (Digital Signaling level 1) signaling format to transmit voice/data over the PSTN network at 1.544 Mbps. T-1 can carry up to 24 uncompressed digital channels of 64 Kbps (DS0) for voice or data.

E-1 is the European equivalent of the T-1, except E-1 carries information at the rate of 2.048 Mbps. E-1 is used to transmit 30 64Kbps digital channels (DS0) for voice or data calls, plus a 64Kbps channel for signaling, and a 64Kbps channel for framing and maintenance.

A T1/E1 circuit is a dedicated circuit and is always composed of two parts: the local loop and the carrier circuit.

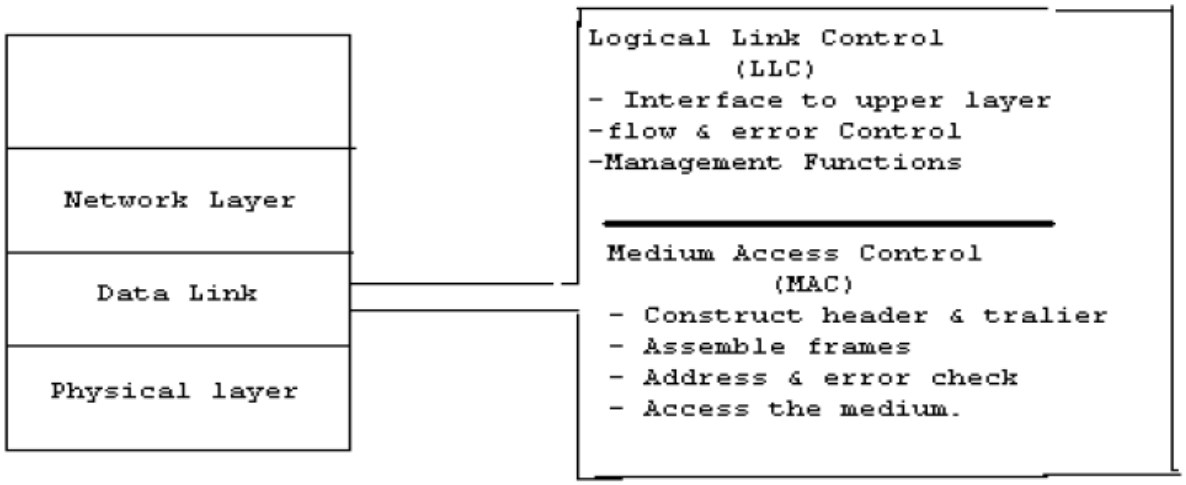
A T1/E1 circuit is the first multiplexed level of the digital signaling multiplexing scheme. T1s use what is called a Stratum 3 clock to maintain what is called clocking on the line.

Chapter 4

Data Link layers

The architecture of a LAN can be considered as a set of layered protocols.
In OSI terms, the higher layer protocols are totally independent of the LAN architecture. Hence, only lower order layers are considered for the design of LAN architecture.
The datalink layer of LAN is split into two sub layers.

I. Medium Access Control (MAC),
II. Logical Link Control Layer (LLC)



LLC Frame Format

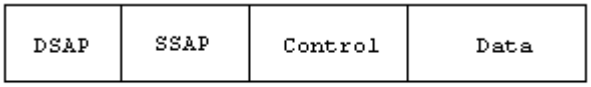


Fig :- LLC Frame Format

Destination Service Access Point (DSAP): IEEE 802.2 header begins with a 1 byte field, which identifies the receiving upper-layer process.

Source Service Access Point (SSAP): Following the DSAP address is the 1-byte address, which identifies the sending upper-layer process.

Control: The Control field employs three different formats, depending on the type of LLC frame used.

- Information (I) frame -- Carries upper-layer information and some control information.
- Supervisory (S) frame -- Provides control information. An S frame can request and suspend transmission, reports on status, and acknowledge receipt of I frames. S frames do not have an Information field.
- Unnumbered (U) frame -- Used for control purposes and is not sequenced. A U frame can be used to initialize secondaries. Depending on the function of the U frame, its Control field is 1 or 2 bytes. Some U frames have an Information field.

Data: Variable-length field bounded by the MAC format implemented. Usually contains IEEE 802.2 Subnetwork Access Protocol (SNAP) header information, as well as application-specific data.

MAC Frame Format

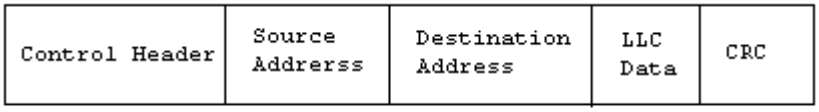


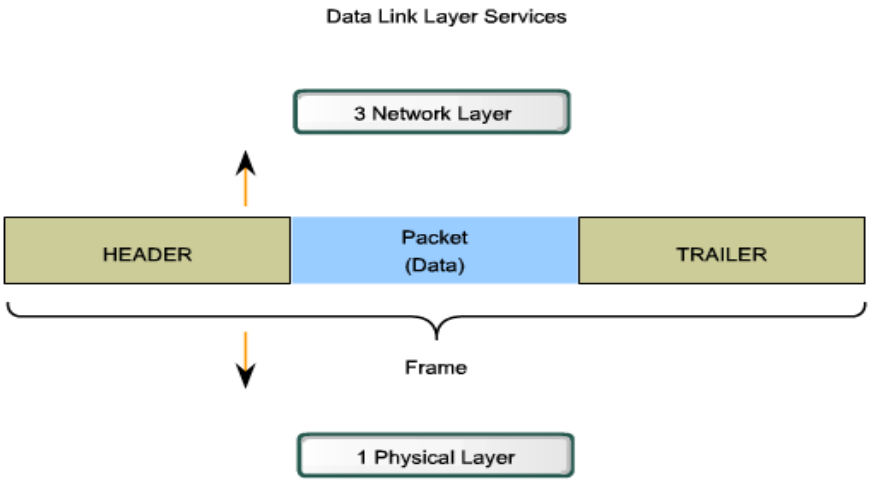
Fig : General MAC frame Format

Framing:

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. The Data Link layer prepares a packet for transport across the local media by encapsulating it with a header and a trailer to create a frame.

The Data Link layer frame includes:

- **Data** - The packet from the Network layer
- **Header** - Contains control information, such as addressing, and is located at the beginning of the PDU
- **Trailer** - Contains control information added to the end of the PDU



Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter. In addition, each envelope defines the sender and receiver addresses since the postal system is a many-to-many carrier facility. Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Fixed-Size Framing

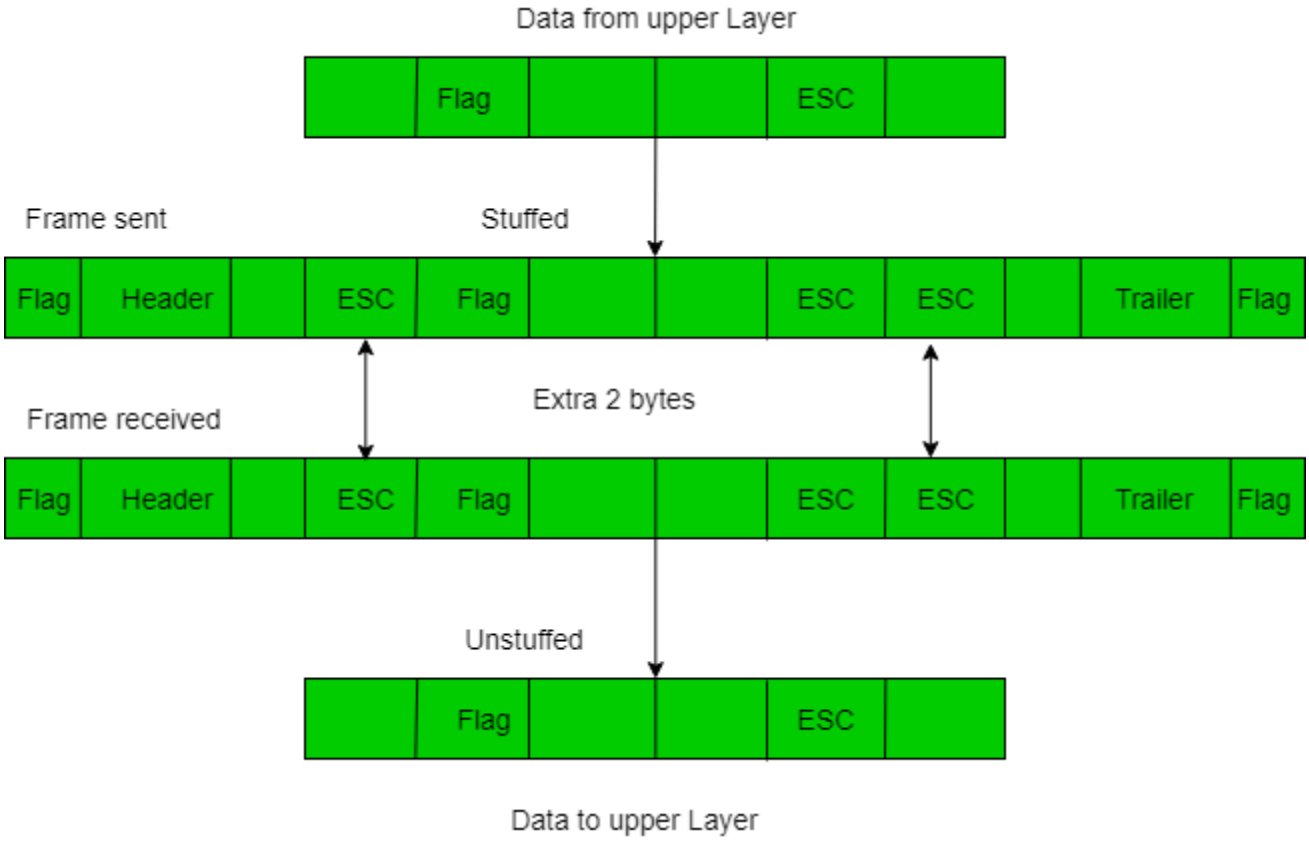
Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells.

Variable-Size Framing

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

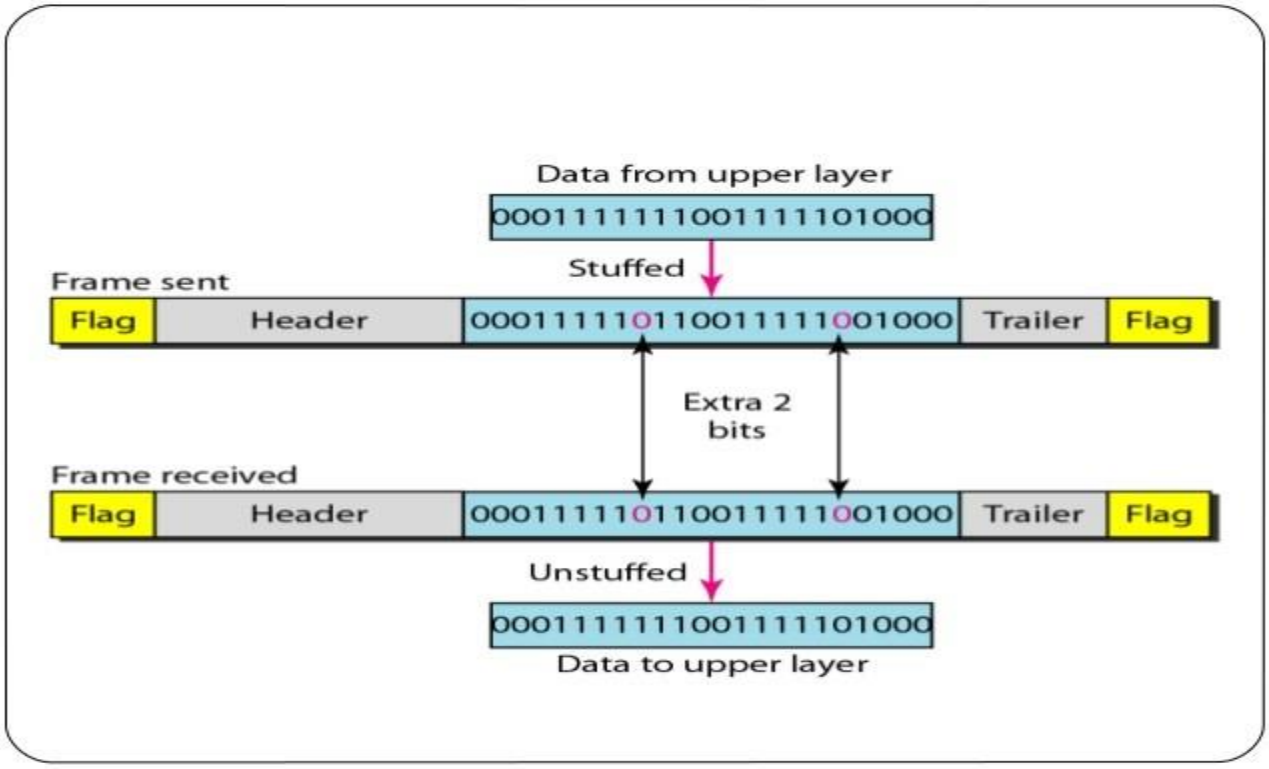
Character-Oriented Protocols

In a character-oriented protocol, data to be carried are 8-bit characters from a coding system such as ASCII. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits. To separate one frame from the next, an 8-bit (I-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame. Any pattern used for the flag could also be part of the information. To fix this problem, a byte-stuffing strategy was added to character-oriented framing. In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag. Character-oriented protocols present a problem in data communications. The universal coding systems in use today, such as Unicode, have 16-bit and 32-bit characters that conflict with 8-bit characters. We can say that in general, the tendency is moving toward the bit-oriented protocols that we discuss next.



Bit-Oriented Protocols

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



This flag can create the same type of problem we saw in the byte-oriented protocols. That is, if the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end of the frame. We do this by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag. The strategy is called bit stuffing. In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver. Note that the extra bit is added after one 0 followed by five 1s regardless of the value of the next bit. This guarantees that the flag field sequence does not inadvertently appear in the frame. This means that if the flag like pattern 01111110 appears in the data, it will change to 011111010 (stuffed) and is not mistaken as a flag by the receiver. The real flag 01111110 is not stuffed by the sender and is recognized by the receiver.

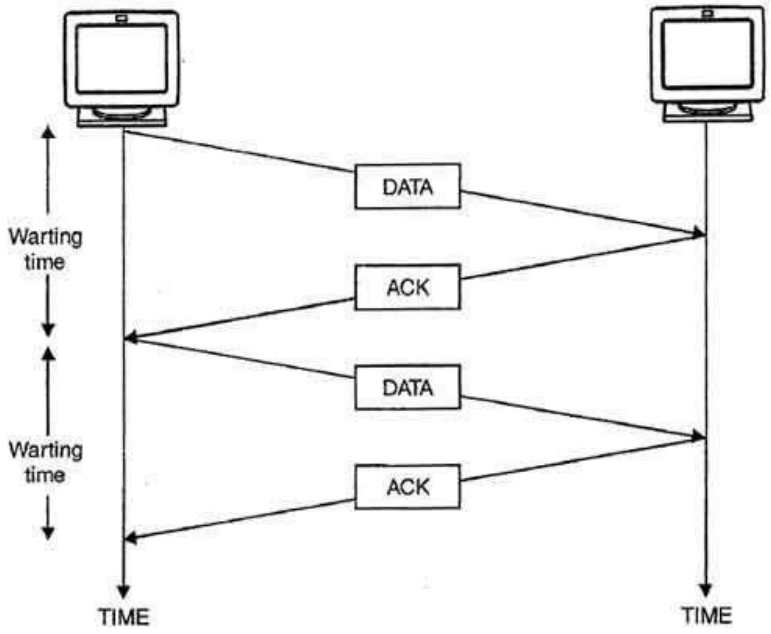
Flow Control

Flow Control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data should not be allowed to overwhelm the receiver. Receiver should also be able to inform the transmitter before its limits (this limit may be amount of memory used to store the incoming data or the processing power at the receiver end) are reached and the sender must send fewer frames. Hence, Flow control refers to the set of procedures used to restrict the amount of data the transmitter can send before waiting for acknowledgment.

There are two methods developed for flow control namely Stop-and-wait and Sliding-window.

Stop & Wait Protocol

- In this method of flow control, the sender sends a single frame to receiver & waits for an acknowledgment.
- The next frame is sent by sender only when acknowledgment of previous frame is received.
- This process of sending a frame & waiting for an acknowledgment continues as long as the sender has data to send.
- To end up the transmission sender transmits end of transmission (EOT) frame.
- The main advantage of stop & wait protocols is its accuracy. Next frame is transmitted only when the first frame is acknowledged. So there is no chance of frame being lost.
- The main disadvantage of this method is that it is inefficient. It makes the transmission process slow. In this method single frame travels from source to destination and single acknowledgment travels from destination to source. As a result each frame sent and received uses the entire time needed to traverse the link. Moreover, if two devices are distance apart, a lot of time is wasted waiting for ACKs that leads to increase in total transmission time.



Stop & Wait Method.

Sliding Window Protocol

- In sliding window method, multiple frames are sent by sender at a time before needing an acknowledgment.

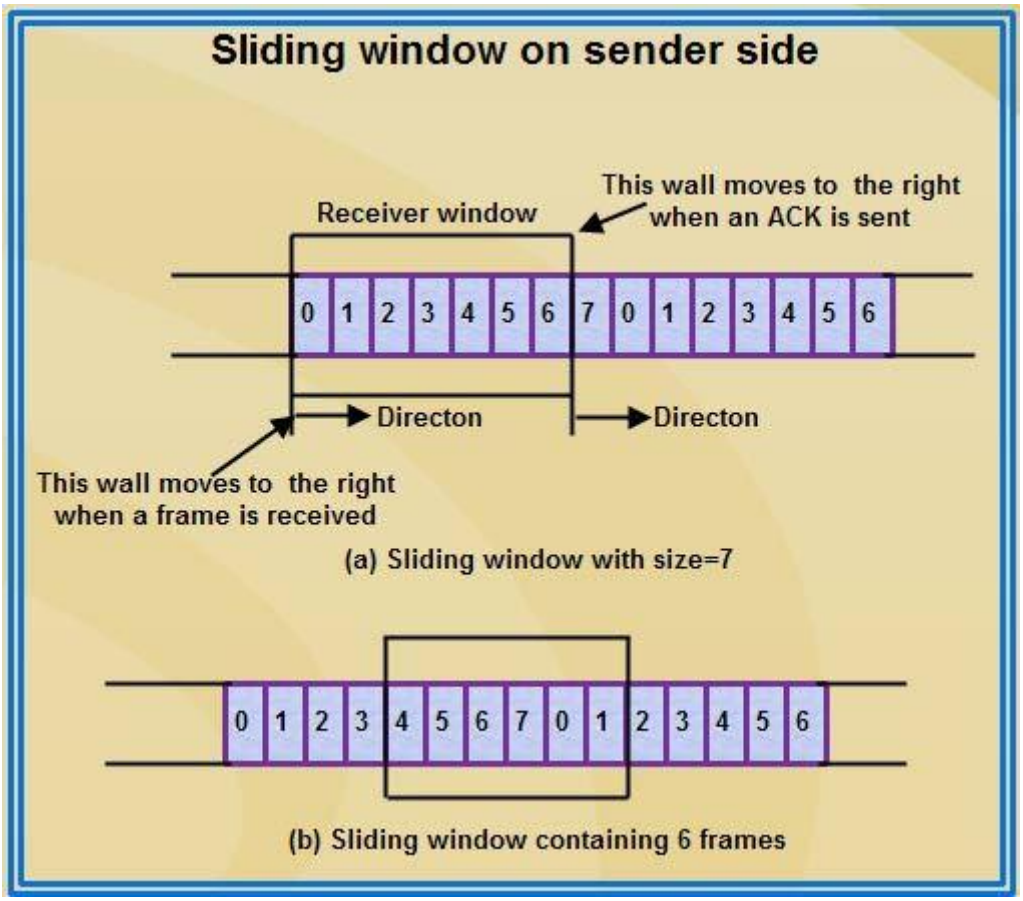
- Multiple frames sent by source are acknowledged by receiver using a single ACK frame.

Sliding Window

- Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.
- It provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.
- Frames may be acknowledged by receiver at any point even when window is not full on receiver side.
- Frames may be transmitted by source even when window is not yet full on sender side.
- The windows have a specific size in which the frames are numbered modulo- n, which means they are numbered from 0 to n-l. For e.g. if n = 8, the frames are numbered 0, 1,2,3,4,5,6, 7, 0, 1,2,3,4,5,6, 7, 0, 1, ...
- The size of window is n-1. For e.g. In this case it is 7. Therefore, a maximum of n-l frames may be sent before an acknowledgment.
- When the receiver sends an ACK, it includes the number of next frame it expects to receive. For example in order to acknowledge the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it comes to know that all the frames up to number 4 have been received.

Sliding Window on Sender Side

- At the beginning of a transmission, the sender's window contains n-l frames.
- As the frames are sent by source, the left boundary of the window moves inward, shrinking the size of window. This means if window size is w, if four frames are sent by source after the last acknowledgment, then the number of frames left in window is w-4.
- When the receiver sends an ACK, the source's window expand i.e. (right boundary moves outward) to allow in a number of new frames equal to the number of frames acknowledged by that ACK.
- For example, Let the window size is 7 (see diagram (a)), if frames 0 through 3 have been sent and no acknowledgment has been received, then the sender's window contains three frames - 4,5,6.
- Now, if an ACK numbered 3 is received by source, it means three frames (0, 1, 2) have been received by receiver and are undamaged.
- The sender's window will now expand to include the next three frames in its buffer. At this point the sender's window will contain six frames (4, 5, 6, 7, 0, 1). (See diagram (b)).

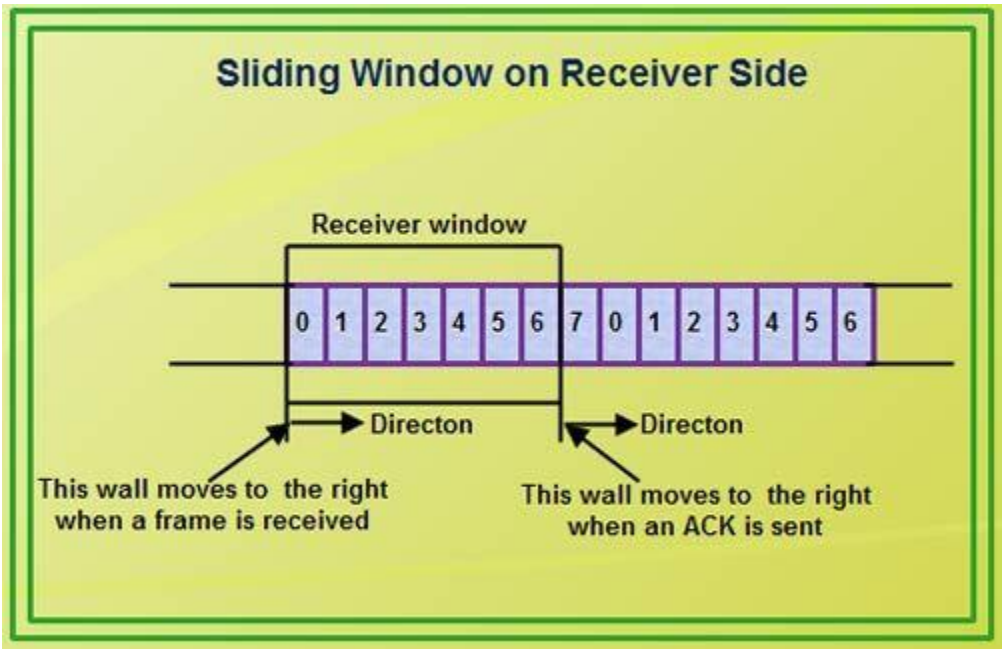


Sliding Window on Receiver Side

- At the beginning of transmission, the receiver's window contains n-1 spaces for frame but not the frames.
- As the new frames come in, the size of window shrinks.
- Therefore the receiver window represents not the number of frames received but the number of frames that may still be received without an acknowledgment ACK must

be sent.

- Given a window of size w, if three frames are received without an ACK being returned, the number of spaces in a window is w-3.
- As soon as acknowledgment is sent, window expands to include the number of frames equal to the number of frames acknowledged.
- For example, let the size of receiver's window is 7 as shown in diagram. It means window contains spaces for 7 frames.
- With the arrival of the first frame, the receiving window shrinks, moving the boundary from space 0 to 1. Now, window has shrunk by one, so the receiver may accept six more frame before it is required to send an ACK.
- If frames 0 through 3 have arrived but have DOC been acknowledged, the window will contain three frame spaces.
- As receiver sends an ACK, the window of the receiver expands to include as many new placeholders as newly acknowledged frames.
- The window expands to include a number of new frame spaces equal to the number of the most recently acknowledged frame minus the number of previously acknowledged frame. For e.g., If window size is 7 and if prior ACK was for frame 2 & the current ACK is for frame 5 the window expands by three (5-2).

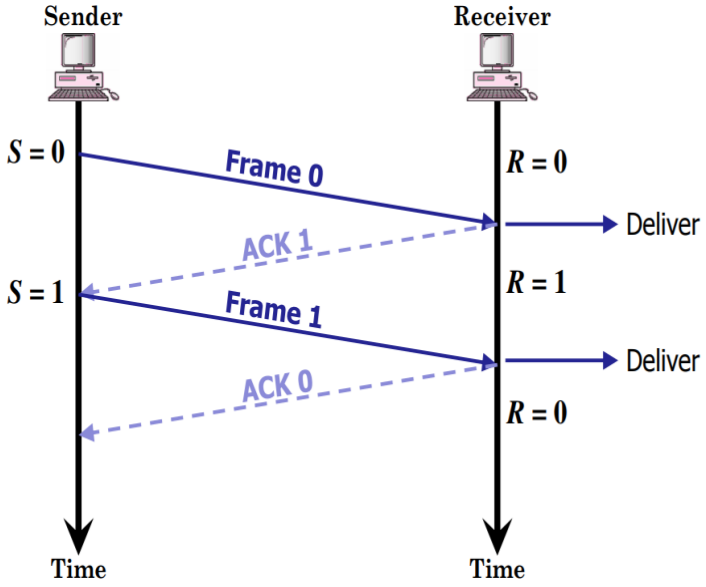


- Therefore, the sliding window of sender shrinks from left when frames of data are sending. The sliding window of the sender expands to right when acknowledgments are received.
- The sliding window of the receiver shrinks from left when frames of data are received. The sliding window of the receiver expands to the right when acknowledgement is sent.

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

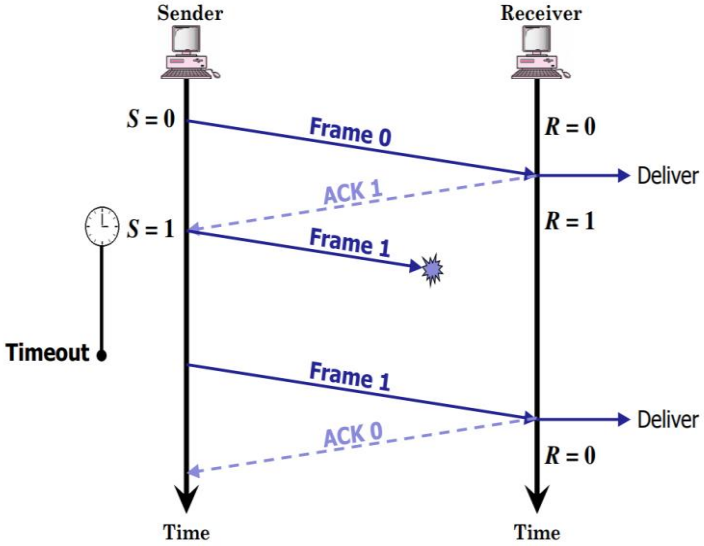
Stop-and-Wait ARQ

In Stop-and-Wait ARQ, which is simplest among all protocols, the sender (say station A) transmits a frame and then waits till it receives positive acknowledgement (ACK) or negative acknowledgement (NACK) from the receiver (say station B). Station B sends an ACK if the frame is received correctly, otherwise it sends NACK. Station A sends a new frame after receiving ACK; otherwise it retransmits the old frame, if it receives a NACK.

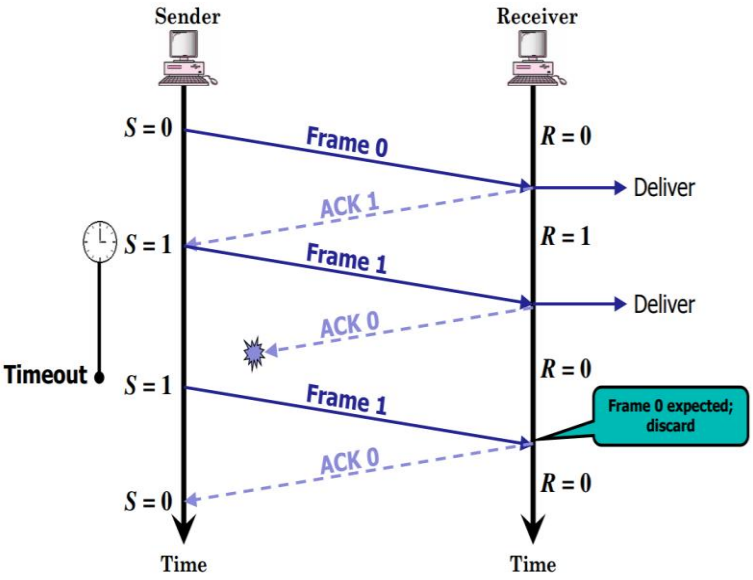


Normal operation

To tackle the problem of a lost or damaged frame, the sender is equipped with a timer. In case of a lost ACK, the sender transmits the old frame. The sender is unaware of this loss, but starts a timer after sending each PDU. Normally an ACK PDU is received before the timer expires. In this case no ACK is received, and the timer counts down to zero and triggers retransmission of the same PDU by the sender.



Lost Frame



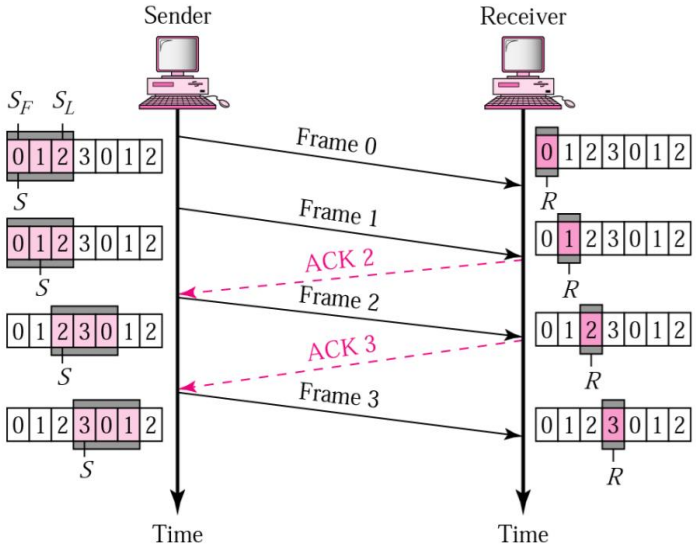
Lost ACK

The receiver now can identify that it has received a duplicate frame from the label of the frame and it is discarded.

The main advantage of stop-and-wait ARQ is its simplicity. It also requires minimum buffer size. However, it makes highly inefficient use of communication links.

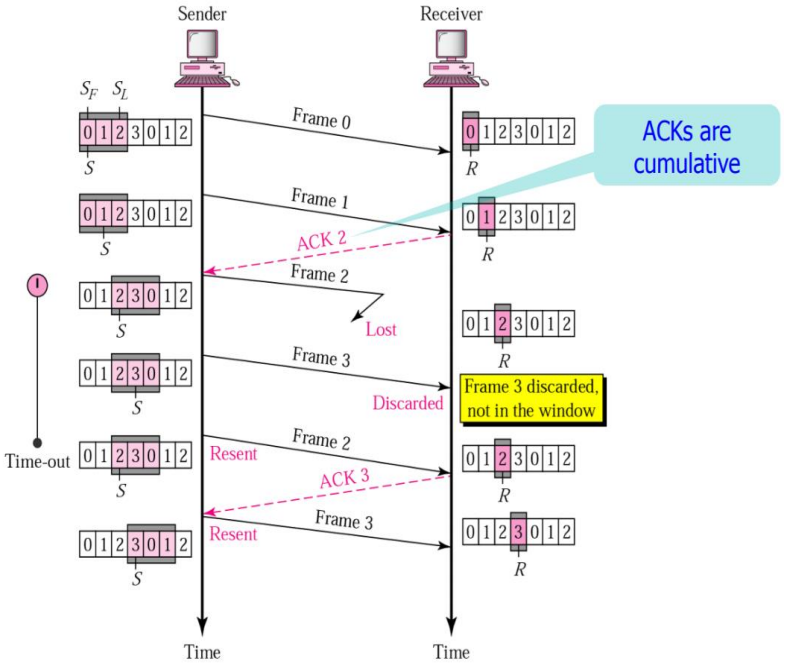
Go-back-N ARQ

The most popular ARQ protocol is the go-back-N ARQ, where the sender sends the frames continuously without waiting for acknowledgement. That is why it is also called as continuous ARQ. As the receiver receives the frames, it keeps on sending ACKs or a NACK, in case a frame is incorrectly received. When the sender receives a NACK, it retransmits the frame in error plus all the succeeding frames. Hence, the name of the protocol is go-back-N ARQ



Normal Operation

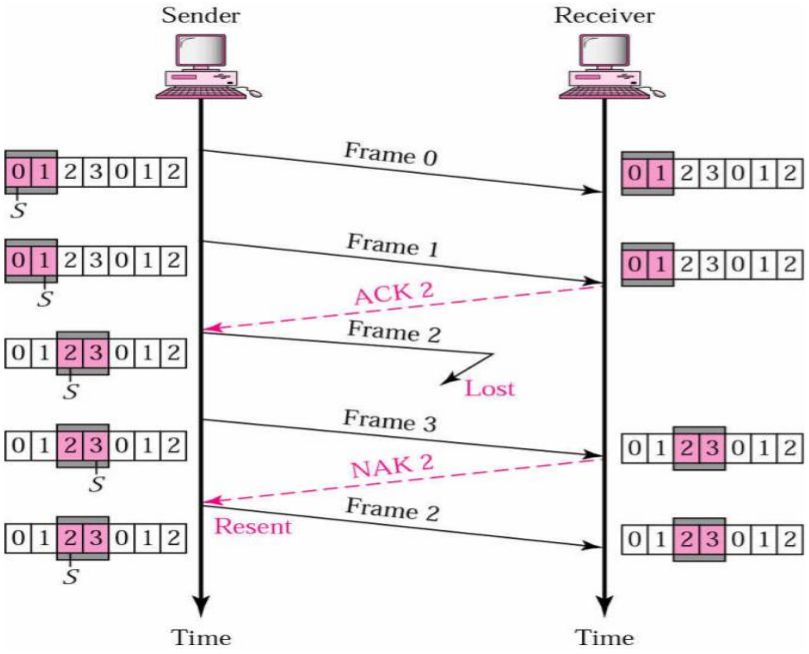
If a frame is lost, the receiver sends NAK after receiving the next frame. In case there is long delay before sending the NAK, the sender will resend the lost frame after its timer times out. If the ACK frame sent by the receiver is lost, the sender resends the frames after its timer times out



Lot Frame

Selective-Repeat ARQ

The selective-repetitive ARQ scheme retransmits only those for which NAKs are received or for which timer has expired. This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames. The receiver also must have storage space to store the post NAK frames and processing power to reinsert frames in proper sequence.



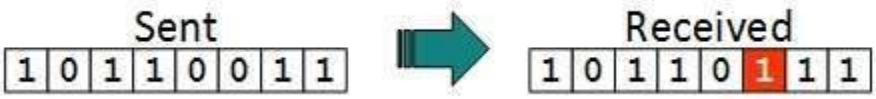
Error Control Mechanisms

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

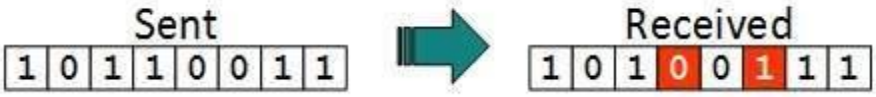
There may be three types of errors:

- **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 than one consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

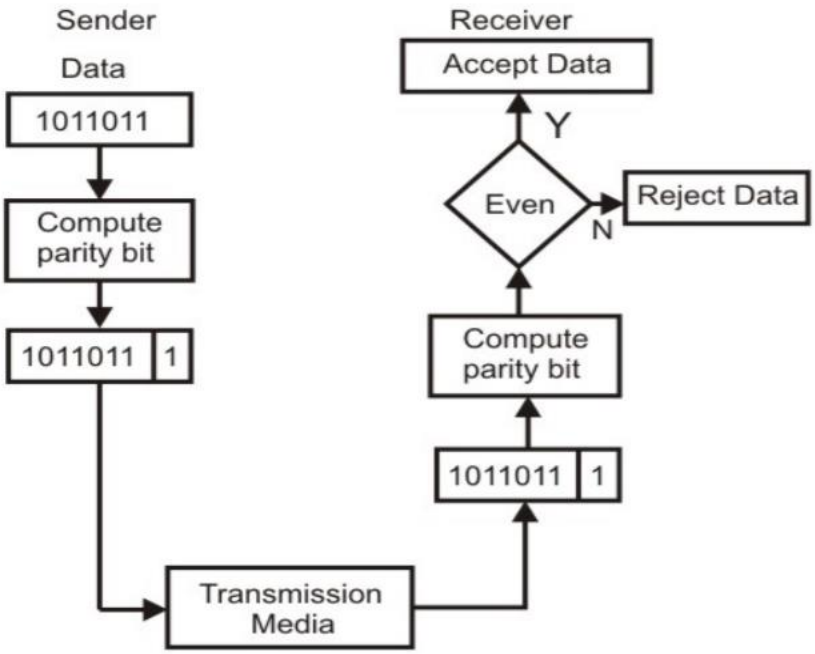
Error Detecting Codes
Basic approach used for error detection is the use of redundancy, where additional bits are added to facilitate detection and correction of errors. Popular techniques are:

- Simple Parity check
- Two-dimensional Parity check
- Cyclic redundancy check

Simple Parity Checking or One-dimension Parity Check

The most common and least expensive mechanism for error- detection is the simple parity check. In this technique, a redundant bit called parity bit, is appended to every data unit so that the number of 1s in the unit (including the parity becomes even).

Blocks of data from the source are subjected to a check bit or Parity bit generator form, where a parity of 1 is added to the block if it contains an odd number of 1's (ON bits) and 0 is added if it contains an even number of 1's. At the receiving end the parity bit is computed from the received data bits and compared with the received parity bit, as shown in figure. This scheme makes the total number of 1's even, that is why it is called even parity checking.



Even-parity checking scheme

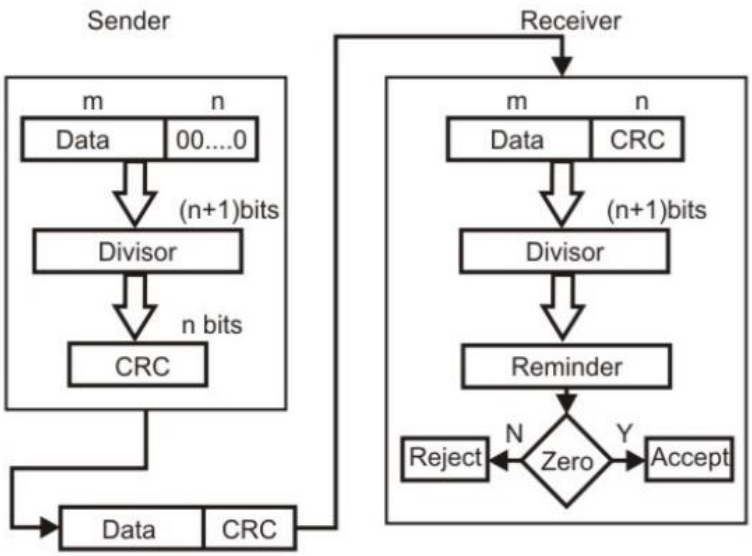
Performance

An observation of the table reveals that to move from one code word to another, at least two data bits should be changed. Hence these set of code words are said to have a minimum distance (hamming distance) of 2, which means that a receiver that has knowledge of the code word set can detect all single bit errors in each code word. However, if two errors occur in the code word, it becomes another valid member of the set and the decoder will see only another valid code word and know nothing of the error. Thus errors in more than one bit cannot be detected. In fact it can be shown that a single parity check code can detect only odd number of errors in a code word.

Cyclic Redundancy Checks (CRC)

This Cyclic Redundancy Check is the most powerful and easy to implement technique. Unlike checksum scheme, which is based on addition, CRC is based on binary division. In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

The generalized technique can be explained as follows. If a k bit message is to be transmitted, the transmitter generates an r-bit sequence, known as Frame Check Sequence (FCS) so that the (k+r) bits are actually being transmitted. Now this r-bit FCS is generated by dividing the original number, appended by r zeros, by a predetermined number. This number, which is (r+1) bit in length, can also be considered as the coefficients of a polynomial, called Generator Polynomial. The remainder of this division process generates the r-bit FCS. On receiving the packet, the receiver divides the (k+r) bit frame by the same predetermined number and if it produces no remainder, it can be assumed that no error has occurred during the transmission. Operations at both the sender and receiver end are shown in figure.



Basic scheme for Cyclic Redundancy Checking

This mathematical operation performed is illustrated in figure by dividing a sample 4- bit number by the coefficient of the generator polynomial x3 +x+1, which is 1011, using the modulo-2 arithmetic. Modulo-2 arithmetic is a binary addition process without any carry over, which is just the Exclusive-OR operation. Consider the case where k=1101. Hence we have to divide 1101000 (i.e. k appended by 3 zeros) by 1011, which produces the remainder r=001, so that the bit frame (k+r) =1101001 is actually being transmitted through the communication channel. At the receiving end, if the received number, i.e., 1101001 is divided by the same generator polynomial 1011 to get the remainder as 000, it can be assumed that the data is free of errors.

```
          1 1 1 1   <-- k
      ____________
1011 | 1 1 0 1 0 0 0
       1 0 1 1
       -------
         1 1 0 0
         1 0 1 1
         -------
           1 1 1 0
           1 0 1 1
           -------
             1 0 1 0
             1 0 1 1
             -------
               0 0 1   <-- r
```

Performance

CRC is a very effective error detection technique. If the divisor is chosen according to the previously mentioned rules, its performance can be summarized as follows:

- CRC can detect all single-bit errors
- CRC can detect all double-bit errors (three 1's)
- CRC can detect any odd number of errors (X+1)
- CRC can detect all burst errors of less than the degree of the polynomial.
- CRC detects most of the larger burst errors with a high probability.
- For example CRC-12 detects 99.97% of errors with a length 12 or more.

Error Correcting Codes

Error Correction can be handled in two ways.

- One is when an error is discovered; the receiver can have the sender retransmit the entire data unit. This is known as backward error correction.
- In the other, receiver can use an error-correcting code, which automatically corrects certain errors. This is known as forward error correction.

Hamming Codes

The most common types of error-correcting codes used in RAM are based on the codes devised by R. W. Hamming. In the Hamming code, k parity bits are added to an n-bit data word, forming a new word of n+k bits. The bit positions are numbered in sequence from 1 to n+k. Those positions numbered with powers of two are reserved for the parity bits. The remaining bits are the data bits. The code can be used with words of any length.

General Algorithm of Hamming code

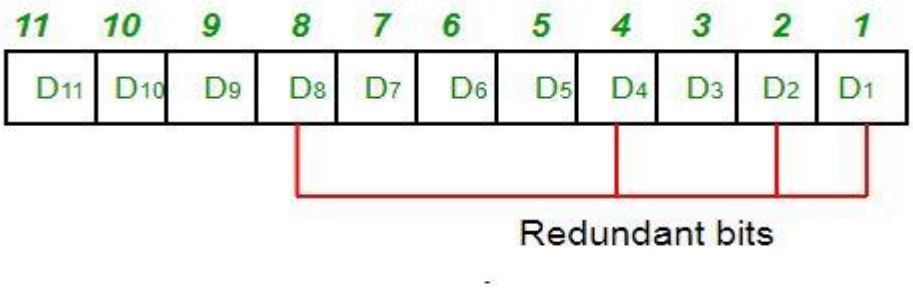
The Hamming Code is simply the use of extra parity bits to allow the identification of an error.

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

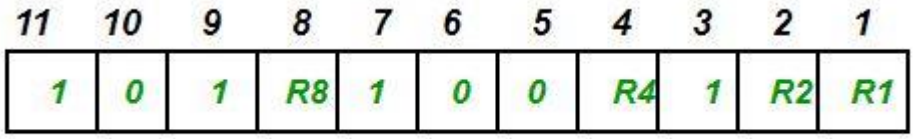
Determining the position of redundant bits

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

1. The number of data bits = 7
2. The number of redundant bits = 4
3. The total number of bits = 11
4. The redundant bits are placed at positions corresponding to power of 2: 1, 2, 4, and 8

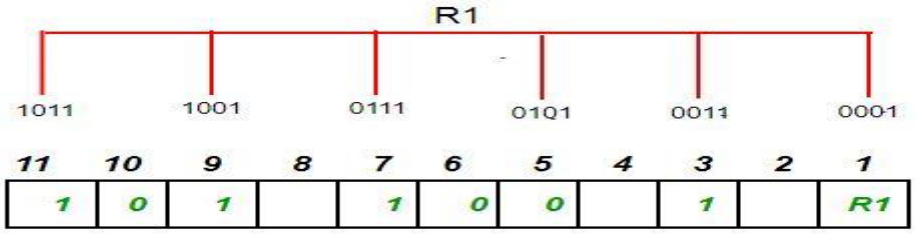


Suppose the data to be transmitted is 1011001, the bits will be placed as follows:



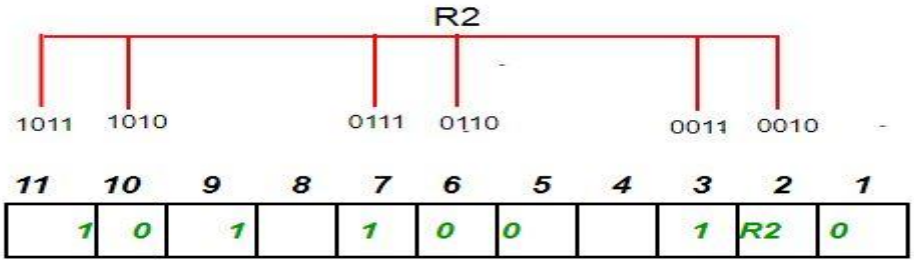
Determining the Parity bits –

1. R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.
   R1: bits 1, 3, 5, 7, 9, 11



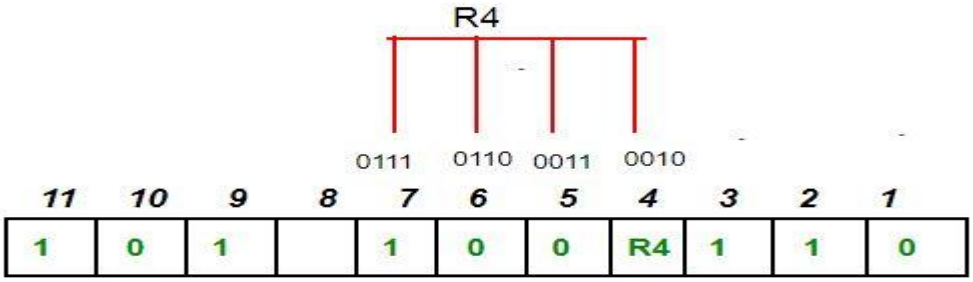
   To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0

2. R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.
   R2: bits 2,3,6,7,10,11



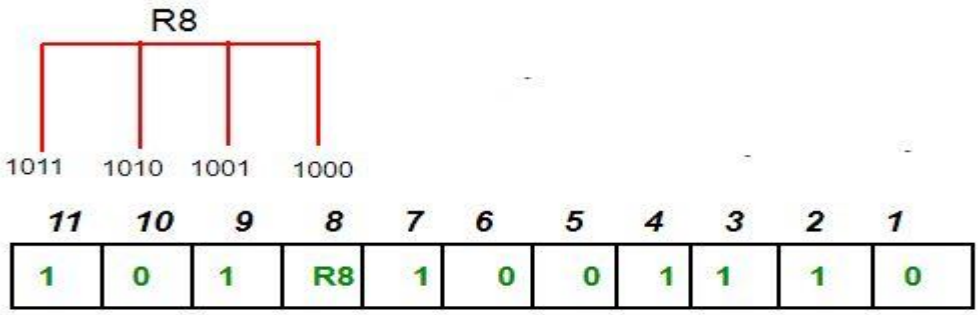
   To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is an odd number the value of R2(parity bit's value)=1

3. R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit.
   R4: bits 4, 5, 6, 7



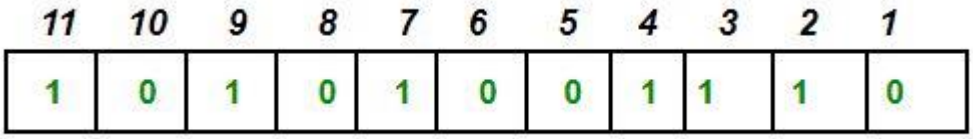
To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is an odd number the value of R4(parity bit's value) = 1

4. R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.
   R8: bit 8,9,10,11



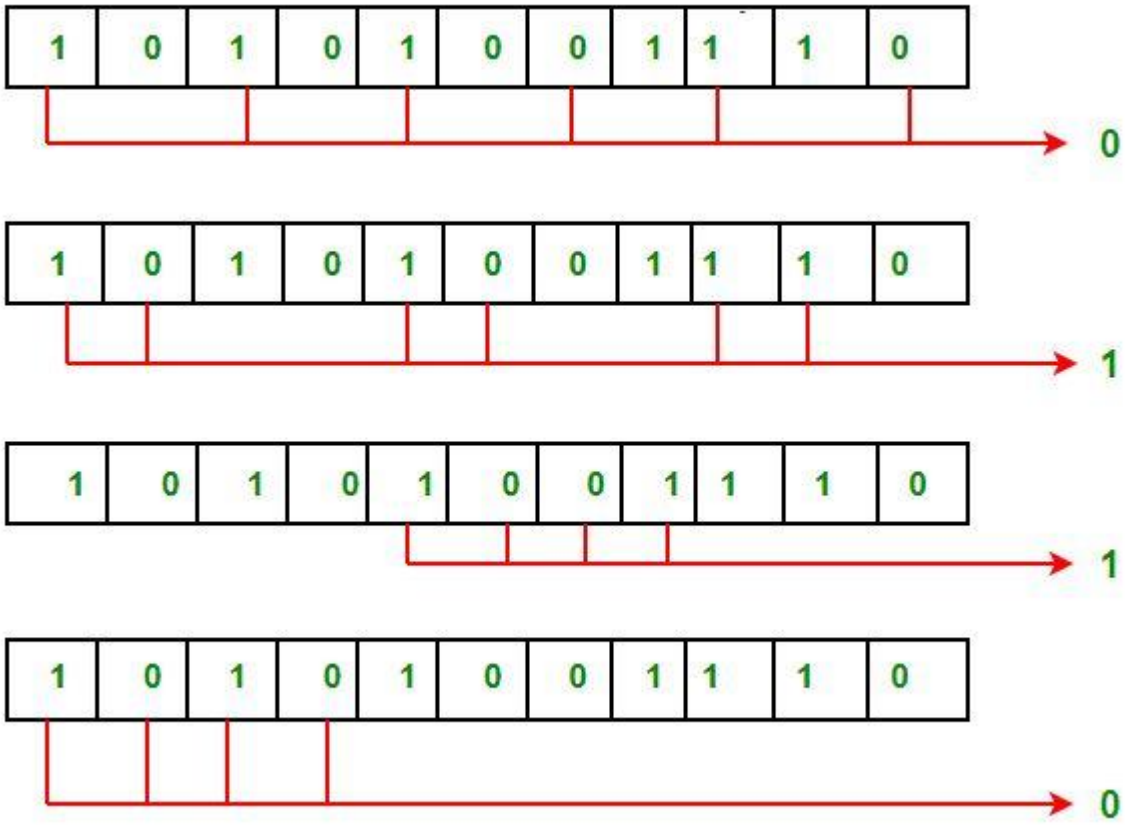
To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8(parity bit's value)=0.

Thus, the data transferred is:



Error detection and correction

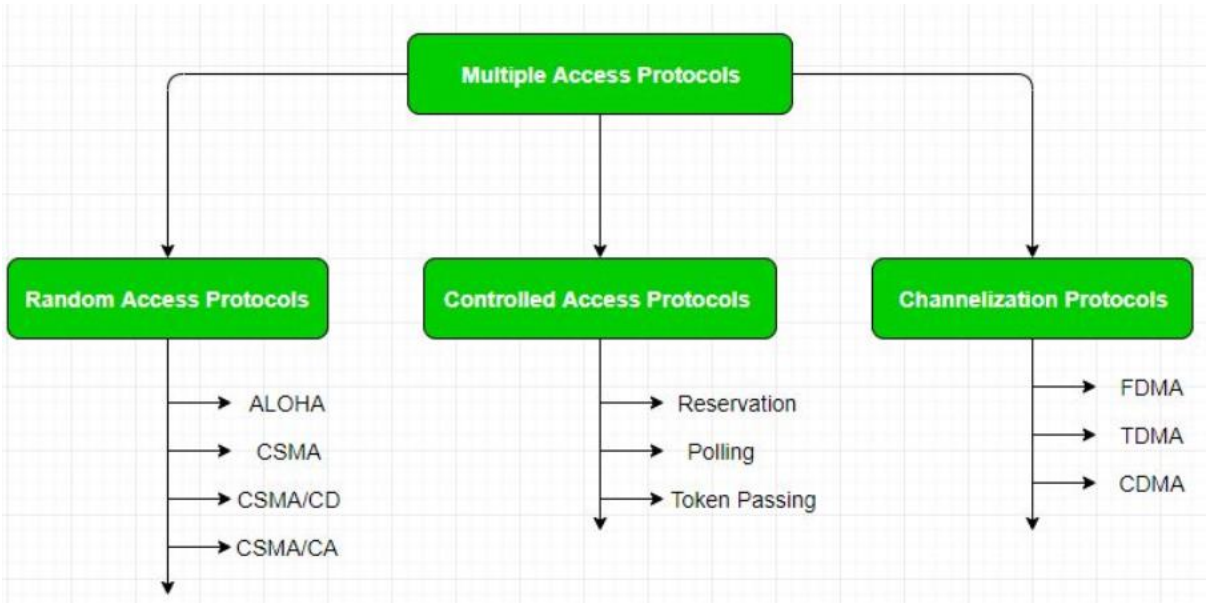
Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then it gives new parity values in the binary number:



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

Multiple Access Control

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created (data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.
Thus, protocols are required for sharing data on non-dedicated channels. Multiple access protocols can be subdivided further as –



Random Access Protocol
In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state (idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

1. ALOHA
2. CSMA
    - CSMA/CD
    - CSMA/CA

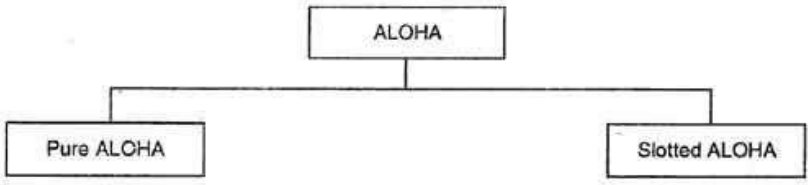
ALOHA

ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node

transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted. Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision.

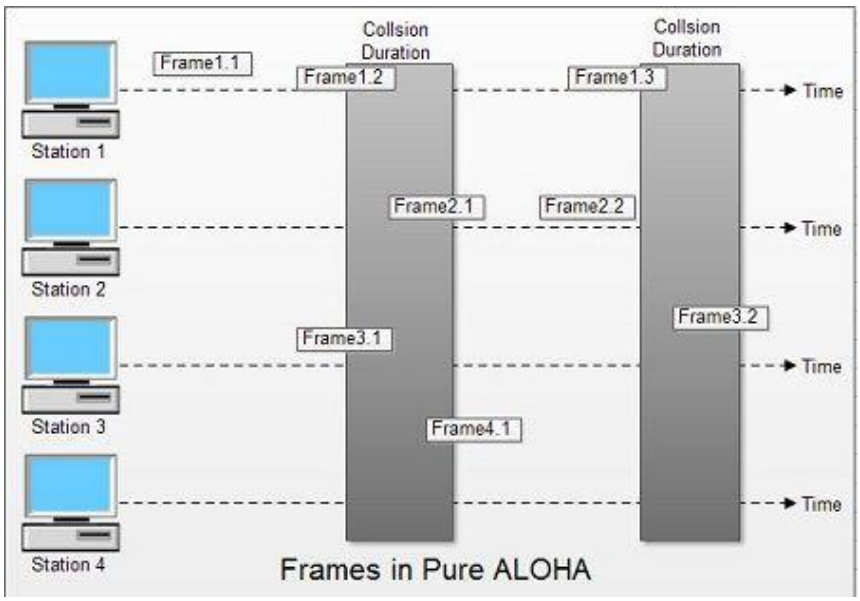
There are two different versions of ALOHA



Types of ALOHA

Pure ALOHA

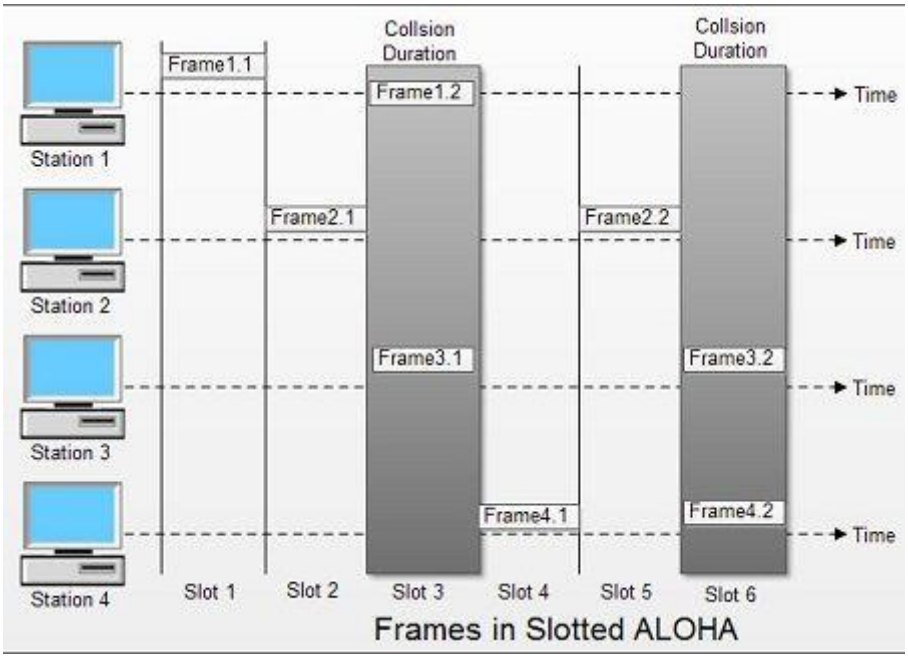
- In pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.
- Figure shows an example of frame collisions in pure ALOHA.



- In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.
- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

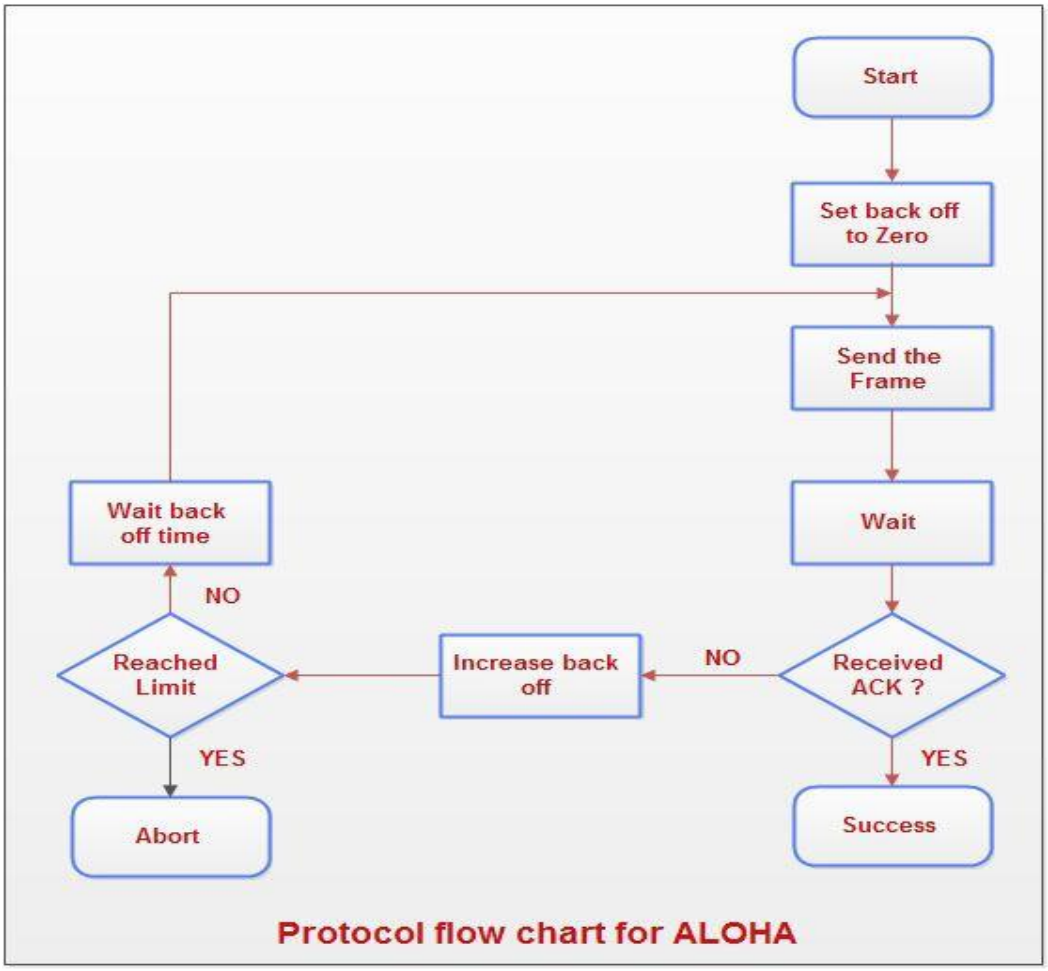
Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.



- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half

Protocol Flow Chart for ALOHA



Explanation:

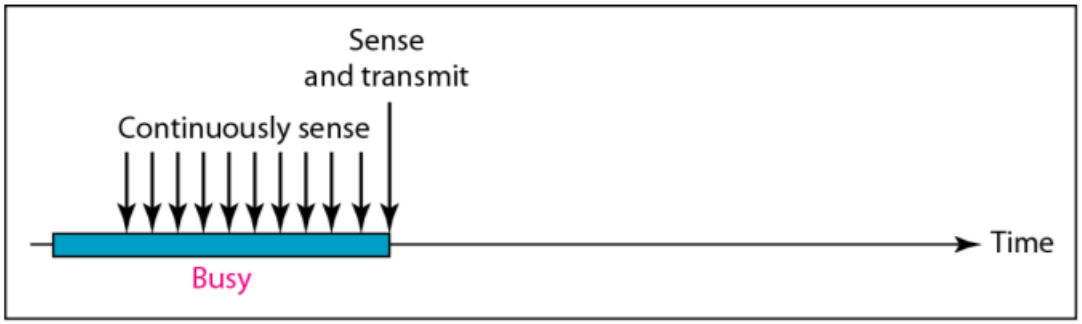
- A station which has a frame ready will send it.
- Then it waits for some time.
- If it receives the acknowledgement then the transmission is successful.
- Otherwise the station uses a backoff strategy, and sends the packet again.
- After many times if there is no acknowledgement then the station aborts the idea of transmission.

Carrier Sense Multiple Access (CSMA)

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. CSMA requires that each station first listen to the medium (or check the state of the medium) before sending. it is based on the principle "sense before transmit". CSMA can reduce the possibility of collision, but it cannot eliminate it. The possibility of collision still exists because of propagation delay.

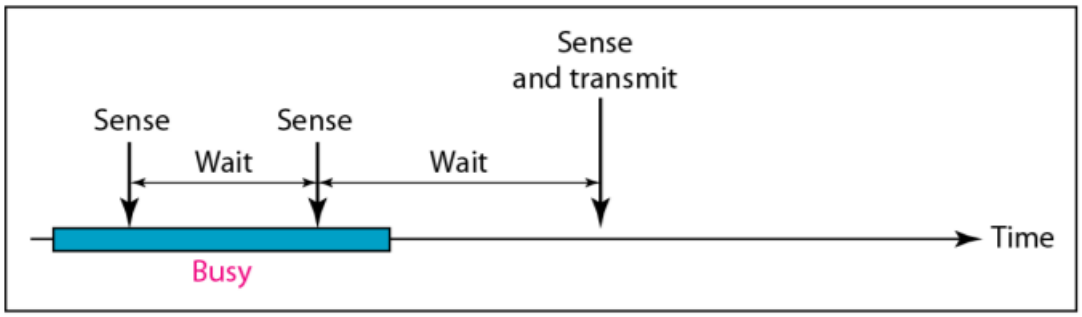
What should a station do if the channel is busy or idle? Three methods have been devised are:

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



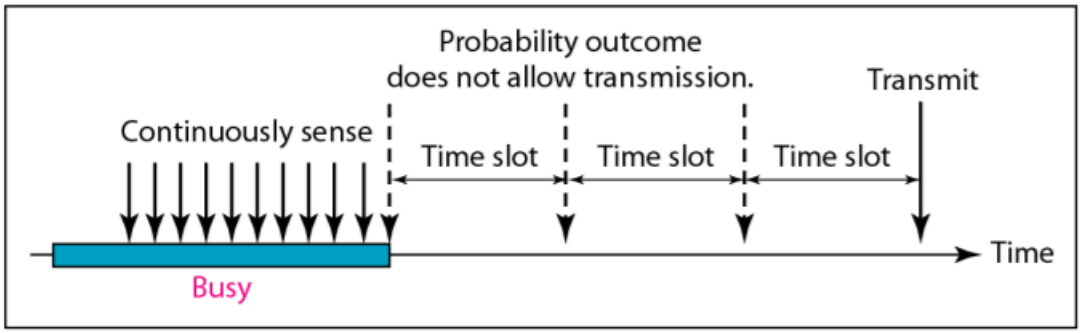
a. 1-persistent

2. **Nonpersistent**: In the nonpersistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.



b. Nonpersistent

3. **P-Persistent**: The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. ν The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.



c. p-persistent

CSMA/CD

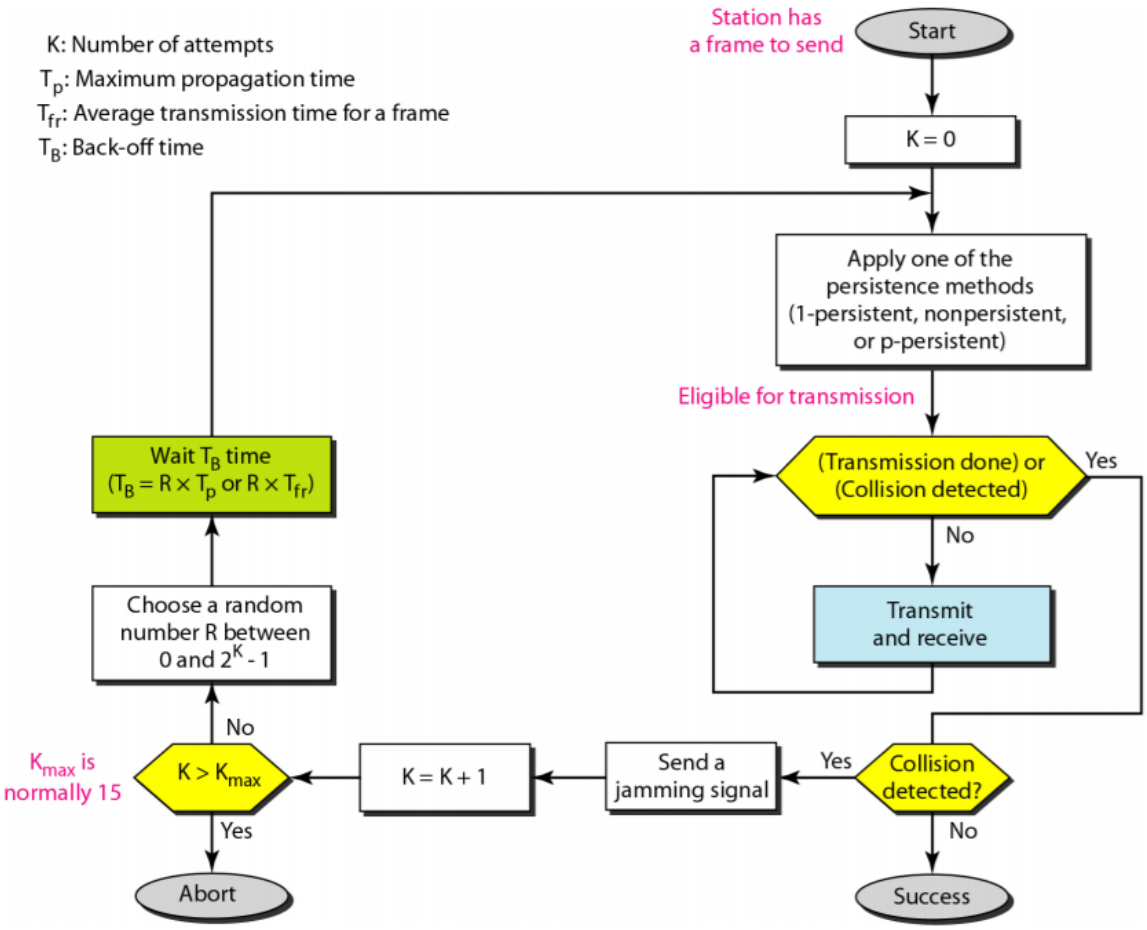
CSMA/CD protocol can be considered as a refinement over the CSMA scheme. It has evolved to overcome one glaring inefficiency of CSMA. In CSMA scheme, when two packets collide the channel remains unutilized for the entire duration of transmission time of both the packets. If the propagation time is small (which is usually the case) compared to the packet transmission time, wasted channel capacity can be considerable. This wastage of channel capacity can be reduced if the nodes continue to monitor the channel while transmitting a packet and immediately cease transmission when collision is detected. This refined scheme is known as Carrier Sensed Multiple Access with Collision Detection (CSMA/CD) or Listen-While-Talk.

On top of the CSMA, the following rules are added to convert it into CSMA/CD:

I. If a collision is detected during transmission of a packet, the node immediately ceases transmission and it transmits jamming signal for a brief duration to ensure that all stations know that collision has occurred.

II. After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed.

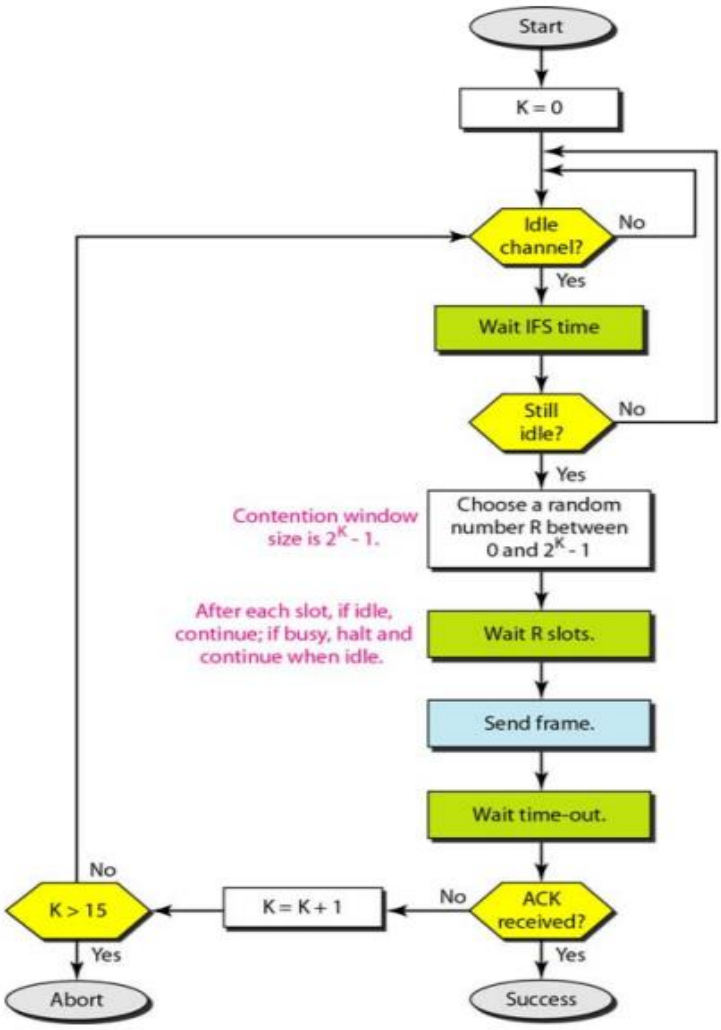
Flow diagram for the CSMA/CD



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

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a protocol for carrier transmission in networks. Unlike CSMA/CD (Carrier Sense Multiple Access/Collision Detect) which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen. In CSMA/CA, as soon as a node receives a packet that is to be sent, it checks to be sure the channel is clear (no other node is transmitting at the time). If the channel is clear, then the packet is sent. If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear. This period of time is called the backoff factor, and is counted down by a backoff counter. If the channel is clear when the backoff counter reaches zero, the node transmits the packet. If the channel is not clear when the backoff counter reaches zero, the backoff factor is set again, and the process is repeated.

Flow diagram for the CSMA/CD



Chapter 5
Network/Internet Layer Protocols and Addressing

IP Address:

Each computer in a TCP/IP network must be given a unique identifier, or IP address. This address, which operates at Layer 3, allows one computer to locate another computer on a network. All computers also have a unique physical address, which is known as a MAC address. These are assigned by the manufacturer of the NIC. MAC addresses operate at Layer 2 of the OSI model.

An IP address (IPv4) is a 32-bit sequence of ones and zeros. To make the IP address easier to work with, it is usually written as four decimal numbers separated by periods. For example, an IP address of one computer is 192.168.1.2. Another computer might have the address 128.10.2.1. This is called the dotted decimal format. Each part of the address is called an octet because it is made up of eight binary digits. For example, the IP address 192.168.1.8 would be 11000000.10101000.00000001.00001000 in binary notation. The dotted decimal notation is an easier method to understand than the binary ones and zeros method. This dotted decimal notation also prevents a large number of transposition errors that would result if only the binary numbers were used.

Ipv4 Header:

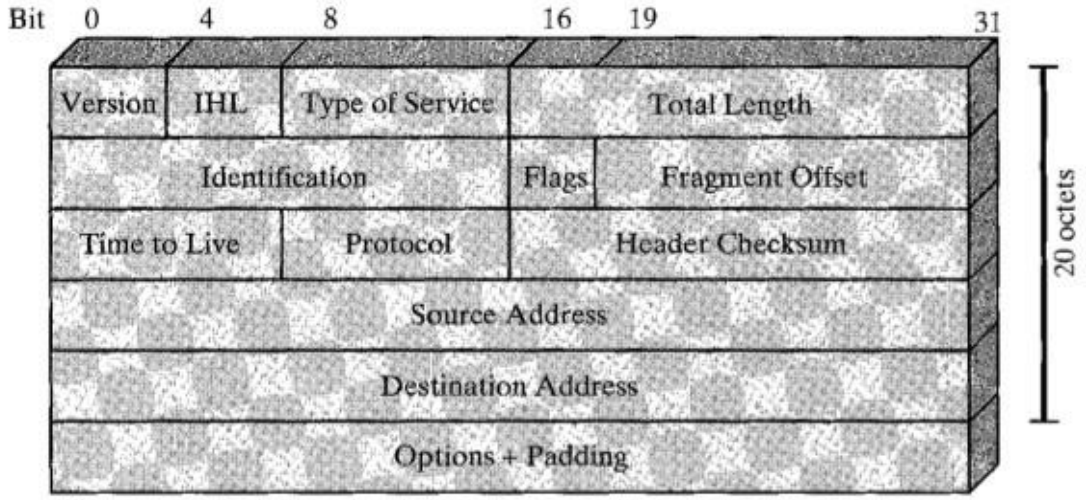


Fig: IPV4 Header

- **Version (4 bits):** Indicates the version number, to allow evolution of the protocol.
- **Internet Header Length (IHL 4 bits):** Length of header in 32 bit words. The minimum value is five for a minimum header length of 20 octets.
- **Type-of-Service:** The Type-of-Service field contains an 8-bit binary value that is used to determine the priority of each packet. This value enables a Quality-of-Service (QoS) mechanism to be applied to high priority packets, such as those carrying telephony voice data. The router processing the packets can be configured to decide which packet it is to forward first base on the Type-of-Service value.
- **Total length:** Total datagram length, in octets.
- **Identifier (16 bits):** A sequence number that, together with the source address, destination address, and user protocol, is intended to uniquely identify a datagram. Thus, the identifier should be unique for the datagram's source address, destination address, and user protocol for the time during which the datagram will remain in the internet.
- **Fragment Offset:** A router may have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU. When fragmentation occurs, the IPv4 packet uses the Fragment Offset field and the MF flag in the IP header to reconstruct the packet when it arrives at the destination host. The fragment offset field identifies the order in which to place the packet fragment in the reconstruction.
- **Flags(3 bits):** Only two of the bits are currently defined: MF(More Fragments) and DF(Don't Fragment):
- **More Fragments flag (MF):** The More Fragments (MF) flag is a single bit in the Flag field used with the Fragment Offset for the fragmentation and reconstruction of packets. The More Fragments flag bit is set; it means that it is not the last fragment of a packet. When a receiving host sees a packet arrive with the MF = 1, it examines the Fragment Offset to see where this fragment is to be placed in the reconstructed packet. When a receiving host receives a frame with the MF = 0 and a non-zero value in the Fragment offset, it places that fragment as the last part of the reconstructed packet. An unfragmented packet has all zero fragmentation information (MF = 0, fragment offset =0).
- **Don't Fragment flag (DF):** The Don't Fragment (DF) flag is a single bit in the Flag field that indicates that fragmentation of the packet is not allowed. If the Don't Fragment flag bit is set, then fragmentation of this packet is NOT permitted. If a router needs to fragment a packet to allow it to be passed downward to the Data Link layer but the DF bit is set to 1, then the router will discard this packet.
- **IP Destination Address**: The IP Destination Address field contains a 32-bit binary value that represents the packet destination Network layer host address.
- **IP Source Address**: The IP Source Address field contains a 32-bit binary value that represents the packet source Network layer host address.
- **Time-to-Live:** The Time-to-Live (TTL) is an 8-bit binary value that indicates the remaining "life" of the packet. The TTL value is decreased by at least one each time the packet is processed by a router (that is, each hop). When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow. This mechanism prevents packets that cannot reach their destination from being forwarded indefinitely between routers in a routing loop. If routing loops were permitted to continue, the network would become congested with data packets that will never reach their destination. Decrementing the TTL value at each hop ensures that it eventually becomes zero and that the packet with the expired TTL field will be dropped.

- **Protocol:** This 8-bit binary value indicates the data payload type that the packet is carrying. The Protocol field enables the Network layer to pass the data to the appropriate upper-layer protocol.
  Example values are:
  01 ICMP
  06 TCP
  17 UDP
- **Header checksum (16 bits):** An error-detecting code applied to the header only. Because some header fields may change during transit (e.g., time to live, segmentation-related fields), this is reverified and recomputed at each router. The checksum field is the 16-bit one's complement addition of all 16-bit words in the header. For purposes of computation, the checksum field is itself initialized to a value of zero.
- **Options (variable):** Encodes the options requested by the sending user.
- **Padding (variable):** Used to ensure that the datagram header is a multiple of 32 bits.
- **Data (variable):** The data field must be an integer multiple of 8 bits. The maximum length of the datagram (data field plus header) is 65,535 octets.

IP addresses are divided into class:

IP Address Class	First Octet Address Range	Used for
Class A	0-127	Unicast (Very large Network)
Class B	128-191	Unicast (Medium to Large Network)
Class C	192-223	Unicast (Small Network)
Class D	224-239	Multicast
Class E	240-255	Reserved

Class A Blocks
A class A address block was designed to support extremely large networks with more than 16 million host addresses. Class A IPv4 addresses used a fixed /8 prefix with the first octet to indicate the network address. The remaining three octets were used for host addresses.

The first bit of a Class A address is always 0. With that first bit a 0, the lowest number that can be represented is 00000000, decimal 0. The highest number that can be represented is 01111111, decimal 127. The numbers 0 and 127 are reserved and cannot be used as network addresses. Any address that starts with a value between 1 and 126 in the first octet is a Class A address.

No. of Class A Network: 2^7
No. of Usable Host address per Network: 2^{24}-2 (Minus 2 because 2 addresses are reserved for network and broadcast address)

Class B Blocks
Class B address space was designed to support the needs of moderate to large size networks with more than 65,000 hosts. A class B IP address used the two high-order octets to indicate the network address. The other two octets specified host addresses. As with class A, address space for the remaining address classes needed to be reserved.

The first two bits of the first octet of a Class B address are always 10. The remaining six bits may be populated with either 1s or 0s. Therefore, the lowest number that can be represented

with a Class B address is 10000000, decimal 128. The highest number that can be represented is 10111111, decimal 191. Any address that starts with a value in the range of 128 to 191 in the first octet is a Class B address.

No of Class B Network: 2^{14}

No. of Usable Host address per Network: 2^{16}-2

Class C Blocks:
The class C address space was the most commonly available of the historic address classes. This address space was intended to provide addresses for small networks with a maximum of 254 hosts. Class C address blocks used a /24 prefix. This meant that a class C network used only the last octet as host addresses with the three high-order octets used to indicate the network address.

A Class C address begins with binary 110. Therefore, the lowest number that can be represented is 11000000, decimal 192. The highest number that can be represented is 11011111, decimal 223. If an address contains a number in the range of 192 to 223 in the first octet, it is a Class C address.

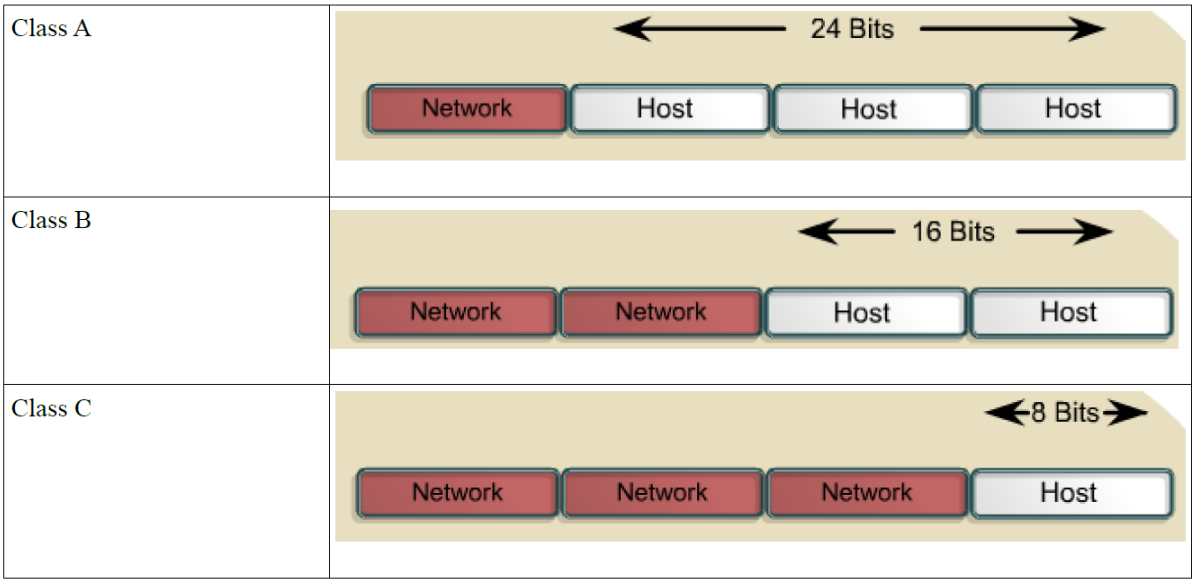
No of Class C Network: 2^{21}
No. of Usable Host address per Network: 2^{8}-2

Class D Blocks:
The Class D address class was created to enable multicasting in an IP address. A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses. Therefore, a single station can simultaneously transmit a single stream of data to multiple recipients.

The Class D address space, much like the other address spaces, is mathematically constrained. The first four bits of a Class D address must be 1110. Therefore, the first octet range for Class D addresses is 11100000 to 11101111, or 224 to 239. An IP address that starts with a value in the range of 224 to 239 in the first octet is a Class D address.

Class E Block:
A Class E address has been defined. However, the Internet Engineering Task Force (IETF) reserves these addresses for its own research. Therefore, no Class E addresses have been released for use in the Internet. The first four bits of a Class E address are always set to 1s. Therefore, the first octet range for Class E addresses is 11110000 to 11111111, or 240 to 255.

Every IP address also has two parts. The first part identifies the network (Network ID) where the system is connected and the second part identifies the system (Host ID).



Within the address range of each IPv4 network, we have three types of addresses:

- Network address - The address by which we refer to the network
- Broadcast address - A special address used to send data to all hosts in the network
- Host addresses - The addresses assigned to the end devices in the network

Special Ipv4 addresses:

- **Default Route:** we represent the IPv4 default route as 0.0.0.0. The default route is used as a "catch all" route when a more specific route is not available. The use of this address also reserves all addresses in the 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8) address block.
- **Network and Broadcast Addresses:** As explained earlier, within each network the first and last addresses cannot be assigned to hosts. These are the network address and the broadcast address, respectively.
- **Loopback:** One such reserved address is the IPv4 loopback address 127.0.0.1. The loopback is a special address that hosts use to direct traffic to them. Although only the single 127.0.0.1 address is used, addresses 127.0.0.0 to 127.255.255.255 are reserved. Any address within this block will loop back within the local host. No address within this block should ever appear on any network.
- **Link-Local Addresses:** IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16) are designated as link-local addresses. These addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available. These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from a Dynamic Host Configuration Protocol (DHCP) server.
- **TEST-NET Addresses:** The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0 /24) is set aside for teaching and learning purposes. These addresses can be used in documentation and network examples.
- **Network Prefixes:** An important question is: How do we know how many bits represent the network portion and how many bits represent the host portion? When we

express an IPv4 network address, we add a prefix length to the network address. The prefix length is the number of bits in the address that gives us the network portion. For example, in 172.16.4.0 /24, the /24 is the prefix length - it tells us that the first 24 bits are the network address. This leaves the remaining 8 bits, the last octet, as the host portion.

Private and Public IP addresses:

- Public IP addresses: Public IP addresses are assigned by the InterNIC (Internet's Network Information Centre) and consists of class based network Ids or blocks of CIDR based addresses (called CIDR blocks) that are globally rout-able to the Internet and are unique.
- Private IP address: An address that is used for internal networks. These addresses are not rout-able to the Internet.
  The private address blocks are:
  10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)
  172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)
  192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)

Subnet Mask:
To define the network and host portions of an address, the devices use a separate 32-bit pattern called a subnet mask. We express the subnet mask in the same dotted decimal format as the IPv4 address. The subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion.
The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

Default Subnet Mask:
Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0

CIDR:
A routing system used by routers and gateways on the backbone of the Internet for routing packets. CIDR replaces the old class method of allocating 8, 16, or 24 bits to the network ID, and instead allows any number of contiguous bits in the IP address to be allocated as the network ID. For example, if a company needs a few thousand IP addresses for its network, it can allocate 11 or 12 bits of the address for the network ID instead of 8 bits for a class C (which wouldn't work because you would need to use several class C networks) or 16 bits for class B (which is wasteful).

How It Works?
CIDR assigns a numerical prefix to each IP address. For example, a typical destination IP address using CIDR might be 177.67.5.44/13. The prefix 13 indicates that the first 13 bits of the IP address identify the network, while the remaining 32 - 13 = 19 bits identify the host. The prefix helps to identify the Internet destination gateway or group of gateways to which the packet will be forwarded. Prefixes vary in size, with longer prefixes indicating more specific destinations. Routers use the longest possible prefix in their routing tables when determining how to forward each packet. CIDR enables packets to be sent to groups of networks instead of to individual networks, which considerably simplifies the

complex routing tables of the Internet's backbone routers.

How to Create Subnets?
To create subnetworks, you take bits from the host portion of the IP address and reserve them to define the subnet address.

How many bits to borrow?
I. No of subnetwork = 2^{BB}
II. No. of usable hosts per subnetwork=2^{BR}-2

TB=BR + BB
TB=Total bits in host portion
BB=Bits borrowed
BR=Bits Remaining

Subnetting Class C Addresses
There are many different ways to subnet a network. The right way is the way that works best for you. In a Class C address, only 8 bits are available for defining the hosts. Remember that subnet bits start at the left and go to the right, without skipping bits. This means that the only Class C subnet masks can be the following:

Binary	Decimal	CIDR
00000000	0	/24
10000000	128	/25
11000000	192	/26
11100000	224	/27
11110000	240	/28
11111000	248	/29
11111100	252	/30

We can't use a /31 or /32 because we have to have at least 2 host bits for assigning IP addresses to hosts.

All you need to do is answer five simple questions:
How many subnets does the chosen subnet mask produce?
How many valid hosts per subnet are available?
What are the valid subnets?
I. What's the broadcast address of each subnet?
II. What are the valid hosts in each subnet?

Subnetting Class C Address: 192.168.10.0/26
255.255.255.192 (/26)
In this second example, we're going to subnet the network address 192.168.10.0 using the subnet mask 255.255.255.192.
192.168.10.0 = Network addresses
255.255.255.192 = Subnet mask
Now, let's answer the big five:
How many subnets? Since 192 is 2 bits on (11000000), the answer would be 2^2 = 4 subnets.

How many hosts per subnet? We have 6 host bits off (11000000), so the equation would

be $2^6 - 2 = 62$ hosts.

What are the valid subnets? 256 – 192 = 64. Remember, we start at zero and count in our block size, so our subnets are 0, 64, 128, and 192. (Magic Number=256-Subnet Mask)

What's the broadcast address for each subnet? The number right before the value of the next subnet is all host bits turned on and equals the broadcast address. For the zero subnet, the next subnet is 64, so the broadcast address for the zero subnet is 63.

What are the valid hosts? These are the numbers between the subnet and broadcast address. The easiest way to find the hosts is to write out the subnet address and the broadcast address. This way, the valid hosts are obvious.

The following table shows the 0, 64, 128, and 192 subnets, the valid host ranges of each, and the broadcast address of each subnet:

The Subnet	0	64	128	192
The Broadcast Address	63	127	191	255
Usable Host Address	1-62	65-126	129-190	193-254

Subnetting Class B Address: 172.16.0.0/17
255.255.128.0 (/17)
172.16.0.0 = Network address
255.255.128.0 = Subnet mask

Subnets? $2^1 = 2$ (same as Class C).
Hosts? $2^{15} - 2 = 32{,}766$ (7 bits in the third octet, and 8 in the fourth).
Valid subnets? 256 – 128 = 128. 0, 128. Remember that subnetting is performed in the third octet, so the subnet numbers are really 0.0 and 128.0, as shown in the next table.

These are the exact numbers we used with Class C; we use them in the third octet and add a 0 in the fourth octet for the network address.

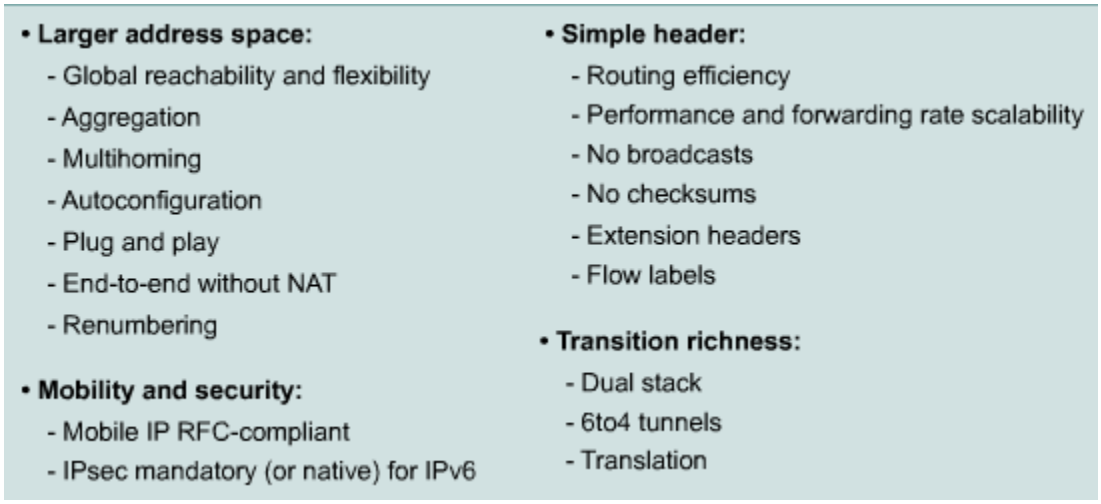
Broadcast address for each subnet?

Valid hosts?

The following table shows the two subnets available, the valid host range, and the broadcast address of each:

Subnet	172.16.0.0	172.16.128.0
Broadcast	172.16.127.255	172.16.255.255
Usable Host Range	172.16.0.1-172.16.127.254	172.16.128.1-172.16.255.254

IPV6:
Features of IPV6:



- **Larger address space**: Offers improved global reachability and flexibility; the aggregation of prefixes that are announced in routing tables; multihoming to several Internet service providers (ISPs) auto configuration that can include link-layer addresses in the address space; plug-and-play options; public-to private readdressing end to end without address translation; and simplified mechanisms for address renumbering and modification.
- **Simpler header:** Provides better routing efficiency; no broadcasts and thus no potential threat of broadcast storms; no requirement for processing checksums; simpler and more efficient extension header mechanisms; and flow labels for per-flow processing with no need to open the transport inner packet to identify the various traffic flows.
- **Mobility and security:** Ensures compliance with mobile IP and IPsec standards functionality; mobility is built in, so any IPv6 node can use it when necessary; and enables people to move around in networks with mobile network devices—with many having wireless connectivity.

  Mobile IP is an Internet Engineering Task Force (IETF) standard available for both IPv4 and IPv6. The standard enables mobile devices to move without breaks in established network connections. Because IPv4 does not automatically provide this kind of mobility, you must add it with additional configurations.

  IPsec is the IETF standard for IP network security, available for both IPv4 and IPv6. Although the functionalities are essentially identical in both environments, IPsec is mandatory in IPv6. IPsec is enabled on every IPv6 node and is available for use. The availability of IPsec on all nodes makes the IPv6 Internet more secure. IPsec also requires keys for each party, which implies a global key deployment and distribution.
- **Transition richness:** You can incorporate existing IPv4 capabilities in IPv6 in the following ways:
  - Configure a dual stack with both IPv4 and IPv6 on the interface of a network device.

- Use the technique IPv6 over IPv4 (also called 6to4 tunneling), which uses an IPv4 tunnel to carry IPv6 traffic. This method (RFC 3056) replaces IPv4-compatible tunneling (RFC 2893). Cisco IOS Software Release 12.3(2)T (and later) also allows protocol translation (NAT-PT) between IPv6 and IPv4. This translation allows direct communication between hosts speaking different protocols.

IPV6 Header

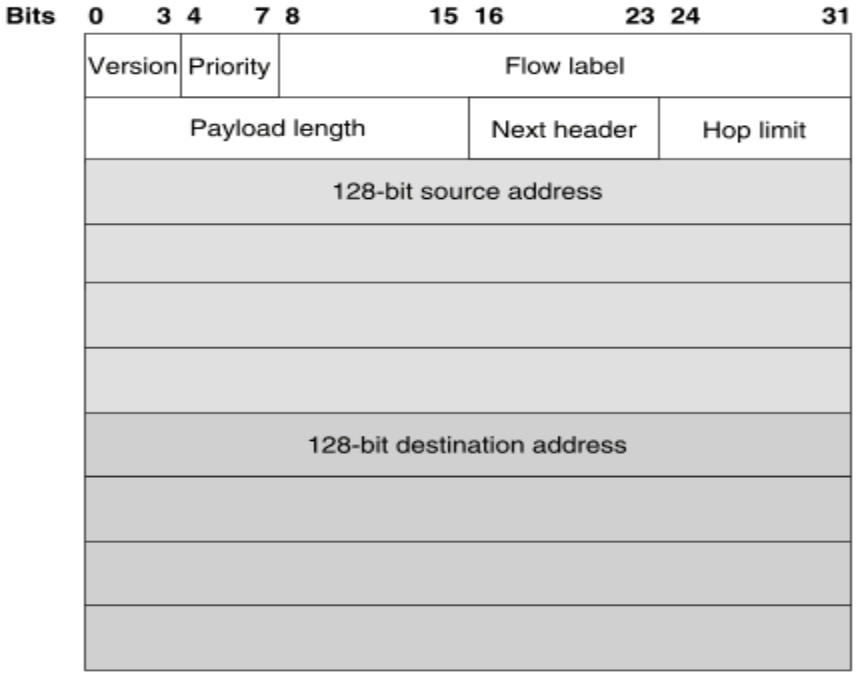


Figure: IPV6 Header

Specifically, IPv6 omits the following fields in its header.

- header length (the length is constant)
- identification
- flags
- fragment offset (this is moved into fragmentation extension headers)
- header checksum (the upper-layer protocol or security extension header handles data integrity)

IPv6 options improve over IPv4 by being placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. Most extension headers are not examined or processed by any router along a packet's delivery path until it arrives at its final destination. This mechanism improves router performance for packets containing options. In IPv4, the presence of any options requires the router to examine all options.

Another improvement is that IPv6 extension headers, unlike IPv4 options, can be of arbitrary length and the total amount of options that a packet carries is not limited to 40 bytes. This feature, and the manner in which it is processed, permit IPv6 options to be used for functions that were not practical in IPv4, such as the IPv6 Authentication and Security Encapsulation options.

By using extension headers, instead of a protocol specifier and options fields, newly defined extensions can be integrated more easily into IPv6.

IPV6 Addressing:

Address Representation:
Represented by breaking 128 bit into Eight 16-bit segments (Each 4 Hex character each). Each segment is written in Hexadecimal separated by colons. Hex digit are not case sensitive.
Rule 1:
Drop leading zeros:
2001:0050:0000:0235:0ab4:3456:456b:e560
2001:050:0:235:ab4:3456:456b:e560
Rule2:
Successive fields of zeros can be represented as "::" , But double colon appear only once in the address. FF01:0:0:0:0:0:0:1
FF01::1
Note : An address parser identifies the number of missing zeros by separating the two parts and entering 0 until the 128 bits are complete. If two "::" notations are placed in the address, there is no way to identify the size of each block of zeros.

IPV4 VS IPV6

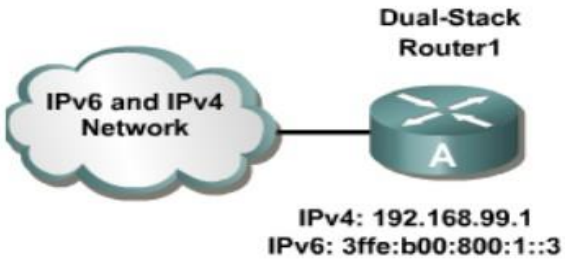
IPV4	IPV6
source and destination addresses are 32 bits	Source and destination addresses are 128 bits.
ipv4 support small address space.	Supports a very large address space sufficient for each and every people on earth.
ipv4 header includes checksum.	ipv6 header doesn't includes the checksum.
addresses are represented in dotted decimal format. (Eg. 192.168.5.1)	Addresses are represented in 16-bit segments Each segment is written in Hexadecimal separated by colons. (Eg. 2001:0050:020c:0235:0ab4:3456:456b:e560
Header includes options	All optional data is moved to IPV6 extension header
Broadcast address are used to send traffic to all nodes on a subnet	There is no IPV6 broadcast address. Instead a link local scope all-nodes multicast address is used
No identification of packet flow for QOS handling by router is present within the ipv4 header	Packet flow identification for QOS handling by routers is present within the IPV6 header using the flow label field.
uses host address (A) resource records in the Domain name system(DNS) to map host names to ipv4 addresses.	Uses AAAA records in the DNS to map host names ipv6 addresses.
Both routers and the sending host fragment packets.	Only the sending host fragments packets; routers do not.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway, and it is optional	. ICMPv6 Router Solicitation and Router Advertisement messages are used to determine the IP .address of the best default gateway, and they are required.

IPV6 Transition Mechanism:

I. Dual Stack
II. Tunneling Technique
III. Translation technique

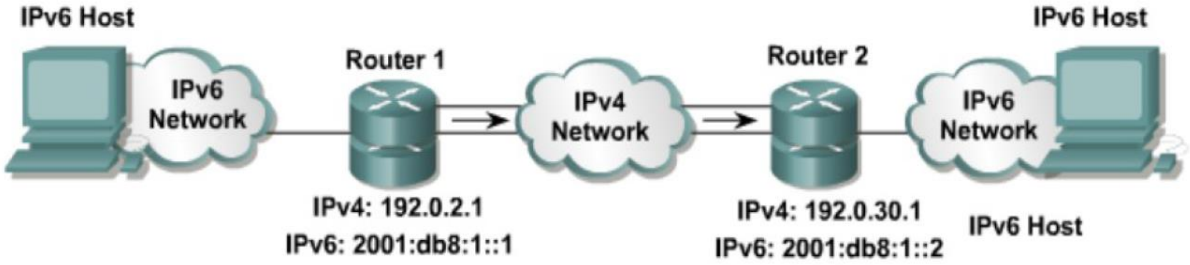
Dual Stack:

Dual stack is an integration method where a node has implementation and connectivity to both Ipv4 and ipv6 network. If both ipv4 and ipv6 are configured on an interface, this interface is dual-stacked.



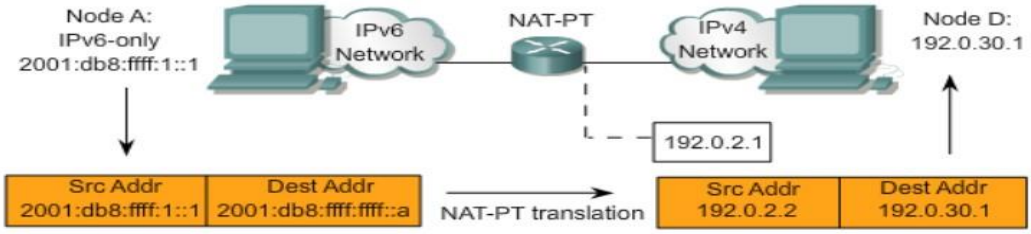
Tunneling Technique

With manually configured IPv6 tunnels, an IPv6 address is configured on a tunnel interface, and manually configured IPv4 addresses are assigned to the tunnel source and the tunnel destination. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks.



NAT-Protocol Translation (NAT-PT)

It is a translation mechanism that sits between an IPv6 network and an Ipv4 network. The translator translates IPv6 packets into IPv4 packets and vice versa.



Design issues for the network layer.

The network layer has been designed with the following goals:

I. The services provided should be independent of the underlying technology. Users of the service need not be aware of the physical implementation of the network - for all they know, they're messages could be transported via carrier pigeon! This design goal has great importance when we consider the great variety of networks in operation. In the area of Public networks, networks in underdeveloped countries are nowhere near the technological prowess of those in the countries like the US or Ireland. The design of the layer must not disable us from connecting to networks of different technologies.

II. The transport layer (that is the host computer) should be shielded from the number, type and different topologies of the subnets he uses. That is, all the transport layer want is a communication link, it need not know how that link is made.

III. Finally, there is a need for some uniform addressing scheme for network addresses.

With these goals in mind, two different types of service emerged: Connection oriented and connectionless. A connection-oriented service is one in which the user is given a "reliable" end to end connection. To communicate, the user requests a connection, then uses the connection to his heart's content, and then closes the connection. A telephone call is the classic example of a connection oriented service.

In a connection-less service, the user simply bundles his information together, puts an address on it, and then sends it off, in the hope that it will reach its destination. There is no guarantee that the bundle will arrive. So connection less service is one reminiscent of the postal system. A letter is sent, that is, put in the post box. It is then in the "postal network" where it gets bounced around and hopefully will leave the network in the correct place, that is, in the addressee's letter box. We can never be totally sure that the letter will arrive, but we know that there is a high probability that it will, and so we place our trust in the postal network.

Now, the question was which service would the network layer provide, a connection-oriented or a connectionless one?

With a connection oriented service, the user must pay for the length (ie the duration) of his connection. Usually this will involve a fixed start up fee. Now, if the user intends to send a constant stream of data down the line, this is great - he is given a reliable service for as long as he wants. However, say the user wished to send only a packet or two of data - now the cost of setting up the connection greatly overpowers the cost of sending that one packet. Consider also the case where the user wishes to send a packet once every 3 minutes. In a connection-oriented service, the line will thus be idle for the majority of the time, thus wasting bandwidth. So, connection-oriented services seem to be useful only when the user wishes to send a constant stream of data.

One would therefore think that the reliable nature of the connection oriented service would prompt people to choose it over the connectionless service - this is in fact not the case. One can never ensure that the network is 100% reliable; in fact for many applications we must assume that the network is not reliable at all. With this in mind, many applications perform their own error detection, flow and congestion control at a higher level in the protocol stack, that is, on their own machine, in the transport layer. So, if the sender and the receiver are going to engage in their own control mechanisms, why put this functionality into the network layer? This is the argument for the connectionless service: the network layer should provide a

raw means of sending packets from a to b, and that is all. Proponents of this argument are quick to point out that the standard of our networks has increased greatly in the past years, that packets of information rarely ever do get lost, so much of the correction facilities in the network layer are redundant and serve only to complicate the layer and slow down transfer.

It's interesting to note here that it is easy to provide a connection oriented service over an inherently connectionless service, so in fact defining the service of the network layer as connectionless is the general solution. However, at the time of defining the network layer, the controversy between the two camps was (and still is) unresolved, and so instead of deciding on one service, the ISO allowed both.

Routing and Routing Protocols:

The primary responsibility of a router is to direct packets destined for local and remote networks by:

- Determining the best path to send packets
- Forwarding packets toward their destination

The router uses its routing table to determine the best path to forward the packet. When the router receives a packet, it examines its destination IP address and searches for the best match with a network address in the router's routing table. The routing table also includes the interface to be used to forward the packet. Once a match is found, the router encapsulates the IP packet into the data link frame of the outgoing or exit interface, and the packet is then forwarded toward its destination.

Static Routes:
Static routes are configured manually; network administrators must add and delete static routes to reflect any network topology changes. In a large network, the manual maintenance of routing tables could require a lot of administrative time. On small networks with few possible changes, static routes require very little maintenance. Static routing is not as scalable as dynamic routing because of the extra administrative requirements. Even in large networks, static routes that are intended to accomplish a specific purpose are often configured in conjunction with a dynamic routing protocol.

When to use static Routing:
A network consists of only a few routers. Using a dynamic routing protocol in such a case does not present any substantial benefit. On the contrary, dynamic routing may add more administrative overhead.

A network is connected to the Internet only through a single ISP. There is no need to use a dynamic routing protocol across this link because the ISP represents the only exit point to the Internet.

A large network is configured in a hub-and-spoke topology. A hub-and-spoke topology consists of a central location (the hub) and multiple branch locations (spokes), with each spoke having only one connection to the hub. Using dynamic routing would be unnecessary because each branch has only one path to a given destination-through the central location.

Connected Routes:
Those network that are directly connected to the Router are called connected routes and are

not needed to configure on the router for routing. They are automatically routed by the Router.

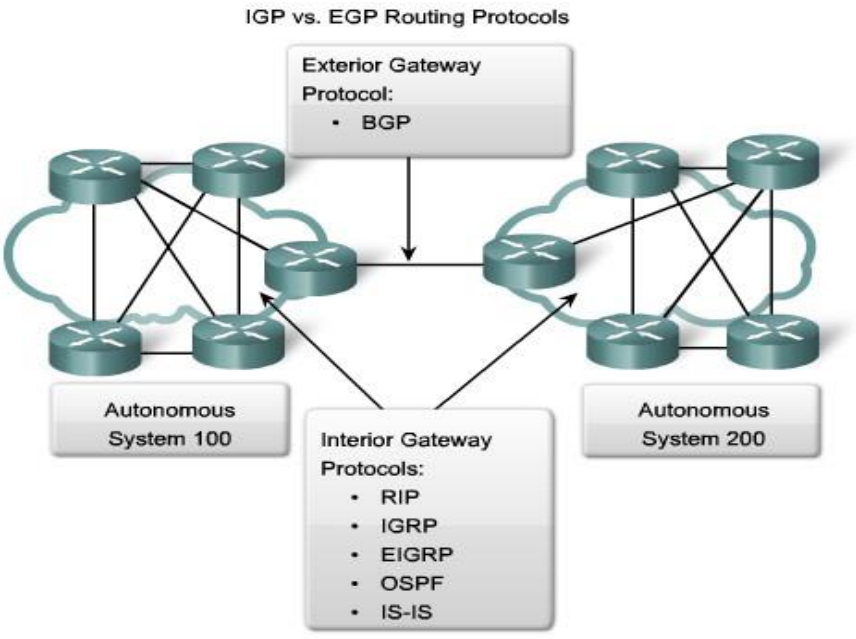
Dynamic Routes:
Dynamic routing protocol uses a route that a routing protocol adjusts automatically for topology or traffic changes.

Non-adaptive routing algorithm When a ROUTER uses a non-adaptive routing algorithm it consults a static table in order to determine to which computer it should send a PACKET of data. This is in contrast to an ADAPTIVE ROUTING ALGORITHM, which bases its decisions on data which reflects current traffic conditions (Also called static route)

Adaptive routing algorithm When a ROUTER uses an adaptive routing algorithm to decide the next computer to which to transfer a PACKET of data, it examines the traffic conditions in order to determine a route which is as near optimal as possible. For example, it tries to pick a route which involves communication lines which have light traffic. This strategy is in contrast to a NON-ADAPTIVE ROUTING ALGORITHM. (Also called Dynamic route)

Routing Protocol:
A routing protocol is the communication used between routers. A routing protocol allows routers to share information about networks and their proximity to each other. Routers use this information to build and maintain routing tables.

Autonomous System:
An AS is a collection of networks under a common administration that share a common routing strategy. To the outside world, an AS is viewed as a single entity. The AS may be run by one or more operators while it presents a consistent view of routing to the external world. The American Registry of Internet Numbers (ARIN), a service provider, or an administrator assigns a 16-bit identification number to each AS.



Dynamic Routing Protocol:

A. Interior Gateway protocol (IGP)
   I. Distance Vector Protocol
   II. Link State Protocol
B. Exterior Gateway Protocol (EGP)

Interior gateway protocol (IGP): Within one Autonomous System.

Exterior Routing Protocol (EGP): Between the Autonomous System. Example BGP (Boarder gateway protocol)

Metric:

There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and differentiate between the available paths. For this purpose a metric is used. A metric is a value used by routing protocols to assign costs to reach remote networks. The metric is used to determine which path is most preferable when there are multiple paths to the same remote network.

Each routing protocol uses its own metric. For example, RIP uses hop count, EIGRP uses a combination of bandwidth and delay, and Cisco's implementation of OSPF uses bandwidth.

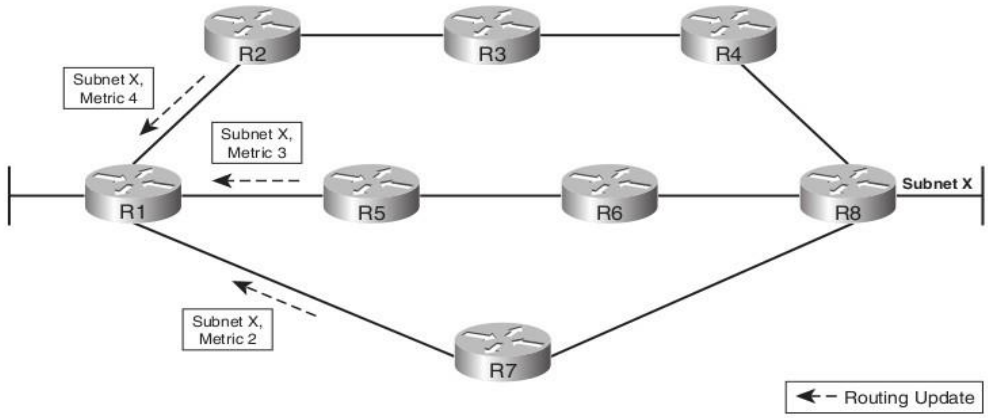
Distance Vector Routing Algorithm:

As the name implies, distance vector means that routes are advertised as vectors of distance and direction. Distance is defined in terms of a metric such as hop count and direction is simply the next-hop router or exit interface. A router using a distance vector routing protocol does not have the knowledge of the entire path to a destination network. Instead the router knows only:

- The direction or interface in which packets should be forwarded and
- The distance or how far it is to the destination network.

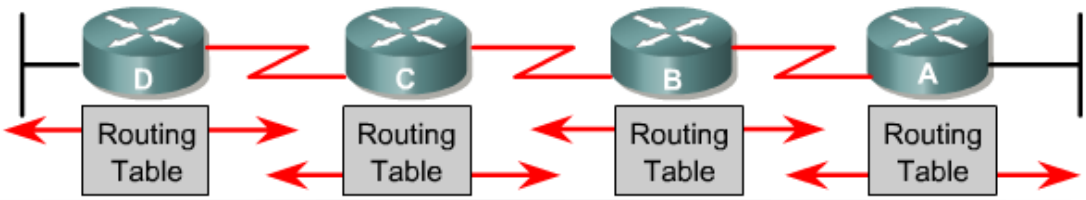
To show you more exactly what a distance vector protocol does, Figure shows a view of what a router learns with a distance vector routing protocol. The figure shows an internetwork in which R1 learns about three routes to reach subnet X:

- The four-hop route through R2
- The three-hop route through R5
- The two-hop route through R7

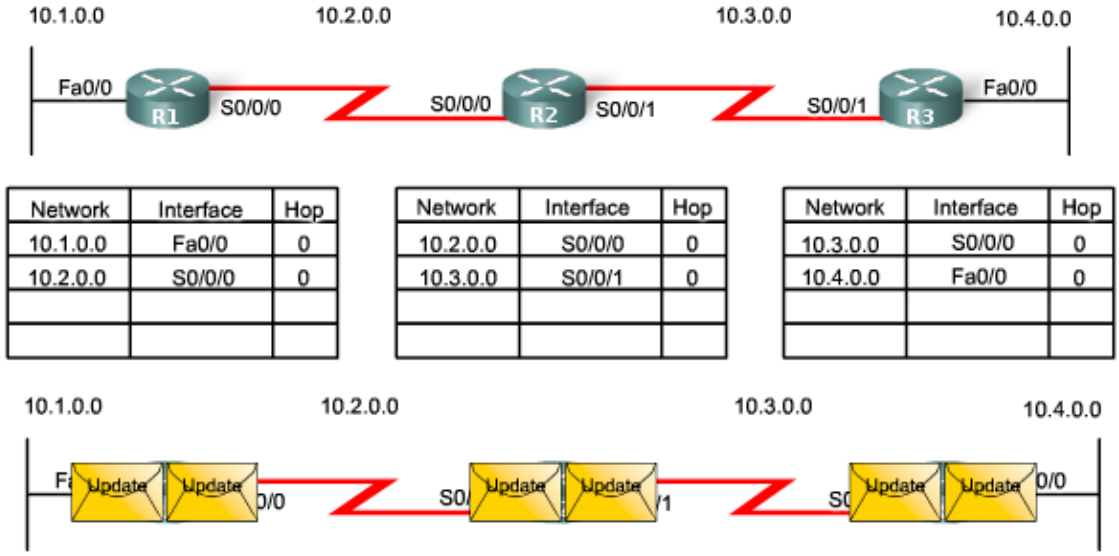


R1 learns about the subnet, and a metric associated with that subnet, and nothing more. R1 must then pick the best route to reach subnet X. In this case, it picks the two-hop route through R7, because that route has the lowest metric.

Distance vector protocols typically use the Bellman-Ford algorithm for the best path route determination.



Pass periodic copies of a routing table to neighbor routers and accumulate distance vectors.



Initial Update:

R1

- Sends an update about network 10.1.0.0 out the Serial0/0/0 interface
- Sends an update about network 10.2.0.0 out the FastEthernet0/0 interface
- Receives update from R2 about network 10.3.0.0 with a metric of 1
- Stores network 10.3.0.0 in the routing table with a metric of 1

R2

- Sends an update about network 10.3.0.0 out the Serial 0/0/0 interface
- Sends an update about network 10.2.0.0 out the Serial 0/0/1 interface
- Receives an update from R1 about network 10.1.0.0 with a metric of 1
- Stores network 10.1.0.0 in the routing table with a metric of 1
- Receives an update from R3 about network 10.4.0.0 with a metric of 1
- Stores network 10.4.0.0 in the routing table with a metric of 1

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/0	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

R3

- Sends an update about network 10.4.0.0 out the Serial 0/0/0 interface
- Sends an update about network 10.3.0.0 out the FastEthernet0/0
- Receives an update from R2 about network 10.2.0.0 with a metric of 1
- Stores network 10.2.0.0 in the routing table with a metric of 1

After this first round of update exchanges, each router knows about the connected networks of their directly connected neighbors. However, did you notice that R1 does not yet know about 10.4.0.0 and that R3 does not yet know about 10.1.0.0? Full knowledge and a converged network will not take place until there is another exchange of routing information.

Next Update:

R1

- Sends an update about network 10.1.0.0 out the Serial 0/0/0 interface.
- Sends an update about networks 10.2.0.0 and 10.3.0.0 out the FastEthernet0/0 interface.
- Receives an update from R2 about network 10.4.0.0 with a metric of 2.
- Stores network 10.4.0.0 in the routing table with a metric of 2.
- Same update from R2 contains information about network 10.3.0.0 with a metric of 1. There is no change; therefore, the routing information remains the same.

R2

- Sends an update about networks 10.3.0.0 and 10.4.0.0 out of Serial 0/0/0 interface.
- Sends an update about networks 10.1.0.0 and 10.2.0.0 out of Serial 0/0/1 interface.
- Receives an update from R1 about network 10.1.0.0. There is no change; therefore, the routing information remains the same.
- Receives an update from R3 about network 10.4.0.0. There is no change; therefore, the routing information remains the same.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

R3

- Sends an update about network 10.4.0.0 out the Serial 0/0/0 interface.
- Sends an update about networks 10.2.0.0 and 10.3.0.0 out the FastEthernet0/0 interface.
- Receives an update from R2 about network 10.1.0.0 with a metric of 2.
- Stores network 10.1.0.0 in the routing table with a metric of 2.
- Same update from R2 contains information about network 10.2.0.0 with a metric of 1. There is no change; therefore, the routing information remains the same.

Note: Distance vector routing protocols typically implement a technique known as split horizon. Split horizon prevents information from being sent out the same interface from which it was received. For example, R2 would not send an update out Serial 0/0/0 containing the network 10.1.0.0 because R2 learned about that network through Serial 0/0/0.

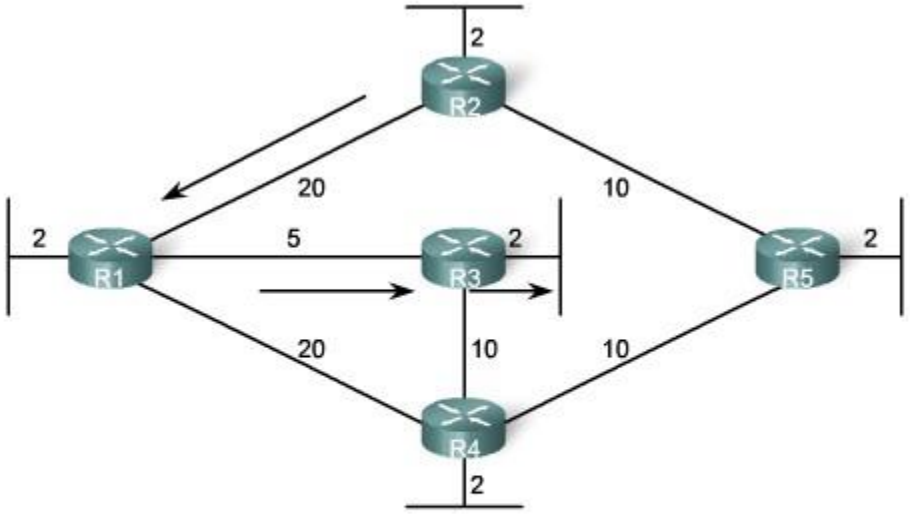
Link State Routing Algorithm:

Also known as shortest path Routing algorithm.

Link states:

Information about the state of (Router interfaces) links is known as link-states. As you can see in the figure, this information includes:

- The interface's IP address and subnet mask.
- The type of network, such as Ethernet (broadcast) or Serial point-to-point link.
- The cost of that link.
- Any neighbor routers on that link.



Shortest Path for host on R2 LAN to reach host on R3 LAN:
R2 to R1 (20) + R1 to R3 (5) + R3 to LAN (2) = 27

So exactly how does a link-state routing protocol work? All routers will complete the following generic link-state routing process to reach a state of convergence:

1. Each router learns about its own links, its own directly connected networks. This is done by detecting that an interface is in the up state.
2. Each router is responsible for meeting its neighbors on directly connected networks. link state routers do this by exchanging Hello packets with other link-state routers on directly connected networks.
3. Each router builds a Link-State Packet (LSP) containing the state of each directly connected link. This is done by recording all the pertinent information about each neighbor, including neighbor ID, link type, and bandwidth.
4. Each router floods the LSP to all neighbors, who then store all LSPs received in a database. Neighbors then flood the LSPs to their neighbors until all routers in the area have received the LSPs. Each router stores a copy of each LSP received from its neighbors in a local database.

5. Each router uses the database to construct a complete map of the topology and computes the best path to each destination network. Like having a road map, the router now has a complete map of all destinations in the topology and the routes to reach them. The SPF algorithm is used to construct the map of the topology and to determine the best path to each network.

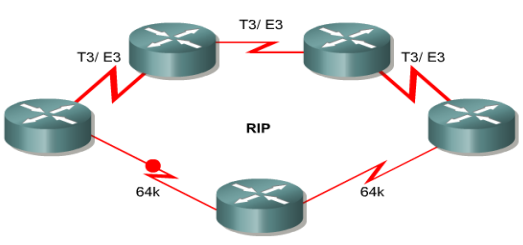
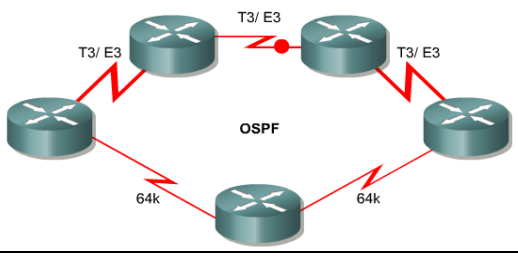
Advantages of Link state Routing protocol:

Build the topological map:
Link-state routing protocols create a topological map, or SPF tree of the network topology. Distance vector routing protocols do not have a topological map of the network.

Faster Convergence:
When receiving a Link-state Packet (LSP), link-state routing protocols immediately flood the LSP out all interfaces except for the interface from which the LSP was received. This way, it achieves the faster convergence. With distance vector routing algorithm, router needs to process each routing update and update its routing table before flooding them out other interfaces.

Event Driven Updates:
After the initial flooding of LSPs, link-state routing protocols only send out an LSP when there is a change in the topology. The LSP contains only the information regarding the affected link. Unlike some distance vector routing protocols, link-state routing protocols do not send periodic updates.

Distance vector vs. Link state:

S. No	Distance Vector	Link State
1	Uses hop count as Metric	Uses shortest path.
2	2View the network from the perspective of neighbor.	Gets common view of entire network topology.
3	Has frequent and periodic updates	Has event triggered updates.
4	Slow convergence	Faster convergence
5	Susceptible to routing loops.	Not as susceptible to routing loops.
6	Easy to configure and administer.	Difficult to configure and administer.
7	Requires less memory and processing power of routers	Requires more processing power and memory than distance vector.
8	Consumes a lot of Bandwidth.	Consumes less BW than distance vector
9	Passes copies of routing table to neighbor routers.	Passes link-state routing updates to other routers.
10	Eg. RIP 	Eg. OSPF 

Chapter 6
Transport Layer and Protocols

Transport Layer:

The transport layer provides a logical connection between a source host and a destination host. Transport protocols segment and reassemble data sent by upper-layer applications into the same data stream, or logical connection, between end points.

- Creates packet from bytes stream received from the application layer.
- Uses port number to create process to process communication.
- Uses a sliding window protocol to achieve flow control.
- Uses acknowledgement packet, timeout and retransmission to achieve error control.

The primary duty of the transport layer is to provide end-to-end control and reliability as data travels through this cloud. This is accomplished through the use of sliding windows, sequence numbers, and acknowledgments. The transport layer also defines end-to-end connectivity between host applications. Transport layer protocols include TCP and UDP.

TCP

TCP is a connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. In a connection-oriented environment, a connection is established between both ends before the transfer of information can begin. TCP breaks messages into segments, reassembles them at the destination, and resends anything that is not received. TCP supplies a virtual circuit between end-user applications.

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.

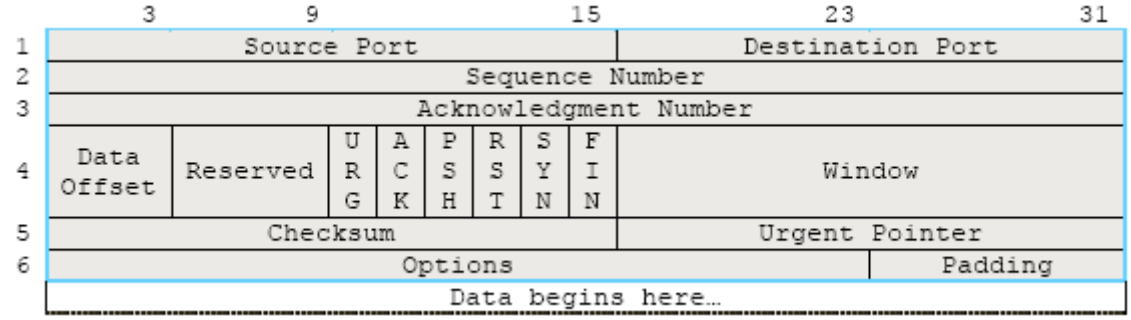
TCP Services

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

TCP Header Format:

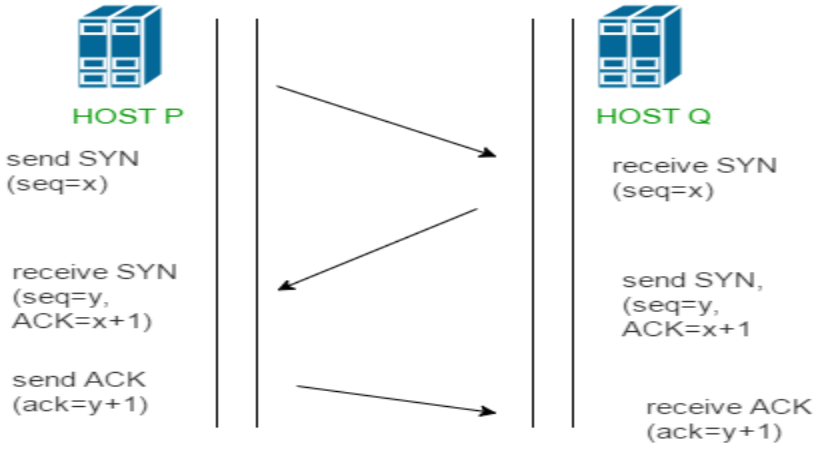
TCP uses only a single type of protocol data unit, called a TCP segment. The header is shown in Figure. Because one header must serve to perform all protocol mechanisms, it is rather large, with a minimum length of 20 octets.



The following are the definitions of the fields in the TCP segment:

- Source port – Number of the port that sends data
- Destination port – Number of the port that receives data
- Sequence number – Number used to ensure the data arrives in the correct order
- Acknowledgment number – Next expected TCP octet
- HLEN – Number of 32-bit words in the header
- Reserved – Set to zero
- Code bits – Control functions, such as setup and termination of a session
- Window – Number of octets that the sender will accept
- Checksum – Calculated checksum of the header and data fields
- Urgent pointer – Indicates the end of the urgent data
- Option – One option currently defined, maximum TCP segment size
- Data – Upper-layer protocol data
- Code Bits or Flags (6 bits).
    - URG: Urgent pointer field significant.
    - ACK: Acknowledgment field significant.
    - PSH: Push function.
    - RST: Reset the connection.
    - SYN: Synchronize the sequence numbers.
    - FIN: No more data from sender.

TCP Handshake



- **Step 1 (SYN) :** In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with
- **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with
- **Step 3 (ACK) :** In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start eh actual data transfer

The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.

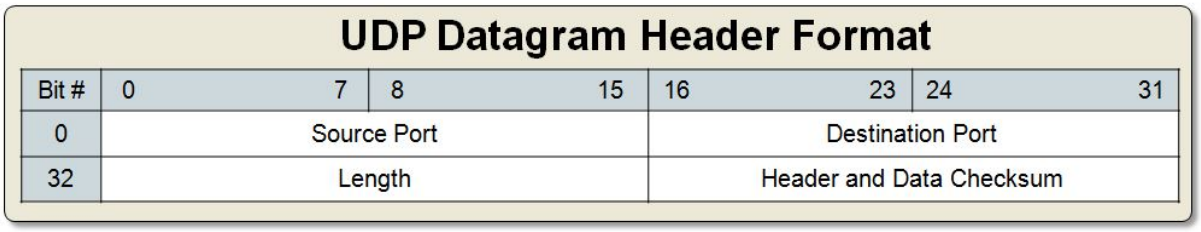
UDP (User Datagram Protocol):

UDP is the connectionless transport protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without guaranteed delivery. It relies on higher-layer protocols to handle errors and retransmit data.

Features of UDP:

- Provides connectionless, unreliable service.
- So UDP faster than TCP.
- Adds only checksum and process-to-process addressing to IP.
- Used for DNS and NFS.
- Used when socket is opened in datagram mode.
- It sends bulk quantity of packets.
- No acknowledgment.
- Good for video streaming it is an unreliable protocol.
- It does not care about the delivery of the packets or the sequence of delivery.
- No flow control /congestion control, sender can overrun receiver's buffer.
- Real time application like video conferencing needs (Because it is faster).
- An UDP datagram is used in Network File System (NFS), DNS, SNMP, TFTP etc.
- It has no handshaking or flow control.
- It not even has windowing capability.
- It is a fire and forget type protocol.
- An application can use a UDP port number and another application can use the same port number for a TCP session from the same IP address.
- UDP and IP are on different levels of the OSI stack and correspond to other protocols like TCP and ICMP.
- No connection establishment tear down; data is just sent right away.
- For data transfer with UDP a lock-step protocol is required (to be implemented by the application).
- No error control; corrupted data is not retransmitted (even though UDP header has a checksum to detect errors and report these to the application).

UDP Header Format



The following are the definitions of the fields in the UDP segment:

Source port number

- This is the port number used by the process running on the source host.
- It is 16 bits long, which means that the port number can range from 0 to 65,535.
- If the source host is the client, the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host.
- If the source host is the server, the port number, in most cases, is a well-known port number.

Destination port number

- This is the port number used by the process running on the destination host. It is also 16 bits long.
- If the destination host is the server, the port number, in most cases, is a well-known port number.
- If the destination host is the client, the port number, in most cases, is an ephemeral port number.

Length

- This is a 16-bit field that defines the total length of the user datagram, header plus data.
- The 16 bits can define a total length of 0 to 65,535 bytes. The length field in a UDP user datagram is actually not necessary.

Checksum

- This field is used to detect errors over the entire user datagram (header plus data).

TCP VS UDP

Characteristics Description	UDP	TCP
Acronym for	User Datagram Protocol	Transmission Control Protocol
General Description	Simple High speed low functionality "wrapper" that interface applications to the network layer and does little else	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol connection Setup	Connection less; data is sent without setup	Connection-oriented; Connection must be Established prior to transmission.
Data interface to application	Message base-based is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure
Reliability and Acknowledgements	Unreliable best-effort delivery without acknowledgements	Reliable delivery of message all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Overhead	Very Low	Low, but higher than UDP
Transmission speed	Very High	High but not as high as UDP
Data. Quantity Suitability	Small to moderate amounts of data	Small to very large amounts of data.

Socket Programming:

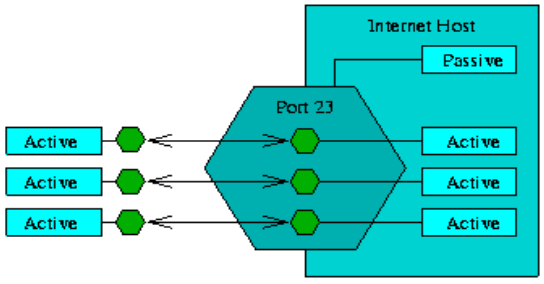
Sockets are the combination of IP address plus corresponding TCP/UDP port numbers. For applications to work with TCP/IP, Application Program Interface (API) is required. API serves as an interface between different software programs and facilitates their interaction, similar to the way the user interface facilitates interaction between humans and computers.

Sockets come in two primary flavors

An **active socket** is connected to a remote active socket via an open data connection. Closing the connection destroys the active sockets at each endpoint.

A **passive socket** is not connected, but rather awaits an incoming connection, which will spawn a new active socket.

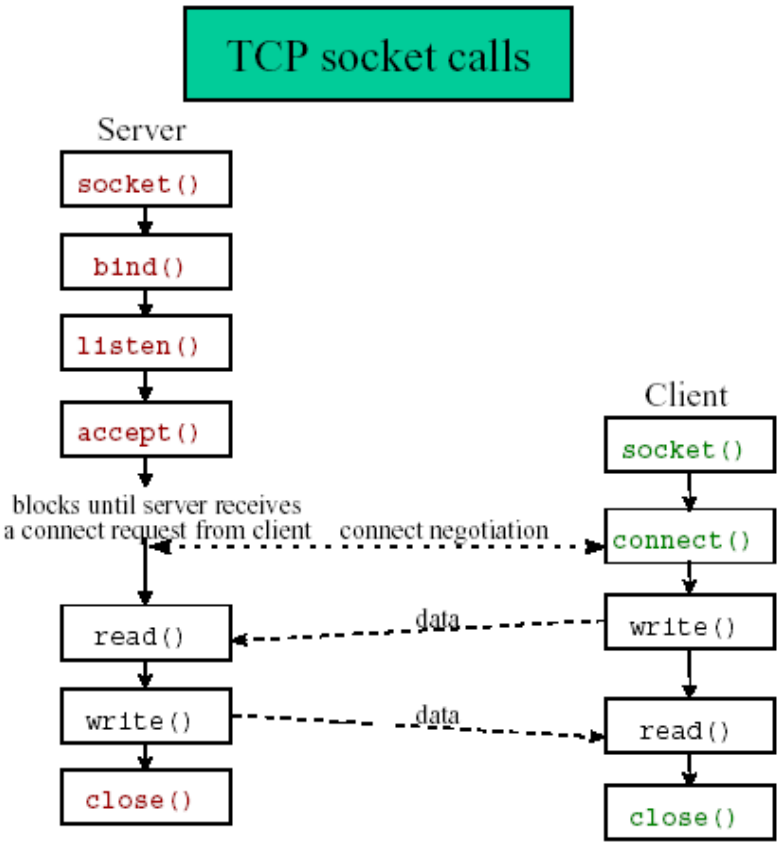
A socket is not a port, though there is a close relationship between them. A socket is associated with a port, though this is a many-to-one relationship. Each port can have a single passive socket, awaiting incoming connections, and multiple active sockets, each corresponding to an open connection on the port.



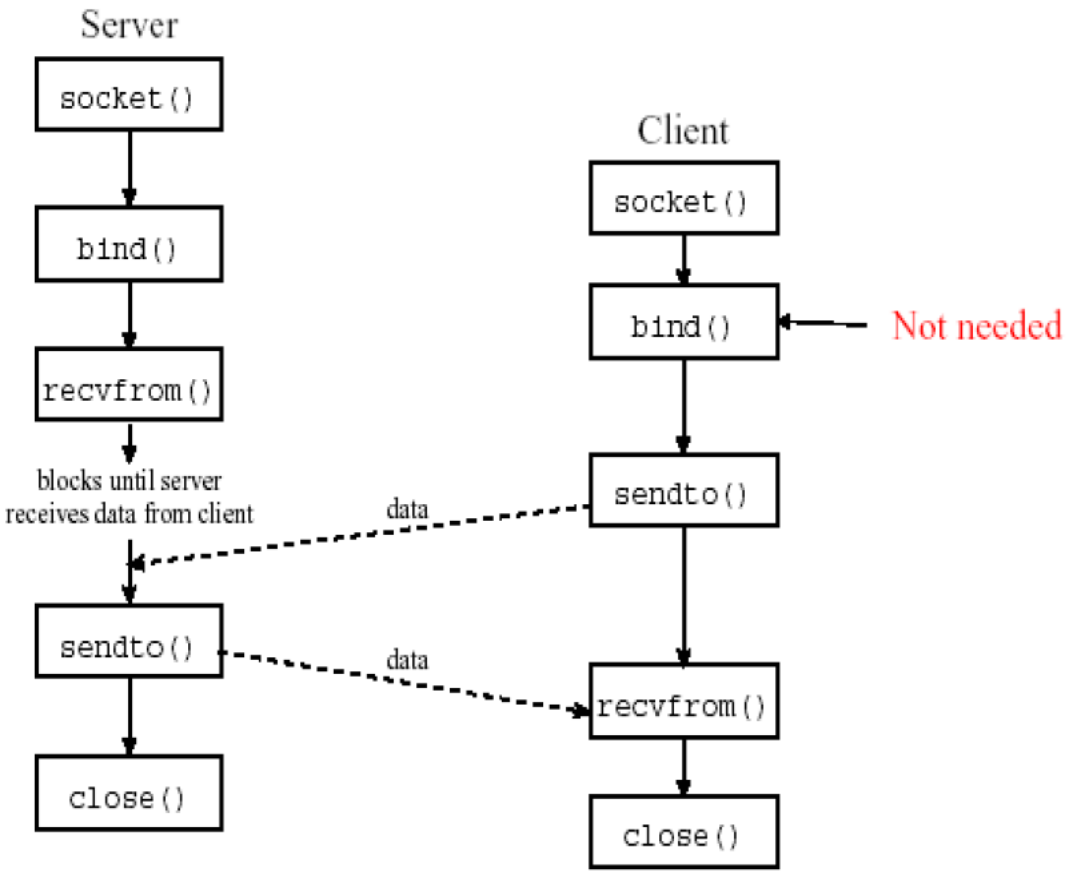
Sockets are the combination of IP address plus corresponding TCP/UDP port numbers. It is like PBX phone systems, where the IP address is the phone number, and the port is the extension. Every paired of connected socket has a source IP/port and a destination IP/port. Users of Internet applications are normally aware of all except the local port number, this is allocated when connection is established and is almost entirely arbitrary unlike the well-known port numbers associated with popular applications.

There are three types of sockets:

1. **Stream**
   Stream sockets provide reliable, connection-based communications. In connection-based communications, the two processes must establish a logical connection with each other. A stream of bytes is then sent without errors or duplication and is received in the order in which it was sent. Stream sockets correspond to the TCP protocol in TCP/IP.
2. **Datagram**
   Datagram sockets communicate via discrete messages, called datagrams, which are sent as packets. Datagram sockets are connectionless; that is, the communicating processes do not have a logical connection with each other. The delivery of their data is unreliable. The datagrams can be lost or duplicated, or they may not arrive in the order in which they were sent. Datagram sockets correspond to the UDP protocol in TCP/IP.
3. Raw
   Raw sockets provide direct access to the lower-layer protocols, for example, IP and the Internet Control Message Protocol (ICMP).



UDP socket calls

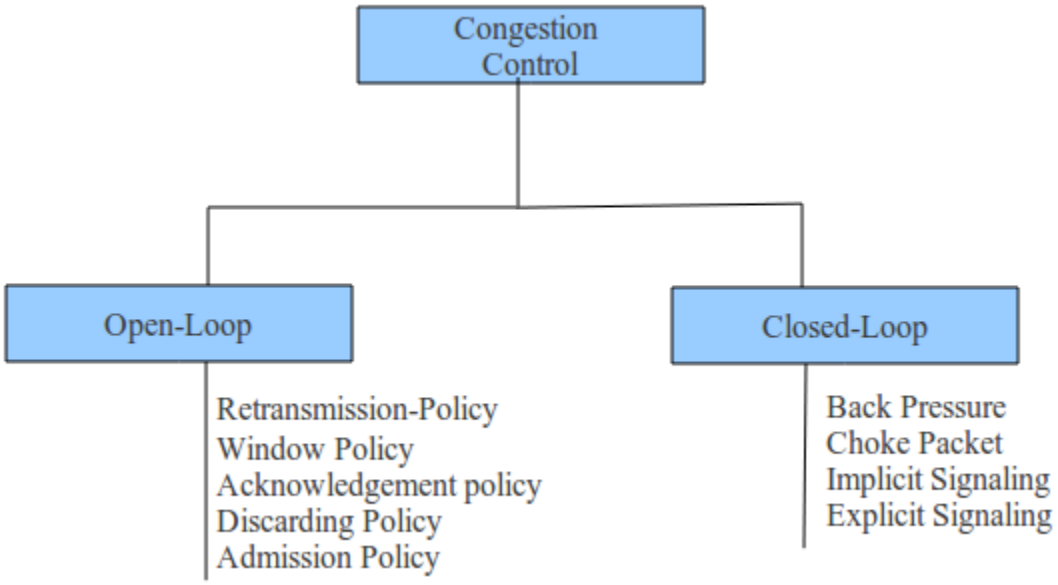


Chapter 7
Congestion Control and Quality of Services

Congestion in a network may occur if the load on the network (the number of packets sent to the network) is greater than the capacity of the network(the number of packets a network can handle). Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

- When too many packets are pumped into the system, congestion occur leading into degradation of performance.
- Congestion tends to feed upon it and backups.
- Congestion shows lack of balance between various networking equipment.
- It is a global issue.

In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal) as shown in Figure



Open Loop Congestion Control:
In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination.

1. **Retransmission Policy**
   Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion. For example, the retransmission policy used by TCP is designed to prevent or alleviate congestion.

2. **Window Policy**
   The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

3. **Acknowledgment Policy**
   The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. Several approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only N packets at a time. We need to know that the acknowledgments are also part of the load in a network. Sending fewer acknowledgments means imposing fewer loads on the network.

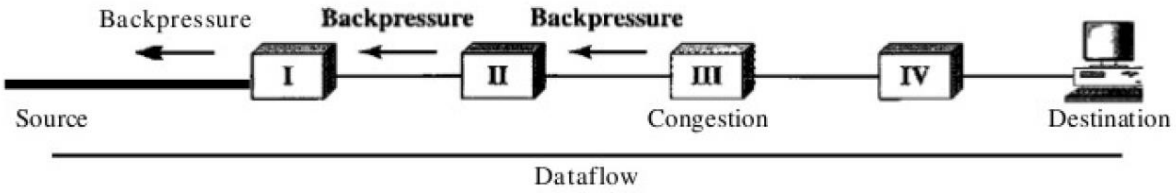
4. **Discarding Policy**
   A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

5. **Admission Policy**
   An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual- circuit connection if there is congestion in the network or if there is a possibility of future congestion.

Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols.

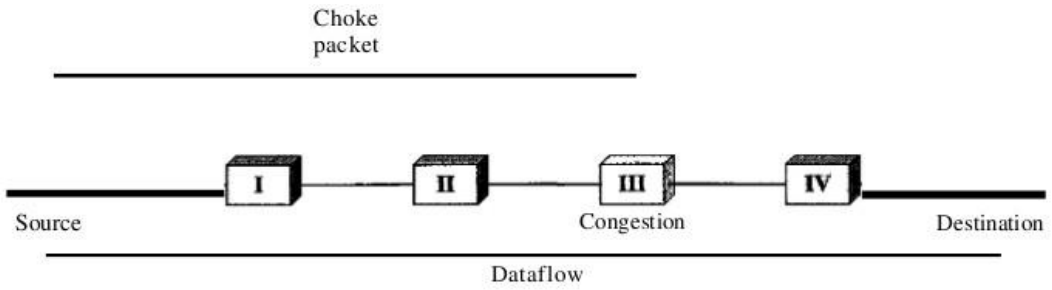
1. **Back-pressure**
   The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes. And so on. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is corning.



Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion. If so, node I inform the source of data to slow down. This, in time, alleviates the congestion.

2. **Choke Packet**

A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has traveled are not warned. We have seen an example of this type of control in ICMP. When a router in the Internet is overwhelmed datagrams, it may discard some of them; but it informs the source, host, using a source quench ICMP message. The warning message goes directly to the source station; the intermediate routers, and does not take any action. Figure shows the idea of a choke packet.



3. **Implicit Signaling**

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

4. **Explicit Signaling**

The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data. Explicit signaling, as we will see in Frame Relay congestion control, can occur in either the forward or the backward direction.

Backward Signaling: A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

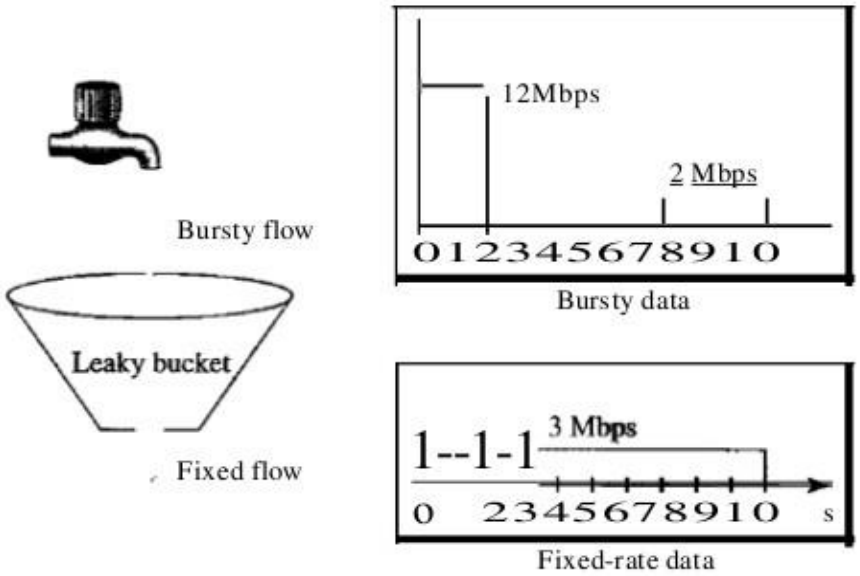
Forward Signaling: A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

Traffic Shaping

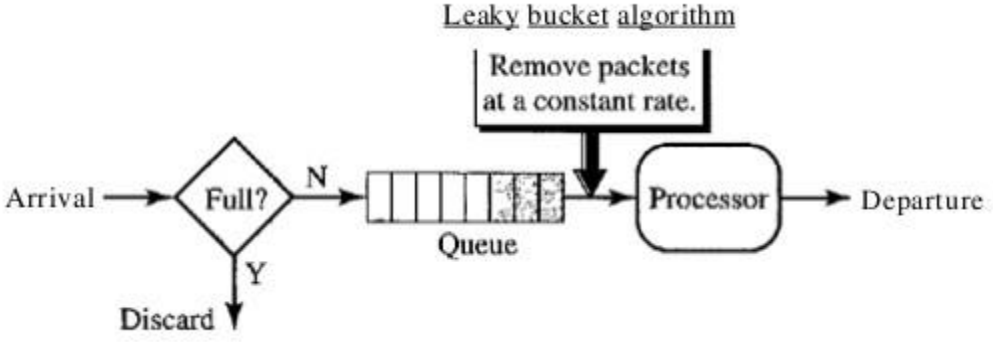
Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic: leaky bucket and token bucket.

Leaky Bucket

If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate. Figure shows a leaky bucket and its effects.



In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In Figure the host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in l0s. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10 s. Without the leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host. We can also see that the leaky bucket may prevent congestion.



Leaky Bucket Implementation

A simple leaky bucket implementation is shown in Figure. A FIFO queue holds the packets. If the traffic consists of fixed-size packets (e.g., cells in ATM networks), the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

The following is an algorithm for variable-length packets:

- Initialize a counter to n at the tick of the clock.
- If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
- Reset the counter and go to step 1.

A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.

Token Bucket Algorithm

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

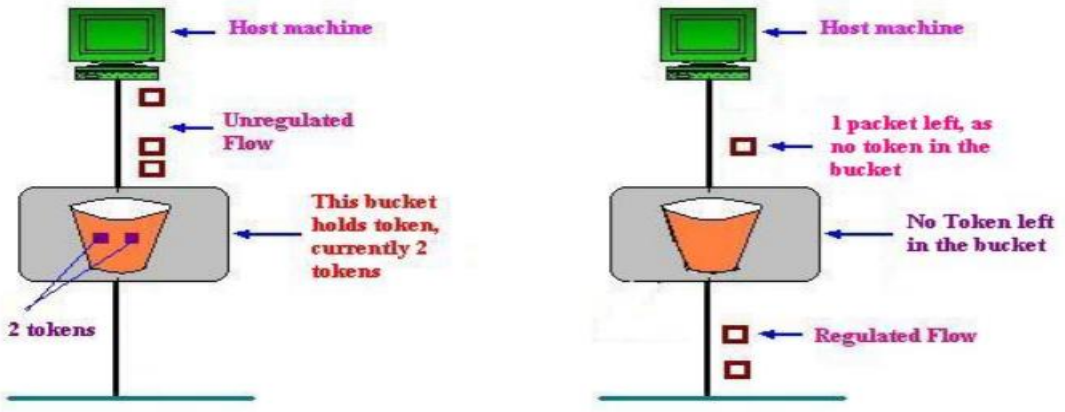
Main steps of this algorithm can be described as follows: *f*

- In regular intervals tokens are thrown into the bucket.
- The bucket has a maximum capacity.
- If there is a ready packet, a token is removed from the bucket, and the packet is send.
- If there is no token in the bucket, the packet cannot be send.

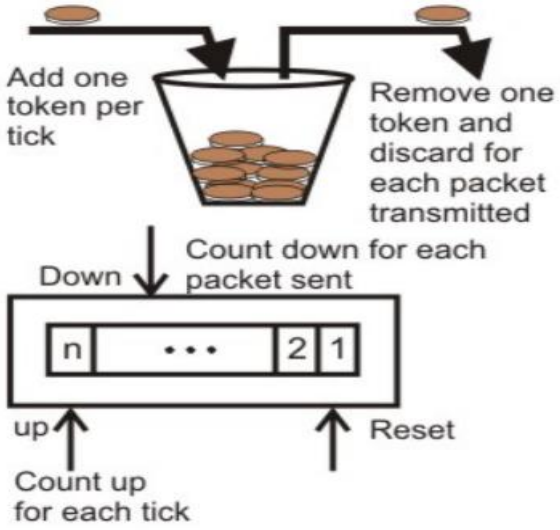
Figure shows the two scenarios before and after the tokens present in the bucket have been consumed. In Figure (a), the bucket holds two tokens, and three packets are waiting to be sent out of the interface, in Figure (b) two packets have been sent out by consuming two tokens, and 1 packet is still left.

The token bucket algorithm is less restrictive than the leaky bucket algorithm, in a sense that it allows bursty traffic. However, the limit of burst is restricted by the number of tokens available in the bucket at a particular instant of time.

The implementation of basic token bucket algorithm is simple; a variable is used just to count the tokens. This counter is incremented every t seconds and is decremented whenever a packet is sent. Whenever this counter reaches zero, no further packet is sent out as shown in Figure (c).



(a) (b)



TCP Congestion Control

Admission control is one such closed-loop technique, where action is taken once congestion is detected in the network.

Different approaches can be followed:

- Simpler one being: do not set-up new connections, once the congestion is signaled. This type of approach is often used in normal telephone networks. When the exchange is overloaded, then no new calls are established.
- Another approach, which can be followed, is: to allow new virtual connections, but route these carefully so that none of the congested router (or none of the problem area) is a part of this route.
- Yet another approach can be: To negotiate different parameters between the host and the network, when the connection is setup. During the setup time itself, Host specifies the volume and shape of traffic, quality of service, maximum delay and other parameters, related to the traffic it would be offering to the network. Once the host specifies its requirement, the resources needed are reserved along the path, before the actual packet follows.

Chapter 8
Application Layer, Servers and Protocols

Hypertext Transfer Protocol (HTTP)
A standard Internet protocol that specifies the client/server interaction processes between Web browsers such as Mozilla Firefox and Web servers such as Apache. Its the network protocol used to deliver virtually all files and other data(collectively called resources) on the World-Wide-Web, whether they are HTML files, image files, query results or anything else. Usually HTTP takes place though TCP/IP Sockets.A Browser is an HTTP client because it sends requests to an HTTP server (Web Sever), which then sends response back to the client. The standard and default port for the HTTP servers to listen is 80, though they can use any port.

What are Resources?
HTTP is used to transmit resources not just files. A resource is some chunk of information that can be identified by a URL (its R in URL). The most common kind of resource is a file, but a resource may also be a dynamically generated query, the output of a CGI script, a document that is available in several languages or anything else.

The original Hypertext Transfer Protocol (HTTP) 1.0 protocol is a stateless protocol whereby a Web browser forms a connection with a Web server, downloads the appropriate file, and then terminates the connection. The browser usually requests a file using an HTTP GET method request on TCP port 80, which consists of a series of HTTP request headers that define the transaction method (GET, POST, HEAD, and so on) and indicates to the server the capabilities of the client. The server responds with a series of HTTP response headers that indicate whether the transaction is successful, the type of data being sent, the type of server, and finally the requested data.

IIS 4 supports a new version of this protocol called HTTP 1.1, which has new features that make it more efficient. These new features include the following:

- **Persistent connections:**
  An HTTP 1.1 server can keep TCP connections open after a file has been transferred, eliminating the need for a connection to be opened and closed each time a file is transferred, as is the case with HTTP 1.0.
- **Pipelining:**
  This is a process whereby an HTTP 1.1 client can send multiple Internet Protocol (IP) packets to the server without waiting for the server to respond to each packet.
- **Buffering:**
  This process allows several HTTP requests by the client to be buffered into a single packet and sent to the server, which results in faster transfer times because fewer and larger packets are used.
- **Host headers:**
  This feature enables an HTTP 1.1–compliant Web server to host multiple Web sites using a single IP address.
- **Http put and http delete commands:**
  These commands enable Web browsers to upload and delete files from Web servers using HTTP

HTTPS VS HTTP

As opposed to HTTP URLs that begin with "http://" and use port 80 by default, HTTPS URLs begin with "https://" and use port 443 by default. HTTP is unsecured and is subject to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information. HTTPS is designed to withstand such attacks and is considered secure against such attacks . HTTP operates at the highest layer of the OSI Model, the Application layer; but the security protocol operates at a lower sub layer, encrypting an HTTP message prior to transmission and decrypting a message upon arrival. Strictly speaking, HTTPS is not a separate protocol, but refers to use of ordinary HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. Everything in the HTTP message is encrypted, including the headers, and the request/response load.

DHCP (Dynamic Host Configuration Protocol)

A standard Internet protocol that enables the dynamic configuration of hosts on an Internet Protocol (IP) internetwork. Dynamic Host Configuration Protocol (DHCP) is an extension of the bootstrap protocol (BOOTP).

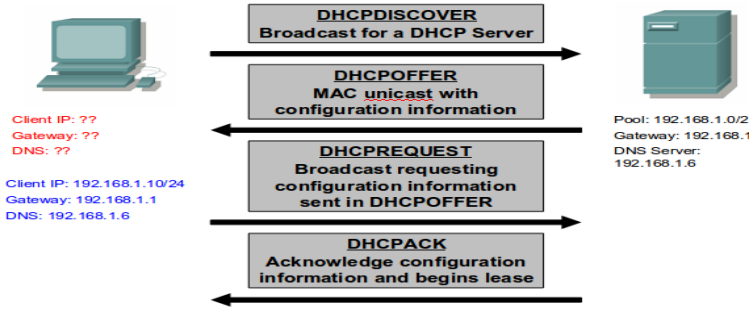
How It Works?

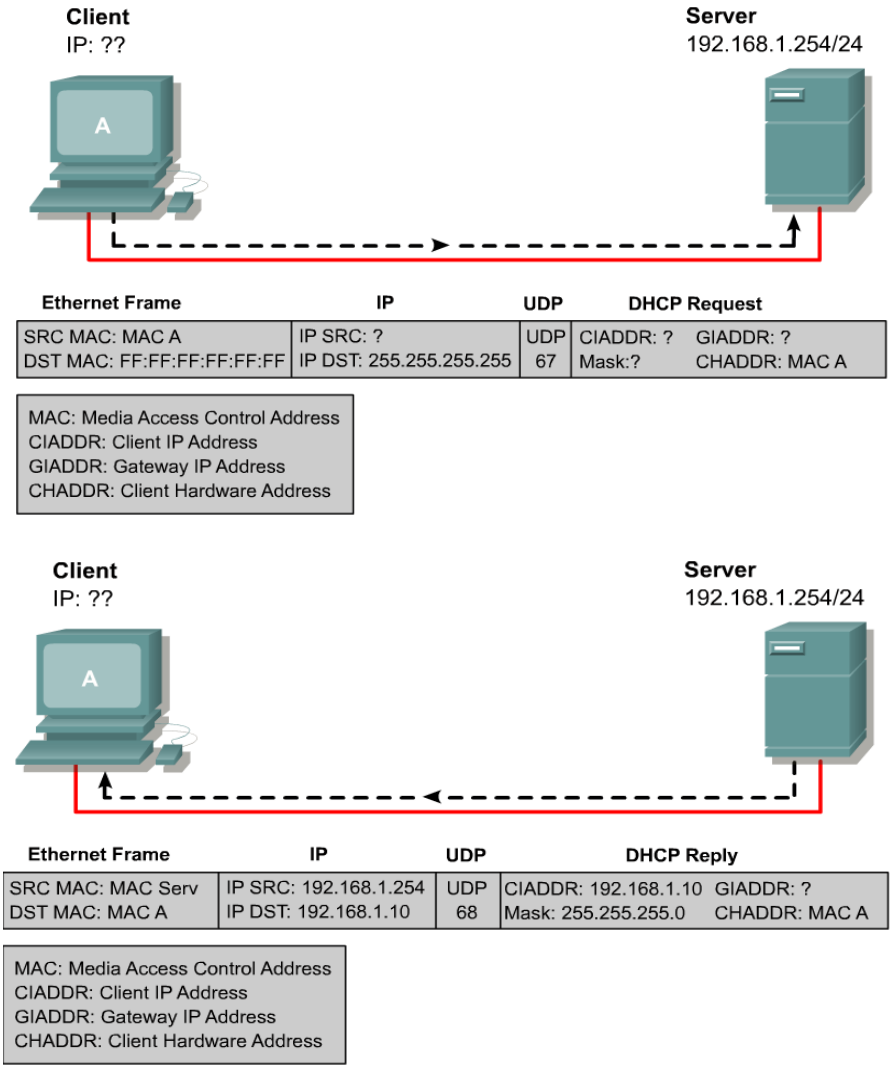
DHCP is a client-server protocol that uses DHCP servers and DHCP clients. A DHCP server is a machine that runs a service that can lease out IP addresses and other TCP/IP information to any client that requests them. For example, on Linux System example Ubuntu you can install the DHCP Server service to perform this function. The DHCP server typically has a pool of IP addresses that it is allowed to distribute to clients, and these clients lease an IP address from the pool for a specific period of time, usually several days. Once the lease is ready to expire, the client contacts the server to arrange for renewal.

DHCP clients are client machines that run special DHCP client software enabling them to communicate with DHCP servers. All versions of Linux and Windows include DHCP client software, which is installed when the TCP/IP protocol stack is installed on the machine.

DHCP clients obtain a DHCP lease for an IP address, a subnet mask, and various DHCP options from DHCP servers in a four-step process:

1. DHCPDISCOVER:
   The client broadcasts a request for a DHCP server.
2. DHCPOFFER:
   DHCP servers on the network offer an address to the client.
3. DHCPREQUEST:
   The client broadcasts a request to lease an address from one of the offering DHCP servers.
4. DHCPACK:
   The DHCP server that the client responds to acknowledges the client, assigns it any configured DHCP options, and updates its DHCP database. The client then initializes and binds its TCP/IP protocol stack and can begin network communication.





Domain Name System (DNS):

IP address are tough for human to remember and impossible to guess. Domain Name System are usually used to translate a hostname or Domain name (eg. nec.edu.np) into an IP address (eg. 202.37.94.177). Domain name comprise a hierarchy so that names are unique, yet easy to remember.

DNS makes its possible to refer to the Internet protocol (IP) based system (hosts) by human friendly names (domain names). Name resolution is that act of determining the IP address of a given hostname. The benefits of DNS are two folds. First Domain Name can be logical and easily remembered. Secondly, should an IP address for a host change, the domain name can still resolve transparently to the users or application. DNS name resolution is a critical Internet service. Many network services require functional name service for correct operation.

Domain names are separated by dots with the topmost element on the right. Each element may be up to 63 characters long; the entire name may be at most 255 characters long. Letters, numbers or dashes may be used in an element.

Domain Name Space:

To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127.

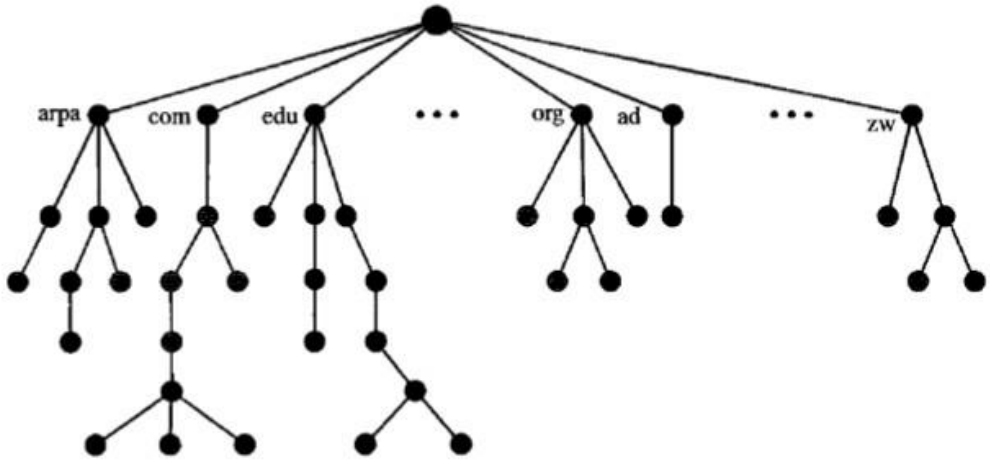


Fig: Domain Name Space

Domain Name

Each node in the tree has a domain name. A full domain name is a sequence of labels separated by dots (.). The domain names are always read from the node up to the root. The last label is the label of the root (null). This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing. Figure shows some domain names.

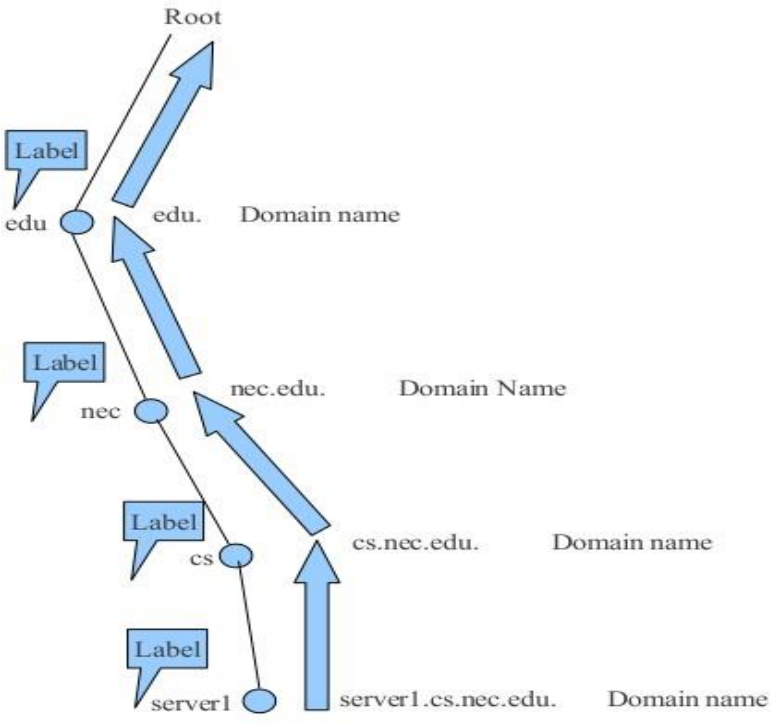


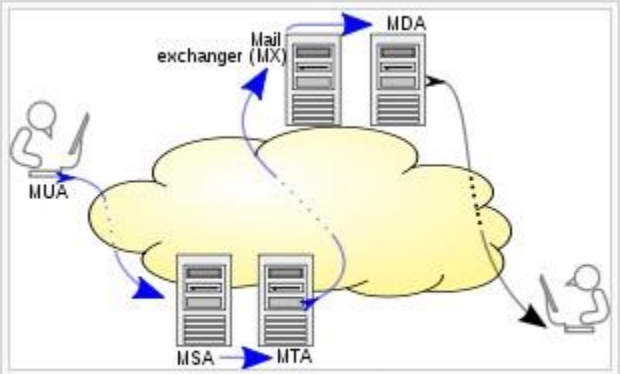
Fig: Domain Name and Labels

Simple Mail Transfer Protocol (SMTP)

One of the most popular network services, email is supported by TCP/IP protocol SMTP. It provides system for sending message to other computers and provide a mail exchange between users. SMTP supports:

- Sending a message to one or more recipients.
- Sending message that includes texts, voice, video or graphics.
- Sending message to users on the network outside the Internet.

SMTP supports sending of email only It cannot pull messages from a remote server on demand. Other protocols, such as the Post Office Protocol (POP) and the Internet Message Access Protocol (IMAP) are specifically designed for retrieving messages and managing mail boxes. However, SMTP has a feature to initiate mail queue processing on a remote server so that the requesting system may receive any messages destined for it (cf. Remote Message Queue Starting). POP and IMAP are preferred protocols when a user's personal computer is only intermittently powered up, or Internet connectivity is only transient and hosts cannot receive message during off-line periods.



Blue arrows can be implemented using SMTP variations.

The overall flow for message creation, mail transport, and delivery may be illustrated as shown.

Email is submitted by a mail client (MUA, mail user agent) to a mail server (MSA, mail submission agent) using SMTP on TCP port 587. Most mailbox providers still allow submission on traditional port 25. From there, the MSA delivers the mail to its mail transfer agent (MTA, mail transfer agent). Often, these two agents are just different instances of the same software launched with different options on the same machine. Local processing can be done either on a single machine, or split among various appliances; in the former case, involved processes can share files; in the latter case, SMTP is used to transfer the message internally, with each host configured to use the next appliance as a smart host. Each process is an MTA in its own right; that is, an SMTP server.

The boundary MTA has to locate the target host. It uses the Domain name system (DNS) to look up the mail exchanger record (MX record) for the recipient's domain (the part of the address on the right of @). The returned MX record contains the name of the target host. The MTA next looks up the A record for that name in order to get the IP address and connect to such host as an SMTP client.

Once the MX target accepts the incoming message, it hands it to a mail delivery agent (MDA) for local mail delivery. An MDA is able to save messages in the relevant mailbox

format. Again, mail reception can be done using many computers or just one —the picture displays two nearby boxes in either case. An MDA may deliver messages directly to storage, or forward them over a network using SMTP, or any other means, including the Local Mail Transfer Protocol (LMTP), a derivative of SMTP designed for this purpose.

Once delivered to the local mail server, the mail is stored for batch retrieval by authenticated mail clients (MUAs). Mail is retrieved by end-user applications, called email clients, using Internet Message Access Protocol (IMAP), a protocol that both facilitates access to mail and manages stored mail, or the Post Office Protocol (POP) which typically uses the traditional m box mail file format or a proprietary system such as Microsoft Exchange/Outlook or Lotus Notes/Domino. Webmail clients may use either method, but the retrieval protocol is often not a formal standard.

IMAP (Internet Mail Access Protocol)
An Internet standard protocol for storing and retrieving messages from Simple Mail Transfer Protocol (SMTP) hosts. Internet Mail Access Protocol version provides functions similar to Post Office Protocol version 3 (POP3), with additional features as described in this entry.

How It Works?
SMTP provides the underlying message transport mechanism for sending e-mail over the Internet, but it does not provide any facility for storing and retrieving messages. SMTP hosts must be continuously connected to one another, but most users do not have a dedicated connection to the Internet.
IMAP4 provides mechanisms for storing messages received by SMTP in a receptacle called a mailbox. An IMAP4 server stores messages received by each user until the user connects to download and read them using an IMAP4 client such as Evolution or Microsoft Outlook Express.

IMAP4 includes a number of features that are not supported by POP3. Specifically, IMAP4 allows users to

- Access multiple folders, including public folders
- Create hierarchies of folders for storing messages
- Leave messages on the server after reading them so that they can access the messages again from another location
- Search a mailbox for a specific message to download
- Flag messages as read
- Selectively download portions of messages or attachments only
- Review the headers of messages before downloading them

To retrieve a message from an IMAP4 server, an IMAP4 client first establishes a Transmission Control Protocol (TCP) session using TCP port 143. The client then identifies itself to the server and issues a series of IMAP4 commands:

- LIST:
  Retrieves a list of folders in the client's mailbox
- SELECT:
  Selects a particular folder to access its messages
- FETCH:
  Retrieves individual messages

- LOGOUT:
  Ends the IMAP4 session

Post Office Protocol version 3 (POP3)

An Internet standard protocol for storing and retrieving messages from Simple Mail Transfer Protocol (SMTP) hosts.

How It Works?
SMTP provides the underlying transport mechanism for sending e-mail messages over the Internet, but it does not provide any facility for storing messages and retrieving them. SMTP hosts must be continuously connected to one another, but most users do not have a dedicated connection to the Internet.

Post Office Protocol version 3 (POP3) provides mechanisms for storing messages sent to each user and received by SMTP in a receptacle called a mailbox. A POP3 server stores messages for each user until the user connects to download and read them using a POP3client such as Microsoft Outlook 98, Microsoft Outlook Express, or Microsoft Mail and News.

To retrieve a message from a POP3 server, a POP3 client establishes a Transmission Control Protocol (TCP) session using TCP port 110, identifies itself to the server, and then issues a series of POP3 commands:

- stat:
  Asks the server for the number of messages waiting to be retrieved
- list:
  Determines the size of each message to be retrieved
- retr:
  Retrieves individual messages
- Quit:
  Ends the POP3 session

After a POP3 client reads a message in its mailbox on a POP3 server, the message is deleted. Primarily because of this, POP3 is being supplanted by Internet Mail Access Protocol version 4 (IMAP4), which offers better support for mobile users. POP3 is supported by Microsoft Exchange Server.

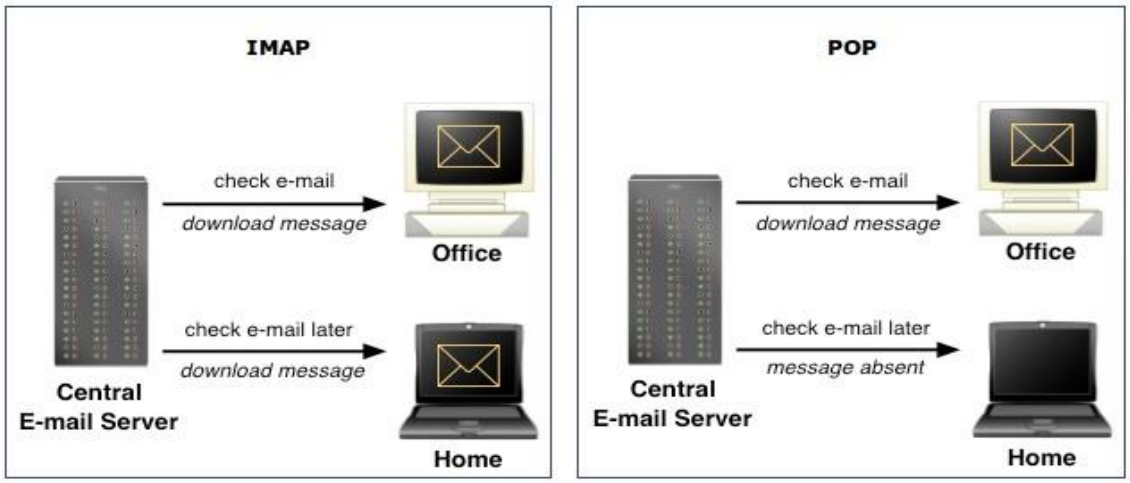
IMAP VS POP:

What's the difference?
The main difference, as far as we are concerned here, is the way in which IMAP or POP controls your e-mail inbox.

When you use IMAP you are accessing your inbox on the mail server. IMAP does not actually move messages onto your computer. You can think of an e-mail program using IMAP as a window to your messages on the server. Although the messages appear on your computer while you work with them, they remain on the central mail server.

POP does the opposite. Instead of just showing you what is in your inbox on the U's mail server, it checks the server for new messages, downloads all the new messages in your inbox onto your computer, and then deletes them from the server. This means that every time you

use POP to view your new messages; they are no longer on the central mail server. Figure illustrates these concepts



IMAP makes it easier to view mail from home, work, and other locations

Because IMAP leaves all of your messages on the central mail server, you can view these messages from any location with Internet access. This means the U of M e-mail inbox you view from home will be the same one you see at work.

Since POP downloads new messages to your computer and removes them from the server, you will not be able to see those new messages on another computer when you check your inbox. Those messages exist only on the computer that downloaded them using POP.

However, if you use IMAP and create e-mail folders on the server, these folders are accessible from anywhere you read your e-mail using IMAP. If you use POP and create e-mail folders, they are stored locally, and you cannot access these folders from anywhere except the computer on which you created them.

POP can create problems if you alternate between it and IMAP. There is an option in many POP e-mail programs to leave copies of the messages on the server, but this option has complications. When you leave copies of the messages on the server, then access your e-mail using Webmail or another IMAP e-mail client, the POP client
may create duplicate messages next time it accesses the inbox; you will see each of the messages more than once, and you will have to clean out (delete) the unwanted ones.

Virtual Private Network (VPN)

The Internet is a worldwide, publicly accessible IP network. Due to its vast global proliferation, it has become a viable method of interconnecting remote sites. However, the fact that it is a public infrastructure has deterred most enterprises from adopting it as a viable remote access method for branch and SOHO sites.
A virtual private network (VPN) is a concept that describes how to create a private network over a public network infrastructure while maintaining confidentiality and security. VPNs use cryptographic tunneling protocols to provide sender authentication, message integrity, and confidentiality by protecting against packet sniffing. VPNs can be implemented at Layers 2, 3, and 4 of the Open Systems Interconnection (OSI) model. Figure illustrates a typical VPN topology. Components required to establish a VPN include:

- An existing network with servers and workstations
- Connection to the Internet
- VPN gateways (i.e., routers, PIX, ASA, VPN concentrators) that act as endpoints to establish, manage, and control VPN connections
- Software to create and manage tunnels

The key to VPN technology is security. VPNs secure data by encapsulating the data, encrypting the data, or both encapsulating the data and then encrypting it:

- Encapsulation is also referred to as tunneling because encapsulation transmits data transparently from network to network through a shared network infrastructure.
- Encryption codes data into a different format. Decryption decodes encrypted data into the data's original unencrypted format.

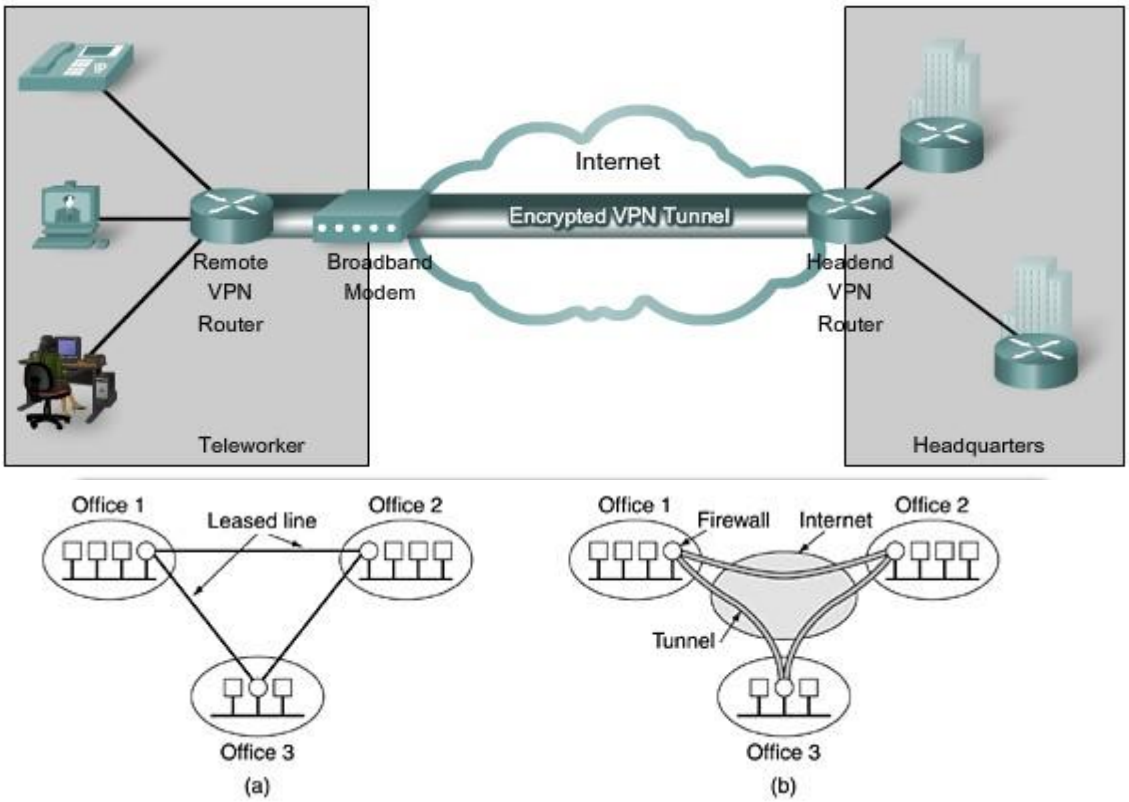


Fig:(a) A leased-line private network. (b) A virtual private network.

Basically, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

A well-designed VPN can greatly benefit a company. For example, it can:

- Extend geographic connectivity
- improve security
- Reduce operational costs versus traditional WAN
- Reduce transit time and transportation costs for remote users
- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide telecommuter support
- Provide broadband networking compatibility

- Provide faster ROI (return on investment) than traditional WAN

What features are needed in a well-designed VPN? It should incorporate:

- Security
- Reliability
- Scalability
- Network management
- Policy management

IPSEC

IPsec provides a mechanism for secure data transmission over IP networks, ensuring confidentiality, integrity, and authenticity of data communications over unprotected networks such as the Internet . IPsec encompasses a suite of protocols and is not bound to any specific encryption or authentication algorithms, key generation technique, or security association (SA). IPsec provides the rules while existing algorithms provide the encryption, authentication, key management, and so on. IPsec acts at the network layer, protecting and authenticating IP packets between IPsec devices (peers), such as Cisco PIX Firewalls, Adaptive Security Appliances (ASA), Cisco routers, the Cisco Secure VPN Client, and other IPsec-compliant products.

IPsec provides the following essential security functions:

- **Data confidentiality:** IPsec ensures confidentiality by using encryption. Data encryption prevents third parties from reading the data, especially data that is transmitted over public networks or wireless networks. The IPsec sender can encrypt packets before transmitting the packets across a network and prevent anyone from hearing or viewing the communication (eavesdropping).
- **Data integrity:** IPsec ensures that data arrives unchanged at the destination; that is, that the data is not manipulated at any point along the communication path. IPsec ensures data integrity by using hashes.
- **Data origin authentication:** The IPsec receiver can authenticate the source of the IPsec packets. Authentication ensures that the connection is actually made with the desired communication partner.
- **Anti-replay:** Anti-replay protection verifies that each packet is unique, not duplicated. IPsec packets are protected by comparing the sequence number of the received packets and a sliding window on the destination host, or security gateway. A packet whose sequence number is before the sliding window is considered late, or a duplicate. Late and duplicate packets are dropped.

Proxy server

A computer that can act on the behalf of other computers to request content from the Internet or an intranet. Proxy Server is placed between a user's machine and the Internet. It can act as a firewall to provide protection and as a cache area to speed up Web page display. A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Proxy servers have two main purposes:

- **Improve Performance:** Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users.
- **Filter Requests:** Proxy servers can also be used to filter requests.

Types of Proxy:

1. **Forward Proxy:**
   Forward proxies are proxies where the client server names the target server to connect to. Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).The terms "forward proxy" and "forwarding proxy" are a general description of behavior (forwarding traffic) and thus ambiguous. Except for Reverse proxy

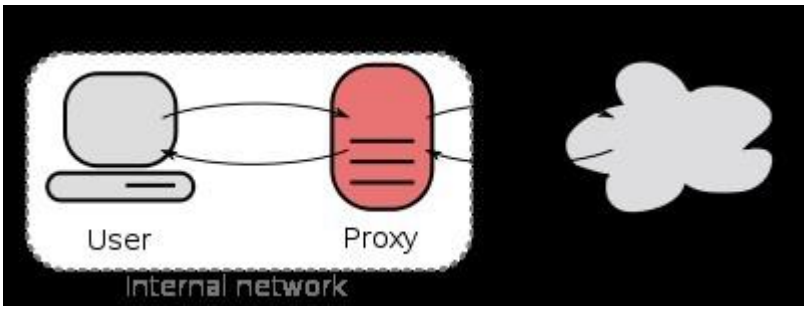


Fig:A forward proxy taking requests from an internal network and forwarding them to the Internet

2. **Open Proxy:**
   An open proxy is a forward proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet.[4] An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services.

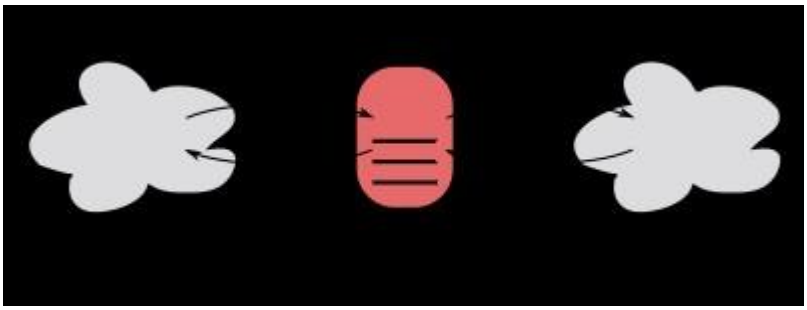
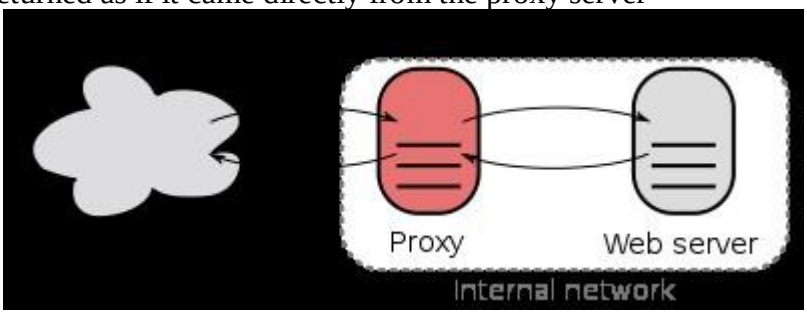


Fig: An open proxy forwarding requests from and to anywhere on the Internet.

3. **Reverse Proxy:**
   A reverse proxy is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more origin servers which handle the request. The

response is returned as if it came directly from the proxy server



ù

Fig: A reverse proxy taking requests from the Internet and forwarding them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network.

File Transfer Protocol (FTP)

An Internet standard application-level TCP/IP protocol that can be used for transferring files between hosts on a TCP/IP internetwork.

How It Works?

File Transfer Protocol (FTP) is one of the earliest Internet protocols, and is still used for uploading and downloading files between clients and servers. An FTP client is an application that can issue FTP commands to an FTP server, while an FTP server is a service or daemon running on a server that responds to FTP commands from a client. FTP commands can be used to change directories, change transfer modes between binary and ASCII, upload files, and download files. FTP uses Transmission Control Protocol (TCP) for reliable network communication by establishing a session before initiating data transfer. TCP port number 21 on the FTP server listens for connection attempts from an FTP client and is used as a control port for establishing a connection between the client and server, for allowing the client to send an FTP command to the server, and for returning the server's response to the command. Once a control connection has been established, the server opens port number 20 to form a new connection with the client for transferring the actual data during uploads and downloads.

While transferring Data over the network, two modes can be used:

1. Ascii Mode
2. Binary Mode

The two types differ from the way they send the data. When a file is sent using an ASCII-type transfer, the individual letters, numbers and characters are sent. The receiving machine saves these in a text file in the appropriate format (for example, a Unix machine saves it in a Unix format, a Macintosh saves it in a Mac format). Hence if an ASCII transfer is used it can be assumed plain text is sent, which is stored by the receiving computer in its own format.

Sending a file in binary mode is different. The sending machine sends each file bit for bit and as such the recipient stores the bit-stream as it receives it.

By default, most FTP clients use ASCII mode. Some clients, nevertheless are more clever and try to determine the required transfer-mode by inspecting the file's contents.

Chapter9:
Network Management and Security:

Introduction to Network Management:
Network management is defined as monitoring, testing, configuring, and troubleshooting network components to meet a set of requirements defined by an organization. These requirements include the smooth, efficient operation of the network that provides the predefined quality of service for users. To accomplish this task, a network management system uses hardware, software, and humans.

Functions of Network Management System:

1. Configuration Management
2. Fault Management
3. Performance Management
4. Security management
5. Accounting management

Configuration Management
A large network is usually made up of hundreds of entities that are physically or logically connected to one another. These entities have an initial configuration when the network is set up, but can change with time. Desktop computers may be replaced by others; application software may be updated to a newer version; and users may move from one group to another. The configuration management system must know, at any time, the status of each entity and its relation to other entities. Configuration management can be subdivided into two parts reconfiguration and Documentation.

Fault Management:
Falls on two categories.

- Reactive Fault Management
  A reactive fault management system is responsible for detecting, isolating, correcting, and recording faults. It handles short-term solutions to faults.
- Proactive Fault Management
  Proactive fault management tries to prevent faults from occurring. Although this is not always possible, some types of failures can be predicted and prevented.

Performance management:
It is is closely related to fault management and tries to monitor and control the network to ensure that it is running as efficiently as possible.

Security Management
Security management is responsible for controlling access to the network based on the predefined policy.

Accounting Management
Accounting management is the control of users' access to network resources through charges. Charging does not necessarily mean cash transfer; it may mean debiting the departments or divisions for budgeting purposes. Today, organizations use an accounting management system for the following reasons:

- It prevents users from monopolizing limited network resources.
- It prevents users from using the system inefficiently.
- Network managers can do short- and long-term planning based on the demand for network use.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

The Simple Network Management Protocol (SNMP) is a framework for managing devices in an Internet using the TCPIIP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an Internet.

Concept

SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers . SNMP is an application-level protocol in which a few manager stations control a set of agents. The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.

Managers and Agents

A management station, called a manager, is a host that runs the SNMP client program. A managed station, called an agent, is a router (or a host) that runs the SNMP server program. Management is achieved through simple interaction between a manager and an agent. The agent keeps performance information in a database. The manager has access to the values in the database. For example, a router can store in appropriate variables the number of packets received and forwarded. The manager can fetch and compare the values of these two variables to see if the router is congested or not.

An SNMP-managed network consists of three key components:

- Managed device
- Agent — software which runs on managed devices
- Network management system (NMS) — software which runs on the manager

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP specific form.

A network management system (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required

for network management. One or more NMSs may exist on any managed network.

Management with SNMP is based on three basic ideas:

- A manager checks an agent by requesting information that reflects the behavior of the agent.
- A manager forces an agent to perform a task by resetting values in the agent database.
- An agent contributes to the management process by warning the manager of an unusual situation.

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162. The agent may generate notifications from any available port.

To do management tasks, SNMP uses two other protocols:

- Structure of Management Information (SMI)
- Management Information Base (MIB).

Role of SNMP
SNMP has some very specific roles in network management. It defines the format of the packet to be sent from a manager to an agent and vice versa. It also interprets the result and creates statistics (often with the help of other management software). The packets exchanged contain the object (variable) names and their status (values). SNMP is responsible for reading and changing these values.

Roles of SMI
SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values. SM1 does not define the number of objects an entity should manage or name the objects to be managed or define the association between the objects and their values.
The Structure of Management Information, version 2 (SMIv2) is a component for network management. Its functions are

- To name objects
- To define the type of data that can be stored in an object
- To show how to encode data for transmission over the network

SMI is a guideline for SNMP. It emphasizes three attributes to handle an object: name, data type, and encoding method .

Roles of MIB
For each entity to be managed, this protocol must define the number of objects, name them according to the rules defined by SMI, and associate a type to each named object .MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed. Each agent has its own MIB2, which is a collection of all the objects that the manager can manage. The objects in MIB2 are categorized under 10 different groups: system, interface, address translation, ip, icmp, tcp, udp, egp, transmission, and snmp.

Cryptography

Cryptography is derived from the Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing". Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

Encryption and Decryption

Plain-text and Cipher-text

The original message, before being transformed, is called plaintext. After the message is transformed, it is called cipher-text. An encryption algorithm transforms the plain text into cipher text; a decryption algorithm transforms the cipher-text back into plain- text. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Cipher

We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for a secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and the plain-text. These create the cipher-text. To decrypt a message, we need a decryption algorithm, a decryption key, and the cipher-text. These reveal the original plain-text.

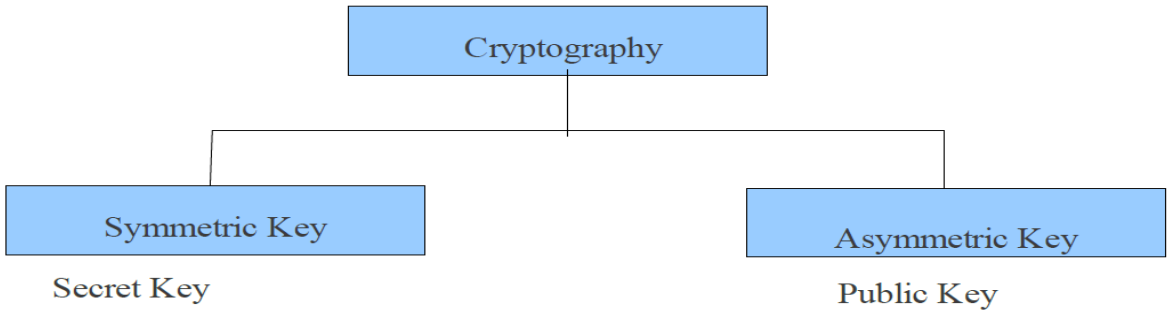
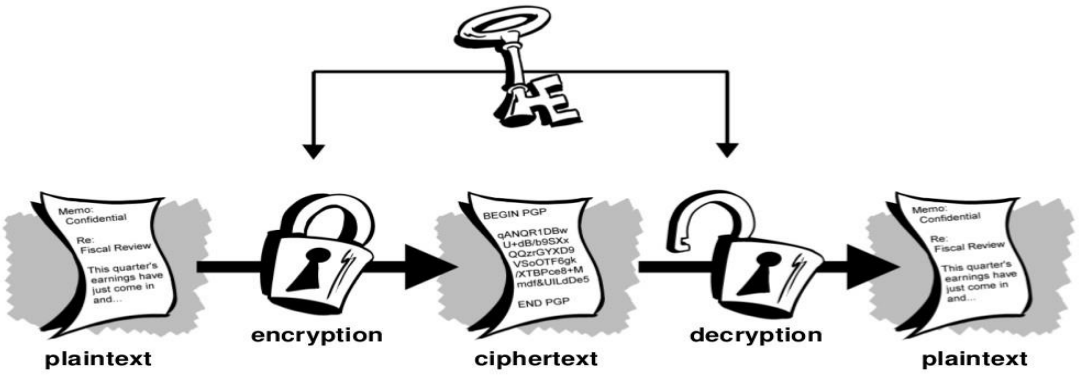


Fig:Categories of Cryptography

Symmetric-key

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government. Figure below shows an illustration of the conventional encryption process.

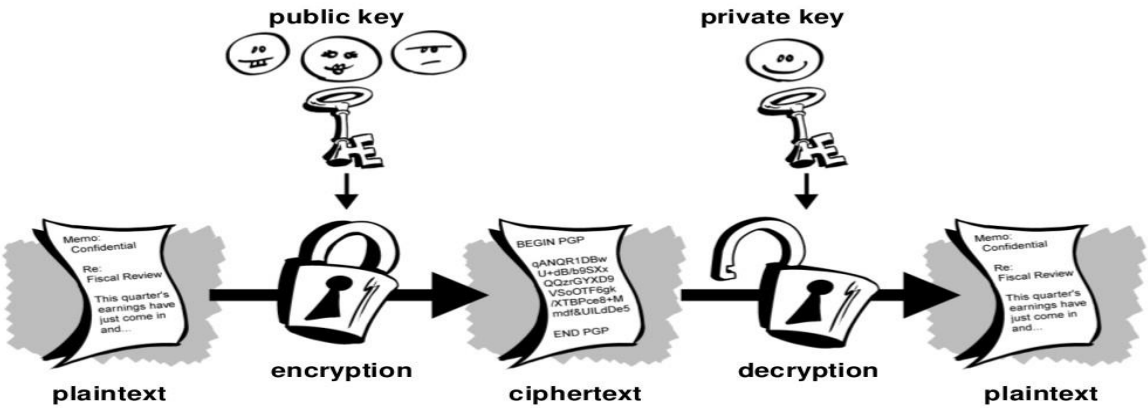


Conventional encryption has benefits. It is very fast. It is especially useful for encrypting data that is not going anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution.

For a sender and recipient to communicate securely using conventional encryption, they must agree upon a key and keep it secret between themselves. If they are in different physical locations, they must trust a courier, the Bat Phone, or some other secure communication medium to prevent the disclosure of the secret key during transmission. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key.

Asymmetric-Key Cryptography

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read . It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.



The Essential steps in Asymmetric-key cryptography are the following:

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the keys in a public register or other accessible file. This is the public key. The companion key is kept private. Each user maintains a collection of public keys obtained from others
3. If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows the Alice's private key.

With this approach, all the participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed. As long as a user protects his and her private key, incoming communication is secure. At any time, a user change the private key and publish the companion public key replace the old public key.

Comparison

Let us compare symmetric-key and asymmetric-key cryptography. Encryption can be thought of as electronic locking; decryption as electronic unlocking. The sender puts the message in a box and locks the box by using a key; the receiver unlocks the box with a key and takes out the message. The difference lies in the mechanism of the locking and unlocking and the type of keys used. In symmetric-key cryptography, the same key locks and unlocks the box. In asymmetric-key cryptography, one key locks the box, but another key is needed to unlock it.

Traditional Cipher used in Symmetric-key Cryptography:
Two types:

1. Substitution cipher
2. Transposition cipher

Substitution cipher:

A substitution cipher substitutes one symbol with another. If the symbols in the plain- text are alphabetic characters, we replace one character with another. For example, we can replace character A with D, and character T with Z. If the symbols are digits (0 to 9), we can replace 3 with 7, and 2 with 6. It is also known and Ceaser's Cipher who invented it.

For example, if we encode the word “SECRET” using Caesar’s key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet. So starting with ABCDEFGHIJKLMNOPQRSTUVWXYZ and sliding everything up by 3, you get DEFGHIJKLMNOPQRSTUVWXYZABC where D=A, E=B, F=C, and so on. Using this scheme, the plaintext, “SECRET” encrypts as “VHFUHW.” To allow someone else to read the cipher text, you tell them that the key is 3.

Transposition Ciphers

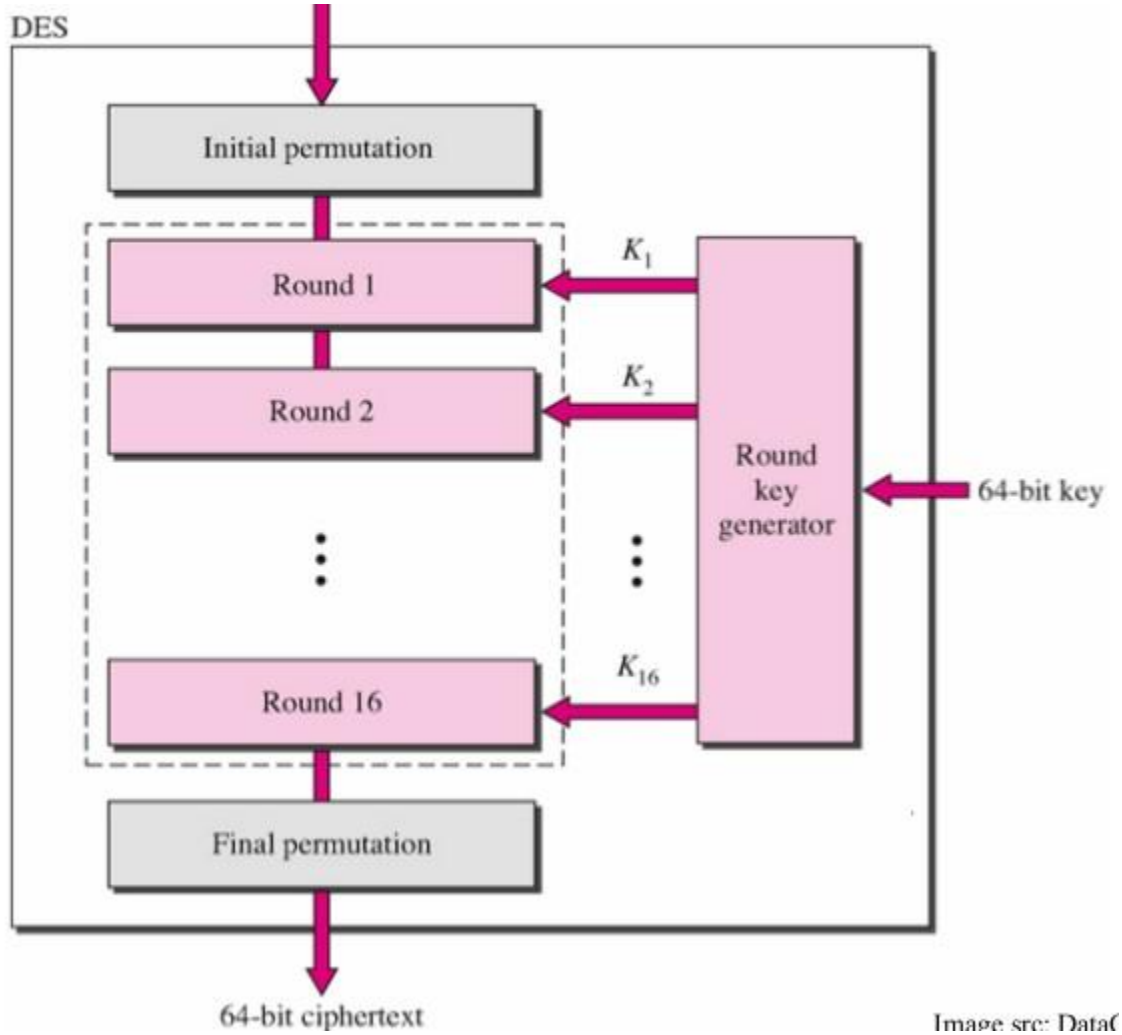
In a transposition cipher, there is no substitution of characters; instead, their locations change. A character in the first position of the plaintext may appear in the tenth position of the cipher text. A character in the eighth position may appear in the first position. In other words, a transposition cipher reorders the symbols in a block of symbols.

Key: In a transposition cipher, the key is a mapping between the position of the symbols in the plaintext and cipher text. For example, the following shows the key using a block of four characters:

Plaintext: 2 4 1 3
Cipher text: 1 2 3 4
In encryption, we move the character at position 2 to position 1, the character at position 4 to position 2, and so on. In decryption, we do the reverse.

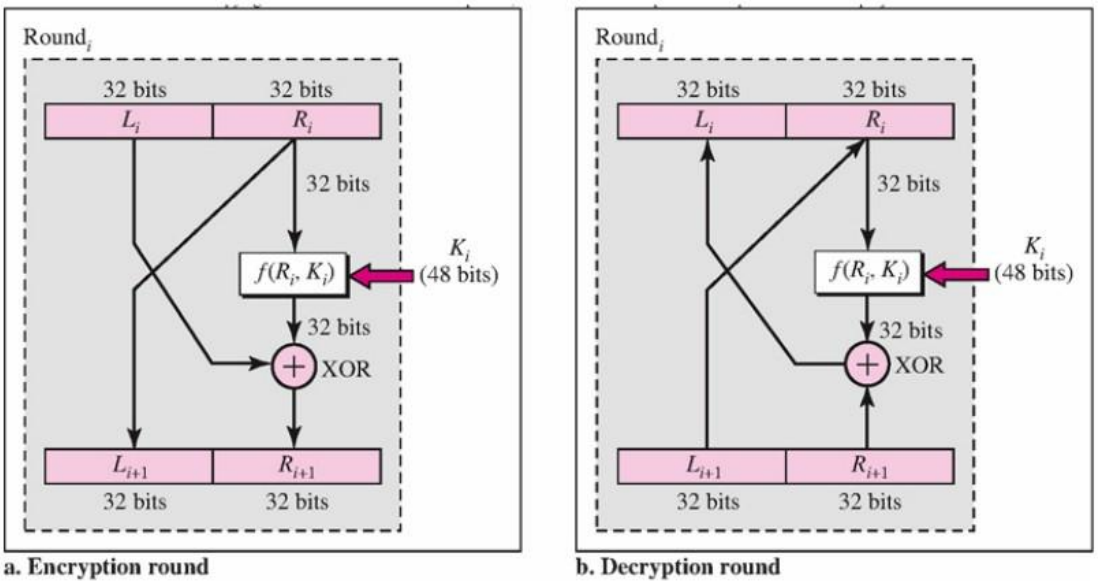
Encryption algorithm:
The most commonly used symmetric encryption are block ciphers. A block cipher processes the plain text input in fixed size blocks and produces a block of cipher text of equal size for each plain text block.
The two most important symmetric algorithms, both of which are block ciphers, are
Data Encryption Standard (DES)
Advanced Encryption Standard (AES)

DES (Data Encryption Standard):
The Data Encryption Standard, is a block cipher operating on 64-bit data blocks. DES was designed by IBM and adopted by the U.S. government as the standard encryption method for nonmilitary and nonclassified use. The algorithm encrypts a 64-bit plaintext block using a 64-bit key, as shown in Figure



DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated). Although the 16 iteration round ciphers are conceptually the same, each uses a

different key derived from the original key. The initial and final permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64-bit input and permutes them according to predefined values. Each round of DES is a complex round cipher, as shown in Figure below. Note that the structure of the encryption round ciphers is different from that of the decryption one.



Asymmetric Key Cryptography:
Some examples of public-key cryptosystems are :
Elgamal (named for its inventor, Taher Elgamal),
RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman),
Diffie-Hellman (named for its inventors),
DSA ,the Digital Signature Algorithm (invented by David Kravitz).

RSA Algorithm

This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars **Ron Rivest, Adi Shamir,** and **Len Adleman** and hence, it is termed as RSA cryptosystem.

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair

Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below −

- **Generate the RSA modulus (n)**
    - Select two large primes, p and q.

- Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

- **Find Derived Number (e)**
  - Number **e** must be greater than 1 and less than (p − 1)(q − 1).
  - There must be no common factor for e and (p − 1)(q − 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are coprime.

- **Form the public key**
  - The pair of numbers (n, e) form the RSA public key and is made public.
  - Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.

- **Generate the private key**
  - Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
  - Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).
  - This relationship is written mathematically as follows −

$$ed = 1 \bmod (p-1)(q-1)$$

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example

An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

- Let two primes be p = 7 and q = 13. Thus, modulus n = pq = 7 x 13 = 91.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and (p − 1)(q − 1) = 6 × 12 = 72, except for 1.
- The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
- Check that the d calculated is correct by computing −

$$de = 29 \times 5 = 145 = 1 \bmod 72$$

- Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption

Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as −

$$C = P^e \bmod n$$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
- Returning to our Key Generation example with plaintext P = 10, we get ciphertext C −

$$C = 10^5 \bmod 91$$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a ciphertext C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$$\text{Plaintext} = C^d \bmod n$$

- Returning again to our numerical example, the ciphertext C = 82 would get decrypted to number 10 using private key 29 −

$$\text{Plaintext} = 82^{29} \bmod 91 = 10$$

RSA Analysis

The security of RSA depends on the strengths of two separate functions. The RSA cryptosystem is most popular public-key cryptosystem strength of which is based on the practical difficulty of factoring the very large numbers.

- **Encryption Function** − It is considered as a one-way function of converting plaintext into cipher text and it can be reversed only with the knowledge of private key d.
- **Key Generation** − The difficulty of determining a private key from an RSA public key is equivalent to factoring the modulus n. An attacker thus cannot use knowledge of an RSA public key to determine an RSA private key unless he can factor n. It is also a one way function, going from p & q values to modulus n is easy but reverse is not possible.

If either of these two functions are proved non one-way, then RSA will be broken. In fact, if a technique for factoring efficiently is developed then RSA will no longer be safe.

The strength of RSA encryption drastically goes down against attacks if the number p and q are not large primes and/ or chosen public key e is a small number.