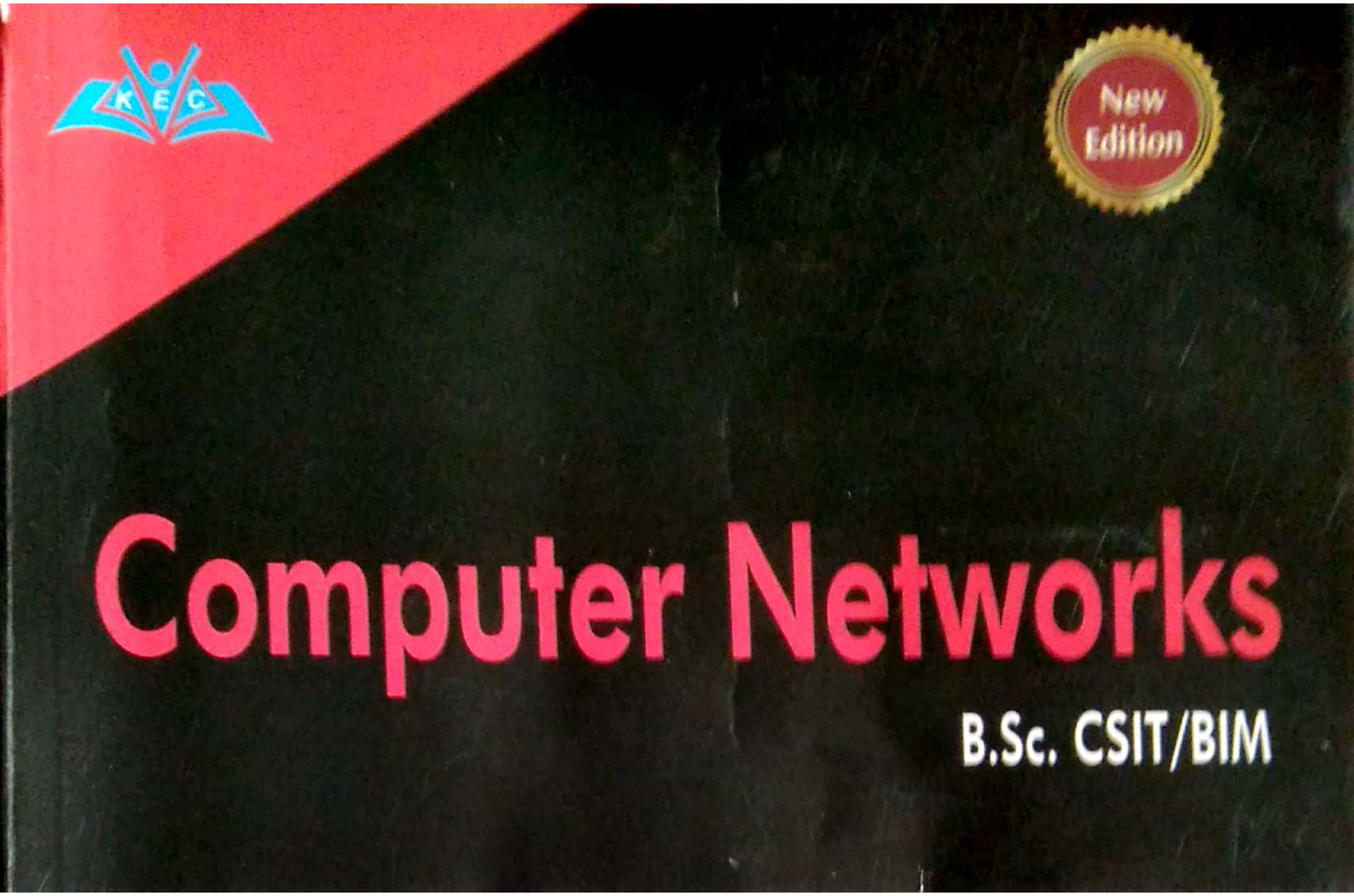


Chapter 1
INTRODUCTION TO COMPUTER NETWORK

Introduction

Each of the past three centuries was dominated by a single new technology. The 18th century was the era of the great mechanical systems accompanying the Industrial Revolution. The 19th century was the age of the steam engine. During the 20th century, the key technology was information gathering, processing, and distribution. Among other developments, we saw the installation of worldwide telephone networks, the inventions of radio and television, the birth and unprecedented growth of the computer industry, the launching of communication satellites, and, of course, the Internet.

The computers and communications have been merged together and their merger has had a profound effect on the manner in which computer systems are organized. The old model in which a single computer used to serve all the computational needs of an organization has been replaced by a new one in which a large number of separate but interconnected computers do the job. Such systems are called as **computer networks.** Two computers are said to be interconnected if they interchange information. The connection between the separate computers can be done via a copper wire, fiber optics, microwaves or communication satellite. A printer, computer, or any machine that is capable of communicating on the network is referred to as a device or node. We can also say that computer network is an interconnection of various computers to share software, hardware and data through a communication medium between them. The computers connected in a network share files, folders, applications and resources like scanner, web-cams, printers etc. The best example of computer network is the Internet.

A computer network is an interconnection of various computers to share software, hardware, resources and data through a communication medium between them. A Computer Networking is a set of autonomous computers that permits distributed processing of the information and data and increased Communication of resources. Any Computer Networking communication need a sender, a receiver and a communication medium to transfer signal or Data from sender to the receiver. We need sender, receiver, communication channel, protocols and operating system to establish a computer networking.

Definition, Uses, Benefits

What is Computer Network?

A computer network can be described as a system of interconnected devices that can communicate using some common standards (called protocols). These devices communicate to exchange resources (e.g. files and printers) and services.

Here is an example network consisting of two computers connected together:

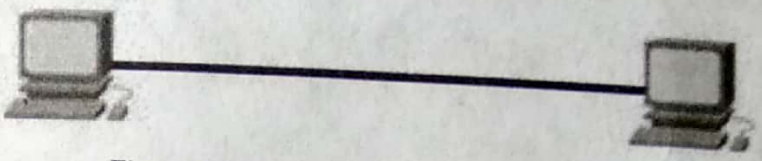


Figure 1.1 Network of two computers only

In the example above, the two computers are directly connected using a cable. This small network can be used to exchange data between just these two computers.

What if we want to expand our network? Then we can use a network device, either a switch or a hub, to connect more than two computers together:

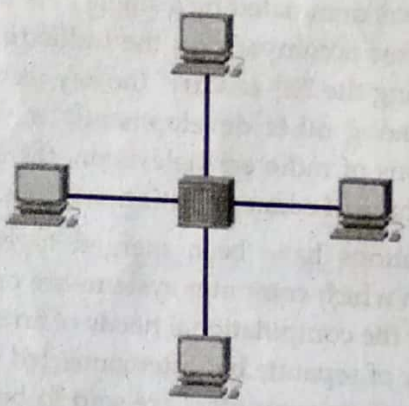


Figure 1.2 Network with hub

Now all of the devices on the network can communicate with each other.

Uses of Computer Network

Since computer network is an interconnection of computers, printers, scanners and other hardware devices and software applications. Networks connect users within a defined physical space (such as within an office building). The Internet is a network that connects users from all parts of the world. Educational institutions, government agencies, health care facilities, banking and other financial institutions, and residential applications use computer networking to send and receive data and share resources.

Business Application

Many organizations have a large number of computers in operation. These computers may be within the same building, campus, city or different cities. Even though the computers are located in different locations, the organizations want to keep track of inventories, monitor productivity, do the ordering and billing etc. Following are some business applications of computer networks:

1. Resource sharing:

The goal is to make all programs, equipment (like printers etc.), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

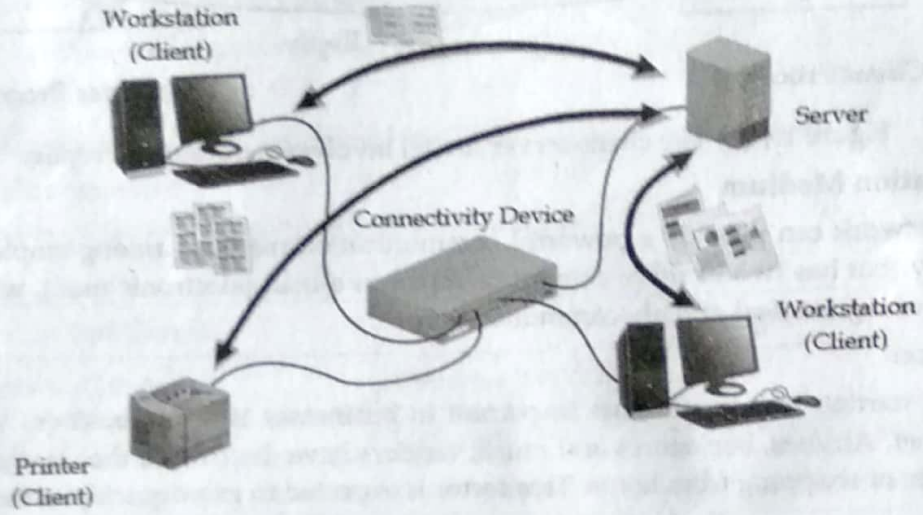


Figure 1.3: Resource sharing on a client/server network

2. Server-Client model:

One can imagine a company's information system as consisting of one or more databases and some employees who need to access it remotely. In this model, the data is stored on powerful computers called Servers. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simple machines, called Clients, on their desks, using which they access remote data.

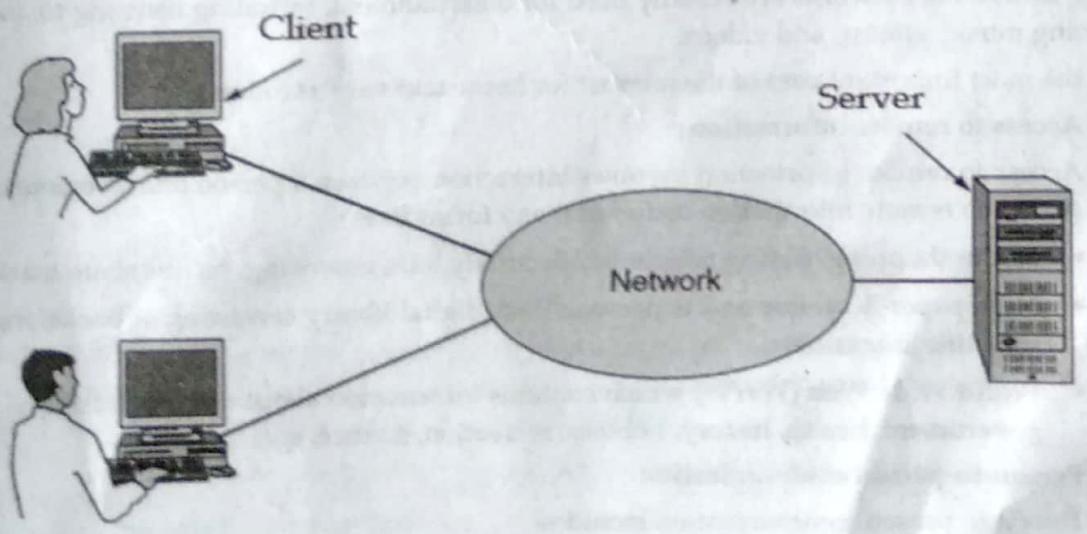


Figure 1.4 (a) A network with two clients and one server

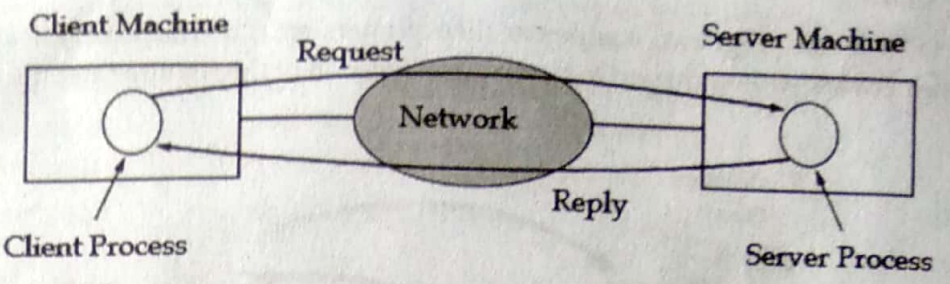


Figure 1.4 (b) The client-server model involves requests and replies

3. Communication Medium

A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication

4. E-Commerce:

A goal that is starting to become more important in businesses is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future.

Home Applications

In 1977, Ken Olsen was president of the Digital Equipment Corporation, then the number two computer vendor in the world (after IBM). When asked why Digital was not going after the personal computer market in a big way, he said: "There is no reason for any individual to have a computer in his home." History showed otherwise and Digital no longer exists. People initially bought computers for word processing and games. Recently, the biggest reason to buy a home computer was probably for Internet access. Now, many consumer electronic devices, such as set-top boxes, game consoles, and clock radios, come with embedded computers and computer networks, especially wireless networks, and home networks are broadly used for entertainment, including listening to, looking at, and creating music, photos, and videos.

Some of the most important uses of the internet for home users are as follows:

1. **Access to remote information**

   Access to remote information involves interaction between a person and a remote database. Access to remote information comes in many forms like:

   - Home shopping, paying telephone, electricity bills, e-banking, on line share market etc.
   - Newspaper is on-line and is personalized, digital library consisting of books, magazines, scientific journals etc.
   - World Wide Web (WWW) which contains information about the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.

2. **Person-to-person communication**

   Person to person communication includes:

   - Electronic-mail (e-mail)
   - Real time e-mail i.e. video conferencing allows remote users to communicate with no delay by seeing and hearing each other. Video-conferencing is being used for remote school, getting medical opinion from distant specialists etc.

- Worldwide newsgroups in which one person posts a message and all other subscribers to the newsgroup can read it or give their feedbacks.

3. **Interactive entertainment**

Interactive entertainment includes:

- Multi-person real-time simulation games.
- Video on demand.
- Participation in live TV programs likes quiz, contest, discussions etc.

4. **Electronic commerce**

The most popular forms are listed in the below table:

Table 1.1: Some forms of e-commerce

Tag	Full Name	Example
B2C	Business-to-Consumer	Ordering books on-line
B2B	Business-to-Business	Car manufacture ordering tires from supplier
C2C	Consumer-to-Consumer	Auctioning second-hand products on line
G2C	Government-to-Consumer	Government distributing tax form electronically
P2P	Peer-to-Peer	File sharing

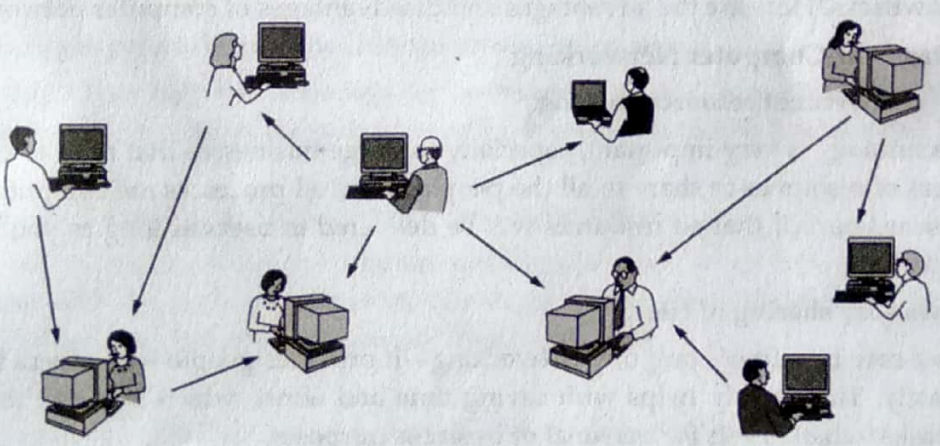


Figure 1.5 In a peer-to-peer system there are no fixed clients and servers.

Mobile Users

Mobile computers, such as notebook computers and mobile phones, is one of the fastest-growing segment of the entire computer industry. Although wireless networking and mobile computing are often related, they are not identical, as the below table shows.

Table 1.2: Combinations of wireless networks and mobile computing

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Social Issues

Computer networks, like the printing press 500 years ago, allow ordinary citizens to distribute and view content in ways that were not previously possible. But along with the good comes the bad, as this new-found freedom brings with it many unsolved social, political, and ethical issues. Let us just briefly mention a few of them; a thorough study would require a full book, at least.

Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

The trouble comes with topics that people actually care about, like politics, religion, or sex. Views that are publicly posted may be deeply offensive to some people. Worse yet, they may not be politically correct. Furthermore, opinions need not be limited to text; high-resolution color photographs and video clips are easily shared over computer networks. Some people take a live-and-let-live view, but others feel that posting certain material (e.g., verbal attacks on particular countries or religions, pornography, etc.) is simply unacceptable and that such content must be censored. Different countries have different and conflicting laws in this area. Thus, the debate rages.

Advantages and Disadvantages of Computer Networks

With computers wirelessly linked together through a network, computer networking has been an essential means of sharing information. It is a practice widely used in the modern world, as it provides a multitude of benefits to individuals and businesses alike. However, it does not come without any drawbacks. Here are the advantages and disadvantages of computer networking:

List of Advantages of Computer Networking

1. **It offers convenient resource sharing.**

   This technology is very important, especially for large businesses that need to produce huge numbers of resources to share to all the people. Since all processes are computer based, you can assure yourself that all resources will be delivered to users as long as you have reliable connectivity.

2. **It allows easy sharing of files.**

   This is a core benefit of computer networking—it provides people with access to share their files easily. This greatly helps with saving time and effort, which they can then spend on other tasks, whether it is for personal or business purposes.

3. **It provides the benefit of flexibility.**

   Computer networking is known to offer high flexibility in a sense that you are given the chance to explore everything about a certain type of software without affecting its functionality. You will have the accessibility to all information that you need.

4. **Its system is inexpensive to operate.**

   Installing computer networking software would typically not cost a lot, and mostly, they are dependable when it comes to helping you share information on a network or the web. Moreover, you do not need to entirely change software as you just need to install updates, unless the need arises.

5. **It increases storage capacity.**

   Since you are sharing resources and files to others, it is just normal that you should be able to sufficiently store all the data and files. With this technology, it is a must that you should

have storage capacity that can accommodate all that you need to keep your activities and operations up and running.

6. **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.

7. **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.

List of Disadvantages of Computer Networking

1. **It comes with the risk of security issues.**

   Considering the large number of people using a computer network and sharing files and resources, your security would normally be at risk. As you can see, there are illegal activities on a network, especially on the web, which you need to be aware and careful of.

2. **It encourages people to become dependent on computers.**

   Since this technology's process mostly involves the use of computers, people have been relying on these machines rather than exerting some physical effort, which can be bad health wise.

3. **It opens up a doorway for computer viruses and malware.**

   There will be cases where you would unwittingly store some corrupted files into your computer that can destroy your entire operating system. Nevertheless, you can always use anti-virus software to keep this situation from happening.

4. **It lacks robustness.**

   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.

5. **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.

6. **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.

Overview of Network Topologies

Network topology refers to the physical or logical layout of a network. It defines the way different nodes are placed and interconnected with each other. Alternately, network topology may describe how the data is transferred between these nodes. There are two types of network topologies: physical and logical. Physical topology emphasizes the physical layout of the connected devices and nodes, while the logical topology focuses on the pattern of data transfer between network nodes.

1. **Bus Topology**

   In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

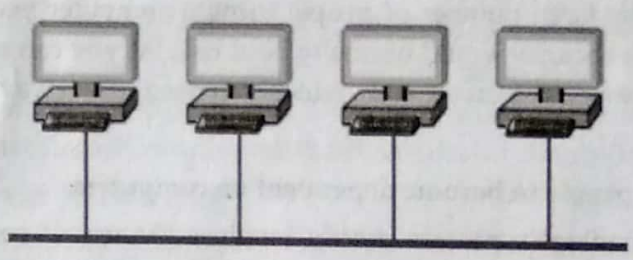


Figure 1.6: Bus Topology

Both ends of the shared channel have line terminator. The data is sent in only one direction and s soon as it reaches the extreme end, the terminator removes the data from the line.

2. **Star Topology**

   All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. Instead of hub device any of the following can be: **Layer 1** device such as hub or repeater, **Layer 2** device such as switch or bridge and **Layer 3** device such as router or gateway.

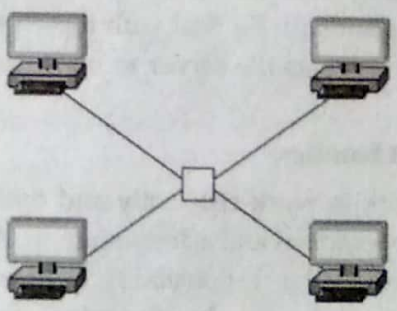


Figure 1.7: Star Topology

As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Advantages of Star Topology

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

Disadvantages of Star Topology

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

Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.

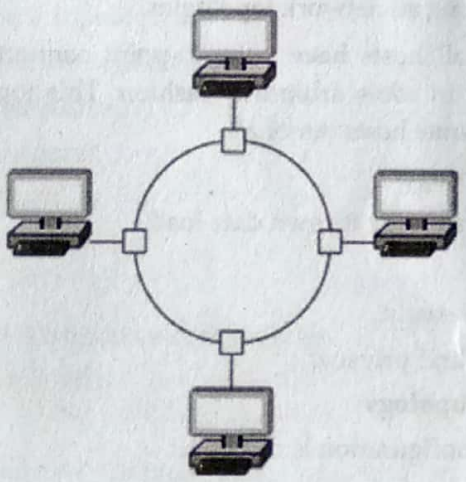


Figure 1.8: Ring Topology

Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

Advantages of Ring Topology

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

Disadvantages of Ring Topology

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

4. Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.

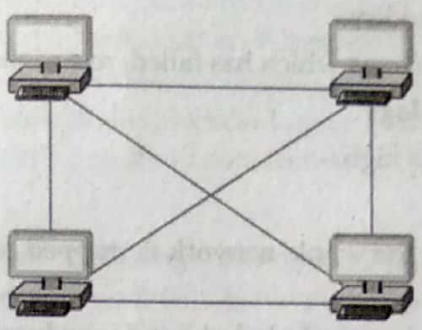


Figure 1.9: Mesh Topology

Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

1. **Full Mesh:** All hosts have a point-to-point connection to every other host in the network. Thus for every new host n (n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.
2. **Partially Mesh:** Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

Advantages of Mesh Topology

- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

5. Tree Topology

Also known as Hierarchical topology, this is the most common form of network topology in use presently. This topology imitates as extended Star topology and inherits properties of bus topology. This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.

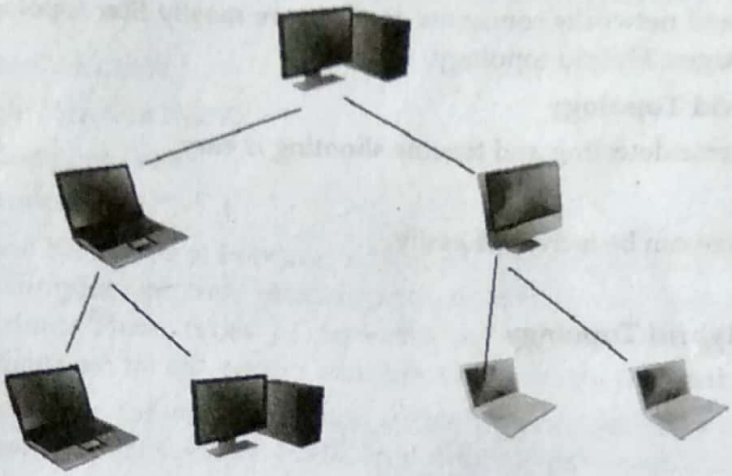


Figure 1.10: Tree Topology

All neighboring hosts have point-to-point connection between them. Similar to the Bus topology, if the root goes down, then the entire network suffers even though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.

Advantages of Tree Topology

- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages of Tree Topology

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.

6. Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.

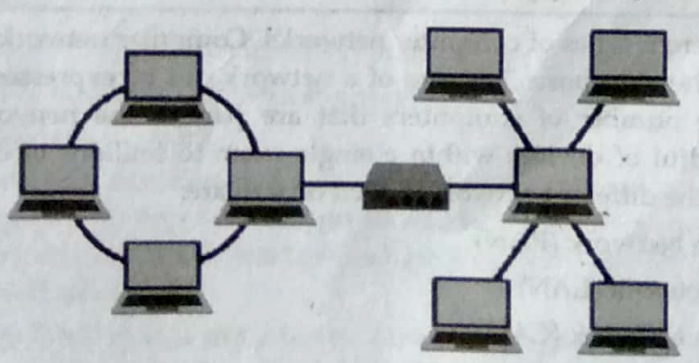


Figure 1.11: Hybrid Topology

The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of

Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology.

Advantages of Hybrid Topology

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

Cellular Topology

The cellular topology is applicable only in case of wireless media that does not require cable connection. In wireless media, each point transmits in a certain geographical area called a cell. Each cell represents a portion of the total network area. Devices that are in the cell communicate through a central hub. Hubs in different cells are interconnected. They route data across the network and provide a complete network infrastructure. The data is transmitted in the cellular digital packet data (CDPD) format.

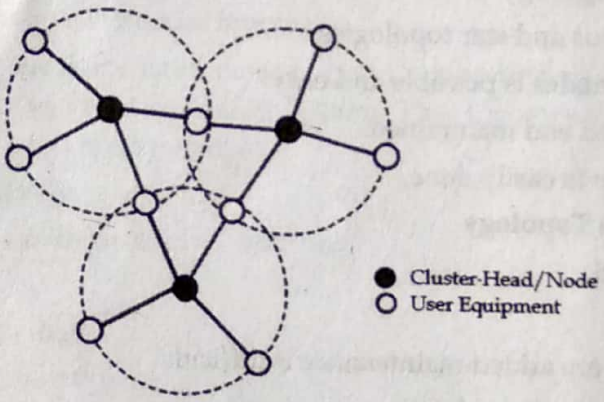


Figure 1.12: Cellular Topology

Overview of Network Types

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose. The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe. Some of the different networks based on size are:

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Campus Area Network (CAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

In terms of purpose, many networks can be considered general purpose, which means they are used for everything from sending files to a printer to accessing the Internet. Some types of networks

however, serve a very particular purpose. Some of the different networks based on their main purpose are:

- Storage Area Network (SAN)
- Enterprise Private Network (EPN)
- Virtual Private Network (VPN)

1. Personal Area Network (PAN)

The smallest and most basic type of network, a Personal Area Network or PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network, or HAN. In a very typical setup, a residence will have a single wired Internet connection connected to a modem. This modem then provides both wired and wireless connections for multiple devices. The network is typically managed from a single computer but can be accessed from any device.

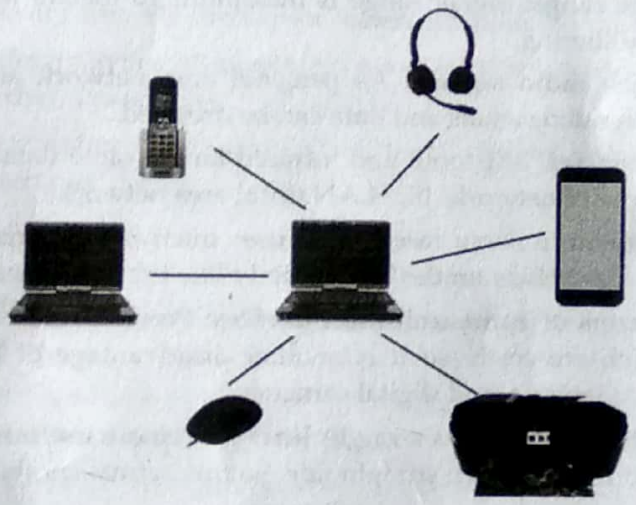


Figure 1.13: Persona Area Network

This type of network provides great flexibility. For example, it allows you to:

- Send a document to the printer in the office upstairs while you are sitting on the couch with your laptop.
- Upload a photo from your cell phone to your desktop computer.
- Watch movies from an online streaming service to your TV.

Advantages of personal area network

- **No extra space requires:** Personal area network does not require extra wire or space. For connecting two devices you only need to enable Bluetooth in both devices to start sharing data among them. For example, connecting wireless keyboard and mouse with the tablet through Bluetooth.
- **Connect many devices at a time:** Many devices can be connected to one device at the same time in a personal area network. You can connect one mobile to many other mobiles or tablets to share files.

- **Cost effective:** No extra wires are needed in this type of network. Also, no extra data charges are involved so PAN is an inexpensive way of communication.
- **Easy to use:** It is easy to use. No advanced setup is required.
- **Reliable:** If you use this type of data connection within 10 meters then your network is stable and reliable.
- **Secure:** This network is secured because all the devices are authorized before data sharing. Third party injection and data hacking are not possible in PAN.
- **Used in office, conference, and meetings:** Infrared is the technology used in TV remotes, AC remotes, and other devices. Bluetooth, infrared and other types of PAN is used to interconnect digital devices in offices, meetings, and conferences.
- **Synchronize data between different devices:** One person can synchronize several devices i.e. download, upload and exchanging data among devices.
- **Portable:** A person can move devices as it is a wireless network and data exchange is not affected. That mean PAN is portable as well.

Disadvantages of Personal Area Network

- **Less distance range:** Signal range is maximum 10 meters which makes limitation for long distance sharing.
- **Interfere with radio signals:** As personal area network also use infrared so it can interfere with radio signals and data can be dropped.
- **Slow data transfer:** Bluetooth and infrared have a slow data transfer rate as compared to another type of networks like LAN (local area network).
- **Health problem:** In some cases, PAN uses microwave signals in some digital devices which have a bad effect on the human body like brain and heart problems may occur.
- **Costly in terms of communication devices:** Personal area network is used in digital devices which are costly so it is another disadvantage of PAN. Examples are smart phones, PDA, laptops, and digital cameras.
- **Infrared signals travel in a straight line:** TV remote use infrared signals which have a problem that they travel in straight line. So this counts another disadvantage of PAN.

2. **Local Area Network (LAN)**

A Local Area Network or LAN is a computer network which spans over a small geographical area such as home, building, office, etc. In LAN, computers are placed relatively close. Since computers are located within small distance, they do not need special devices and cables to connect with each other. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building. LAN networks are also widely used to share resources like printers, shared hard-drive etc.

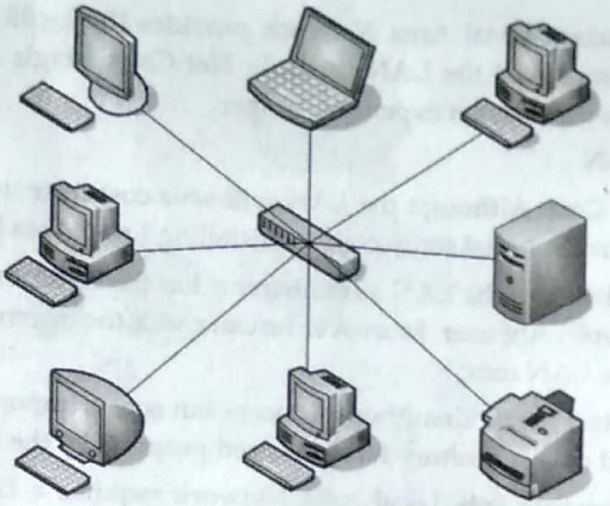


Figure 1.14: Local Area Network

Characteristics of LAN

- LAN's are private networks, not subject to tariffs or other regulatory controls.
- LAN's operate at relatively high speed when compared to the typical WAN.
- There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token Ring.
- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.

Applications of LAN

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc. are some common applications of LAN.

Advantages of LAN

- **Resource Sharing:** Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.
- **Software Applications Sharing:** It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.
- **Easy and Cheap Communication:** Data and messages can easily be transferred over networked computers.
- **Centralized Data:** The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.
- **Data Security:** Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.

- **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

Disadvantages of LAN

- **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.
- **Privacy Violations:** The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.
- **Data Security Threat:** Unauthorised users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
- **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
- **Covers Limited Area:** Local Area Network covers a small area like one office, one building or a group of nearby buildings.

3. Campus Area Network (CAN)

A campus area network is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned by the campus tenant / owner: an enterprise, university, government etc.

4. Metropolitan Area Network (MAN)

A metropolitan area network is a computer network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network. It is mainly hold and operated by single private company or a public company.

Characteristics of MAN

- It generally covers towns and cities (50 km)
- Communication medium used for MAN are optical fibers, cables etc.
- Data rates adequate for distributed computing applications.

Advantages of MAN

- Extremely efficient and provide fast communication via high-speed carriers, such as fiber optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both directions simultaneously.
- A MAN usually encompasses several blocks of a city or an entire city.

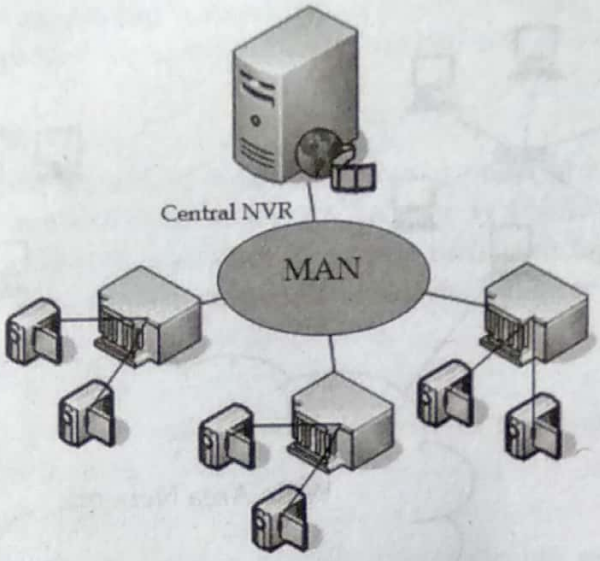


Figure 1.15: Metropolitan Area Network

Disadvantages of MAN

- More cable required for a MAN connection from one place to another.
- It is difficult to make the system secure from hackers and industrial espionage (spying) graphical regions.

Wide Area Network (WAN)

WAN is a computer network which spans over a large geographical area such as state, region, country etc. WANs are typically used to connect two or more LANs or MANs which are located relatively very far from each other. To provide connectivity, this network uses special devices, cables and technologies. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.

Characteristics of WAN

- It generally covers large distances (states, countries, continents).
- Communication medium used are satellite, public telephone networks which are connected by routers.

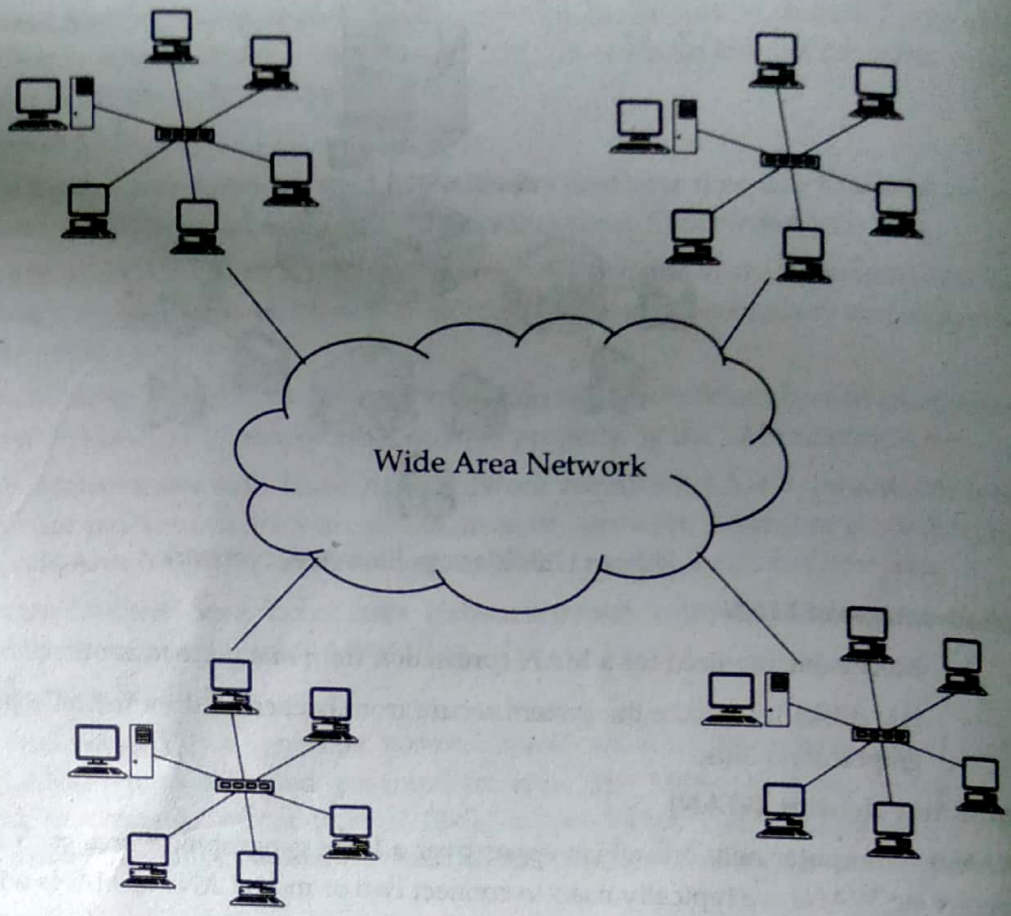


Figure 1.16: Wide Area Network

Advantages of WAN

- Covers a large geographical area so long distance business can connect on the one network.
- Shares software and resources with connecting workstations.
- Messages can be sent very quickly to anyone else on the network. These messages can have picture, sounds or data included with them (called attachments).
- Expensive things (such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
- Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

Disadvantages of WAN

- Need a good firewall to restrict outsiders from entering and disrupting the network.
- Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.
- Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.

- Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.

6. **Storage Area Network (SAN)**

   As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

7. **Enterprise Private Network (EPN)**

   These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

8. **Virtual Private Network (VPN)**

   A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

Networking Types

Client-Server and Peer-to-Peer are the common network models that we use in our day-to-day life. The Client-Server network model focuses on information sharing whereas, the Peer-to-Peer network model focuses on connectivity to the remote computers.

Definition of Client-Server Network Model

The Client-Server network model is widely used network model. Here, Server is a powerful system that stores the data or information in it. On the other hands, the Client is the machine which let the users access the data on the remote server.

The **system administrator** manages the data on the server. The client machines and the server are connected through a network. It allows the clients to access data even if the client machine and server are far apart from each other. In Client-Server model, the client process on the client machine sends the **request** to the server process on the server machine. When the server receives the client request, it lookouts for the requested data and **send** it back with the reply. As all the services are provided by a centralized server, there may be chances of server getting **bottlenecked**, slowing down the efficiency of the system.

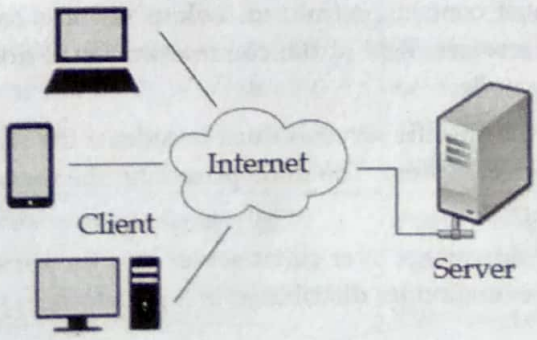


Figure 1.17: Client Server Network Model

Advantages of Client Server Networks

1. Centralized back up is possible.
2. Use of dedicated server improves the performance of whole system.
3. Security is better in these networks as all the shared resources are centrally administered.
4. Use of dedicated servers also increases the speed of sharing resources.

Disadvantages of Client Server Networks

1. It requires specialized servers with large memory and secondary storage. This leads to increase in the cost.
2. The cost of network operating system that manages the various clients is also high.
3. It requires dedicated network administrator.

Definition of Peer-to-Peer Network Model

Unlike Client-Server, the Peer-to-Peer model does not distinguish between client and server instead each node can either be a client or a server depending on the whether the node is requesting or providing the services. Each node is considered as a peer. To become a part of peer-to-peer, a node must initially join the network. After joining it must start to provide services to and must request the services from other nodes in the peer-to-peer system.

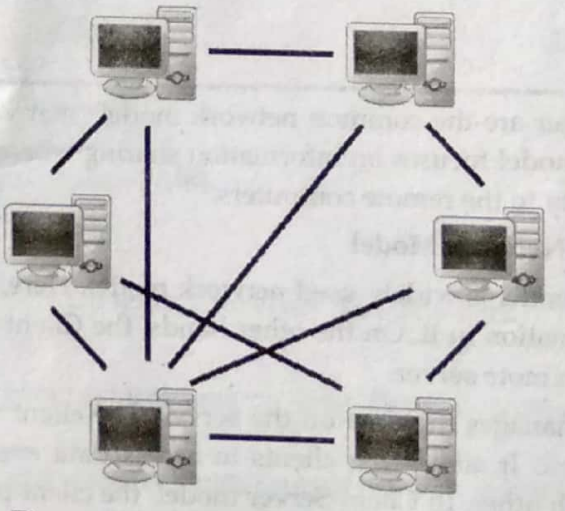


Figure 1.18: Peer-to-Peer Network Model

There are two ways to know which node provides which services; they are as follow:

1. When a node enters the peer-to-peer system, it must register the services it will be providing, into a centralized lookup service on the network. When a node desires for any specific service it must contact centralized lookup services to check out which node will provide the desired services. Rest of the communication is done by the desiring node and the service providing node.
2. A node desiring for the specific services must broadcast the request for services to all other nodes in the peer-to-peer system. The node providing the requested service will respond to the node making the request.

Peer-to-Peer network has the advantage over client-server that the server is not bottlenecked as the services are provided by the several nodes distributed in a peer-to-peer system.

Advantages of Peer-to-Peer Network Model

1. As a peer joins the network, it adds resources to the existing network, adding more members to the system, increases the capacity or resources of the system itself. The throughput of the network increases. Such networks also scale better, as increase in members increases efficiency.
2. Very robust as there is no single point of failure. If one peer fails, just that connection is lost, the network will go on functioning.
3. Since the machines are independent of each other, operation and set up is easier and cheaper than client-server model machines.

Disadvantages of Peer-to-Peer Network Model

1. P2P networks have high bandwidth consumption rates, due to multiple request and responses taking place at the same time from different peers.
2. Lack of security, no checking of authentication takes place. So anyone can send and receive data from anybody.

Difference between Client-Server and Peer-to-Peer Network

The main difference between the Client-Server and Peer-to-Peer network model is that in Client-Server model, the data management is centralized whereas, in Peer-to-Peer each user has its own data and applications. Further, we will discuss some more differences between Client-Server and Peer-to-Peer network model with the help of comparison chart shown below:

Table 1.3: Comparison Chart of Client-Server and Peer-to-Peer Network Model

Basis for Comparison	Client-Server	Peer-to-Peer
Basic	There is a specific server and specific clients connected to the server	Clients and server are not distinguished; each node act as client and server
Service	The client request for service and server respond with the service	Each node can request for services and can also provide the services.
Focus	Sharing the information	Connectivity
Data	The data is stored in a centralized server	Each peer has its own data
Server	When several clients request for the services simultaneously, a server can get bottlenecked.	As the services are provided by several servers distributed in the peer-to-peer system, a server in not bottlenecked.
Expense	The client-server are expensive to implement.	Peer-to-peer are less expensive to implement.
Stability	Client-Server is more stable and scalable.	Peer-to-Peer suffers if the number of peers increases in the system.

Overview of Protocols and Standards

Protocols

In information technology, a protocol (from the Greek protocol on, which was a leaf of paper glued to a manuscript volume, describing its contents) is the special set of rules that end points in a telecommunication connection use when they communicate. In brief **a protocol is defined as a set of rules that governs communication.** Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols attach layer in the telecommunication exchange that both ends of the exchange must recognize and observe. Protocols are often described in an industry or international standard. Some examples of network protocols are hyper-text transfer protocol (**HTTP**), file transfer protocol (**FTP**), transmission control protocol/ internet protocol (**TCP/IP**), secure sockets layer etc.

Network protocols are also similar to natural human languages in that they have three basic components: syntax, semantics, and timing.

Syntax defines how data will be structured, in other words, the order in which pieces of information will be packaged by the sender and opened up by the receiver. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself. The data order is also applied to the order of bits when they are stored or transmitted. Different computers may store data in different bit orders. When these computers communicate, this difference needs to be resolved.

Semantics determine what individual pieces of information within a network protocol mean. They allow the sender and receiver of information to interpret the pieces correctly, depending on where in the stream of data they appear. For example, does an address identify the route to be taken or the final destination of the message?

Timing definitions govern how quickly data can be sent and received, as well as when it should be sent. To work effectively, a protocol needs to ensure that both the sender and the receiver are prepared to communicate with one another at the right time, and that one isn't sending data at speeds too high or low for the other. For example, if a sender produces data at 100 megabits per second (100 Mbps) but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

Standards

Agreeing to common syntax, semantics, and timing definitions for a protocol is easy enough if you're dealing only with other computers in the same office or town, or if all parties are using the same hardware and software. But how do you ensure the whole world sticks to the same conventions within a protocol? That's where standards come in.

Standards are guidelines that explain to all IT stakeholders - from device manufacturers to software programmers and network administrators - how a particular protocol should operate. As long as everyone adheres to a common standard, and provided the definitions of that standard are open to the public, the protocol guarantees two devices can communicate, even if they were built by different companies or are running different operating systems.

Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

- **De facto:** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers that seek to define the functionality of a new product or technology. Examples of de facto standards are MS Office and various DVD standards.
- **De jure:** De jure standards are those that have been legislated by an officially recognized body.

ıdards Organizations

ıdards are developed through the cooperation of standards creation committees, forums, and ernment regulatory agencies.

ıdards Creation Committees

le many organizations are dedicated to the establishment of standards, data communications in th America rely primarily on those published by the following:

- **International Standards Organization (ISO).** The International Standards Organization (ISO; also referred to as the International Organization for Standardization) is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. Created in 1947, the ISO is an entirely voluntary organization dedicated to worldwide agreement on international standards. With a membership that currently includes representative bodies from many industrialized nations, it aims to facilitate the international exchange of goods and services by providing models for compatibility, improved quality, increased productivity, and decreased prices. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity. Of primary concern to this book are the ISO's efforts in the field of information technology, which have resulted in the creation of the Open Systems Interconnection (OSI) model for network communications. The United States is represented in the ISO by ANSI.
- **International Telecommunications Union–Telecommunications Standards Sector (ITU-T).** By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunications Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunications Union–Telecommunications Standards Sector (ITU-T).
- **American National Standards Institute (ANSI).** Despite its name, the American National Standards Institute (ANSI) is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance. ANSI's expressed aims include serving as the national coordinating institution for voluntary standardization in the United States, furthering the adoption of standards as a way of advancing the U.S. economy, and ensuring the participation and protection of the public interests. ANSI members include professional societies, industry associations, governmental and regulatory bodies, and consumer groups.

- **Institute of Electrical and Electronics Engineers (IEEE).** The Institute of Electrical and Electronics Engineers (IEEE) is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communication.
- **Electronic Industries Association (EIA).** Aligned with ANSI, the Electronic Industries Association (EIA) is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communications.
- **World Wide Web Consortium (W3C).** The World Wide Web Consortium (W3C) is the main international standards organization World Wide Web (abbreviated WWW or W3). Tim Berners-Lee founded this consortium at Massachusetts Institute of Technology Laboratory for Computer Science. It was founded to provide computability in industry for new standards. W3C has created regional offices around the world.
- **Open Mobile Alliance (OMA).** The standards organization OMA was created to gather different forums in computer networking and wireless technology under the umbrella of one single authority. Its mission is to provide unified standards for application protocols.

Forums

Telecommunications technology development is moving faster than the ability of standards committees to ratify standards. Standards committees are procedural bodies and by nature slow moving. To accommodate the need for working models and agreements and to facilitate the standardization process, many special-interest groups have developed forums made up of representatives from interested corporations. The forums work with universities and users to test, evaluate, and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies. Some important forums for the telecommunications industry include the following:

- **Frame Relay Forum.** The Frame Relay Forum was formed by Digital Equipment Corporation, Northern Telecom, Cisco, and Strata Com to promote the acceptance and implementation of Frame Relay. Today, it has around 40 members representing North America, Europe, and the Pacific Rim. Issues under review include flow control, encapsulation, translation, and multicasting. The forum's results are submitted to the ISO.
- **ATM Forum.** The ATM Forum promotes the acceptance and use of Asynchronous Transfer Mode (ATM) technology. The ATM Forum is made up of customer premises equipment (e.g., PBX systems) vendors and central office (e.g., telephone exchange) providers. It is concerned with the standardization of services to ensure interoperability.
- **Universal Plug and Play (UPnP) Forum.** The UPnP forum is a computer network forum that supports and promotes simplifying the implementation of networks by creating zero-configuration networking devices. An UPnP-compatible device can join a network without any configuration.

Regulatory Agencies

All communications technology is subject to regulation by government agencies such as the Federal Communications Commission in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications.

- **Federal Communications Commission (FCC).** The Federal Communications Commission (FCC) has authority over interstate and international commerce as it relates to communications.

What is open standards?

Not all standards are open. Sometimes, hardware or software companies try to implement **closed** or **proprietary protocols** that work only with their own products.

Remember the 1990s, when many websites worked well only in particular browsers? A lack of open protocols and standards was the reason. Sometimes closed standards can help a company by giving it an edge in the market. Theoretically, closed standards can make data transfers more secure by concealing the inner workings from hackers looking for a flaw to exploit. But in general, closed standards rarely serve the interests of the IT community as a whole. It's usually better to implement open standards that everyone can use. That makes innovation and interoperability easier.

In the late 1970s, the Open Systems Interconnection (OSI) reference model was created by the International Organization for Standardization (ISO) to break through this barrier. The OSI model was meant to help vendors create interoperable network devices and software in the form of protocols so that different vendor networks could work in peaceable accord with each other. Like world peace, it'll probably never happen completely, but it's still a great goal! Anyway the OSI model is the primary architectural model for networks. It describe show data and network information are communicated from an application on one computer through the network media to an application on another computer. The OSI reference model breaks this approach into layers.

After all, the Internet as we know it today wouldn't exist without a common set of open network protocols (like HTTP, FTP, and IMAP) that everyone uses when serving Web pages, uploading files, or sending email - no matter which operating system they run or type of devices they work with. Open protocols are baked into modern networking.

Network Models

Let's start with a few definitions. A **network model** reflects a design or architecture to accomplish communication between different systems. Network models are also referred to as **network stacks** or **protocol suites**. Examples of network models includes TCP/IP, Sequenced Packet Exchange/Internet Packet Exchange (SPX/IPX) used by Novelle Netware, the Network Basic Input Output System (Net-BIOS), which comprises the building blocks for most Microsoft networking and network applications; and AppleTalk, the network model for Apple Macintosh computers.

A network model usually consists of **layers**. When a communication system is designed in this manner, it's known as a hierarchical or **layered architecture**. Each layer of a model represents specific functionality. Within the layers of a model, there are usually protocols specified to implement specific tasks. You may think of a protocol as a set of rules or a language. Thus, a layer is normally a collection of protocols.

There are a number of different network models. Some of these models relate to a specific implementation, such as the TCP/IP network model. Others simply describe the process of

networking, such as the International Organization for Standardization/Open System Interconnection Reference Model (ISO/ OSI-RM, or more simply, OSI-RM).

A reference model is a non-implementation specific foundation that provides a clear understanding of the functions and processes necessary for consistent nonproprietary protocol development. The OSI reference model satisfies this definition since it provides a set of standards to ensure networking compatibility and interoperability and serves as a guideline for protocol design and instruction. The OSI reference model generically describes the communications process and therefore does not regulate it as manufacturers may create products that combine functions of one or more layers.

In contrast, a **protocol model** closely matches the structure of a protocol suite and may in fact be defined by the protocol suite's implementation. As an example, the TCP/IP protocol model describes the communication process and functions at each layer of the Internet standard TCP/IP protocol suite.

A layered architecture facilitates development in complex environments by grouping specific related functions into separate well-defined layers with clear interfaces. This methodology reduces complexity by breaking the problem space into smaller and simpler components and standardizes interfaces facilitating multi-vendor development and modular component-based engineering. Layered architectures in conjunction with open standards define a common vocabulary necessary for understanding and cooperation in multi-vendor environments and positively results in increased competition and innovation. The architecture's layers may also be called the architecture's stack and these two terms will be used interchangeably. It should be noted that an architecture provides a blueprint that guides not only how the components are constructed but also when in the process they are designed, implemented, maintained and replaced.

Advantages of Reference Models

The OSI model is hierarchical, and there are many advantages that can be applied to any layered model, but as we know, the OSI model's primary purpose is to allow different vendors' networks to interoperate.

Here's a list of some of the more important benefits of using the OSI layered model:

- It divides the network communication process into smaller and simpler components, facilitating component development, design, and troubleshooting.
- It allows multiple-vendor development through the standardization of network components.
- It encourages industry standardization by clearly defining what functions occur at each layer of the model.
- It allows various types of network hardware and software to communicate.
- It prevents changes in one layer from affecting other layers to expedite development.

OSI Reference Model

The International Organization for Standardization (ISO) is a worldwide body that promotes standards internationally. In the late 1970s, ISO began work on developing a standard for multivendor computer interconnectivity. The result, published in the late 1980s, was the Open System Interconnection (OSI) model. The OSI model incorporates protocols that can be used to implement a network stack. These protocols are not used extensively largely due to the popularity of the TCP/IP protocol suite. Consequently, the OSI model, with its well-defined layers, is used

primarily as a reference model, hence, OSI-RM. Many network models are described by way of OSI-RM and so we provide a description of it here. The OSI-RM has seven different layers, divided into two groups. The top three layer define how the applications within the end stations will communicate with each other as well as with users. The bottom four layers define how data is transmitted end to end. The OSI reference model has seven layers which is shown in figure 1.19:

Application (Layer 7)	• Provides a user interface
Presentation (Layer 6)	• Presents data • Handles processing such as encryption
Session (Layer 5)	• Keeps different applications' data separate
Transport (Layer 4)	• Provides reliable or unreliable delivery • Performs error correction before retransmit
Network (Layer 3)	• Provides logical addressing, which routers use for path determination
Data link (Layer 2)	• Combines packets into bytes and bytes into frames • Provides access to media using MAC address • Performs error detection not correction
Physical (Layer 1)	• Moves bits between devices • Specifies voltage, wire speed, and pinout of cables

Figure 1.19: The OSI – Reference Model

Figure 1.19 illustrates the OSI model and provides a brief definition of the functions performed at each layer. The intent of the OSI model is that protocols be developed to perform the functions of each layer.

Organization of the Layers

The seven layers can be grouped into three subgroups

1. **Network Support Layers:** Layers 1, 2, 3 - Physical, Data link and Network are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical addressing, transport timing and reliability.
2. **Transport Layer:** Layer4, transport layer, ensures end-to-end reliable data transmission on a single link.
3. **User Support Layers:** Layers 5, 6, 7 - Session, presentation and application are the user support layers. They allow interoperability among unrelated software systems

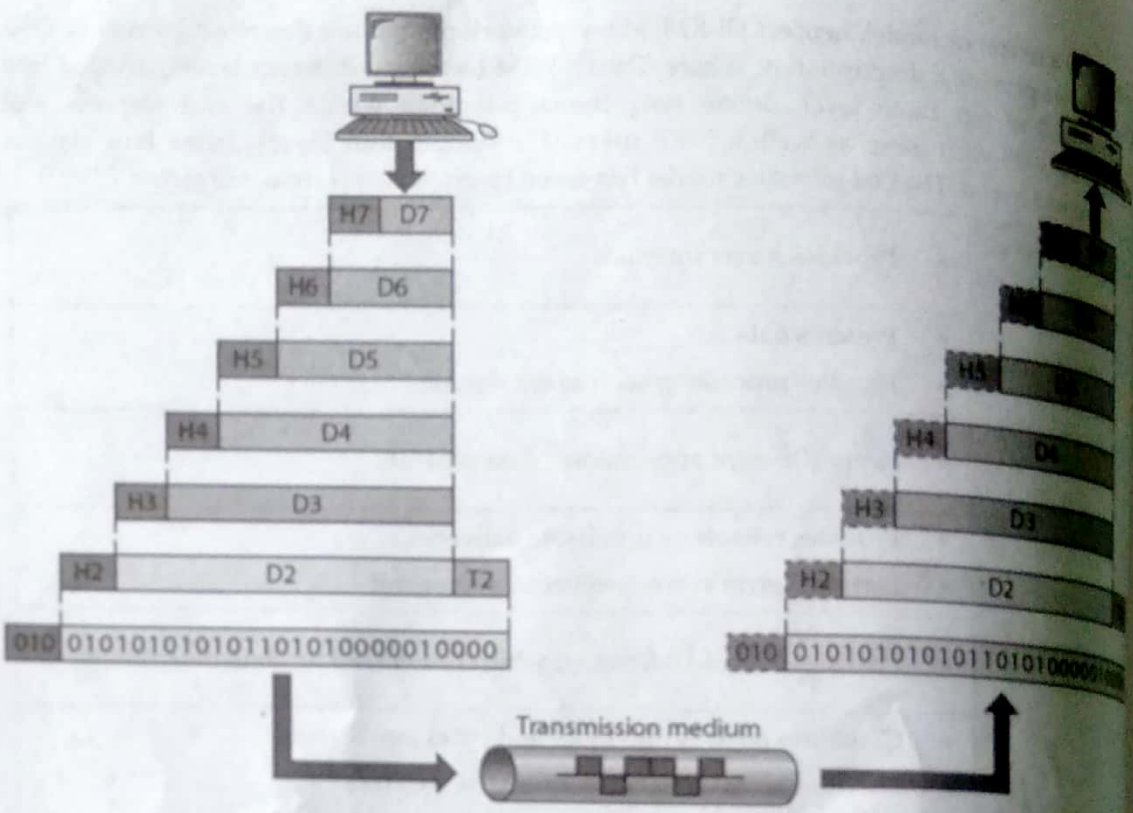


Figure 1.20: Data Exchange using OSI – Reference Model

In Figure 1.20, which gives an overall view of the OSI layers, D7 data means the data unit at layer 7, D6 data means the data unit at layer 6, and so on. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order. At each layer, a header can be added to the data unit. At layer 2, a trailer may also be added. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link. Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

Encapsulation

Figure 1.20 reveals another aspect of data communications in the OSI model: encapsulation. A packet at level 7 is encapsulated in the packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on. In other words, the data part of a packet at level N is carrying the whole packet (data and overhead) from level N+ 1. The concept is called encapsulation because level N is not aware what part of the encapsulated packet is data and what part is the header or trailer for level N, the whole packet coming from level N+ 1 is treated as one integral unit.

Function of Layers in OSI Reference Model

1. **Physical Layer:**

   The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission media. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

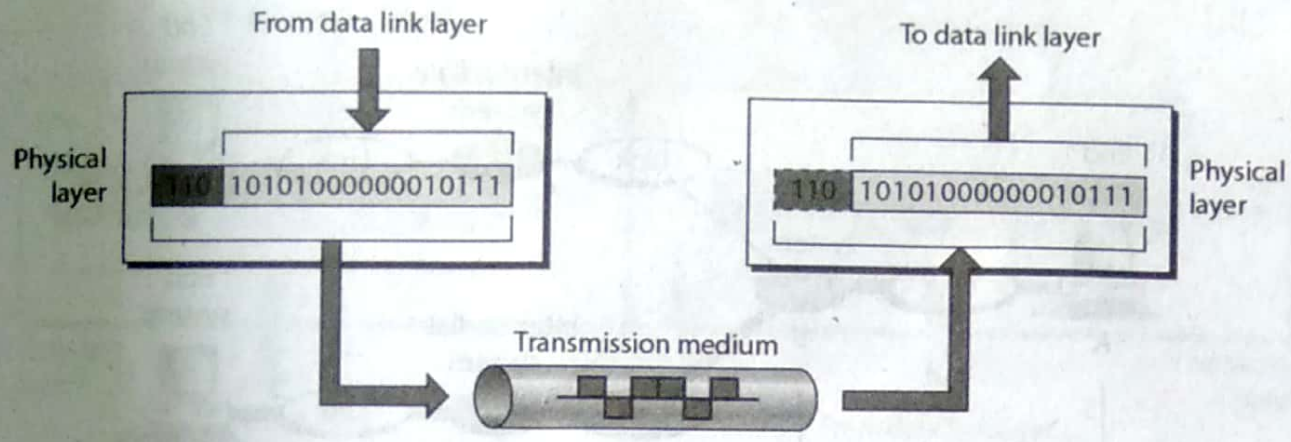


Figure 1.21: Physical Layer

The physical layer is concerned with the following:

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

2. **Data Link Layer:**

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

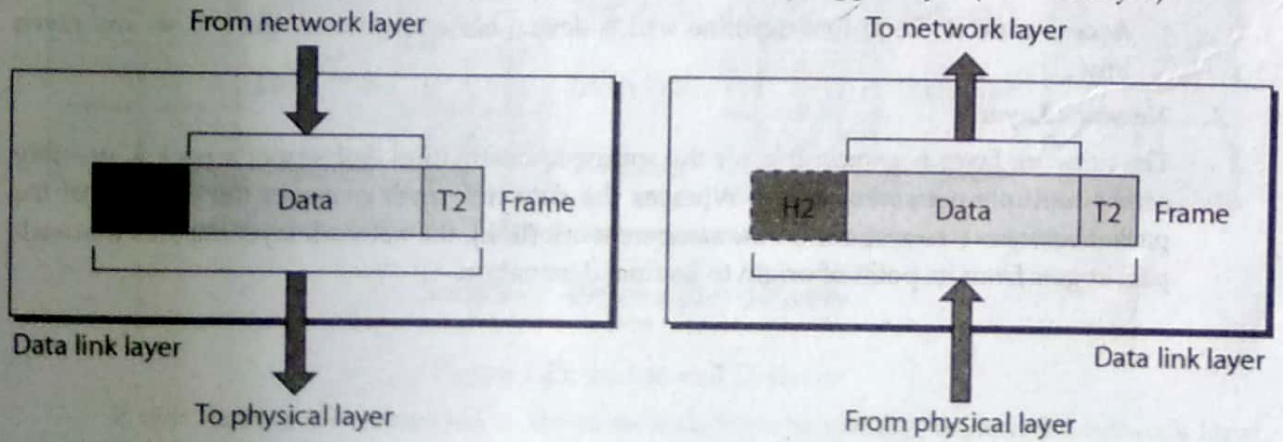


Figure 1.22: Data Link Layer

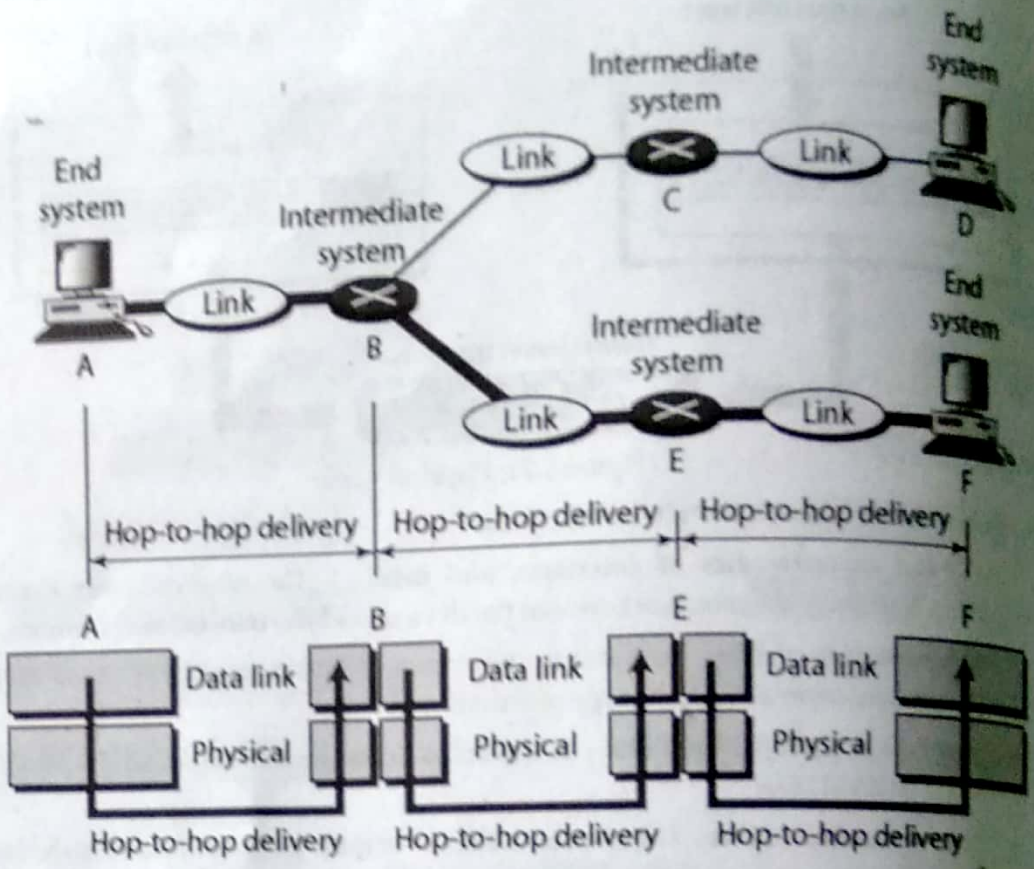


Figure 1.23: Hop-to-hop Delivery

Other responsibilities of the data link layer include the following:

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

3. **Network Layer:**

The network layer is responsible for the source-to-destination delivery of a packet, possi across multiple networks (links). Whereas the data link layer oversees the delivery of t packet between two systems on the same network (link), the network layer ensures that e packet gets from its point of origin to its final destination.

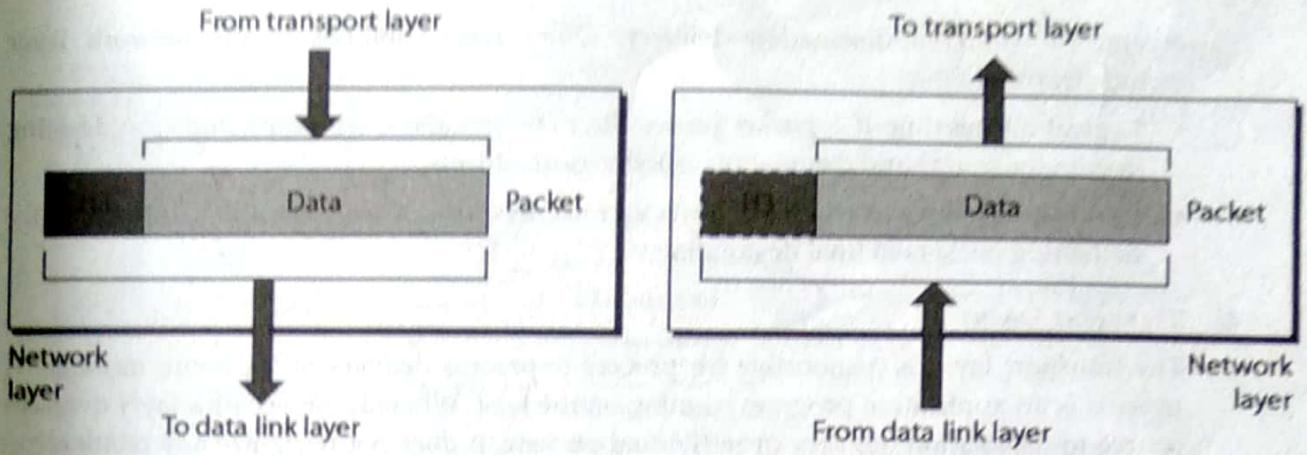


Figure 1.24: Network Layer

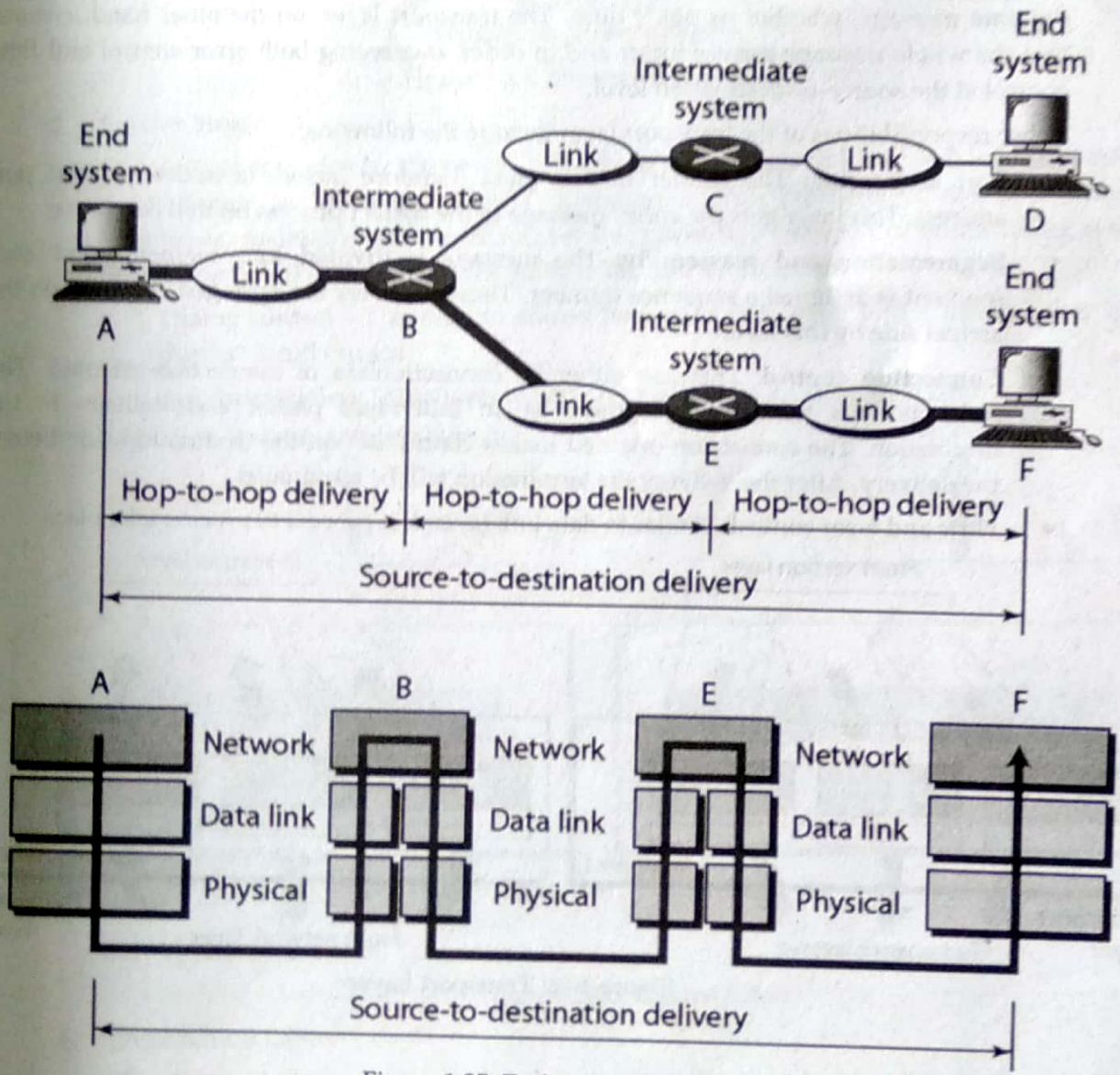


Figure 1.25: End-to-end Delivery

If two systems are connected to the same link, there is usually no need for network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to

accomplish source-to-destination delivery. Other responsibilities of the network layer include the following:

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

4. **Transport Layer:**

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on the host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Other responsibilities of the transport layer include the following:

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

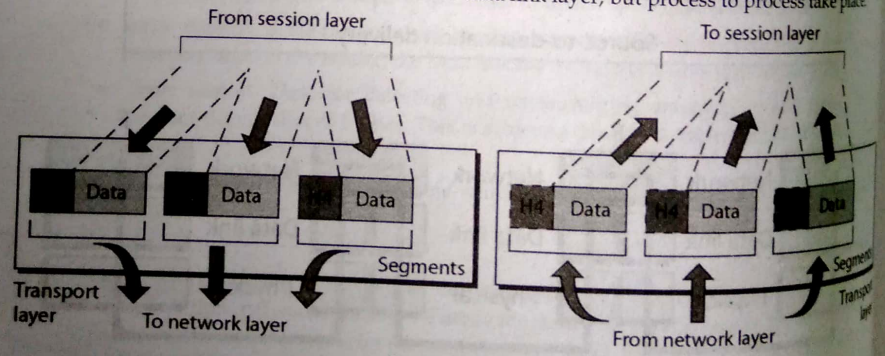


Figure 1.26: Transport Layer

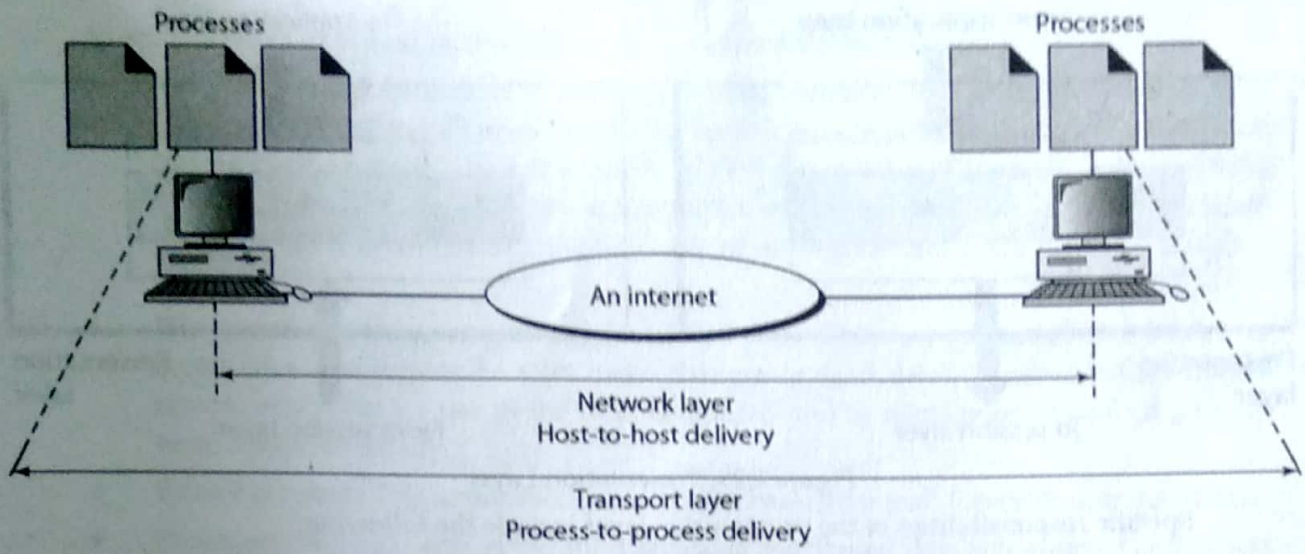


Figure 1.27: Process-to-process Delivery

5. Session Layer:

The services provided by the first four layers (physical, data link, network and transport)are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction between communicating systems. Specific responsibilities of the session layer include the following:

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

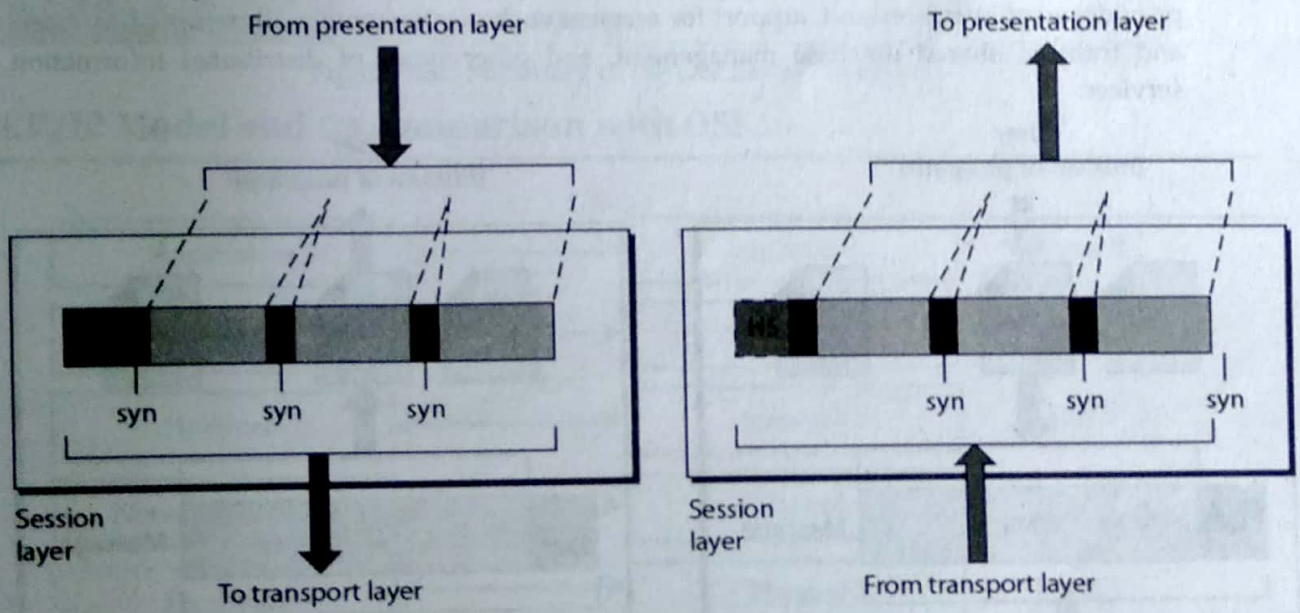


Figure 1.28: Session Layer

6. Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

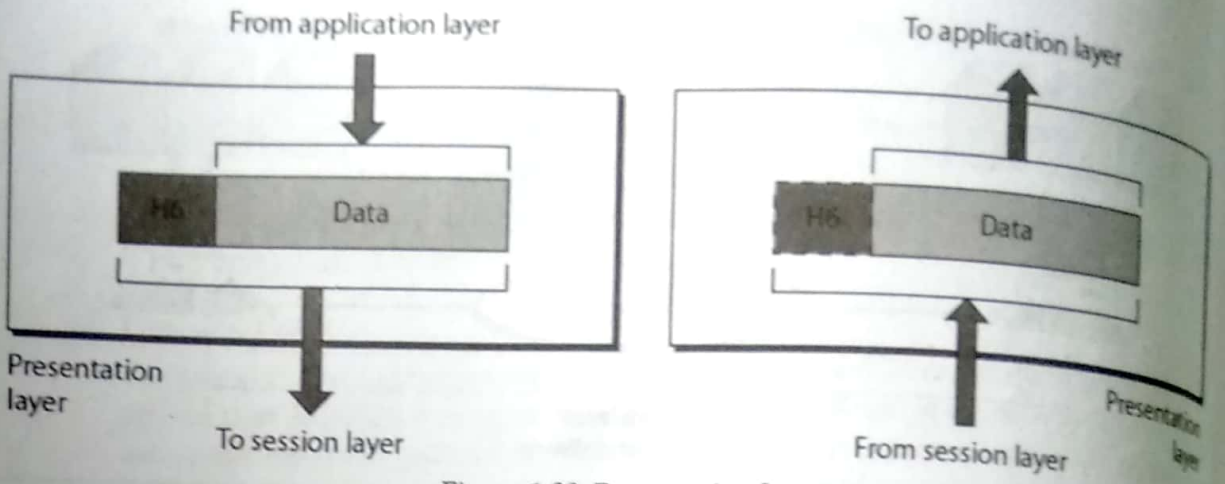


Figure 1.29: Presentation Layer

Specific responsibilities of the presentation layer include the following:

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

7. **Application Layer:**

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

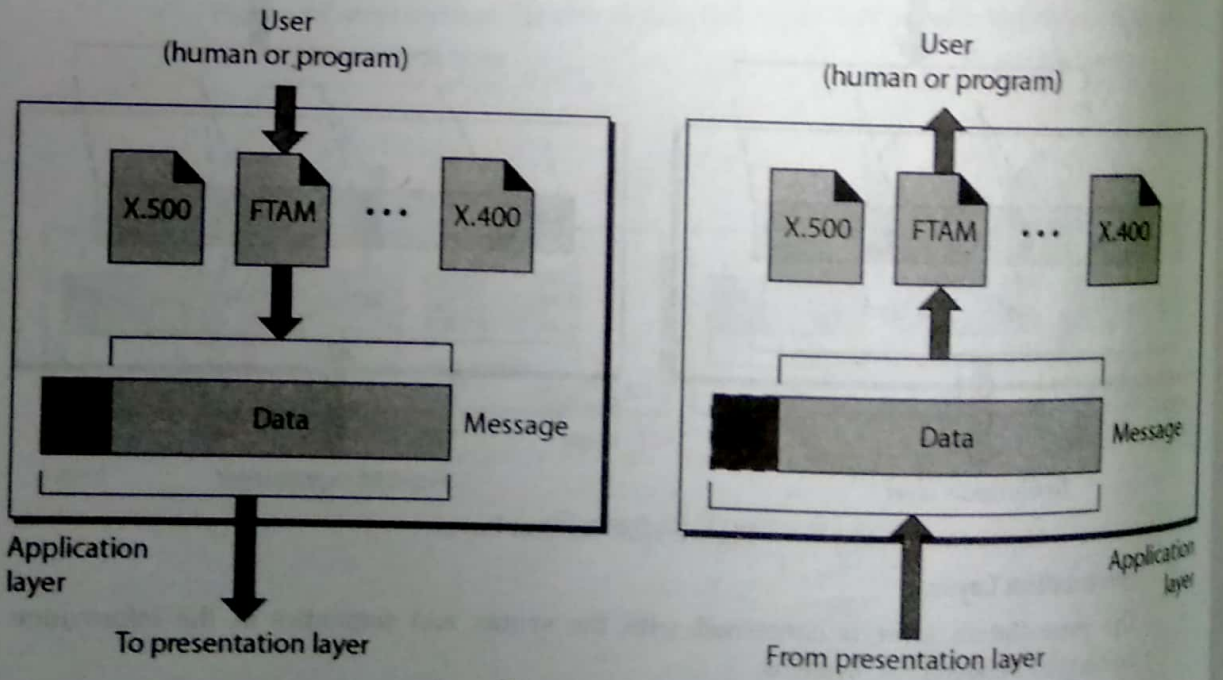


Figure 1.30: Application Layer

Specific services provided by the application layer include the following:

- **Network virtual terminal:** A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which, in turn, talks to the host, and vice-versa. The remote host believes it is communicating with one of its own terminals and allows you to log on.
- **File transfer, access, and management (FTAM):** 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 are mote computer locally.
- **E-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.

Application Layer	• File, print, message, database, and application services
Presentation Layer	• Data encryption, compression, and translation services
Session Layer	• Dialog control
Transport Layer	• End-to-end connection
Network Layer	• Routing
Data link Layer	• Framing
Physical Layer	• Physical topology

Figure 1.31: Summary of the OSI Layer Functions

TCP/IP Model and its comparison with OSI

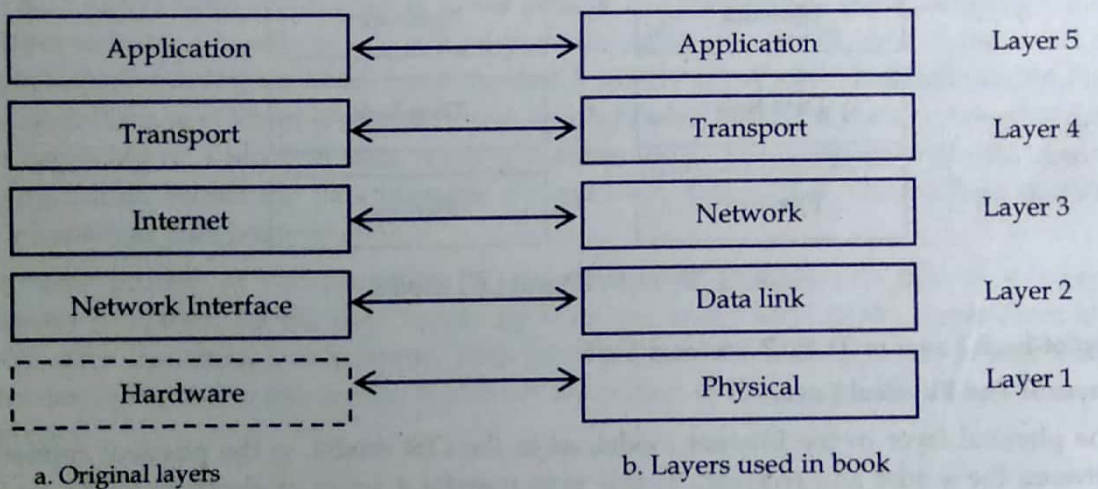


Figure 1.32: Layers in TCP/IP protocol suit

The TCP/IP (Transmission Control Protocol/Internet Protocol) was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suit do not match exactly with those in the OSI model. TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the

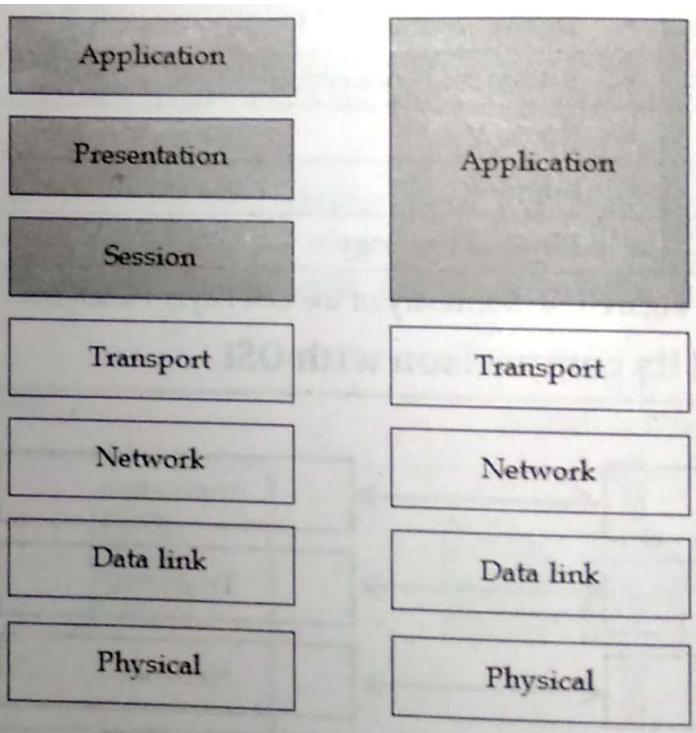


Figure 1.33: TCP/IP and OSI model

Description of Each Layer of TCP/IP Protocol Suit

1. **Layer 1: The Physical Layer**

   The physical layer in the Internet model, as in the OSI model, is the physical connec between the sender and receiver. Its role is to transfer a series of electrical, radio, or l signals through the circuit. The physical layer includes all the hardware devices (computers, modems, and hubs) and physical media (e.g., cables and satellites). The phys layer specifies the type of connection and the electrical signals, radio waves, or light pu that pass through it.

Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers (host-to-network, internet, transport and application) built upon the hardware. Today, however, TCP/IP is thought of as a five-layer (physical, data link, network, transport and application) model. Figure 1.32 shows both configurations.

Comparison between OSI and TCP/IP Protocol Suit

When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model, as shown in Figure 1.33.

Two reasons were mentioned for this decision. First, TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport layer protocols. Second, the application layer is not only one piece of software. Many applications can be developed at this layer. If some of the functionalities mentioned in the session and presentation are needed for a particular application, it can be included in the development of that piece of software.

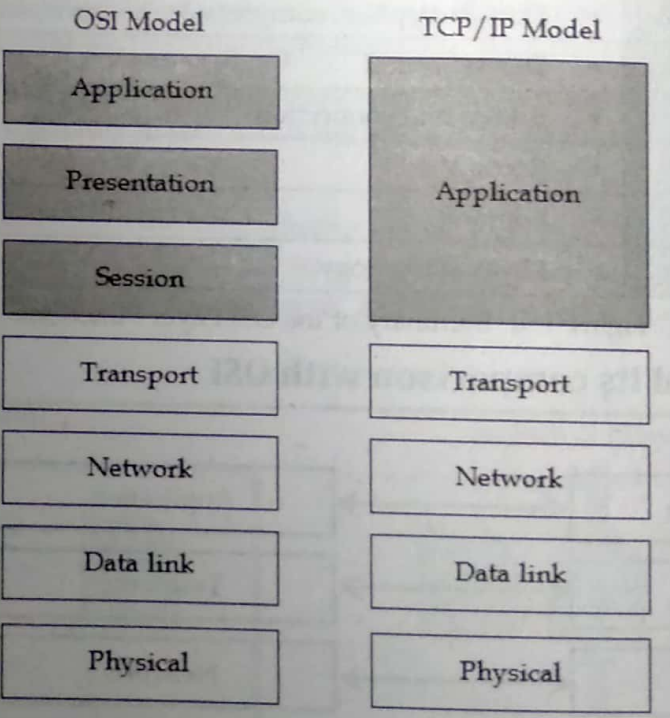


Figure 1.33: TCP/IP and OSI model

Description of Each Layer of TCP/IP Protocol Suit

1. **Layer 1: The Physical Layer**

   The physical layer in the Internet model, as in the OSI model, is the physical connection between the sender and receiver. Its role is to transfer a series of electrical, radio, or light signals through the circuit. The physical layer includes all the hardware devices (e.g., computers, modems, and hubs) and physical media (e.g., cables and satellites). The physical layer specifies the type of connection and the electrical signals, radio waves, or light pulses that pass through it.

2. **Layer 2: The Data Link Layer**

   The data link layer is responsible for moving a message from one computer to the next computer in the network path from the sender to the receiver. The data link layer in the Internet model performs the same three functions as the data link layer in the OSI model. First, it controls the physical layer by deciding when to transmit messages over the media. Second, it formats the messages by indicating where they start and end. Third, it detects and corrects any errors that have occurred during transmission.

3. **Layer 3: The Network Layer**

   The network layer in the Internet model performs the same functions as the network layer in the OSI model. First, it performs routing, in that it selects the next computer to which the message should be sent. Second, it can find the address of that computer if it doesn't already know it.

4. **Layer 4: The Transport Layer**

   The transport layer in the Internet model is very similar to the transport layer in the OSI model. It performs two functions. First, it is responsible for linking the application layer software to the network and establishing end-to-end connections between the sender and receiver when such connections are needed. Second, it is responsible for breaking long messages into several smaller messages to make them easier to transmit. The transport layer can also detect lost messages and request that they be resent.

5. **Layer 5: Application Layer**

   The application layer is the application software used by the network user and includes much of what the OSI model contains in the application, presentation, and session layers. It is the user's access to the network. By using the application software, the user defines what messages are sent over the network. It discusses the architecture of network applications and several types of network application software and the types of messages they generate.

Encapsulation and Decapsulation

When data moves from upper layer to lower level of TCP/IP protocol stack (outgoing transmission) each layer includes a bundle of relevant information called a header along with the actual data. The data package containing the header and the data from the upper layer then becomes the data that is repackaged at the next lower level with lower layer's header. Header is the supplemental data placed at the beginning of a block of data when it is transmitted. This supplemental data is used at the receiving side to extract the data from the encapsulated data packet. This packing of data at each layer is known as data encapsulation.

The reverse process of encapsulation (or decapsulation) occurs when data is received on the destination computer. As the data moves up from the lower layer to the upper layer of TCP/IP protocol stack (incoming transmission), each layer unpacks the corresponding header and uses the information contained in the header to deliver the packet to the exact network application waiting for the data.

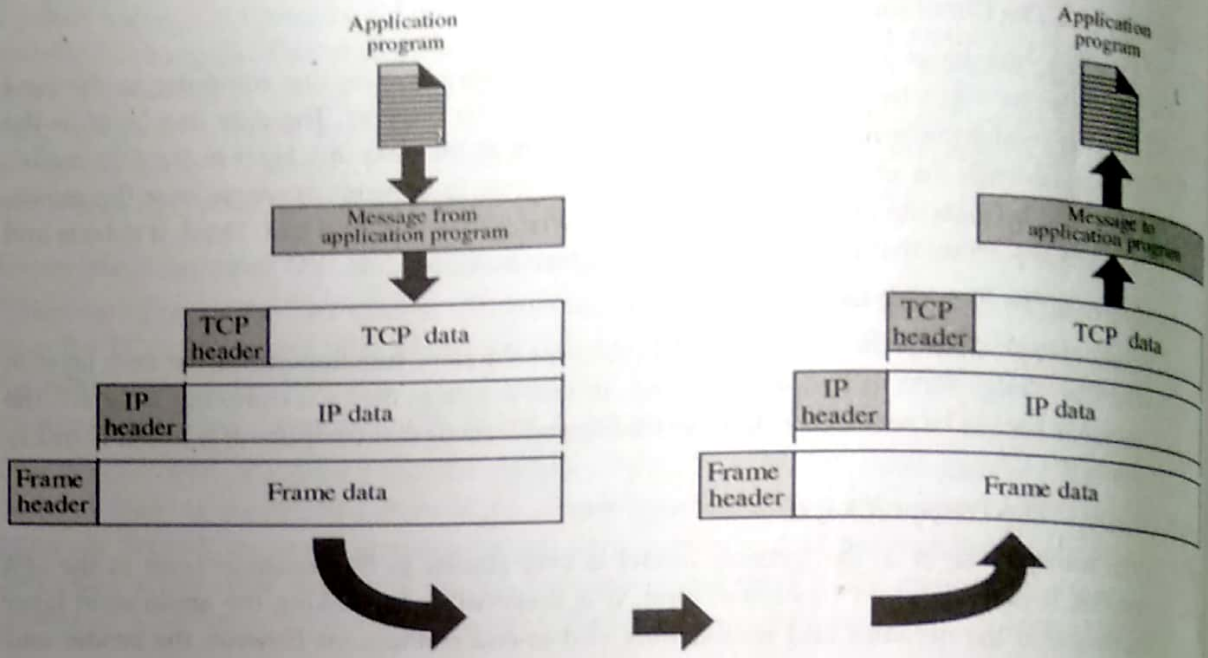


Figure 1.34: Encapsulation and Decapsulation in TCP/IP Model

Addressing

Any communication that involves two parties needs two addresses: source address and destination address. Although it looks as if we need five pairs of addresses, one pair per layer, we normally have only four because the physical layer does not need addresses; the unit of data exchange at the physical layer is a bit, which definitely cannot have an address.

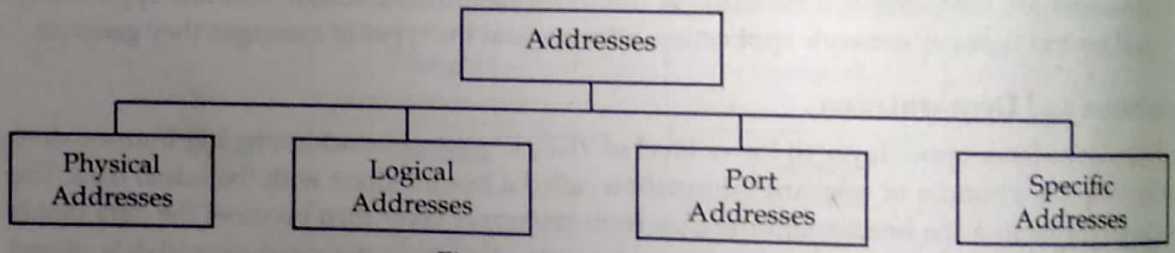


Figure 1.35: Address in TCP/IP

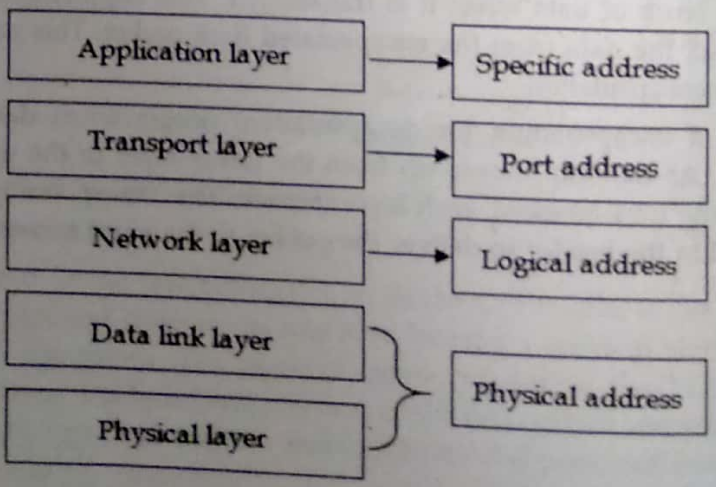


Figure 1.36: Relationship of layers and addresses in TCP/IP

Figure 1.36 shows the addressing at each layer. As the figure shows, there is a relationship between the layer, the address used in that layer, and the packet name at that layer. At the application layer, we normally use names to define the site that provides services, such as facebook.com, or the e-mail address, such as somebody@gmail.com. At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination. Port numbers are local addresses that distinguish between several programs running at the same time. At the network-layer, the addresses are global, with the whole Internet as the scope. A network-layer address uniquely defines the connection of a device to the Internet. The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN).

Table 1.3: Differences between OSI and TCP/IP reference model

OSI (Open System Interconnection)	TCP/IP (Transmission Control Protocol/ Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 or 5 layers

Connection-oriented and Connection-less Network Services

Communication can be established in two ways between two or more devices that are connection-oriented and connection-less. Network layers can offer these two different types of services to its predecessor layer for transferring data.

Connection-oriented Service

A connection-oriented service is one that establishes a dedicated connection between the communicating entities before data communication commences. It is modeled after the telephone system. To use a connection-oriented service, the user first establishes a connection, uses it and then releases it. In connection-oriented services, the data streams/packets are delivered to the receiver in the same order in which they have been sent by the sender.

Connection-oriented Services may be done in either of the following ways:

1. **Circuit-switched connection:** In circuit switching, a dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
2. **Virtual circuit-switched connection:** Here, the data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. However, other connections may also be using this path.

Connection-oriented Services may be of the following types:

1. Reliable Message Stream: e.g. sequence of pages
2. Reliable Byte Stream: e.g. song download
3. Unreliable Connection: e.g. VoIP (Voice over Internet Protocol)

Advantages of Connection-Oriented Services

1. This is mostly a reliable connection.
2. Congestions are less frequent.
3. Sequencing of data packets is guaranteed.
4. Problems related to duplicate data packets are alleviated.
5. Suitable for long connection.

Disadvantages of Connection-Oriented Services

1. Resource allocation is needed before communication. This often leads to under-utilized network resources.
2. The lesser speed of connection due to the time is taken for establishing and relinquishing the connection.
3. In the case of router failures or network congestions, there are no alternative ways to continue communication.

Connection-less Service

A Connection-less service is a data communication between two nodes where the sender sends data without ensuring whether the receiver is available to receive the data. Here, each data packet has the destination address and is routed independently irrespective of the other packets. Thus the data packets may follow different paths to reach the destination. There's no need to setup connection before sending a message and relinquish it after the message has been sent. The data packets in a connection-less service are usually called data grams.

Protocols for Connection-less Services are:

1. Internet Protocol (IP)
2. User Datagram Protocol (UDP)
3. Internet Control Message Protocol (ICMP)

Connection-less Services may be of the following types:

1. Unreliable datagram e.g. electronic junk mail.
2. A datagram with Acknowledgement: e.g. text messages with delivery report
3. Request-Reply: e.g. queries from remote databases

Advantages of Connection-less Services

1. It has low overhead.
2. It enables to broadcast and multicast messages, where the sender sends messages to multiple recipients.
3. It is simpler and has low overhead.
4. It does not require any time for circuit setup.
5. In case of router failures or network congestions, the data packets are routed through alternate paths. Hence, communication is not disrupted.

Disadvantages of Connection-less Services

1. It is not a reliable connection. It does not guarantee that there will not be a loss of packets, wrong delivery, out – of – sequence delivery or duplication of packets.
2. Each data packet requires longer data fields since it should hold all the destination address and the routing information.
3. They are prone to network congestions.

Differences between Connection-oriented and Connection-less Services

Connection-oriented services involve the establishment and termination of the connection while connection-less services don't require any connection creation and termination processes for transferring data. Another difference between connection-oriented and connection-less services is connection-oriented communication uses a stream of data and is vulnerable to router failure while connection-less communication uses messages and is robust to router failure. Detail comparison is shown in table below:

Table 1.4: Differences between connection-oriented and connection-less services

Basis for Comparison	**Connection-oriented Service**	**Connection-less Service**
Prior Connection Requirement	Necessary	Not required
Reliability	Ensures reliable transfer of data.	Not guaranteed.
Congestion	Unlikely	Occur likely.
Transferring mode	It can be implemented using circuit switching and virtual circuit.	It is implemented using packet switching.

Lost data retransmission	Feasible	Practically, not possible.
Suitability	Suitable for long and steady communication.	Suitable for bursty Transmission.
Signaling	Used for connection establishment.	There is no concept of signaling.
Packet forwarding	Packets sequentially travel to their destination node and follows the same route.	Packets reach the destination randomly without following the same route.

Internet, ISPs, Backbone Network Overview

Brief History of Internet

A network is a group of connected, communicating devices such as computers and printers. An internet (note the lowercase i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase I), composed of hundreds of thousands of interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

ARPANET

In the mid-1960s, mainframe computers in research organizations were stand-alone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DOD) was interested in finding a way to connect computers together so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP). The IMPs, in turn, would be connected to each other. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.

Birth of the Internet

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetting Project*. They wanted to link different networks together so that a host on one network could communicate with a host on a second, different network. There were many problems to overcome: diverse packet sizes, diverse interfaces, and diverse transmission rates, as well as differing reliability requirements. Cerf and Kahn devised the idea of a device called a gateway to serve as the intermediary hardware to transfer data from one network to another.

Transmission Control Protocol/Internetworking Protocol (TCP/IP)

Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of data. This was a new version of NCP. This paper on transmission control protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway. A radical idea was the transfer of responsibility for error correction from the IMP to the host machine. This ARPA Internet now became the focus of the communication effort. Around this time responsibility for the ARPANET was handed over to the Defense Communication Agency (DCA).

In October 1977, an internet consisting of three different networks (ARPANET, packet radio, and packet satellite) was successfully demonstrated. Communication between networks was now possible. Shortly thereafter, authorities made a decision to split TCP into two protocols: **Transmission Control Protocol (TCP)** and **Internet Protocol (IP)**. IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection. The new combination became known as TCP/IP.

In 1981, under a DARPA contract, UC Berkeley modified the UNIX operating system to include TCP/IP. This inclusion of network software along with a popular operating system did much for the popularity of networking. The open (non-manufacturer specific) implementation on Berkeley UNIX gave every manufacturer a working codebase on which they could build their products.

In 1983, authorities abolished the original ARPANET protocols, and TCP/IP became the official protocol for the ARPANET. Those who wanted to use the Internet to access a computer on a different network had to be running TCP/IP.

MILNET

In 1983, ARPANET split into two networks: MILNET for military users and ARPANET for nonmilitary users.

CSNET

Another milestone in Internet history was the creation of CSNET in 1981. CSNET was a network sponsored by the National Science Foundation (NSF). The network was conceived by universities that were ineligible to join ARPANET due to an absence of defense ties to DARPA. CSNET was a less expensive network; there were no redundant links and the transmission rate was slower. It featured connections to ARPANET and Telenet, the first commercial packet data service.

By the middle 1980s, most U.S. universities with computer science departments were part of CSNET. Other institutions and companies were also forming their own networks and using TCP/IP to interconnect. The term Internet, originally associated with government-funded connected networks, now referred to the connected networks using TCP/IP protocols.

NSFNET

With the success of CSNET, the NSF, in 1986, sponsored NSFNET, a backbone that connected five supercomputer centers located throughout the United States. *Community* networks were allowed access to this backbone, a T-1 line with a 1.544-Mbps data rate, thus providing connectivity throughout the United States. In 1990, ARPANET was officially retired and replaced by NSFNET. In 1995, NSFNET reverted back to its original concept of a research network.

ANSNET

In 1991, the U.S. government decided that NSFNET was not capable of supporting the rapidly increasing Internet traffic. Three companies, IBM, Merit, and MCI, filled the void by forming a

nonprofit organization called Advanced Network and Services (ANS) to build a new, high-speed Internet backbone called ANSNET.

The Internet Today

The Internet today is not a simple hierarchical structure. It is made up of many wide and local area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continuously changing—new networks are being added, existing networks need more addresses, and networks of defunct companies need to be removed. Today most end users who want Internet connection use the services of Internet service providers (ISPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure below shows a conceptual (not geographical) view of the Internet.

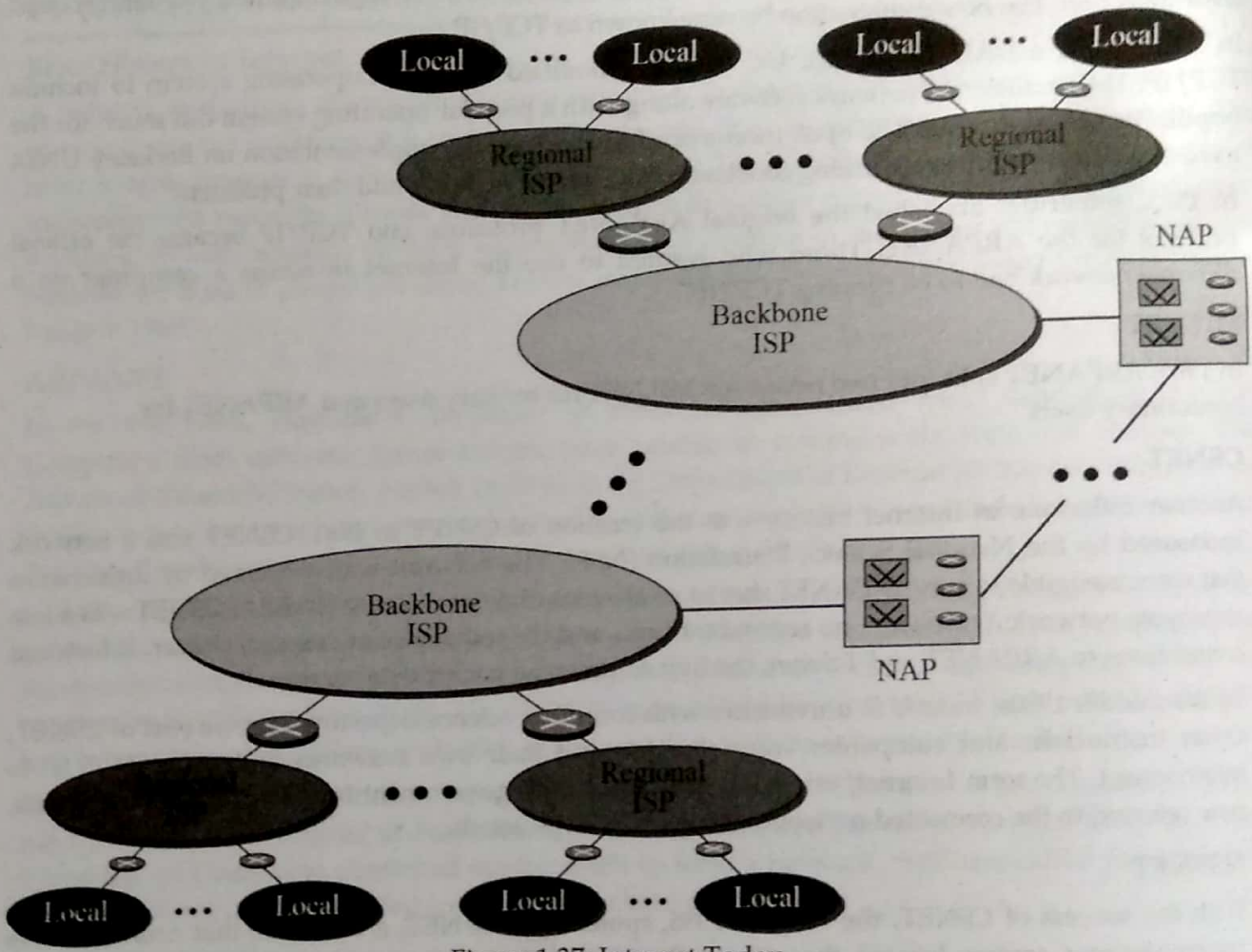


Figure 1.37: Internet Today

Backbone ISPs

Backbone ISPs are created and maintained by specialized companies. There are many backbone ISPs operating in North America; some of the most well-known are Sprint-Link, PSINet, UUNet Technology, AGIS, and internet MCI. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some regional ISP networks are also connected to each other by

private switching stations called peering points. Backbone ISPs normally operate at a high data rate (10 Gbps, for example).

Regional ISPs

Regional ISPs are small ISPs that are connected to one or more backbone ISPs. They are at the second level of hierarchy with a lesser data rate.

Local ISPs

Local ISPs provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to backbone ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network to supply services to its own employees, or a nonprofit organization, such as a college or a university that runs its own network. Each of these can be connected to a regional or backbone service provider.

World Wide Web

The 1990s saw the explosion of the Internet applications due to the emergence of the World Wide Web (WWW). The web was invented at CERN by Tim Berners-Lee. This invention has added the commercial applications to the Internet.

Time Line

The following is a list of important Internet events in chronological order:

- 1969. Four-node ARPANET established.
- 1970. ARPA hosts implement NCP.
- 1973. Development of TCP/IP suite begins.
- 1977. An internet tested using TCP/IP.
- 1978. UNIX distributed to academic/research sites.
- 1981. CSNET established.
- 1983. TCP/IP becomes the official protocol for ARPANET.
- 1983. MILNET was born.
- 1986. NSFNET established.
- 1990. ARPANET decommissioned and replaced by NSFNET.
- 1995. NSFNET goes back to being a research network.
- 1995. Companies known as Internet Service Providers (ISPs) started.

Growth of the Internet

The Internet has grown tremendously. In just a few decades, the number of networks has increased from tens to hundreds of thousands. Concurrently, the number of computers connected to the networks has grown from hundreds to hundreds of millions. The Internet is still growing. Factors that have an impact on this growth include the following:

- **New Protocols:** New protocols need to be added and deprecated ones need to be removed. For example, a protocol superior in many respects to IPv4has been approved as a standard but is not yet fully implemented.
- **New Technology:** New technologies are under development that will increase the capacity of networks and provide more bandwidth to the Internet's users.
- **Increasing Use of Multimedia:** It is predicted that the Internet, once just a vehicle to share data, will be used more and more for multimedia (audio and video).

Chapter 2
PHYSICAL LAYER AND NETWORK MEDIA

Introduction

It is well known that interconnections have historically been a limiting factor in computing power and speed. The physical layer network media is the foundation of any networks and provides the framework for the network architecture. Choosing and implementing the correct and appropriate type of cable is critical to data communication and therefore an organization's success.

A critical component of today's converged communications is scalability citing the debilitating cost of obsolescence as organizations' rely on data communications to remain competitive. With this basis, a network's physical media and its inherent bandwidth can be a limiting factor to an organization's communication needs and business goals. Network designers must consider throughput, cost, size, scalability, connectors and immunities to environmental factors when designing their system.

As stridently asserted throughout this course, business needs must drive IT design and implementation and cost is a critical factor in today's business climate. Network designers must assess not only the cost of the medium but also the cost of the end and intermediary communication devices that include the network interface cards (NIC), hubs, switches and repeaters. Furthermore, network designers must not only consider the cost of network installation and management but they must also understand the maintenance phase is the most expensive phase of the System Development Life Cycle (SDLC). It is critical that organizations draw on industry best practices and perform the proper systems analysis and design prior to network implementation. Fortunately, network designers can draw from standardized structured cabling best practices that have quickly matured over the last 20 years.

As a basis, data transmissions can be distinguished between analog and digital transmissions. Analog signals are continuous electromagnetic signals characterized by variable voltages whereas digital signals are discrete and directly represent encoded digital logic. It should be noted that analog electromagnetic digital signals are often determined within a specified range whereas digital fiber-optic signals are far more precise. Bandwidth is a measure of the difference between the lowest and highest frequencies a media can transmit and is expressed in hertz (Hz). Higher frequencies can transmit more data in a given period of time since they accommodate more transitions. Throughput

is defined to be the amount of effective data that a network can accommodate during a given tim and is usually measured in megabits per second (Mbps). Throughput is determined by the physica nature the media, the networks' physical and logical configuration and the network's managemen protocols. Lastly, it should be noted that network analysis and queuing theory has shown that th full utilization of a network's bandwidth will never be realized. As network traffic increases, th individual waiting times increase according to an exponential curve and ultimately result i unacceptable delays or even the collapse of the network.

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

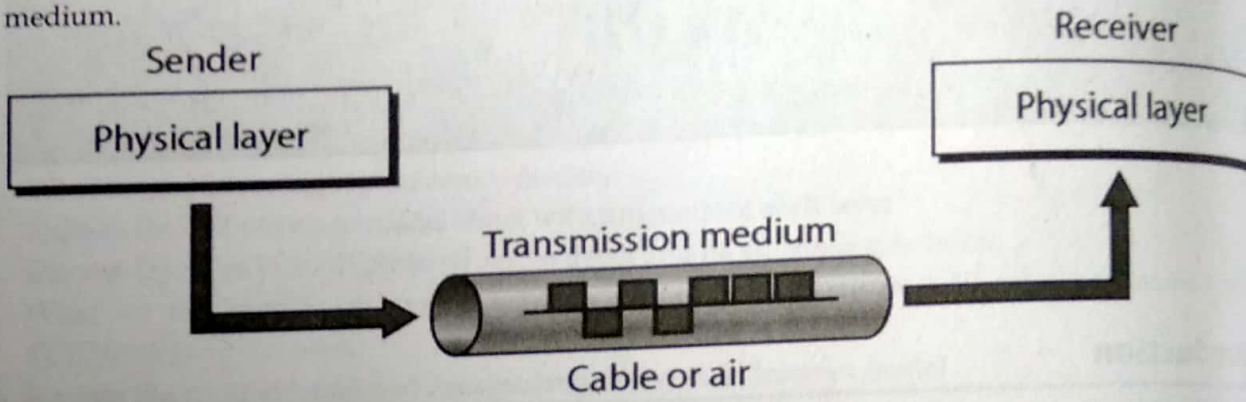


Figure 2.1 Transmission Media and Physical Layer

The physical layer is concerned with the following:

- **Physical characteristics of interfaces and media** - The physical layer defines t characteristics of the interface between the devices and the transmission medium.
- **Representation of bits** - To transmit the stream of bits, it must be encoded to signals. T physical layer defines the type of encoding.
- **Data Rate or Transmission rate** - The number of bits sent each second – is also defined the physical layer.
- **Synchronization of bits** - The sender and receiver must be synchronized at the bit lev Their clocks must be synchronized.

Network Devices

Network devices are the devices used for organizing a network, connecting to a network, routing packets, strengthening the signals, communicating with others, surfing the web, sharing files on network and many more uses.

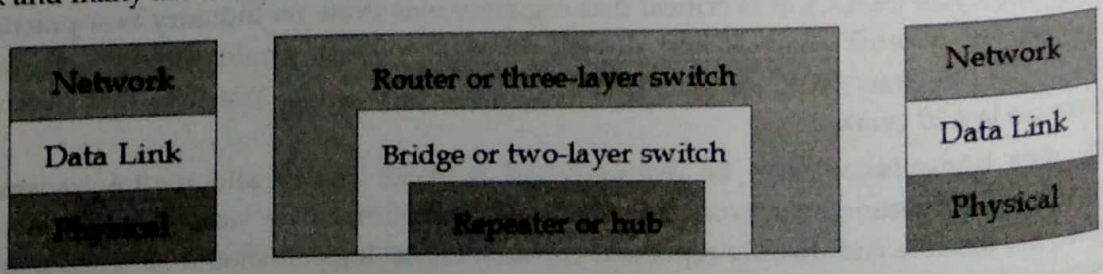


Figure 2.2 Layer 1, layer 2 and layer 3 connecting devices

To build a home network or connect to other network you will need to have some comm networking devices like internal or external modem, wireless router, cables, connectors and clipp tools. Types of network device are:

- NIC
- Hub
- Switch
- Router
- Bridge
- Gateway
- Modem
- Repeater
- Access Point

NIC

A Network Interface Card (NIC) is circuit board or a card that allows computers to communicate over a network via cables or wirelessly. It is also called as LAN adaptor, network adaptor or network card. Enable clients, servers, printers and other devices to transmit and receive data over the network. Operates on physical and data link layer of OSI model. Every network adaptor is assigned a unique 48-bit Media Access Control (MAC) address, which is stored in ROM to identify themselves in a network or a LAN. Available maximum data transfer rate is 10, 100 and 1000 MBPS. Typically network adaptor has RJ45 or BNC or both sockets for connecting and a LED to show up it is active and transmitting the data. Connects to a network via cables like CAT5, Co-axial, fiber-optics etc. And wirelessly by a small antenna.

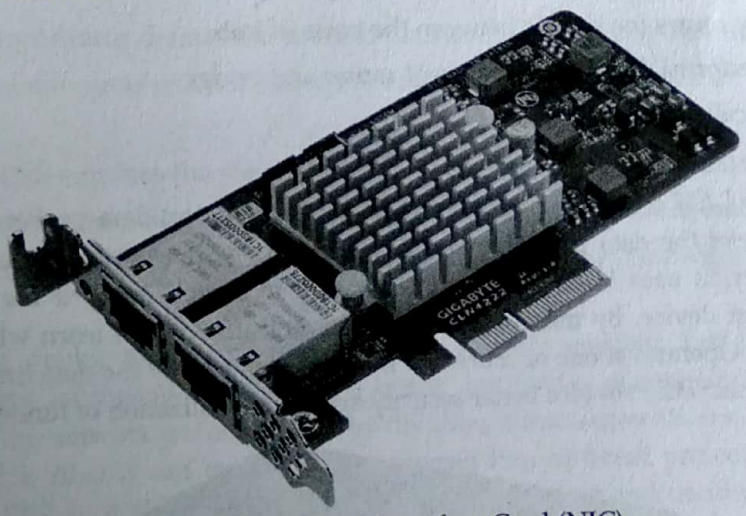


Figure 2.3 Network Interface Card (NIC)

Hub

Hub is a connecting device in which various types of cables are connected to centralize network traffic through a single connecting point. Hub with multiple ports are used to connect topologies, segments of LAN and to monitor network traffic. It manages and controls the send and receive data to and from the computers. Hub works on the physical layer of OSI or TCP/IP model. To avoid collision of data CSMA/CD protocol is used and protocol varies depending upon the vendor.

Figure 2.4 Ethernet hub with four port

The types of hub are as follows:

Active hub

- Can store, amplify, split and retransmit the received signals.
- Requires additional electronic circuit for performing different functions.
- It does work of repeater to amplify the signal, so it is also called as repeater.

Passive hub

- Can only forward received signal without amplifying it.
- It doesn't content any additional electronic circuit.

Intelligent hub

- Performs functions of both active and passive hub.
- Quickly routes the signals between the ports of hub.
- Also performs different functions of router and bridge.
- So it is called as intelligent hub.

Switch

Switch is a multiple LAN connecting device, which takes incoming data packet from any multiple input ports and passes the data packet to specific output port. It works same as hub but does its work very efficiently. It uses MAC address information to switch forward the data packets to a particular destination device. By monitoring the network traffic, it can learn where the particular addresses is located. Operates at one or more OSI model layers mainly the data link layer. Minimizes the collision of data packets. Provides better security and better utilization of limited bandwidth.

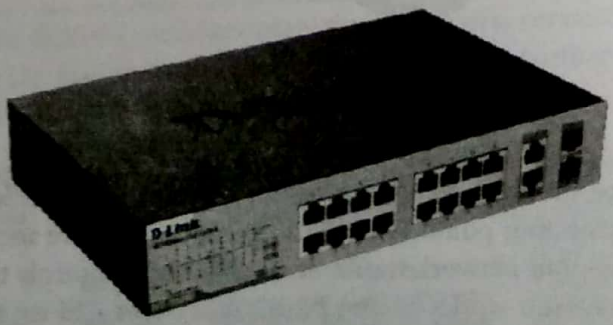


Figure 2.5 Switch

It uses two different method for switching the packets:

1. **In cut-through method** switch examines the header of the packet and decides, where to pass the packet before it receives the whole packet. Increases the chances of errors without verifying the data integrity.

2. **In store and forward method** switch reads the entire packet in its memory and checks for error before transmitting the packet. This method is slower and time consuming but error free.

Router

Router is internetwork connecting device that determines most efficient path for sending a data packet to any given network. Used to connect two or more similar or dissimilar topological LANs or WLANs. Shares available bandwidth with multiple computers in a network. Provides a better protection as a hardware firewall against hacking. Routers are intelligent enough to determine shortest and fastest path from source to destination in a network using algorithms. Operates at network layer of OSI model. Wireless routers are now widely used in home and offices as they allow a user to connect easily without installing any cables. Basically router is of two types i.e. wired routers and wireless routers.

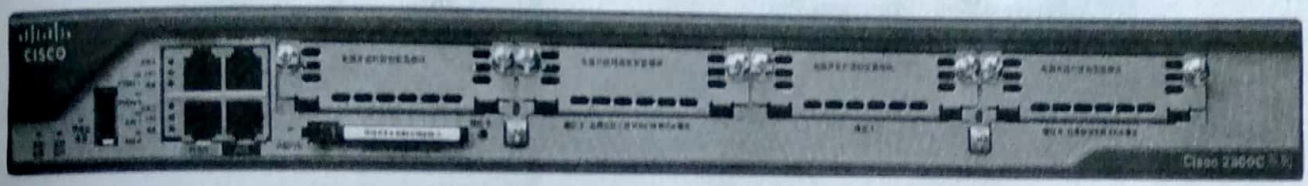


Figure 2.6 Cisco 2800 Series Router

Routers are also classified based on defining paths and they are as follows:

Static Router

- System administrator defines the shortest path in the network by executing commands.
- Have some limitations and not that much effective than dynamic router.

Dynamic Router

- Router itself determines the shortest path between the computers in the network.
- System administrator doesn't need to interact with router that saves time and cost.
- This types of routers are used in greater extend compare to static router.

Bridge

Bridge is a networking device that connects two or more LAN's together. Bridge is used when number of LANs starts increasing, the network traffic begins on overwhelming to available bandwidth. It reduces the network traffic of LAN by dividing it into segments and operates at data link layer of OSI model. Also it can transfer data between two different protocols like Ethernet (802.3) and token bus (802.4). It checks the MAC address of the frame and decides to forward the frame or to discard the frame.

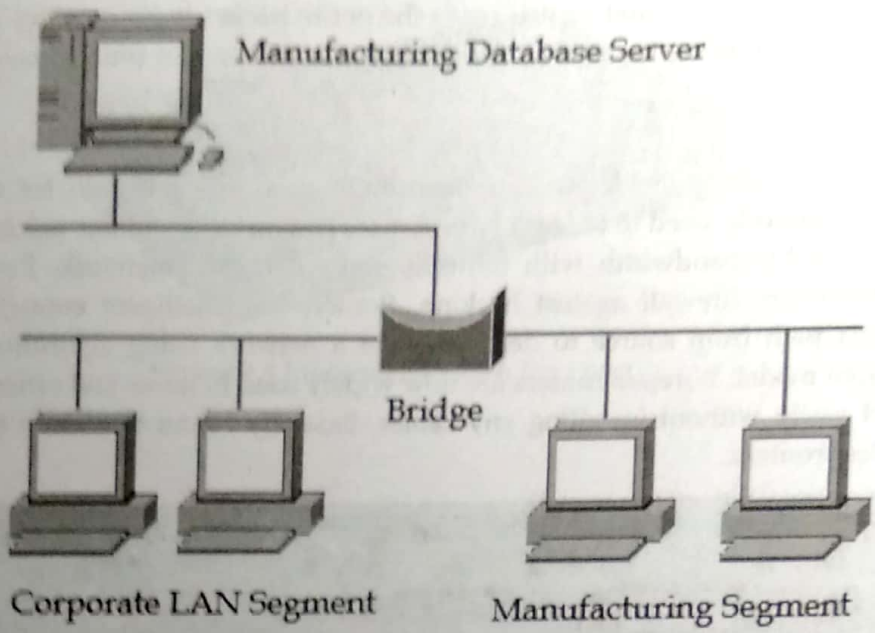


Figure 2.7: Bridge Connecting Similar Network

Types of bridge are:

Transparent Bridge

- Source and destination devices are unaware of the bridge in between them, so called as transparent bridge.
- Accepts all incoming frames to the bridge.
- If the frame is unknown forward the frame to all LANs.
- If the frame is from the same LAN discard the frame from bridge.
- If the incoming frame is from different LAN accept it and forward it to particular LAN.

Source Route Bridge

- Used on token ring networks.
- Bridge derives the entire path of the frame embedded in the header of the frame and decides how to forward the frame throughout the network till it reaches its destination.

Translational Bridge

- Used when LANs have dissimilar protocols or speeds.
- Like Ethernet and token ring or Ethernet and FDDI.

Gateway

Gateway is a network point that act as entry point to other network and translates one data format to another. Following are some common functions of the gateway:

- **Protocol translation:** translates protocol format into required protocol format of the network, such as X.25 to TCP/IP.
- **Network address translation:** translates your public IP address to the private IP addresses on your network.
- **DHCP service:** automatically assigns IP address to a computer from a defined range of addresses for a given network.

- Monitoring and regulating each packet entering and leaving the network.

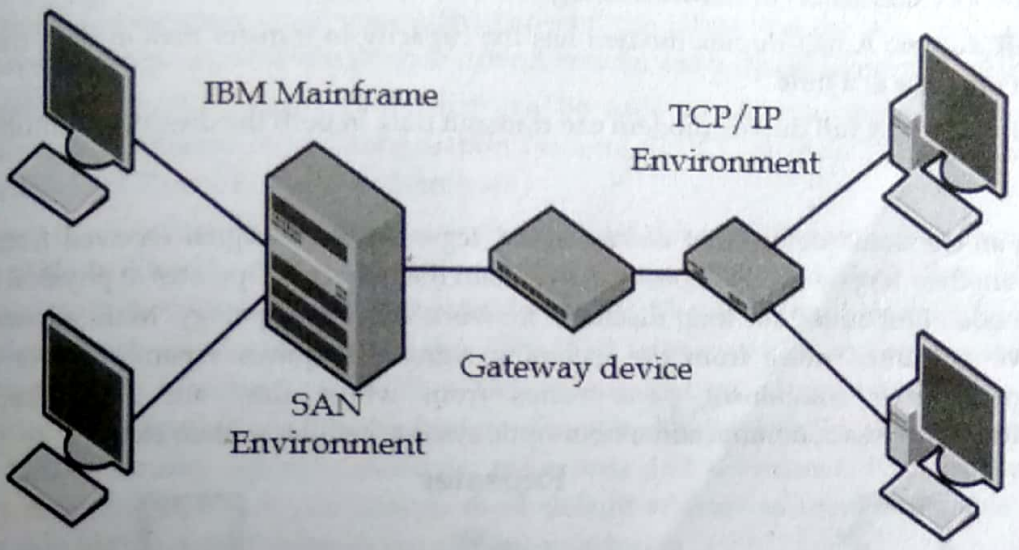


Figure 2.8: Gateway connecting two different environments (SAN and TCP/IP)

Uses of gateway are:

- To route the traffic from one network to another.
- To connect LAN to WAN or VPN (Virtual Private Network).
- Acts as a proxy server and firewall server to protect from virus, malware and harmful attacks.
- To keep history of accessed website, bandwidth usage, timing of each user of the network in a database.

Modem

Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines. Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location. The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer. The digital data is usually transferred to or from the modem over a serial line through an industry standard interface, RS-232. Many telephone companies offer DSL services, and many cable operators use modems as end terminals for identification and recognition of home and personal users. Modems work on both the Physical and Data Link layers.

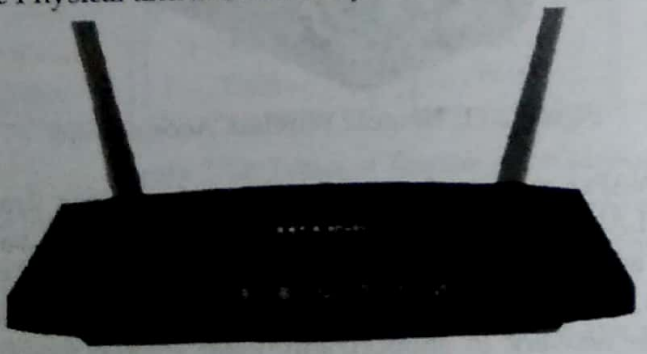


Figure 2.9: TP-Link Wi-Fi Router

Depending on direction of data transmission, modem can be of these types:

- **Simplex:** A simplex modem can transfer data in only one direction, from digital devic network (modulator) or network to digital device (demodulator).
- **Half duplex:** A half-duplex modem has the capacity to transfer data in both the directi but only one at a time.
- **Full duplex**: A full duplex modem can transmit data in both the directions simultaneousl

Repeater

Repeater is an electronic device that reshapes and regenerates the signal received from one L segment to another. Mostly used to boost the signals in the network. Operates at physical layer in OSI layer model. Best suited for long distances network and bus topology. Main advantage is t they remove unwanted noise from the incoming signals. Requires separate power supply functioning. Repeater component parts varies from where they are used like in digi communication, wireless communication, fiber-optic system, cellular system etc.

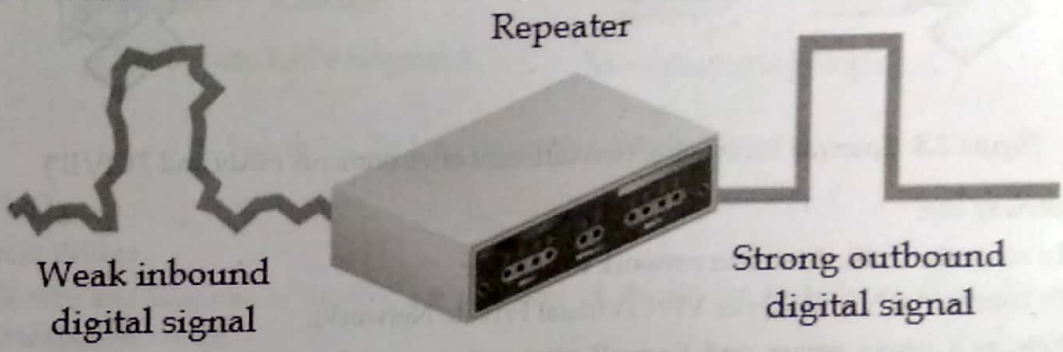


Figure 2.10: Repeater

Access Point

While an access point (AP) can technically involve either a wired or wireless connection, commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and can operate either as a bridge connecting a standard wired network to wireless devices or as a rout passing data transmissions from one access point to another.

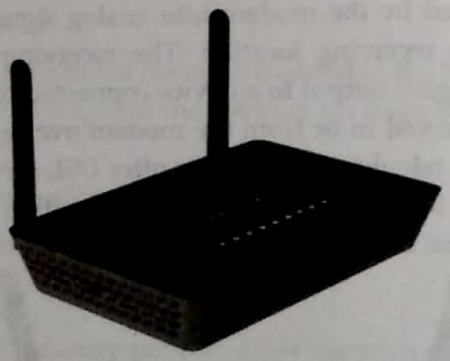


Figure 2.11: Netgear Wireless Access Point

Wireless access points (WAPs) consist of a transmitter and receiver (transceiver) device used t create a wireless LAN (WLAN). Access points typically are separate network devices with a built-i antenna, transmitter and adapter. APs use the wireless infrastructure network mode to provide connection point between WLANs and a wired Ethernet LAN. They also have several ports, givin you a way to expand the network to support additional clients. Depending on the size of th network, one or more APs might be required to provide full coverage. Additional APs are used t

allow access to more wireless clients and to expand the range of the wireless network. Each AP is limited by its transmission range — the distance a client can be from an AP and still obtain a usable signal and data process speed. The actual distance depends on the wireless standard, the obstructions and environmental conditions between the client and the AP. Higher end APs have high-powered antennas, enabling them to extend how far the wireless signal can travel.

APs might also provide many ports that can be used to increase the network's size, firewall capabilities and Dynamic Host Configuration Protocol (DHCP) service. Therefore, we get APs that are a switch, DHCP server, router and firewall.

To connect to a wireless AP, you need a service set identifier (SSID) name. 802.11 wireless networks use the SSID to identify all systems belonging to the same network, and client stations must be configured with the SSID to be authenticated to the AP. The AP might broadcast the SSID, allowing all wireless clients in the area to see the AP's SSID. However, for security reasons, APs can be configured not to broadcast the SSID, which means that an administrator needs to give client systems the SSID instead of allowing it to be discovered automatically. Wireless devices ship with default SSIDs, security settings, channels, passwords and usernames. For security reasons, it is strongly recommended that you change these default settings as soon as possible because many internet sites list the default settings used by manufacturers.

Access points can be fat or thin. Fat APs, sometimes still referred to as autonomous APs, need to be manually configured with network and security settings; then they are essentially left alone to serve clients until they can no longer function. Thin APs allow remote configuration using a controller. Since thin clients do not need to be manually configured, they can be easily reconfigured and monitored. Access points can also be controller-based or stand-alone.

Transmission Medias and Ethernet Cable Standards

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

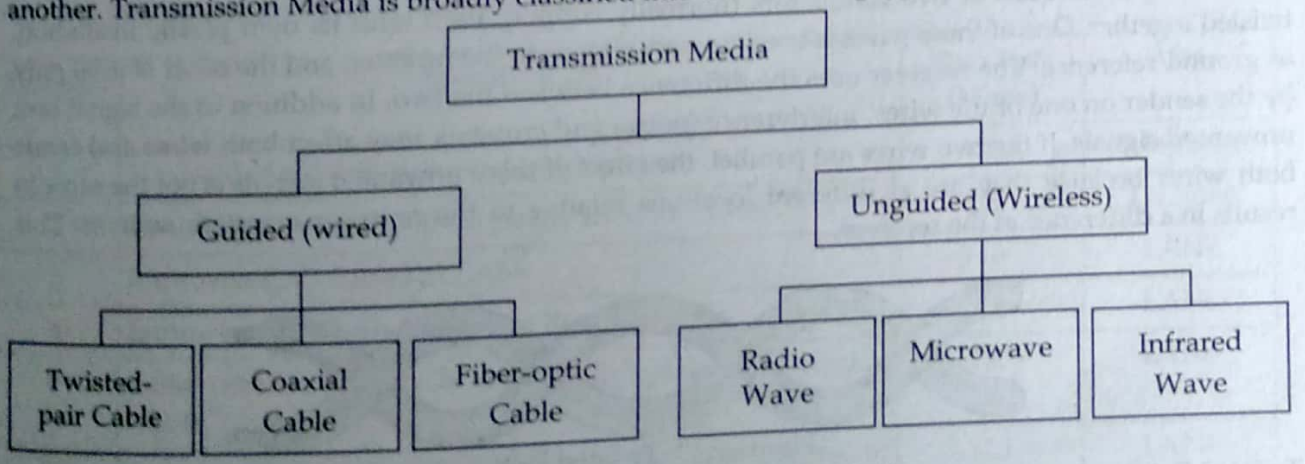


Figure 2.12: Types of Transmission Media

In considering the design of data transmission systems, key concerns are data rate and distance: the greater the data rate and distance the better. A number of design factors relating to the transmission medium and the signal determine the data rate and distance:

- **Bandwidth:** All other factors remaining constant, the greater the bandwidth of a signal, the higher the data rate that can be achieved.

- **Transmission impairments:** Impairments, such as attenuation, limit the distance. Fo guided media, twisted pair generally suffers more impairment than coaxial cable, which i turn suffers more than optical fiber.
- **Interference:** Interference from competing signals in overlapping frequency bands ca distort or wipe out a signal. Interference is of particular concern for unguided media, but i also a problem with guided media. For guided media, interference can be caused b emanations from nearby cables. For example, twisted pairs are often bundled together an conduits often carry multiple cables. Interference can also be experienced from unguide transmissions. Proper shielding of a guided medium can minimize this problem.
- **Number of receivers:** A guided medium can be used to construct a point-to-point link or a shared link with multiple attachments. In the latter case, each attachment introduces some attenuation and distortion on the line, limiting distance and/or data rate.

Guided (Bounded or Wired) Transmission 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.

1. Twisted-Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points:

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 μs/km.
- Repeater spacing is 2km.

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of these wires is used to carry signals to the receiver, and the other is used only as ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver.

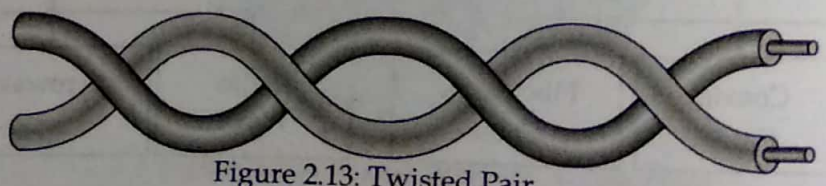


Figure 2.13: Twisted Pair

Twisted Pair is of two types:

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

Unshielded Twisted Pair (UTP) Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own color plastic insulator. Identification is the reason behind coloured plastic insulation. UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11**(RJ stands for registered jack) connector and 4 pair cable use **RJ-45** connector.

Figure 2.14: Unshielded Twisted Pair Cable

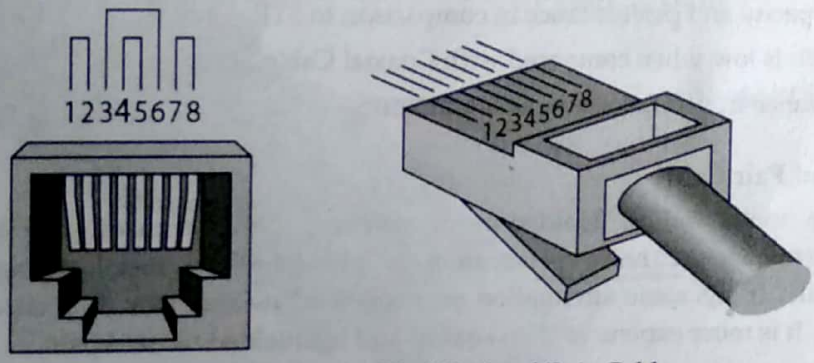


Figure 2.15: Unshielded Twisted Pair Cable

Table 2.1: Categories of unshielded twisted-pair cables

Category	Specification	Data Rate (Mbps)	Use
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs

7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Advantages of UTP Cable

- Least expensive
- Easy to install
- High speed capacity
- Higher grades of UTP are used in LAN technologies like Ethernet.
- It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages of UPT Cable

- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Bandwidth is low when compared with Coaxial Cable
- Short distance transmission due to attenuation

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk. It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

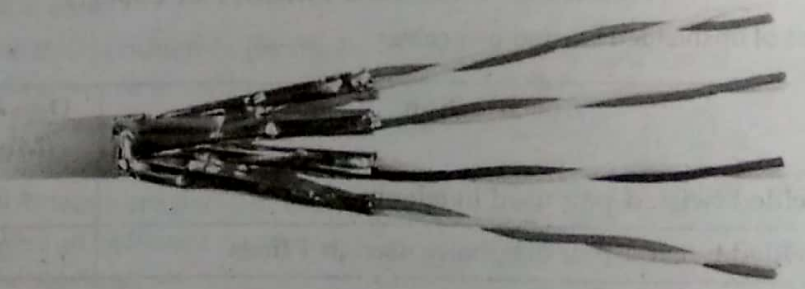


Figure 2.16: Shielded Twisted Pair Cable

Advantages of STP Cable

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signaling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of STP Cable

- Comparatively difficult to install and manufacture

- More expensive
- Bulky

Applications of Shielded Twisted Pair Cable

In telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables. Local Area Network, such as 10Base-T and 100Base-T, also use twisted-pair cables.

2. Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, braid or both. Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

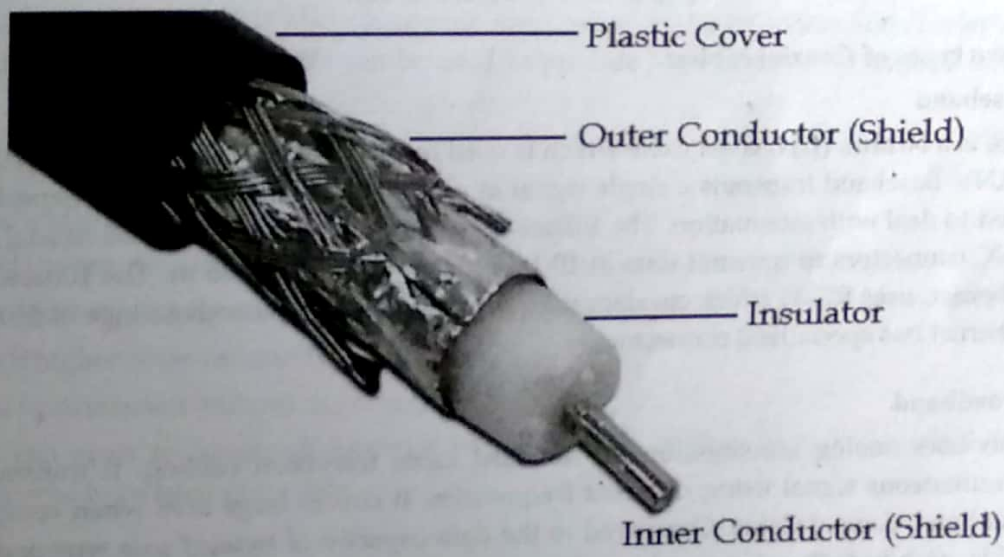


Figure 2.17: Coaxial Cable

Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and the type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in the table below:

Table 2.2: Categories of coaxial cables

Category	Impedance	Use
RG-7 or RG-11	50 Ω	Thick Ethernet
RG-58	50 Ω	Thin Ethernet
RG-59	75 Ω	Cable Television
RG-62	93 Ω	ARCNET

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the **Bayonet Neill-Concelman (BNC)** connector. The figure 2.18shows 3 popular types of these 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 the device, such as a TV set. The BNC T connector is used in Ethernet networks to 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.

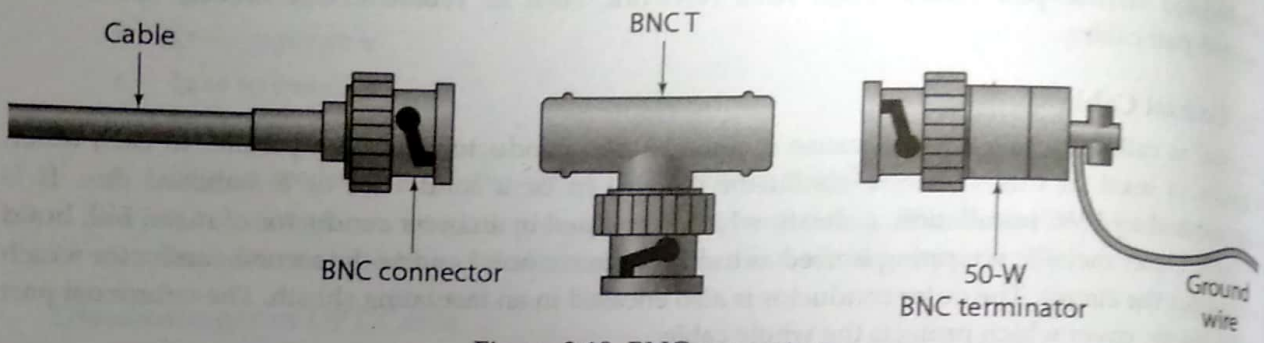


Figure 2.18: BNC connectors

There are two types of Coaxial cables:

- **Baseband**

  This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. Repeaters can be used to deal with attenuation. The 10Base-2, or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10 Mbps with a range of 185 m. The 10Base5, or Thick Ethernet, uses RG-11 (thick coaxial cable) to transmit 10 Mbps with a range of 5000 m. Thick Ethernet has specialized connectors.

- **Broadband**

  This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable. Compared to the data capacity of twisted pair wire and baseband cable, each broadband channel is quite robust, as it can support the equivalent of millions of bits per second. To support such a wide range of frequencies, broadband coaxial cable systems require amplifiers to deal with attenuation approximately every three to four kilometers. Although the splitting and joining of broadband signals and cables is possible, it is a rather precise science that is best left to specialists in the field. Thus, many network administrators often hire outside experts to install and maintain broadband systems.

In addition to the two signal-based categories, coaxial cable also is available in a variety of thicknesses, with two primary physical types: **thick coaxial cable** and **thin coaxial cable.** Thick coaxial cable ranges in size from approximately 6 to 18 mm (1/4 to 3/4 inch) in diameter. Thin coaxial cable is approximately 4 mm (less than 1/4 inch) in diameter. Compared to thick coaxial cable, which typically carries broadband signals, thin coaxial cable has limited noise isolation and typically carries baseband signals. Thick coaxial cable has better noise immunity and is generally used for the transmission of analog data, such as single or multiple video channels.

Applications

Coaxial cable is a versatile transmission medium, used in a wide variety of applications. The most important of these are

- Television distribution
- Long-distance telephone transmission
- Short-run computer system links
- Local area networks

Coaxial cable is widely used as a means of distributing TV signals to individual homes -cable TV. From its modest beginnings as Community Antenna Television (CATV), designed to provide service to remote areas, cable TV reaches almost as many homes and offices as the telephone. A cable TV system can carry dozens or even hundreds of TV channels at ranges up to a few tens of kilometers. Coaxial cable has traditionally been an important part of the long-distance telephone network. Today, it faces increasing competition from optical fiber, terrestrial microwave, and satellite. Using frequency division multiplexing (FDM), a coaxial cable can carry over 10,000 voice channels simultaneously. Coaxial cable is also commonly used for short-range connections between devices. Using digital signaling, coaxial cable can be used to provide high-speed I/O channels on computer systems.

Advantages of Coaxial Cable

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages of Coaxial Cable

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.
- Coaxial cables are more prone to lightning strikes.
- They cover less distance than fiber optic cables.
- They cover less bandwidth than both fiber optic and twisted pair cables.

3. Fiber Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. For better understanding we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction. The figure 2.19 shows how a ray of light changes direction when going from a high dense to a less dense substance.

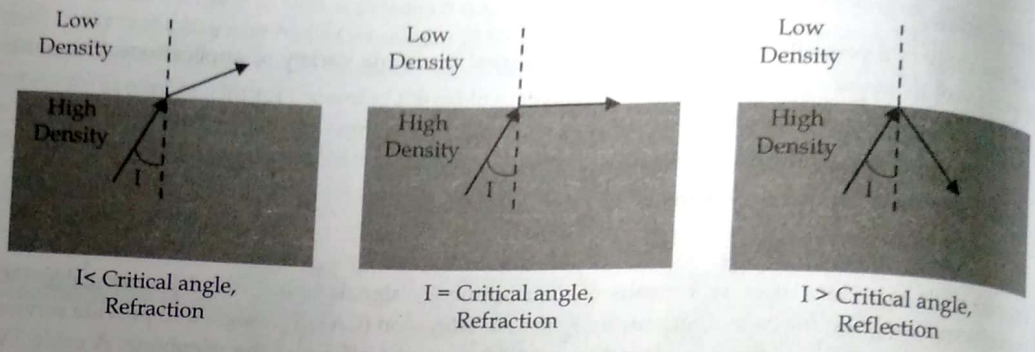


Figure 2.19: Bending of light ray

As figure 2.19 shows:

- If the angle of incidence I(the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface.
- If the angle of incidence is greater than the critical angle, the ray reflects(makes a turn) and travels again in the denser substance.
- If the angle of incidence is equal to the critical angle, the ray refracts and moves parallel to the surface as shown.

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.

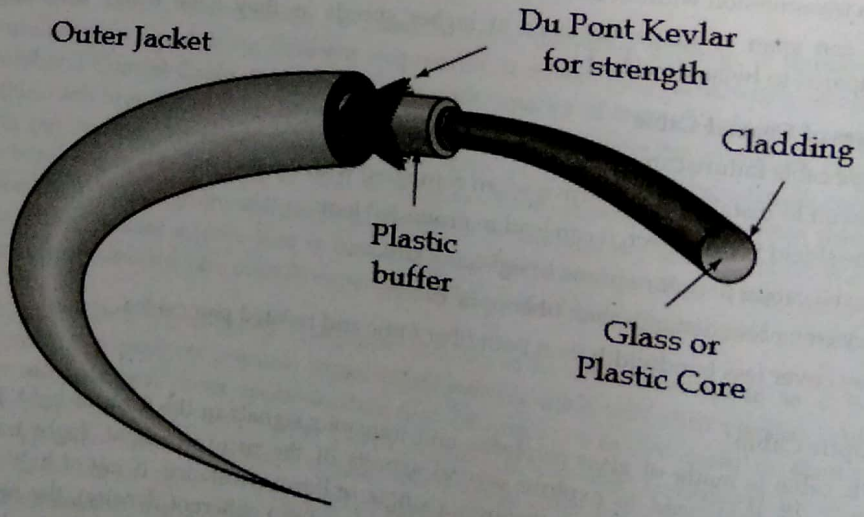


Figure 2.20: Fiber Construction

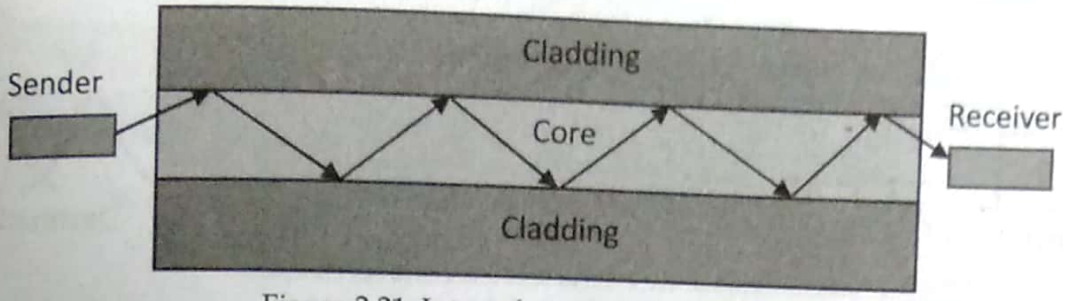


Figure 2.21: Internal view of Optical fiber

Propagation Modes of Fiber Optic Cable

Current technology supports two modes (Multimode and Single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: Step-index and Graded-index.

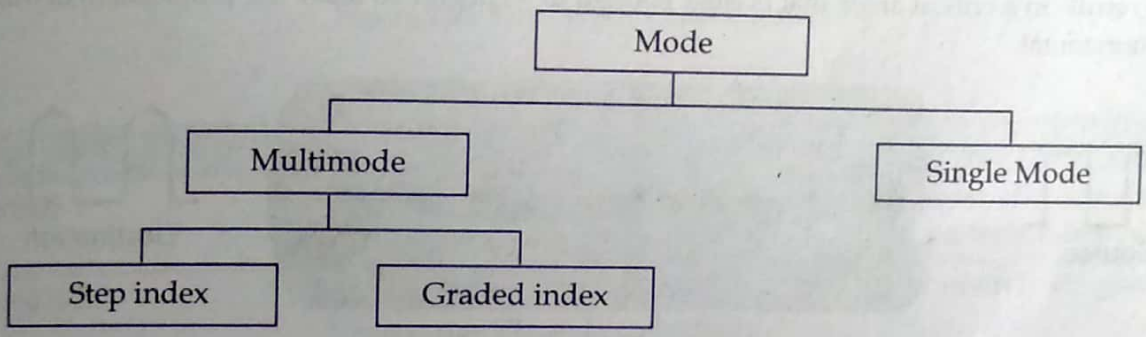


Figure 2.22: Propagation Modes

Multimode Propagation Mode

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core.

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.

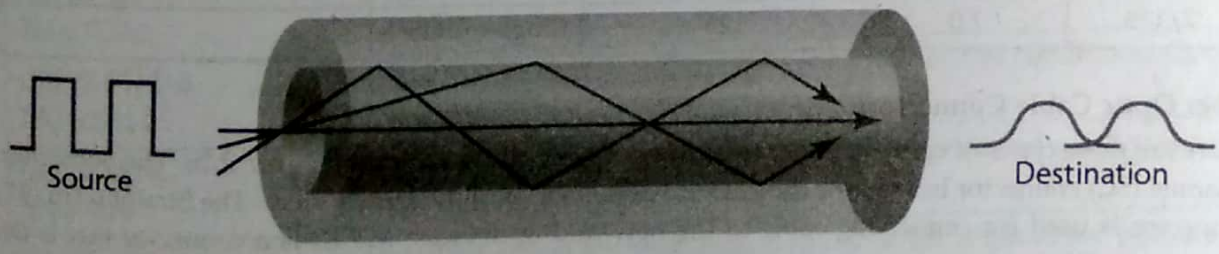


Figure 2.23: Multimode, step-index fiber

A second type of fiber, called **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. Figure 2.24 shows the impact of this variable density on the propagation of light beams.

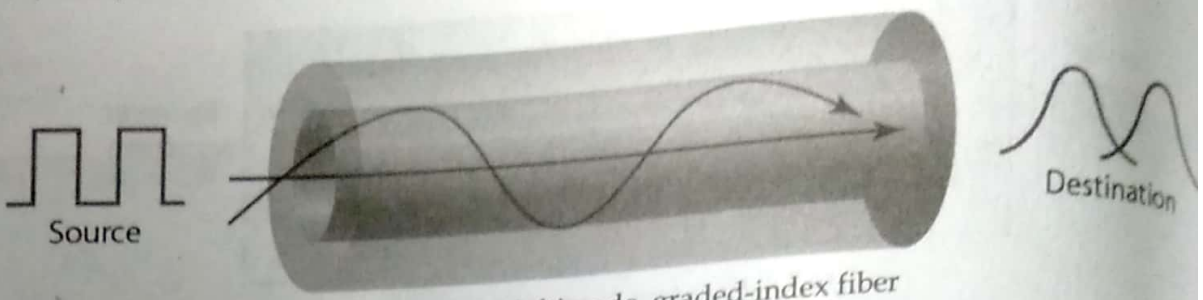


Figure 2.24: Multimode, graded-index fiber

Single Mode Propagation Mode

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. The decrease in density results in a critical angle that is close enough to 90 degree to make the propagation of beams almost horizontal.

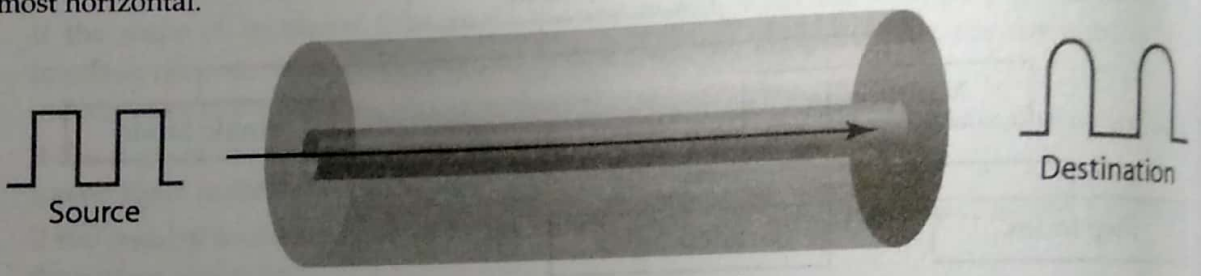


Figure 2.25: Single mode

Fiber Sizes for Fiber Optic Cable

Optical fibers are defined by the ratio of the diameter or their core to the diameter of their cladding both expressed in micrometers. The common sizes are shown in the table 2.3:

Table 2.3: Fiber types

Type	Core (μm)	Cladding (μm)	Mode
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

Fiber Optic Cable Connectors

There are three types of connectors for fiber optic cables, as shown in the figure 2.26. The Subscriber Channel (SC) connector is used for cable TV. It uses push/pull locking system. The Straight-Tip (ST) connector is used for connecting cable to the networking devices. MT-RJ is a connector that is the same size as RJ45.

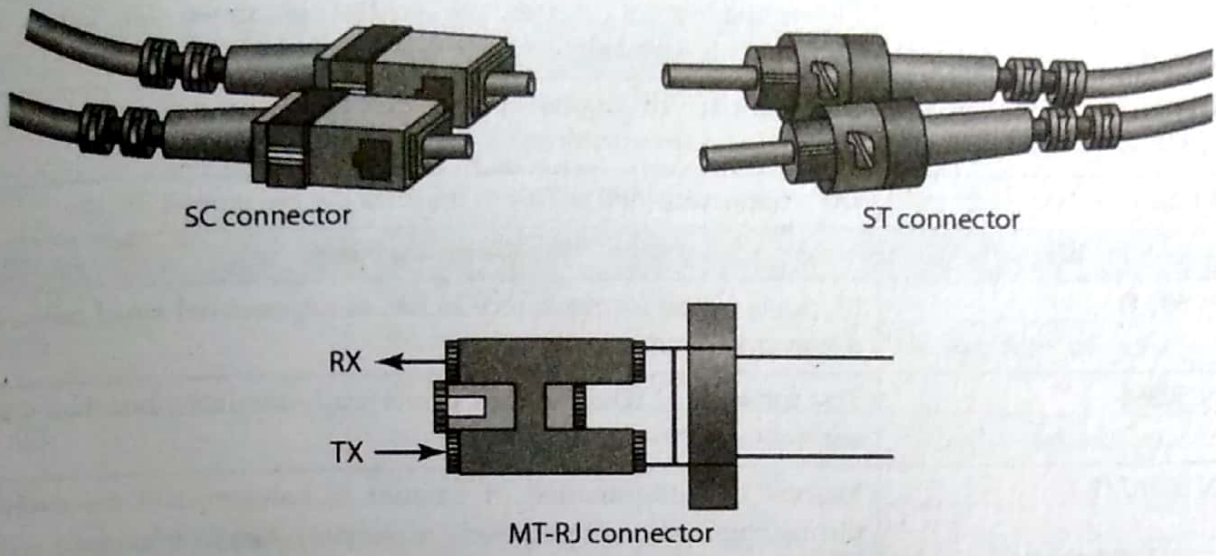


Figure 2.26: Fiber Optic Cable Connectors

Table 2.4: Fiber Optic Cables' Standards

BS	British Standard Institution
BS 6425-1	Method of determination of amount of halogen acid gas evolved during combustion of polymeric materials taken from cables
BS 6425-2	Determination of degree of acidity (corrosivity) of gases by measuring PH and conductivity
BS 6724	Measurement of smoke density using the 3 m test cube (Absorbance)
CEI	**Comitato Elettrotecnico Italiano**
CEI 20-11 / EN 50363	Insulating, sheathing and covering materials for low voltage energy cables
CEI 20-22/2	Prove di incendio su cavi elettrici. Prova di non propagazione dell'incendio
CEI 20-22/3 / EN 50266	Test for vertical flame spread of vertically-mounted bunched wires and cables
CEI 20-35/1 / EN 60332-1	Test for vertical flame propagation for a single insulated wire or cable
CEI 20-36/2 -5 IEC 60331-25	Test for electrical and optical cables under fire conditions. Circuit integrity.
CEI 20-36/4 - EN 50200	Methods of test for resistance to fire of unprotected small cables for use in emergency circuit
CEI 20-36/5 - EN 50362	Method of test for resistance to fire of larger unprotected power and control cables for use in emergency circuits
CEI 20-37/2-1 / EN 50267-2-1	Method of determination of amount of halogen acid gas evolved during combustion of polymeric materials taken from cables
CEI 20-37/2-2 / EN 50267-2-2	Determination of degree of acidity (corrosivity) of gases by measuring PH and conductivity

CEI 20-37/2-3 / EN 50267-2-3	Determination of degree of acidity of gases for cables determination of weighted average of pH an conductivity
CEI 20-37/3 - EN 61034	Measurement of smoke density of cables burning under defin conditions
CEI 20-37/4	Determinazione dell'indice di tossicità dei gas emessi dai cavi
EN	**European Norm**
EN 50200	Methods of test for resistance to fire of unprotected small cables f use in emergency circuit
EN 50266	Test for vertical flame spread of vertically-mounted bunched wir and cables
EN 50267/2-1	Method of determination of amount of halogen acid gas evolve during combustion of polymeric materials taken from cables
EN 50267/2-2	Determination of degree of acidity (corrosivity) of gases b measuring PH and conductivity
EN 60332-1	Test for vertical flame propagation for a single insulated wire o cable
EN 60332-2	Test for vertical flame propagation for a single small insulated wir or cable
EN 61034	Measurement of smoke density of cables burning under defined conditions
IEC	**International Electro technical Commission**
IEC/ISO 11801	Information technology - Generic cabling for customer premises
IEC 60331	Test for electrical and optical cables under fire conditions. Circuit integrity. Part 25 - Optical fiber cables
IEC 60332-1	Test on electric and optical fiber cables under fire conditions. Test on a single vertical insulated wire or cable
IEC 60332-2	Test on electric cables under fire conditions. Test on a single small vertical insulated copper wire or cable
IEC 60332-3	Test on electric cables under fire conditions. Test for vertical flame spread of vertically-mounted bunched wires or cables
IEC 60754-1	Method for determination of amount of halogen acid gas evolved during combustion of polymeric materials taken from cables
IEC 60754-2	Determination of degree of acidity (corrosivity) of gases by measuring pH and conductivity
IEC 60793	Optical fiber
IEC 60794	Optical fiber cables
IEC 61034-2	Measurement of smoke density of electric cables burning under defined conditions (LT)

ITU-T	International Telecommunication Union
G.651.1	Characteristics of a 50/125 μ μ m multimode graded index optical fiber cable for the optical access network
G.652	Characteristics of a single-mode optical fiber and cable
G.655	Characteristics of a non-zero dispersion-shifted single-mode optical fiber and cable
G.656	Characteristics of a fiber and cable with non-zero dispersion for wideband optical transport
G.657	Characteristics of a bending loss insensitive single mode optical fiber and cable for the access network

Advantages of Fiber Optic Cable

Fiber optic has several advantages over metallic cable:

- **Higher bandwidth:** Fiber Optic cable support dramatically higher bandwidths 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.
- **Greater repeater spacing:** Fewer repeaters mean lower cost and fewer sources of error. The performance of optical fiber systems from this point of view has been steadily improving. A signal can run from 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- **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 than can easily be tapped.
- **Electromagnetic isolation:** Optical fiber systems are not affected by external electromagnetic fields. Thus the system is not vulnerable to interference, impulse noise, or crosstalk. By the same token, fibers do not radiate energy, so there is little interference with other equipment and there is a high degree of security from eavesdropping. In addition, fiber is inherently difficult to tap.

Disadvantages of Fiber Optic Cable

There are some disadvantages in the use of optical fiber:

- **Installation and maintenance are difficult:** 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.
- **High 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.

3 KHz	300 GHz	300 THz	900 THz

Figure 2.27: Electromagnetic spectrum for wireless communication

Unguided signals can travel from the source to the destination in several ways: **Ground propagation, Sky propagation** and **Line-of-sight propagation**.

- **Ground Propagation:** In this, radio waves travel through the lowest portion of the atmosphere, hugging the Earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.

Figure 2.28: Ground Propagation (below 2MHz)

- **Sky Propagation:** In this, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to Earth. This type of transmission allows for greater distances with lower output power.

Figure 2.27: Electromagnetic spectrum for wireless communication

Unguided signals can travel from the source to the destination in several ways: **Ground propagation, Sky propagation** and **Line-of-sight propagation**.

- **Ground Propagation:** In this, radio waves travel through the lowest portion of the atmosphere, hugging the Earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.

Figure 2.28: Ground Propagation (below 2MHz)

- **Sky Propagation:** In this, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to Earth. This type of transmission allows for greater distances with lower output power.

Figure 2.29: Sky Propagation (2 – 30 MHz)

- **Line-of-sight Propagation:** in this type, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.

Figure 2.30: Line-of-sight Propagation (above 30 MHz)

The section of the electromagnetic spectrum defined as radio waves and microwaves is divided into eight ranges, called **bands**, each regulated by government authorities. These bands are rated from very low frequency (VLF) to extremely high frequency (EHF).

Table 2.5: Classification of Bands

Band	Range	Propagation	Application
very low frequency (VLF)	3–30 kHz	Ground	Long-range radio navigation
low frequency (LF)	30–300 kHz	Ground	Radio beacons and navigational locators
middle frequency (MF)	300 kHz–3 MHz	Sky	AM radio

high frequency (HF)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft
very high frequency (VHF)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
ultrahigh frequency (UHF)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
superhigh frequency (SF)	3–30 GHz	Line-of-sight	Satellite
extremely high frequency (EHF)	30–300 GHz	Line-of-sight	Radar, Satellite

We can divide wireless transmission into three broad groups:

- Radio waves
- Micro waves
- Infrared waves

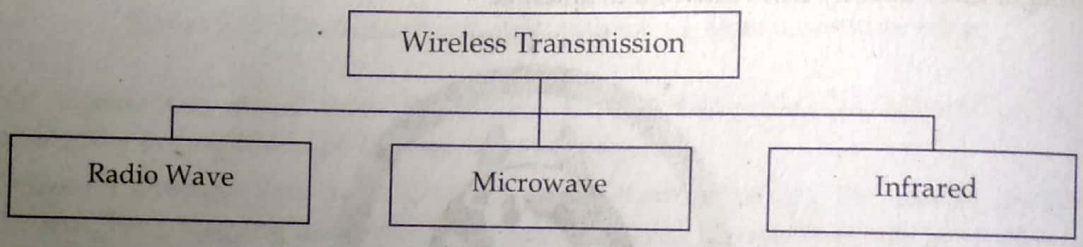


Figure 2.31: Wireless Transmission Waves

1. Radio Waves

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves. Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

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

Omnidirectional Antenna for Radio Waves

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

Figure 2.32: Omnidirectional antenna

Applications of Radio Waves

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

Advantages of Radio Waves

- Wires are not needed as they travel through air, thus a cheaper form of communication.
- Some radio waves are reflected off the ionosphere, so can travel around the Earth.
- Radio wave can carry a message instantaneously over a wide area.
- Aerials to receive radio waves are simpler than for microwaves.

Disadvantages of Radio Waves

- The range of frequencies that can be accessed by existing technology is limited, so there is a lot of competition amongst companies for the use of the frequencies.
- Travel in a straight line, so repeater stations may be needed.

2. Micro Waves

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

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

Unidirectional Antenna for Microwaves

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

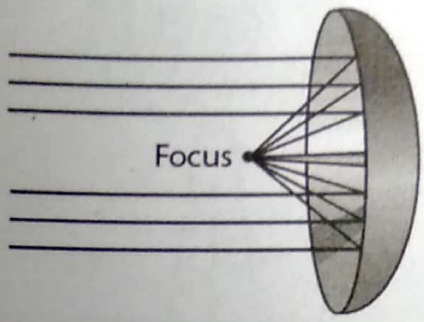


Figure 2.33: Dish antenna

A **parabolic antenna** works as a funnel, catching a wide range of waves and directing them to common point. In this way, more of the signal is recovered than would be possible with a single point receiver. A **horn antenna** looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

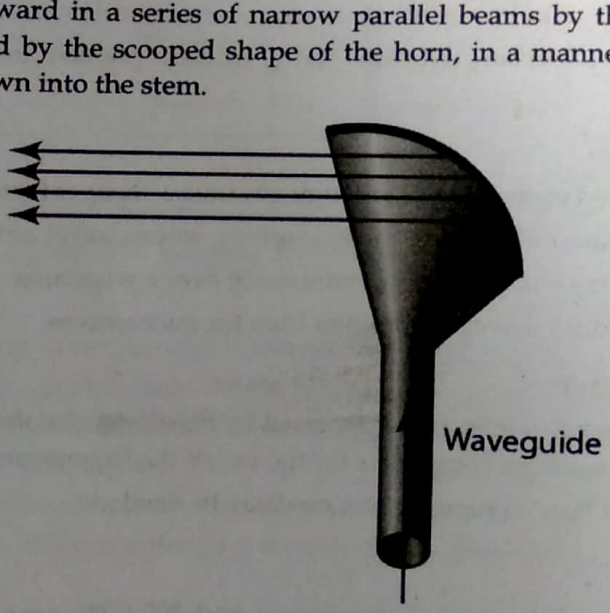


Figure 2.34: Horn antenna

Application

Microwaves 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.

There are two types of Microwave Transmission:

- Terrestrial Microwave
- Satellite Microwave

Terrestrial Microwave

The primary use for terrestrial microwave systems is in long haul telecommunications service, as an alternative to coaxial cable or optical fiber. The microwave facility requires far fewer amplifiers or

rotation, which occurs at a height of 35,863 km at the equator. Two satellites using the same frequency band, if close enough together, will interfere with each other. To avoid this, current standards require a 4° spacing in the 4/6-GHz band and a 3° spacing at 12/14 GHz. Thus the number of possible satellites is quite limited.

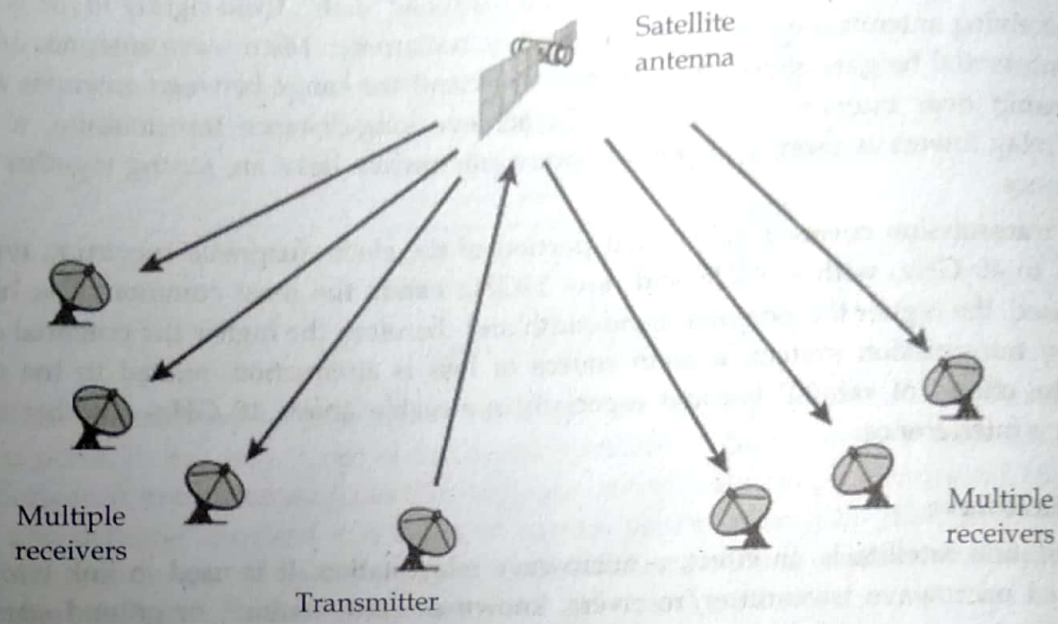


Figure 2.36: Broadcast Link

Among the most important applications for satellites are: Television distribution, Long-distance telephone transmission, Private business networks, and Global positioning.

Advantages of Microwaves

- Wires are not needed as they travel through air, thus a cheaper form of communication.
- Microwave passes through the ionosphere, so are suitable for satellite to Earth transmission.
- Microwave can be modified to carry many signals at one time, including data, television pictures and voice message.

Disadvantages of Microwaves

- Absorbed very easily by natural, e.g. rain, and made objects, e.g. concrete. They are also absorbed by living tissue and may cause harm by their **cooking effect**. Microwaves suffer from attenuation due to atmospheric conditions.
- Need special aerials to receive them.
- Travel in a straight line, so repeater stations may be needed.

3. Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, with high frequencies, cannot penetrate walls. This prevents interference between one system and with another system. It is a region of the electromagnetic radiation spectrum where wavelengths range from about 700 nanometers (nm) to 1 millimeter (mm). Infrared waves are longer than those of visible light, but shorter than those of radio waves. Remote controls use near-infrared light, transmitted with light-emitting diodes (LEDs), to send focused signals to home-entertainment devices, such as televisions. When we use infrared remote control, we

do not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication. Infrared light is also used in fiber optic cables to transmit data.

Applications of Infrared Waves

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

Advantages of Infrared Waves

- Can detect people inside burning buildings and cars.
- Useful in the military for identifying targets.
- Used in scientific experimentation to identify the heat of an object.
- Easy to tell what the readings on an infrared camera mean.

Disadvantages of Infrared Waves

- Can cause minor burns if exposed to skin for long periods of time.
- Can cause cataracts in the eyes after long exposure.
- Cheap laser pointers, if without an IR filter, can damage your eyes with Infrared light after a little while of exposure.

Difference between Guided and Unguided Media

Table 2.6: Guided Vs unguided media

Guided media	Unguided media
The signal energy propagates within the guided media.	The signal energy propagates through the air.
Guided media is mainly used for point to point communication.	Unguided media is mainly used for broadcasting purpose.
The signal propagates in the guided media in the form of voltage, current or photons.	The signal propagates in the unguided media in the form of EM waves.
Examples: twisted pair cables, coaxial cable, optical fiber cable.	Examples: Microwave or radio links, infrared

Circuit, Message & Packet Switching

For transmission of data beyond a local area, communication is typically achieved by transmitting data from source to destination through a network of intermediate switching nodes; this switched network design is typically used to implement LANs as well. The switching nodes are not concerned

with the content of the data; rather, their purpose is to provide a switching facility that will move the data from node to node until they reach their destination.

Figure 2.37 illustrates a simple network. The devices attached to the network may be referred to as stations. The stations may be computers, terminals, telephones, or other communicating devices. We refer to the switching devices whose purpose is to provide communication as nodes. Nodes are connected to one another in some topology by transmission links. Node-station links are generally dedicated point-to-point links. Node-node links are usually multiplexed, using either frequency division multiplexing (FDM) or time division multiplexing (TDM). In a switched communication network, data entering the network from a station are routed to the destination by being switched from node to node. For example, in Figure 2.37, data from station A intended for station F are sent to node 4. They may then be routed via nodes 5 and 6 or nodes 7 and 6 to the destination.

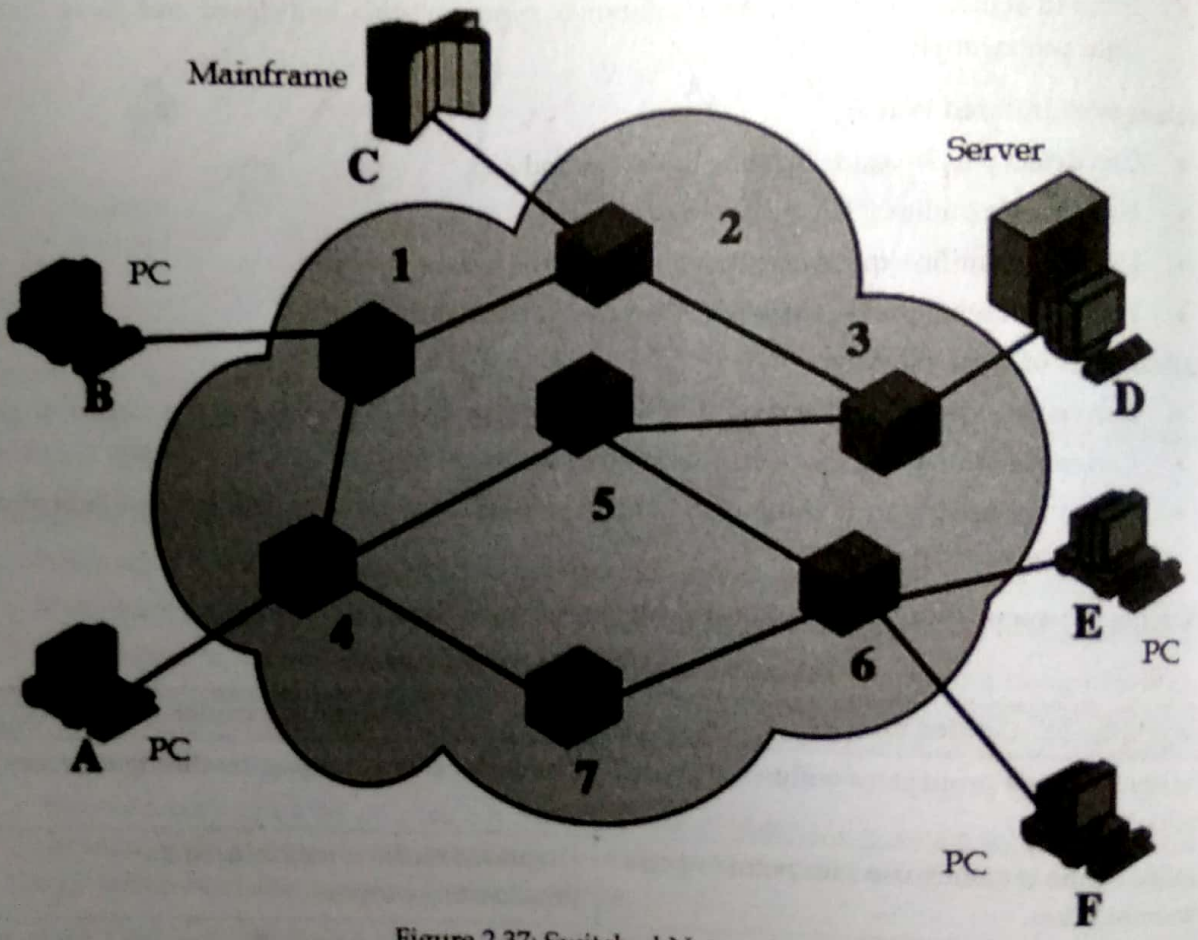


Figure 2.37: Switched Network

Traditionally, three methods of switching have been discussed: **circuit switching, packet switching and message switching.** The first two are commonly used today. The third has been phased out in general communications but still has networking applications. Packet switching can further be divided into two subcategories—**virtual circuit approach and datagram approach**—as shown in Figure 2.38.

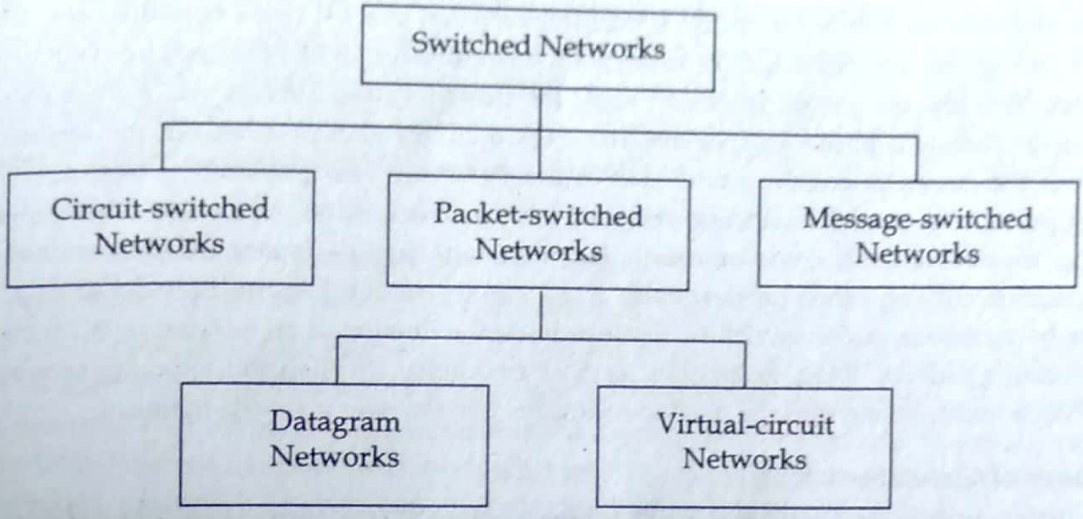


Figure 2.38: Taxonomy of Switched Networks.

1. Circuit Switching

The term **circuit switching** refers to a communication mechanism that establishes a path between a sender and receiver with guaranteed isolation from paths used by other pairs of senders and receivers. Circuit switching is usually associated with telephone technology because a telephone system provides a dedicated connection between two telephones. In fact, the term originated with early dialup telephone networks that used electromechanical switching devices to form a physical circuit. Figure 2.39 illustrates how communication proceeds over a circuit-switched network.

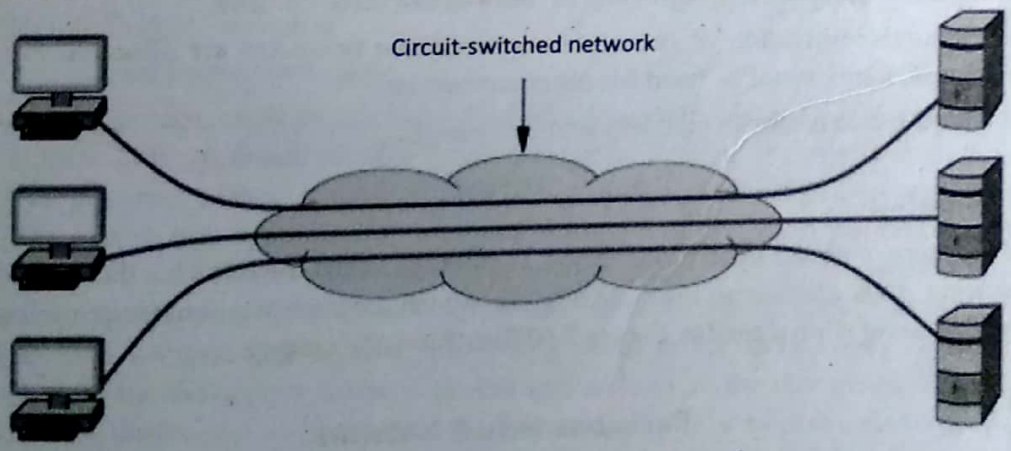


Figure 2.39: Circuit-switched network

Currently, circuit switching networks use electronic devices to establish circuits. Furthermore, instead of having each circuit correspond to a physical path, multiple circuits are multiplexed over shared media, and the result is known as a virtual circuit. Thus, the distinction between circuit switching and other forms of networking does not arise from the existence of separate physical paths. Instead, three general properties define a circuit switched paradigm:

- Point-to-point communication
- Separate steps for circuit creation, use, and termination
- Performance equivalent to an isolated physical path

The first property means that a circuit is formed between exactly two endpoints, and the secon property distinguishes circuits that are switched (i.e., established when needed) from circuits that a permanent (i.e., always remain in place ready for use).Switched circuits use a three-step proce analogous to placing a phone call. In the first step, a circuit is established. In the second, the tw parties use the circuit to communicate, and in the third, the two parties terminate use. The thir property provides a crucial distinction between circuit-switched networks and other types. Circu switching means that the communication between two parties is not affected in any way b communication among other parties, even if all communication is multiplexed over a commo medium. In particular, circuit switching must provide the illusion of an isolated path for each pair communicating entities. Thus, techniques such as frequency division multiplexing or synchronou time division multiplexing must be used to multiplex circuits over a shared medium.

Advantages of Circuit Switching

- It is suitable for long continuous transmission, since a continuous transmission route established, that remains throughout the conversation.
- The dedicated path ensures a steady data rate of communication.
- No intermediate delays are found once the circuit is established. So, they are suitable for rea time communication of both voice and data transmission.

Disadvantages of Circuit Switching

- Circuit switching establishes a dedicated connection between the end parties. This dedicated connection cannot be used for transmitting any other data, even if the data load is very low.
- Bandwidth requirement is high even in cases of low data volume.
- There is underutilization of system resources. Once resources are allocated to a particular connection, they cannot be used for other connections.
- Time required to establish connection may be high.

2. Packet Switching

The main alternative to circuit switching, packet switching, forms the basis for the Internet. A packet switching system uses statistical multiplexing in which communication from multiple sources competes for the use of shared media. Figure 2.40 illustrates the concept.

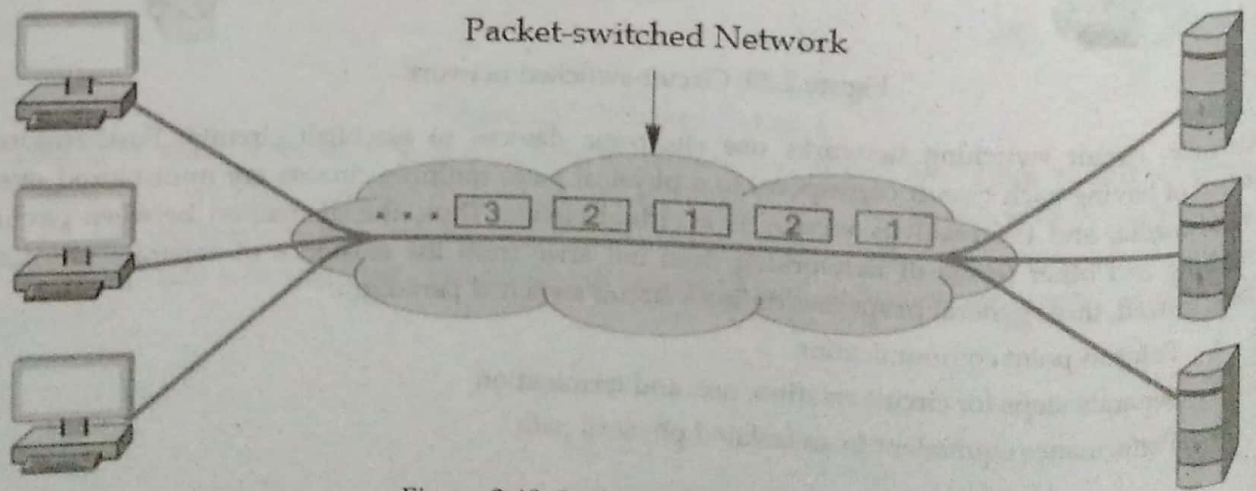


Figure 2.40: Packet-switched network

The chief difference between packet switching and other forms of statistical multiplexing arises because a packet switching system requires a sender to divide each message into blocks of data that are known as packets. The size of a packet varies; each packet switching technology defines a maximum packet size.

Three general properties define a packet switched paradigm:

- Arbitrary, asynchronous communication
- No set-up required before communication begins
- Performance variés due to statistical multiplexing among packets

The first property means that packet switching can allow a sender to communicate with one recipient or multiple recipients, and a given recipient can receive messages from one sender or multiple senders. Furthermore, communication can occur at anytime, and a sender can delay arbitrarily long between successive communications. The second property means that, unlike a circuit switched system, a packet switched system remains ready to deliver a packet to any destination at any time. Thus, a sender does not need to perform initialization before communicating, and does not need to notify the underlying system when communication terminates.

The third property means that multiplexing occurs among packets rather than among bits or bytes. That is, once a sender gains access to the underlying channel, the sender transmits an entire packet, and then allows other senders to transmit a packet. When no other senders are ready to transmit a packet, a single sender can transmit repeatedly. However, if N senders each have a packet to send, a given sender will transmit approximately 1/N of all packets.

Two types of Packet Switching

- Datagram Packet Switching
- Virtual Circuit Packet Switching

In the **datagram** approach, each packet is treated independently, with no reference to packets that have gone before. This approach is illustrated in Figure 2.40, which shows a time sequence of snapshots of the progress of three packets through the network. Each node chooses the next node on a packet's path, taking into account information received from neighboring nodes on traffic, line failures, and so on. So the packets, each with the same destination address, do not all follow the same route, and they may arrive out of sequence at the exit point. In this example, the exit node restores the packets to their original order before delivering them to the destination. In some datagram networks, it is up to the destination rather than the exit node to do the reordering. Also, it is possible for a packet to be destroyed in the network. For example, if a packet-switching node crashes momentarily, all of its queued packets may be lost. Again, it is up to either the exit node or the destination to detect the loss of a packet and decide how to recover it. In this technique, each packet, treated independently, is referred to as a datagram.

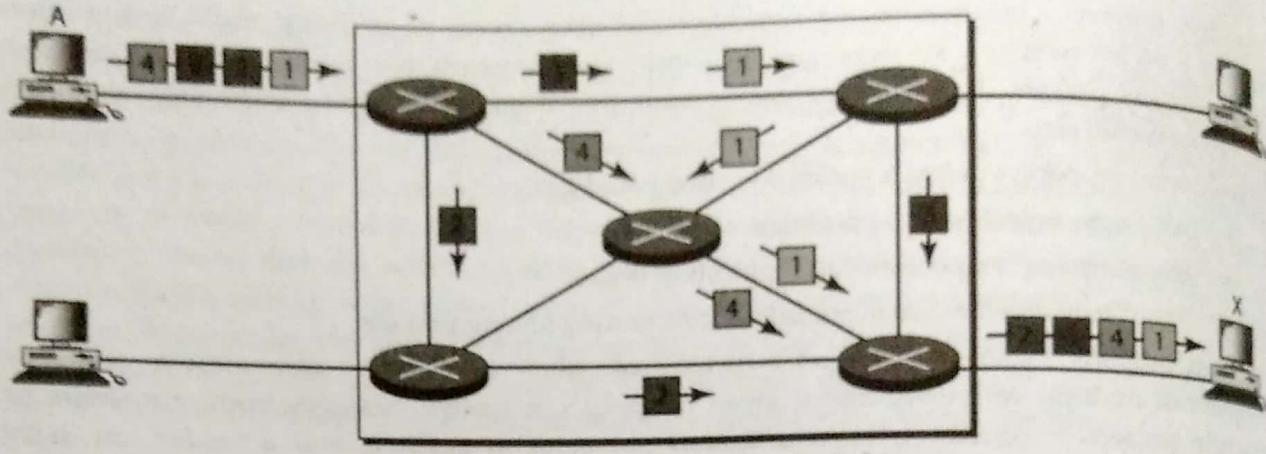


Figure 2.41: Datagram Packet Switching

In the **virtual circuit** approach, a preplanned route is established before any packets are sent. Once the route is established, all the packets between a pair of communicating parties follow this same route through the network. This is illustrated in Figure 2.42 because the route is fixed for the duration of the logical connection, it is somewhat similar to a circuit in a circuit-switching network and is referred to as a virtual circuit. Each packet contains a virtual circuit identifier as well as data. Each node on the pre-established route knows where to direct such packets; no routing decisions are required. At any time, each station can have more than one virtual circuit to any other station and can have virtual circuits to more than one station.

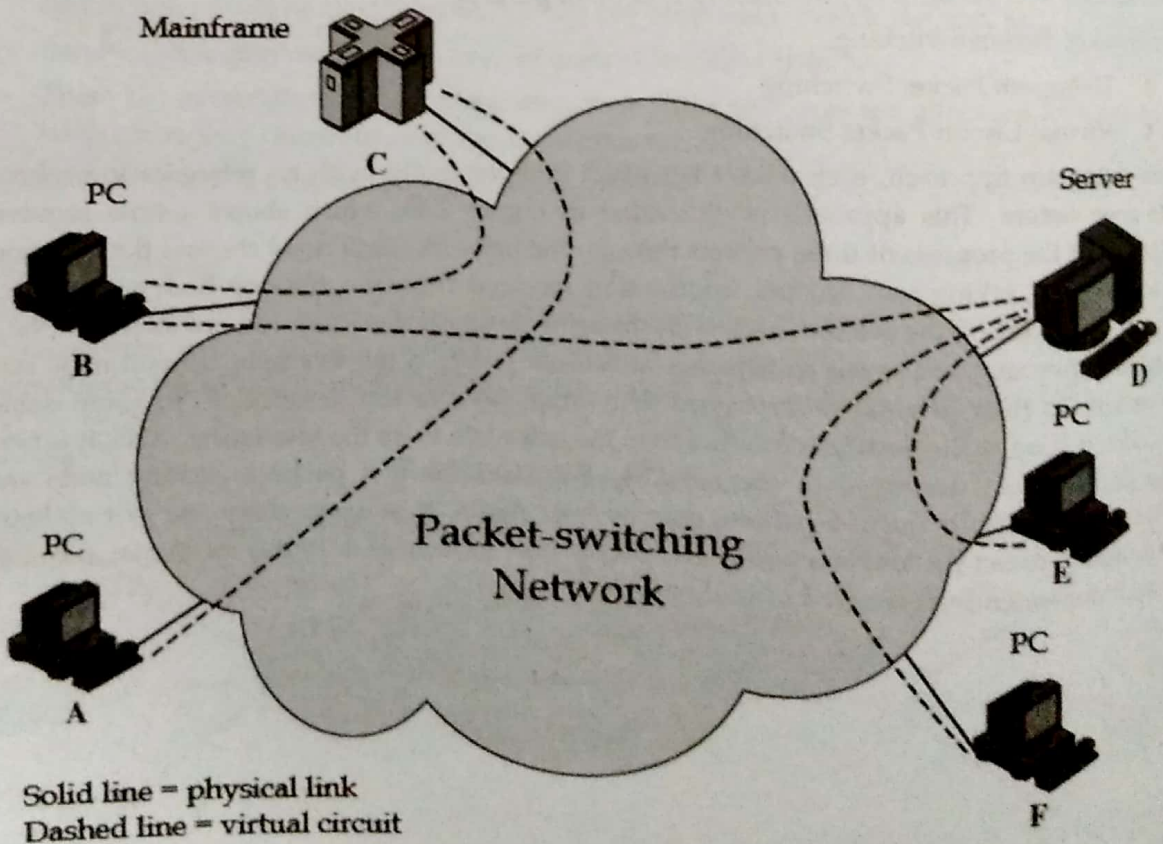


Figure 2.42: Virtual Circuit Switching

So the main characteristic of the virtual circuit technique is that a route between stations is set up prior to data transfer. Note that this does not mean that this is a dedicated path, as in circuit switching. A transmitted packet is buffered at each node, and queued for output over a line, while other packets on other virtual circuits may share the use of the line. The difference from the datagram approach is that, with virtual circuits, the node need not make a routing decision for each packet. It is made only once for all packets using that virtual circuit.

Advantages of Packet Switching:

- Efficient use of Network.
- Easily get around broken bits or packets.
- Circuit Switching charges user on the distance and duration of connection but Packet Switching charges users only on the basis of duration of connectivity.
- High Data Transmission in a Packet Switching is very easy.
- All the packets not follow same route in Packet Switching but in Circuit Switching all the packets follow same rout.
- Packet Switching use digital network and enables digital data to be directly transmitted toward destination.

Disadvantages of Packet Switching:

- In Packet Switching Packets arriving in wrong order.
- Takes Transmission delay.
- Requires Large amount RAM (Random Access Memory) to handle large amount of data communication in packets.
- Switching Nods required more procession power to reconstruct packets
- Packets may be lost on their route, so sequence numbers are required to identify missing packets.

3. Message Switching:

Message switching was a technique developed as an alternate to circuit switching, before packet switching was introduced. In message switching, end users communicate by sending and receiving messages that included the entire data to be shared. Messages are the smallest individual unit. Also, the sender and receiver are not directly connected. There are a number of intermediate nodes transfer data and ensure that the message reaches its destination. Message switched data networks are hence called hop-by-hop systems. They provide two distinct and important characteristics:

1. **Store and forward:** The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise it'll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.
2. **Message delivery**: This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination.

Message switching network consists of transmission links (channels), store-and-forward switch nodes and end stations as shown in the following picture:

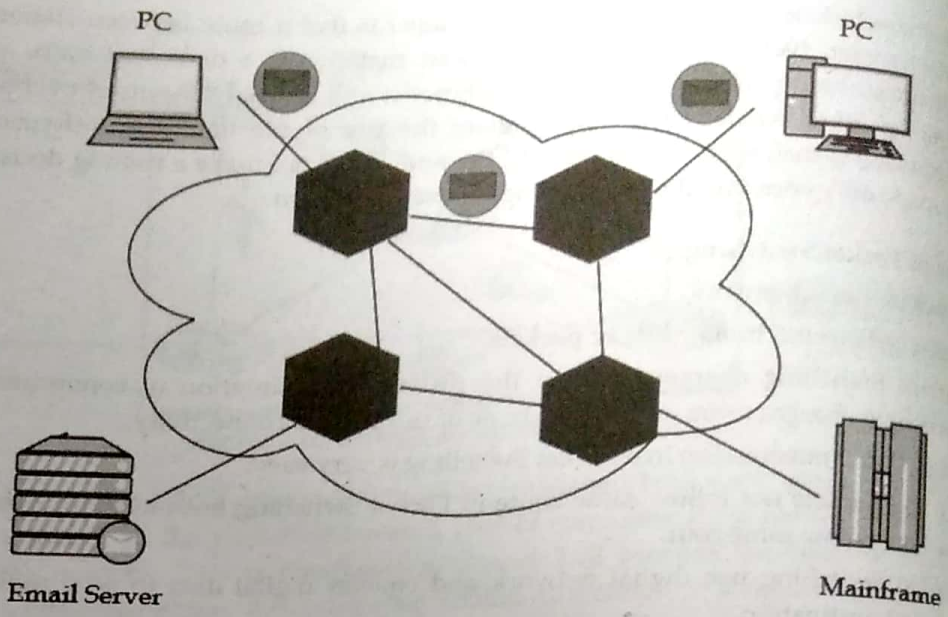


Figure 2.43: Message Switching Network

Characteristics of Message Switching

Message switching is advantageous as it enables efficient usage of network resources. Also, because of the store-and-forward capability of intermediary nodes, traffic can be efficiently regulated and controlled. Message delivery as one unit, rather than in pieces, is another benefit.

However, message switching has certain disadvantages as well. Since messages are stored indefinitely at each intermediate node, switches require large storage capacity. Also, these are pretty slow. This is because at each node, first there us wait till the entire message is received, then it must be stored and transmitted after processing the next node and links to it depending on availability and channel traffic. Hence, message switching cannot be used for real time or interactive applications like video conference.

Applications:

The store-and-forward method was implemented in telegraph message switching centers. Today although many major networks and systems are packet-switched or circuit switched networks, their delivery processes can be based on message switching. For example, in most electronic mail systems the delivery process is based on message switching, while the network is in fact either circuit-switched or packet-switched.

Advantages of Message Switching

- Sharing of communication channels ensures better bandwidth usage.
- It reduces network congestion due to store and forward method. Any switching node can store the messages till the network is available.
- Broadcasting messages requires much less bandwidth than circuit switching.
- Messages of unlimited sizes can be sent.
- It does not have to deal with out of order packets or lost packets as in packet switching.

Disadvantages of Message Switching

- In order to store many messages of unlimited sizes, each intermediate switching node requires large storage capacity.
- Store and forward method introduces delay at each switching node. This renders it unsuitable for real time applications.

ISDN: Interface and Standards

Integrated Services Digital Network (ISDN) is a telephone system network. It is a wide area network becoming widely available. Prior to the ISDN, the phone system was viewed as a way to transport voice, with some special services available for data. The key feature of the ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system.

ISDN is a circuit-switched telephone network system, that also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better voice quality than an analog phone. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 Kbit/s.

Another major market application is Internet access, where ISDN typically provides a maximum of 128 Kbit/s in both upstream and downstream directions (which can be considered to be broadband speed, since it exceeds the narrowband speeds of standard analog 56k telephone lines). ISDN B-channels can be bonded to achieve a greater data rate; typically 3 or 4 BRIs (6 to 8 64 Kbit/s channels) are bonded.

ISDN should not be mistaken for its use with a specific protocol, such as Q.931 whereby ISDN is employed as the network, data-link and physical layers in the context of the OSI model. In a broad sense ISDN can be considered a suite of digital services existing on layers 1, 2 and 3 of the OSI model. ISDN is designed to provide access to voice and data services simultaneously.

However, common use has reduced ISDN to be limited to Q.931 and related protocols, which are a set of protocols for establishing and breaking circuit switched connections, and for advanced call features for the user. They were introduced in 1986. In a videoconference, ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems.

The first generation of ISDN is called as a narrowband ISDN and it is based on the use of 64 kbps channel as the basic unit of switching and has a circuit switching orientation. The main device in the narrowband ISDN is the frame relay. The second generation of ISDN is referred to as the broadband ISDN (B-ISDN).

It supports very high data rates (typically hundreds of Mbps). It has a packet switching orientation. The main important technical contribution of B-ISDN is the asynchronous transfer mode (ATM), which is also called as cell relay.

Features of ISDN

1. Offers point-to-point delivery
2. Network access and network interconnection for multimedia.
3. Different data rates from 64 Kbps up to 2 Mbps are commercially available which can meet many needs for transporting multimedia and is four to many times more than today's analog modems

4. Call set-up times are under one second. ISD N can dramatically speed up transfer of information over the Internet or over a remote LAN connection, especially rich media like graphics, audio video or applications that normally run at LAN speeds.
5. ISDN will be the feeder network for broadband ISDN based on ATM standards.

Advantages of ISDN

1. **Quality**: ISDN connections are very low error rate digital pipes.
2. **Flexibility**: ISDN can be thought of as a configurable leased line. Connections can be established at any time between any two locations where ISDN is available. It offers a very fast (almost transparent) call set-up, so its dialup nature is transparent to most users.
3. **Economy**: ISDN is charged for rent like a telephone call. Usage costs are identical to the telephone service. In general, ISDN is extremely cost-effective for intermittent LAN to LAN connectivity.
4. **Availability:** ISDN is now becoming very widely available because the initiatives taken by the government of various countries.

ISDN User Interfaces

ISDN provides two basic types of interfaces to users.

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

Basic Rate Interface (BRI)

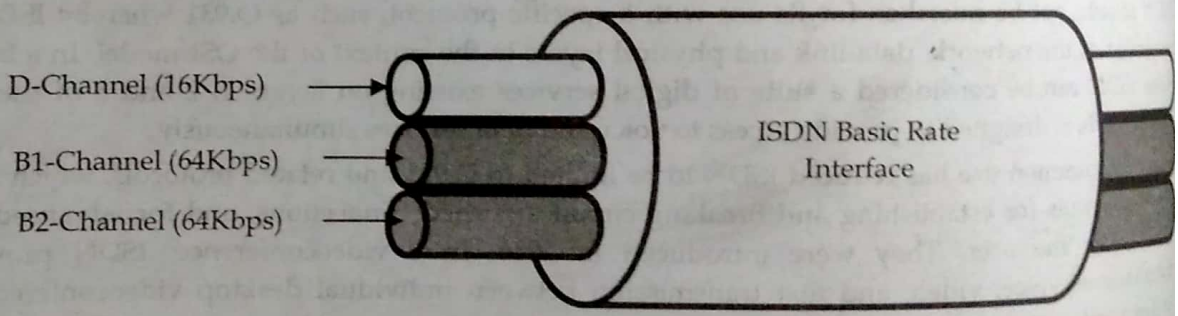


Figure 2.44: ISDN Basic Rate Interface (BRI)

Basic Rate Interface specifies a digital pipe, consisting of two 64 Kbps B channels and one 16 Kbps D channel for a total of 144 Kbps (2B+D). Figure 2.44 shows the structure of Basic Rate Interface. In addition, the BRI service itself requires 48 Kbps operating overhead. BRI therefore requires a digital pipe of 192 Kbps. Conceptually, the BRI service is like a large pipe that contains three smaller pipes, two for the B channels and one for the D channel. The remainder of the space inside the large pipe carries the overhead bits required for its operation. All 192 Kbps can be used to carry a single signal.

The BRI is designed to cater to the needs of home users and small business establishments. In most cases, there is no need to replace the existing local-loop cable. The existing twisted pair local loop can be used to carry digital transmission.

Primary Rate Interface (PRI)

Primary Rate Interface is intended for users with higher data rate requirements, such as large business establishments, offices with a digital PBX or a LAN. Because of differences in the digital

transmission hierarchies used in different countries, it was not possible to reach an agreement on a single data rate.

The United States, Canada and Japan make use of a transmission structure based on 1.544 Mbps; this corresponds to the T-1 transmission facility of AT& T. In Europe, 2.048 Mbps is the standard rate. Both of these data rates are provided as a Primary Rate Interface.

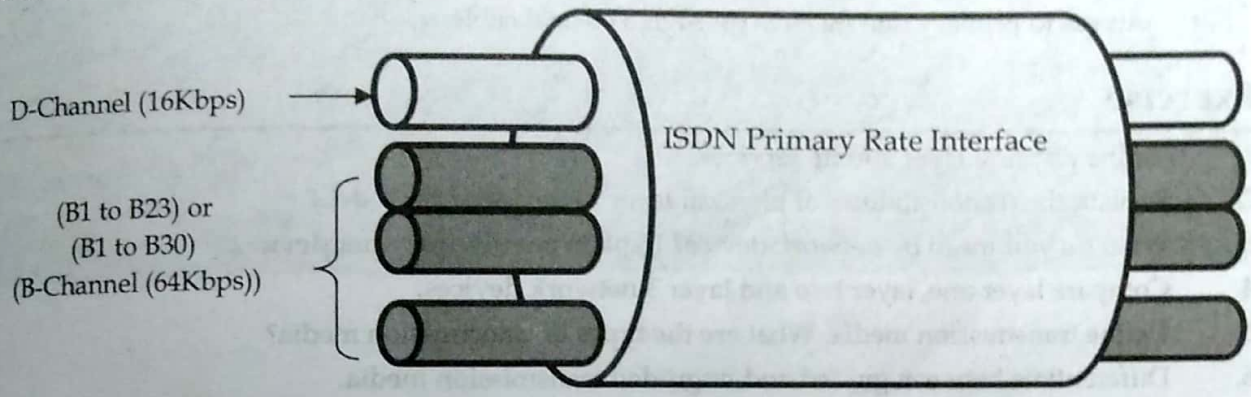


Figure 2.45: ISDN Primary Rate Interface (PRI)

Typically, the channel structure for the 1.544 Mbps rate will be 23 B channels and one 64 Kbps D channel and, for the 2.048 Mbps rate, 30 B channels and one 64 Kbps D channel.

It is also possible for a customer with few requirements to employ fewer B channels, in which case, the channel structure is nB + D, where n ranges from 1 to 23 or from 1 to 30 for the two primary services. Also, a customer with high data-rate demands may be provided with more than one primary physical interface. In this case, a single D channel on one of the interfaces may suffice for all signaling needs, and the other interfaces may consist solely of B channels (24B or 31B).

PRI with H-channels The Primary Rate Interface may also be used to support H channels. Some of these structures include a 64 Kbps D channel for control signaling. When no D channel is present, it is assumed that a D channel on another primary interface at the same subscriber location will provide any required signaling. The following structures are recognized:

Primary Rate Interface (PRI) H0 channel structures: This interface supports multiple 384 Kbps H0channels. The structures are 3H0+D and 4 H0 for the 1.544 Mbps interface and 5H0 +D for the 2.048 Mbps interface.

Primary Rate Interface (PRI) H1 and H12 channel structures: The H1 channel structure consists of one 1,536 Kbps H11 channel. The H12 channel structure consists of one 1,920 Kbps H12 channel and one D channel.

Primary Rate Interface (PRI) structures for mixtures of B and H0channels: This interface consists of zero or one D channel and any possible combination of Band H0 channels up to the capacity of the physical interface (e.g., 3HO+ 5B + D and 3HO+ 6B for the 1.544 MBps interface).

ISDN Standards

Products for ISDN technology from different vendors even with similar features and options may create some compatibility issues. CCITT after good deliberations over the years published the first significant ISDN standards in a number of red binders in 1984 and they were simply known as the Red Book standards. The group subsequently met four years later which culminated in the publication of the 1988 Blue Book standards. These international publications were the foundation for the evolving ISDN national standards. The CCITT eventually was reformed into the group,

which is now called the ITU- T. The standards used to define ISDN make use of the OSI referenc model with the first three layers of this OSI reference model.

There are two standard ISDN connectors:

- For accessing basic rate ISDN, a RJ-45 type plug and socket (similar to a telephone plug) is used using unshielded twisted pair cable.
- Access to primary rate ISDN is through a coaxial cable.

Exercise

1. Define physical layer and its services.
2. Explain the responsibilities of physical layer in the internet model.
3. What do you mean by network device? Explain any five network devices.
4. Compare layer one, layer two and layer 3 network devices.
5. Define transmission media. What are the types of transmission media?
6. Differentiate between guided and unguided transmission media.
7. Discuss each guided and unguided transmission media in detail.
8. What is the significance of the twisting in twisted-pair cable?
9. What is the purpose of cladding in an optical fiber?
10. Name the advantages of optical fiber over twisted-pair and coaxial cable
11. Network for heavy video data transmission is needed to be designed, as network administrator of the company which network will you choose broadband or baseband and why?
12. Explain the modes of fiber optic cable.
13. How does sky propagation differ from line-of-sight propagation?
14. What is the difference between omnidirectional waves and unidirectional waves?
15. Describe the need for switching.
16. Compare a circuit-switched network and a packet-switched network.
17. How virtual circuit packet switching is differ from datagram packet switching.
18. Explain ISDN along with its features.
19. Explain ISDN user interface and ISDN standards.
20. Write short notes on:
    a. Access point
    b. Repeater
    c. Amplifier
    d. Jitter
    e. Total Internal Reflection
    f. Bandwidth
    g. Throughput
    h. Goodput
    i. Attenuation
    j. Distortion
    k. Noise

❑❑❑

Chapter 3
DATA LINK LAYER

Introduction

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate. Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

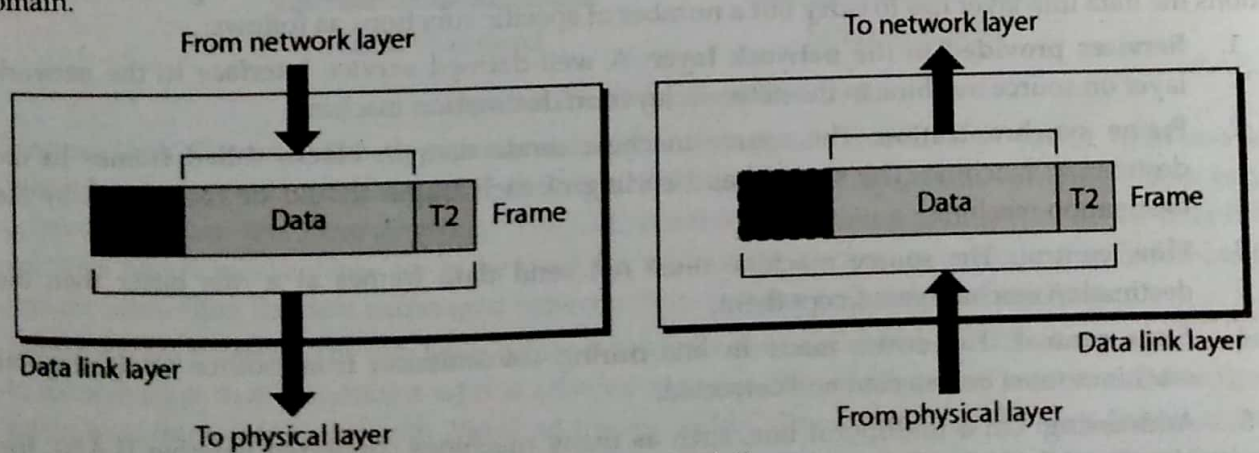


Figure 3.1: Data Link Layer

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

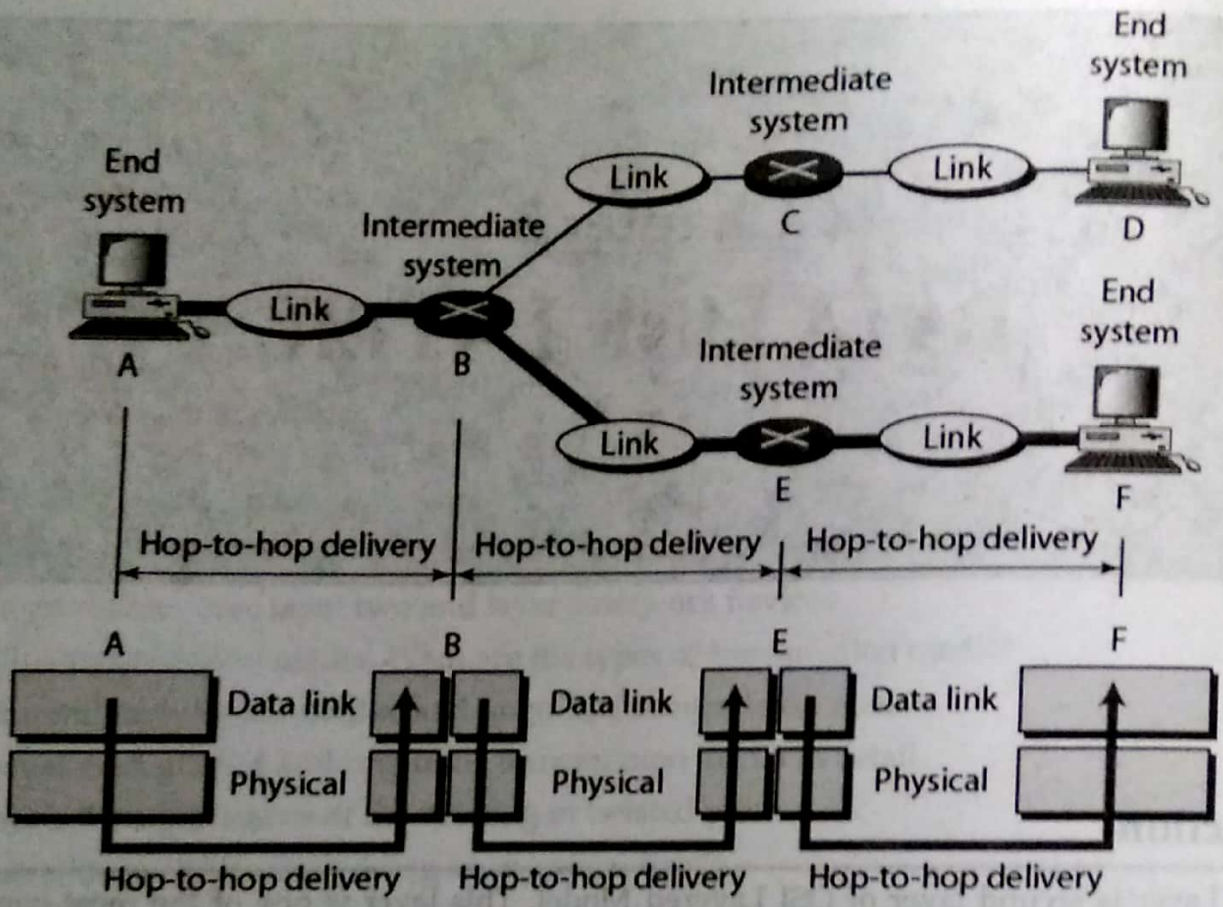


Figure 3.2: Hop-to-hop Delivery

Function of Data Link Layer (DLL)

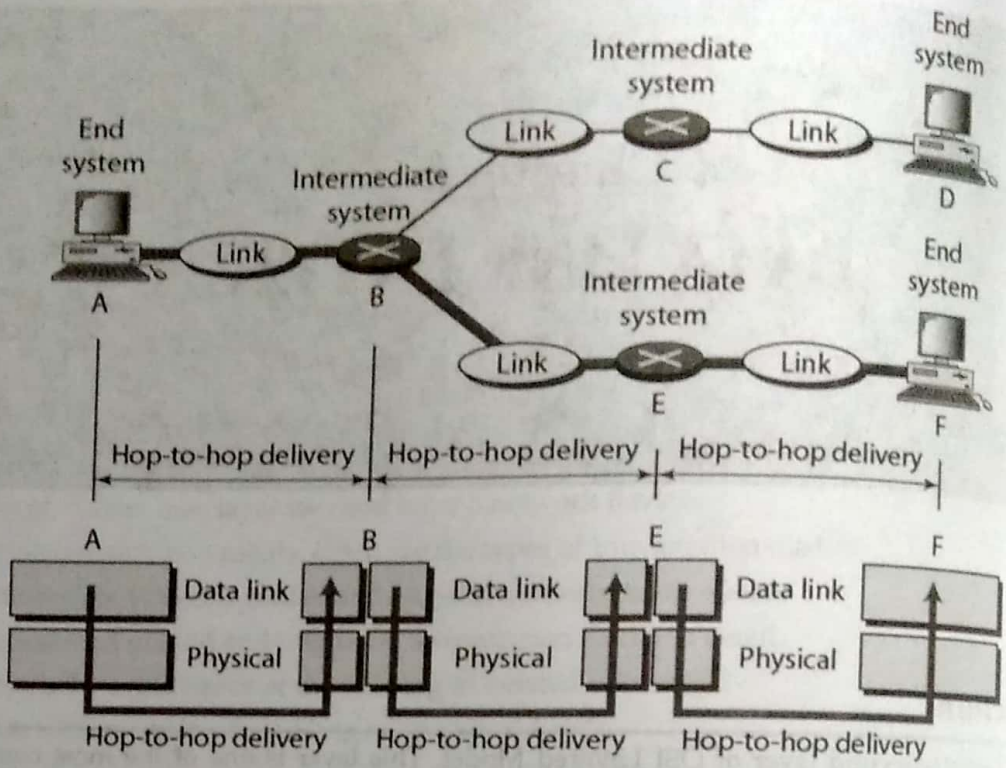


Figure 3.2: Hop-to-hop Delivery

Function of Data Link Layer (DLL)

For effective data communication between two directly connected transmitting and receiving stations the data link layer has to carry out a number of specific functions as follows:

1. **Services provided to the network layer**: A well-defined service interface to the network layer on source machine to the network layer on destination machine.
2. **Frame synchronization:** The source machine sends data in blocks called frames to the destination machine. The starting and ending of each frame should be recognized by the destination machine.
3. **Flow control:** The source machine must not send data frames at a rate faster than the destination machine can accept them.
4. **Error control:** The errors made in bits during transmission from source to destination machines must be detected and corrected.
5. **Addressing:** On a multipoint line, such as many machines connected together (LAN), the identity of the individual machines must be specified while transmitting the data frames.
6. **Control and data on same link:** The data and control information is combined in a frame and transmitted from the source to destination machine. The destination machine must be able to recognize control information from the data being transmitted.
7. **Link Management:** The initiation, maintenance and termination of the link between the source and destination are required for effective exchange of data. It requires co-ordination and co-operation among stations. Protocols or procedures are required for the link management.

8. **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.
9. **Congestion Control:** Although a link may be congested with frames, which may result in frame loss, most data-link-layer protocols do not directly use a congestion control to alleviate congestion, although some wide-area networks do. In general, congestion control is considered an issue in the network layer or the transport layer because of its end-to-end nature. We will discuss congestion control in the network layer and the transport layer in later chapters.

Overview of Logical Link Control and Media Access Control

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

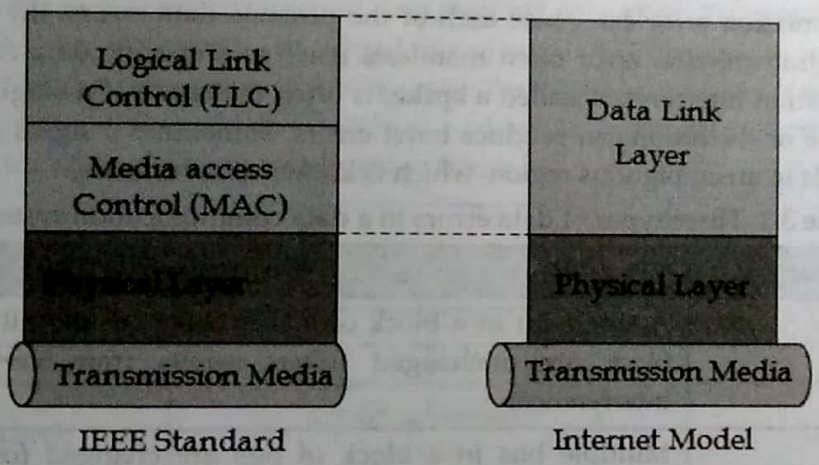


Figure 3.3: Sub Layer of Data link

Logical Link Control: The uppermost sub layer is Logical Link Control (LLC). This sub layer multiplexes protocols running atop the data link layer, and optionally provides flow control, acknowledgment, and error recovery. The LLC provides addressing and control of the data link. It specifies which mechanisms are to be used for addressing stations over the transmission medium and for controlling the data exchanged between the originator and recipient machines.

Media Access Control: The sub layer below it is Media Access Control (MAC). Sometimes this refers to the sub layer that determines who is allowed to access the media at any one time. Other times it refers to a frame structure with MAC addresses inside. There are generally two forms of media access control: distributed and centralized. Both of these may be compared to communication between people: The Media Access Control sub layer also determines where one frame of data ends and the next one starts. There are four means of doing that: a time based, character counting, byte stuffing and bit stuffing.

Error Detection and Correction Techniques

Networks must be able to transfer data from one device to another with acceptable accuracy. For most applications, a system must guarantee that the data received are identical to the data transmitted. Any time data are transmitted from one node to the next, they can become corrupted in

passage. Many factors can alter one or more bits of a message. Some applications require a mechanism for detecting and correcting errors. Some applications can tolerate a small level of error. For example, random error sin audio or video transmissions may be tolerable, but when we transmit text, we expect a very high level of accuracy. At the data-link layer, if a frame is corrupted between the two nodes, it needs to be corrected before it continues its journey to other nodes. However, most link-layer protocols simply discard the frame and let the upper-layer protocols handle the retransmission of the frame. Some multimedia applications, however, try to correct the corrupted frame.

Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of **interference, noise, distortion or attenuation.** These imparities can change the shape of the signal. Instead of examining physics and the exact cause of transmission errors, data communication focuses on the effect of errors on data. Table 3.1 lists the three principal ways transmission errors affect data.

Although any transmission error can cause each of the possible data errors, the table3.1points out that an underlying transmission error often manifests itself as a specific data error. For example, extremely short duration interference, called a **spike**, is often the cause of a single bit error. Longer duration interference or distortion can produce burst errors. Sometimes a signal is neither clearly 1 nor clearly 0, but falls in an ambiguous region, which is known as an **erasure**.

Table 3.1: Three types of data errors in a data communication system.

Types of Error	Description
Single Bit Error	A single bit in a block of bits is changed and all other bits in the block are unchanged (often results from very short-duration interference)
Burst Error	Multiple bits in a block of bits are changed (often results from longer-duration interference)
Erasure (Ambiguity)	The signal that arrives at a receiver is ambiguous (does not clearly correspond to either a logical 1or a logical 0 (can result from distortion or interference)

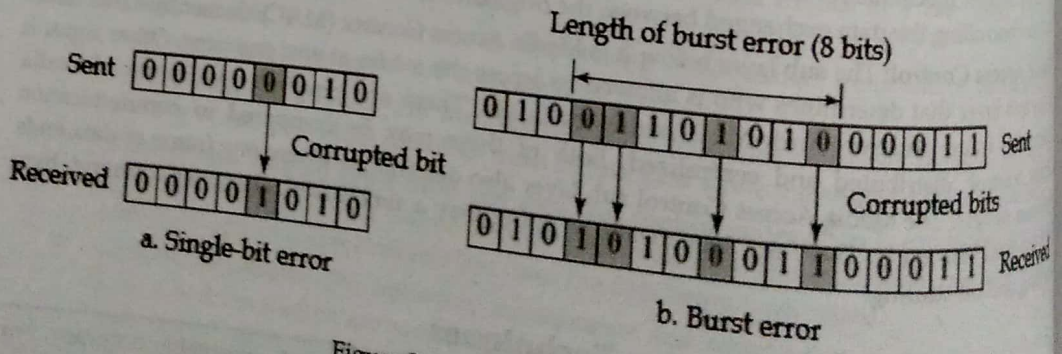


Figure 3.4: Single-bit and burst error

Redundancy

The central concept in detecting or correcting errors is **redundancy**. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits. The concept of including extra information in the transmission for error detection is a good one. But instead of repeating the entire data stream, a shorter group of bits may be appended to the end of each unit. This technique is called redundancy because the extra bits are redundant to the information: they are discarded as soon as the accuracy of the transmission has been determined.

Drawbacks of Redundancy

- Sends n-redundant bits for n-bit message.
- Many errors are undetected if both the copies are corrupted.

Error Detecting Codes

It is implemented either at Data link layer or Transport Layer of OSI Model. Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message. Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors. Some popular techniques for error detection are shown in figure 3.5.

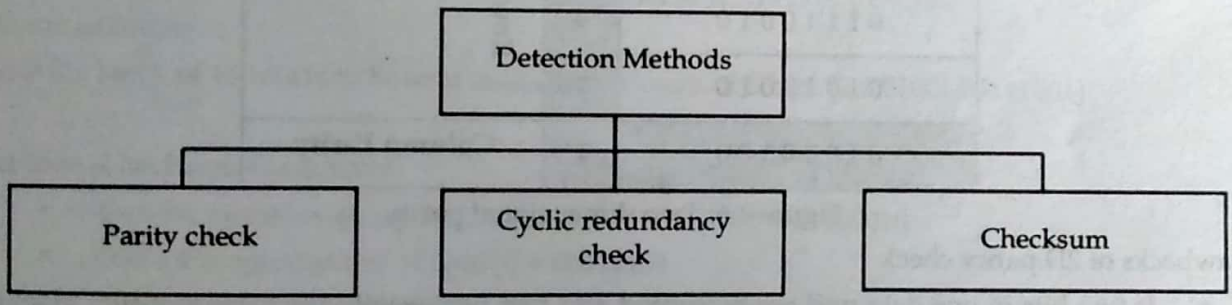


Figure 3.5: Error Detection Techniques

1. Parity Check

A parity bit is an error detection mechanism.

Single Parity Check

Single parity checking (SPC) is a basic form of channel coding in which a sender adds an extra bit to each byte to make an even (or odd) number of 1 bits and a receiver verifies that the incoming data has the correct number of 1 bits.

Single parity checking is a weak form of channel coding that can detect errors, but cannot correct them. Furthermore, parity mechanisms can only handle errors where an odd number of bits are changed. If one of the nine bits (including the parity bit) is changed during transmission, the receiver will declare that the incoming byte is invalid. However, if a burst error occurs in which two, four, six, or eight bits change value, the receiver will incorrectly classify the incoming byte as valid.

Table 3.3: Single parity bit when using even parity or odd parity.

Original Data	Even Parity	Odd Parity
00000000	0	1
10001001	1	0
01010101	0	1
11010110	1	0

Two-Dimensional Parity Check

Performance can be improved by using Two-Dimensional Parity Check which organizes the data in the form of a table. Parity check bits are computed for each row, which is equivalent to the single-parity check. In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block. At the receiving end, the parity bits are compared with the parity bits computed from the received data. Example is shown in figure 3.6.

Original data: 11001110 10111010 01110010 01010010

11001110	1	Row Parity
10111010	1	
01110010	0	
01010010	1	
01010100	1	**Column Parity**

Figure 3.6: Two dimensional parity

Drawbacks of 2D parity check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

2. Checksum

A checksum is an error detection technique based on the concept of redundancy. It is divided into two parts: **checksum generator** and **checksum checker**.

Checksum Generator

A Checksum is generated at the sending side which is shown in figure 3.7. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

Checksum Checker

A Checksum is verified at the receiving side which is shown in figure 3.7. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

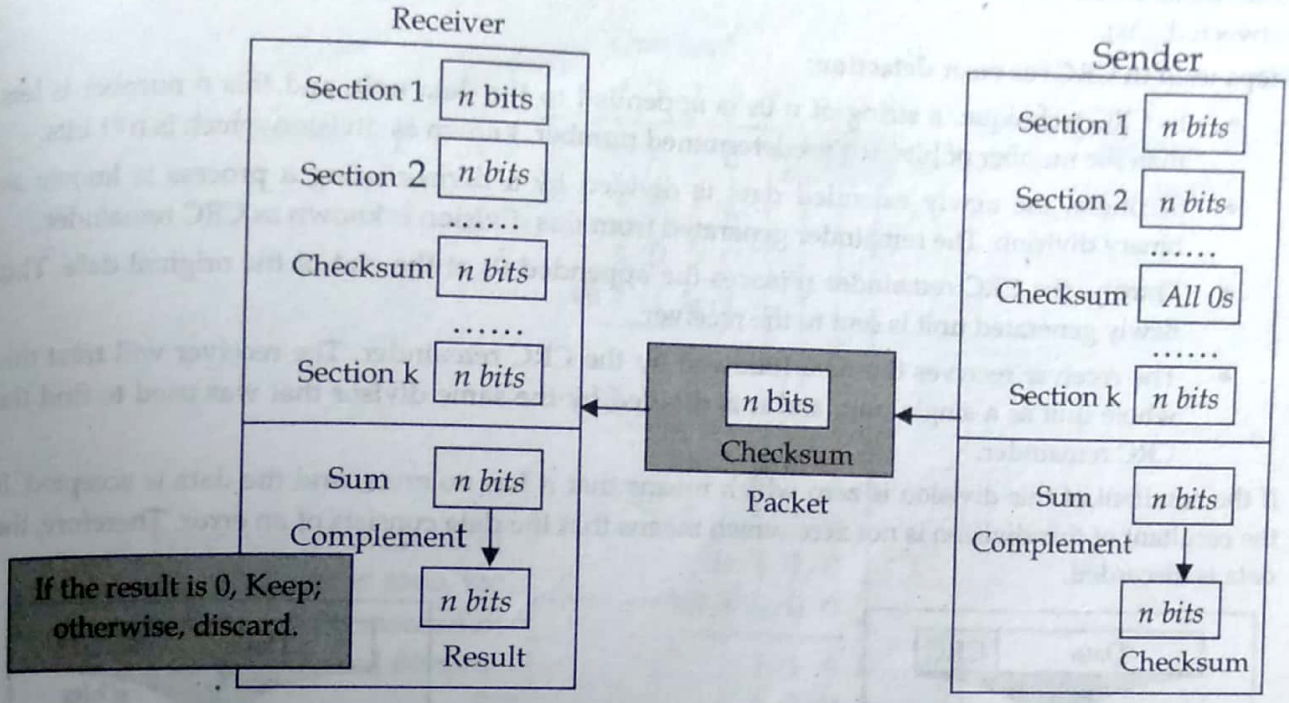


Figure 3.7: Checksum Generator and Checker Concept

Checksum example:

Suppose the block of 16 bits is to be sent using a checksum of 8 bits. [10101001 00111001]

Sender Side (Checksum Generator):

- Two bit numbers are added: 10101001 + 00111001 = 11100010
- One's Complement of 11100010 = **00011101**
- The Pattern sent is: 10101001 00111001 = **00011101**

Receiver Side (Checksum Checker):

- Two bit numbers are added: 10101001 + 00111001 + **00011101** = 11111111
- Compute one's complement of 11111111 = 00000000
- No error in transmission.

3. Cyclic Redundancy Check (CRC)

CRC is a redundancy error technique used to determine the error. Unlike the parity check which is based on addition. CRC is based on binary division. In CRC, instead of adding bits to achieve a desired parity, a sequence of redundant bits, called the CRC or the CRC remainder, is appended to the end of a data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At its 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 intact and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected. Specification of a CRC code requires definition of a so-called generator polynomial. This polynomial becomes the divisor in a polynomial long division, which takes the message as the dividend and in which the quotient is discarded and the remainder becomes the result. The important caveat is that the polynomial coefficients are calculated according to the arithmetic of a

finite field, so the addition operation can always be performed bitwise-parallel (there is no carry between digits).

Steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.
- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted. If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

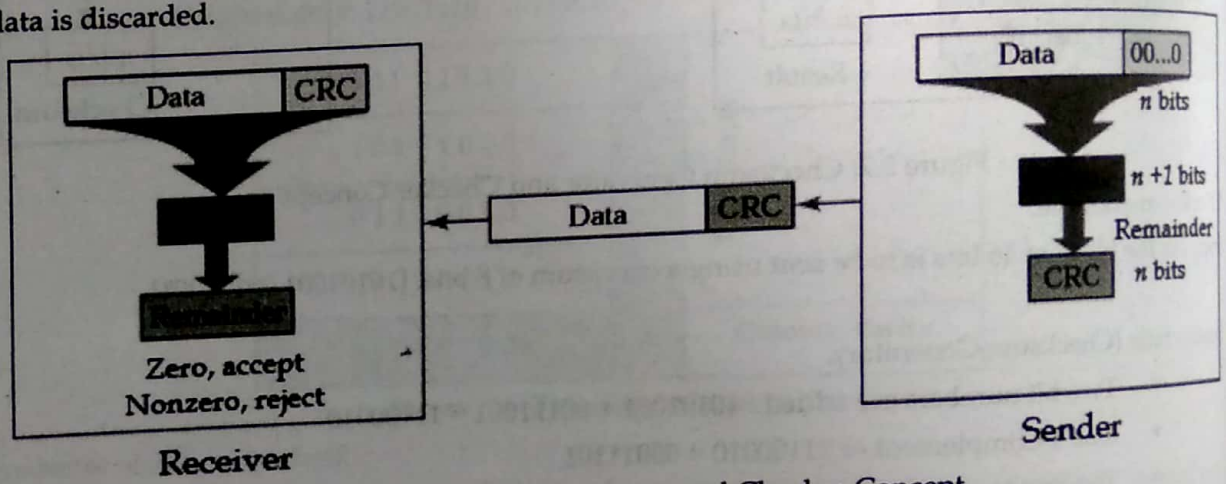


Figure 3.8: CRC Generator and Checker Concept

Let's understand this concept through an example:

Suppose the original data is 100100 and divisor is 1101.

CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 100100000, and the resultant string is divided by the divisor 1101.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 001.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 100100001 which is sent across the network.

CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 100100001 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1101.

Polynomials

CRC generator (the divisor) is most often represented not as a string of 1's and 0's but as an algebra polynomial. The polynomial format is useful for two reasons:

- It is short
- It can be used to prove the concept mathematically

Selection of a Polynomial

A polynomial should have the following properties:

- It should not be divisible by 'x'
- It should be divisible by 'x+1'

The first condition guarantees that all burst errors of a length equal to the degree of the polynomi are detected and second guarantees that all burst errors affecting an odd number of bits are detected

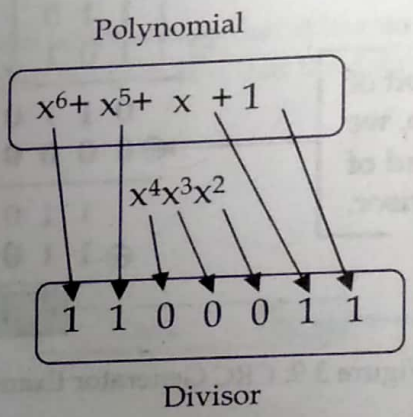


Figure 3.11: CRC polynomial

Table 3.4: Common CRC polynomials.

RCR	C(x)
CRC-8	x^8+x^2+x+1
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x + 1$
CRC-12	$x^{12} + x^{11} + x^3 + x^2 + 1$
CRC-16	$x^{16} + x^{15} + x^2 + 1$
CRC-CCITT	$x^{16} + x^{12} + x^5 + 1$
CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from sender to the receiver. Error correction is the additional ability to reconstruct the original, error- data.

There are two basic ways to design the channel code and protocol for an error correcting system:

- **Automatic Repeat-Request (ARQ):** The transmitter sends the data and also an error dete code, which the receiver uses to check for errors, and request retransmission of erroneous In many cases, the request is implicit; the receiver sends an acknowledgement (ACK

correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time. E.g. stop and wait ARQ, Go-back-N ARQ and Selective Repeat ARQ.

- **Forward Error Correction (FEC):** The transmitter encodes the data with an error-correcting code (ECC) and sends the coded message. The receiver never sends any messages back to the transmitter. The receiver decodes what it receives into the "most likely" data. The codes are designed so that it would take an "unreasonable" amount of noise to trick the receiver into misinterpreting the data. E.g. Hamming Code

A single additional bit can detect the error, but cannot correct it.For correcting the errors, one has to know the exact position of the error. For example, if we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Suppose r is the number of redundant bits and m is the total number of the data bits. The number of redundant bits r can be calculated by using the formula:

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

The value of r is calculated by using the above formula. For example, if the value of m is 4, then the possible smallest value that satisfies the above relation would be 3. Table 3.5 shows some possible m values and the corresponding r values.

Table 3.5: Possible m values and the corresponding r values

Number of Data Bits (m)	Number of Redundancy Bits (r)	Total Bits ($m + r$)
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Hamming Code

To determine the position of the bit which is in error, a technique developed by R. W Hamming is Hamming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Steps for Hamming code

- An information of 'm' bits are added to the redundant bits 'r' to form $m + r$.
- The location of each of the $(m + r)$ digits is assigned a decimal value.
- The 'r' bits are placed in the positions $2^0, 2^1, \ldots\ldots, 2^{k-1}$
- At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

Position of the redundant bits

For example, a seven-bit ASCII code requires four redundancy bits that can be added to the end of the data or intersperse with the original data bits. These redundancy bits are placed in positions 1, 2, 4 and 8. We refer these bits as r_1, r_2, r_3 and r_4. Since, m=7 and r = 4 then $m + r$ = 11

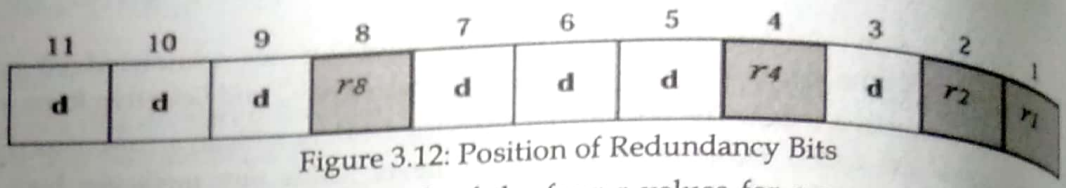


Figure 3.12: Position of Redundancy Bits

The combination used to calculate each of the four r values for a seven-bit data sequence is as follows

- The r_1 bit is calculated using all bits positions whose binary representation include a 1 in the right most position
- r_2 is calculated using all bit position with a 1 in the second position and so on

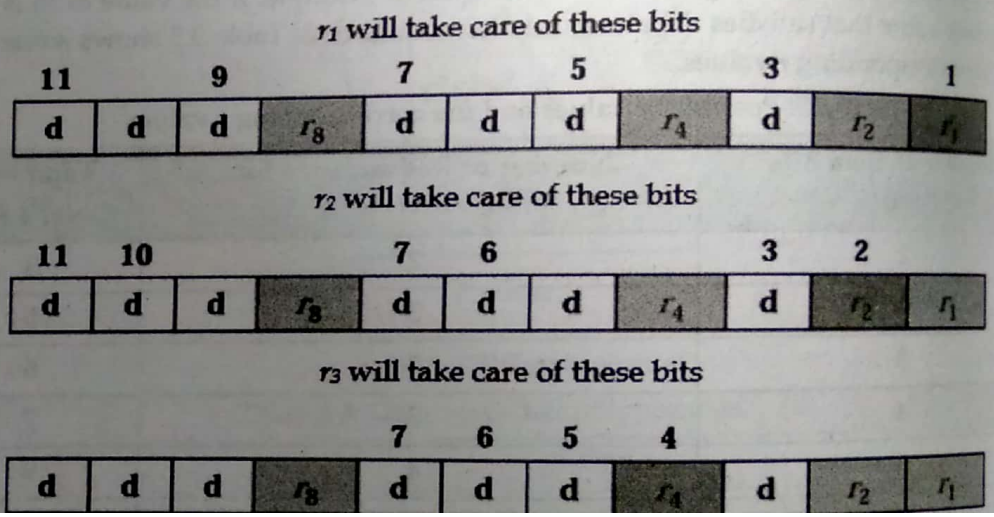
r_1: bits 1,3,5,7,9,11

r_2: bits 2, 3, 6, 7, 10, 11

r_3: bits 4, 5, 6, 7

r_4: bits 8, 9, 10, 11

Also figure 3.13 and 3.14 explain the calculation of the redundancy bits.



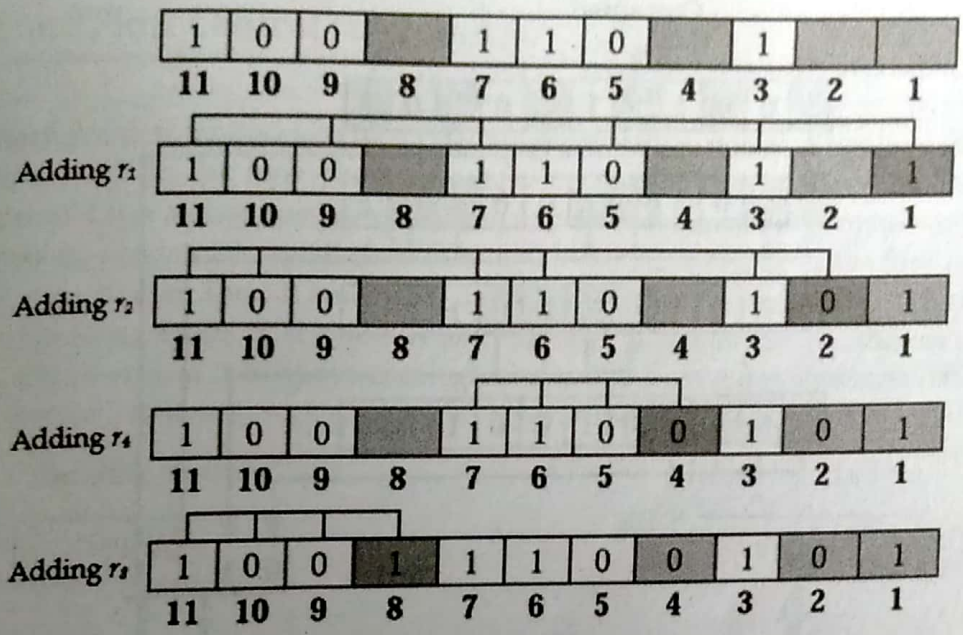


Figure 3.14: Example of Redundancy Bit Calculation

- **Determining r_1 bit:** We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7,9 and11. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r_1 is **odd, therefore, the value of the r_1 bit is 1.**
- **Determining r_2 bit:** We observe from the above figure that the bit positions that includes 1 in the first position are 2, 3, 6, 7, 10 and 11. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r_2 is **even, therefore, the value of the r_2 bit is 0.**
- **Determining r_4 bit:** We observe from the above figure that the bit positions that includes 1 in the first position are 4, 5, 6 and 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r_4 is **even, therefore, the value of the r_4 bit is 0.**
- **Determining r_8 bit:** We observe from the above figure that the bit positions that includes 1 in the first position are 8, 9, 10 and 11. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r_8 is **odd, therefore, the value of the r_8 bit is 1.**

Data transferred is **10011100101.**

Receiver side

Received data = **10010100101**

Total number of bits = $m + r = 11$;

Number of redundant bits r: $2^r \geq m + r + 1$

$2^r \geq 11 + 1$

$2^4 \geq 12$ ***(Satisfied)***

Therefore, the value of r is 4 that satisfies the above relation.

Total number of data bits 'm' = $11 - 4 = 7$

Suppose the 7th bit is changed from 1 to 0 at the receiving end, then parity bits are recalculated as shown in figure 3.15.

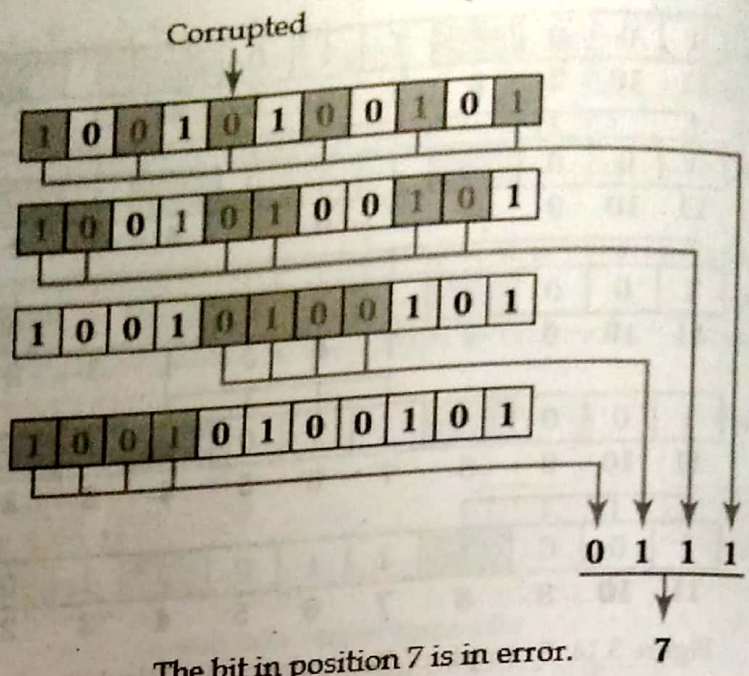


Figure 3.15: Error Detection

- **Determining r_1 bit:** We observe from the above figure that the bit positions that include the first position are 1, 3, 5, 7, 9 and 11. Now, we perform the even-parity check at the positions. The total number of 1 at these bit positions corresponding to r_1 is **odd, therefore value of the r_1 bit is 1.**
- **Determining r_2 bit:** We observe from the above figure that the bit positions that include the first position are 2, 3, 6, 7, 10 and 11. Now, we perform the even-parity check at the positions. The total number of 1 at these bit positions corresponding to r_2 is **odd, therefore value of the r_2 bit is 1.**
- **Determining r_4 bit:** We observe from the above figure that the bit positions that include the first position are 4, 5, 6 and 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r_4 is **odd, therefore, the value of the r_4 bit is 1.**
- **Determining r_8 bit:** We observe from the above figure that the bit positions that include the first position are 8, 9, 10 and 11. Now, we perform the even-parity check at these positions. The total number of 1 at these bit positions corresponding to r_8 is **even, therefore value of the r_8 bit is 0.**

The corresponding decimal value of redundant bits 0111 ($r_8r_4r_2r_1$) is 7. Therefore, error is detected 7th bit position. i.e.

Received data = **10010100101**

Error bit = 7th bit

Corrected data:**10011100101**

Original message bit (removing redundant bit) = 1001101

Framing and Flow Control Mechanism

Framing

In the physical layer, data transmission involves synchronized transmission of bits from the source to the destination. The data link layer packs these bits into frames. Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames makes flow control and error control more efficient.Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.

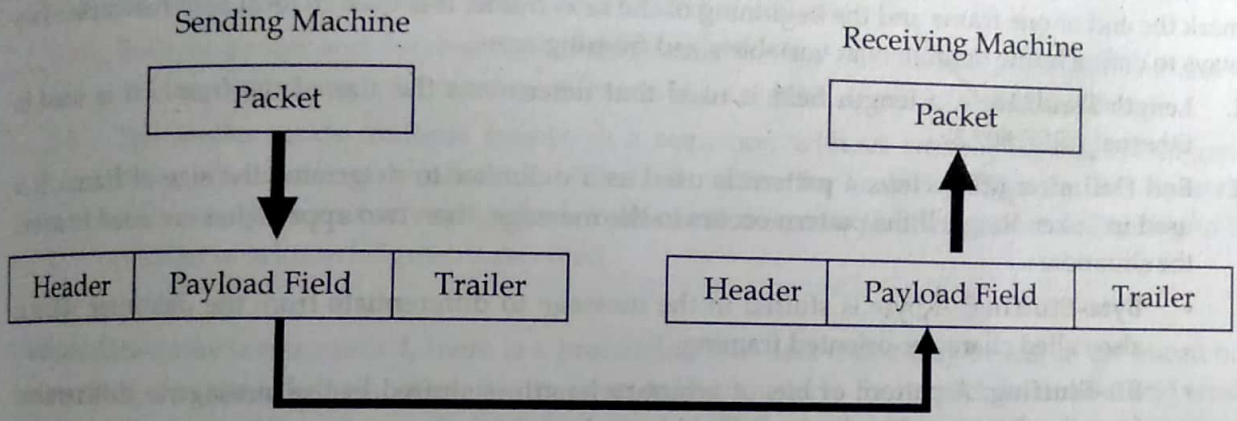


Figure 3.16: Frame

Parts of a Frame

A frame has the following parts:

- **Frame Header**: A frame header contains information used to process the frame. In particular, it contains the source and the destination addresses of the frame.
- **Payload field:** It contains the message to be delivered and is usually much larger than the frame header. In most network technologies, the message is **opaque** in the sense that the network only examines the frame header. Thus, the payload can contain an arbitrary sequence of bytes that are only meaningful to the sender and receiver.
- **Trailer:** It contains the error detection and error correction bits.
- **Flag:** It marks the beginning and end of the frame.

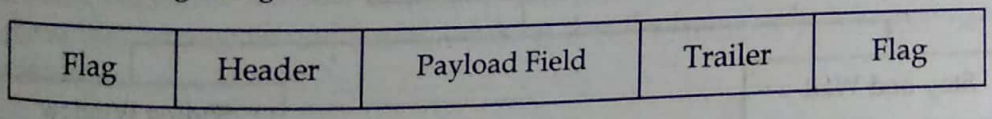


Figure 3.17: Parts of Frame

Problems in Framing:

- **Detecting start of the frame:** When a frame is transmitted, every station must be able to detect it. Station detect frames by looking out for special sequence of bits that marks the beginning of the frame i.e. SFD (Starting Frame Delimiter).
- **How do station detect a frame:** Every station listen to link for SFD pattern through a sequential circuit? If SFD is detected, sequential circuit alerts station. Station checks destination address to accept or reject frame.
- **Detecting end of frame:** When to stop reading the frame.

Types of Framing

Framing can be of two types, fixed sized framing and variable sized framing.

Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame. Example: ATM cells.

- **Drawback:** It suffers from internal fragmentation if data size is less than frame size
- **Solution:** Padding

Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame. It is used in local area networks. Two ways to define frame delimiters in variable sized framing are:

1. **Length Field:** Here, a length field is used that determines the size of the frame. It is used in Ethernet (IEEE 802.3).
2. **End Delimiter (ED):** Here, a pattern is used as a delimiter to determine the size of frame. It is used in Token Rings. If the pattern occurs in the message, then two approaches are used to avoid the situation:
   - **Byte–Stuffing**: A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.
   - **Bit–Stuffing:** A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.

Flow Control

It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver. The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached. It requires a buffer, a block of memory for storing the information until they are processed. Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

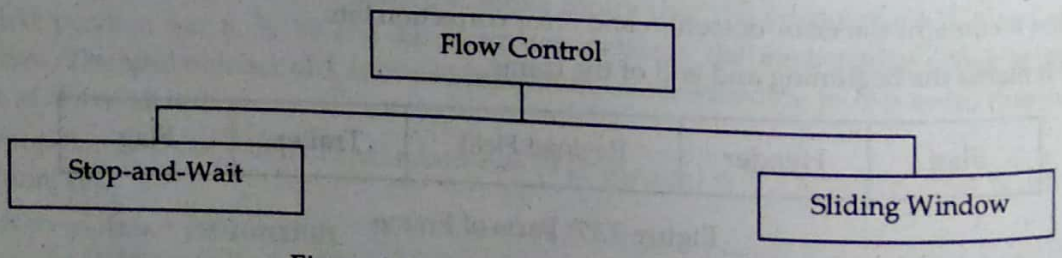


Figure 3.18: Methods of Flow Control

Stop-and-wait

In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends. When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

Sliding Window

This protocol improves the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledgment.

The working principle of this protocol can be described as follows:

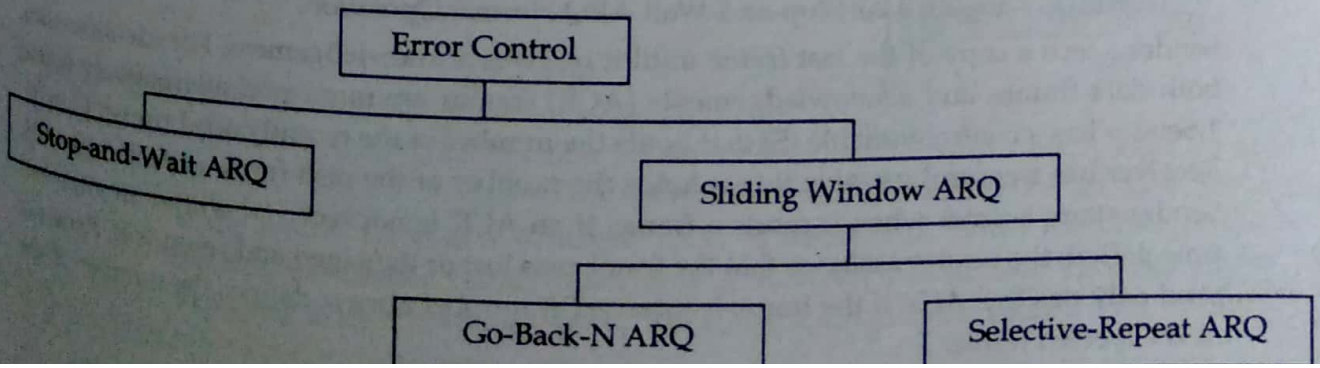
- Both the sender and the receiver has finite sized buffers called windows. The sender and the receiver agrees upon the number of frames to be sent based upon the buffer size.
- The sender sends multiple frames in a sequence, without waiting for acknowledgment. When its sending window is filled, it waits for acknowledgment. On receiving acknowledgment, it advances the window and transmits the next frames, according to the number of acknowledgments received.

Error Control

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

Requirements for error control mechanism:

- **Error detection**: The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK:** When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK:** When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or its acknowledgement is lost in transit.



1. **Stop-and-wait ARQ**

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames. This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

1. The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
2. Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.
3. If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
4. It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Normal Operation

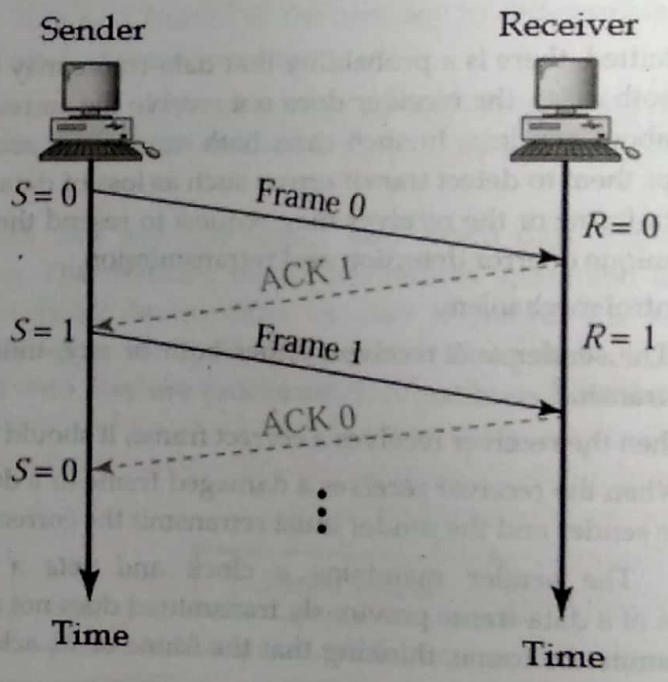


Figure 3.20: Stop-and-Wait ARQ Normal Operation.

Sender keeps a copy of the last frame until it receives acknowledgement. For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1.Sender has a control variable (S) that holds the number of the recently send frame. (0 or 1). Receiver has a control variable R that holds the number of the next frame expected (0 or 1). Sender starts a timer when it sends a frame. If an ACK is not received within an allocated time period, the sender assumes that the frame was lost or damaged and resends it. Receiver send only positive ACK if the frame is intact.ACK number always defines the number of the next expected frame.

Possibilities of the retransmission:

a. Lost Frame

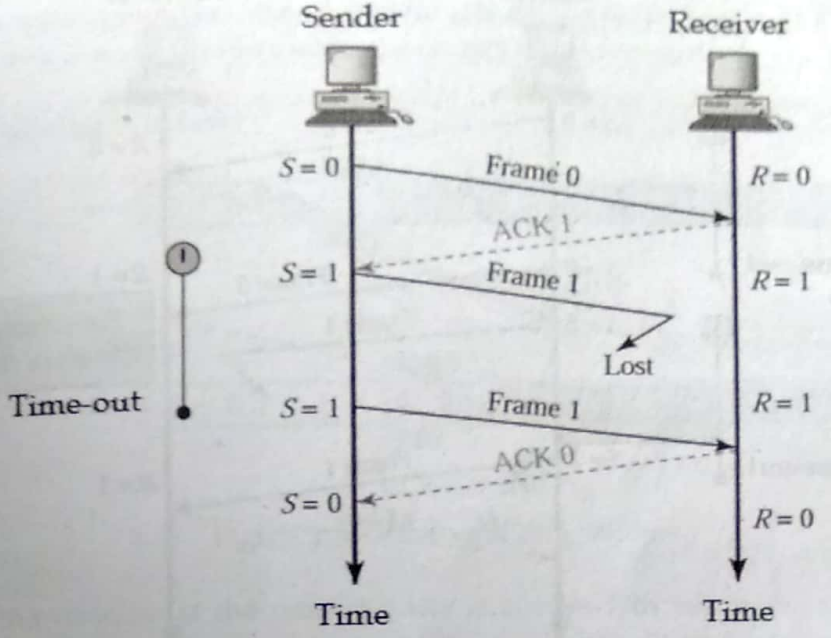


Figure 3.21: Retransmission during Lost Frame

When a receiver receives a damaged frame, it discards it and keeps its value of R. After the timer at the sender expires, another copy of frame 1 is sent.

b. **Lost ACK**

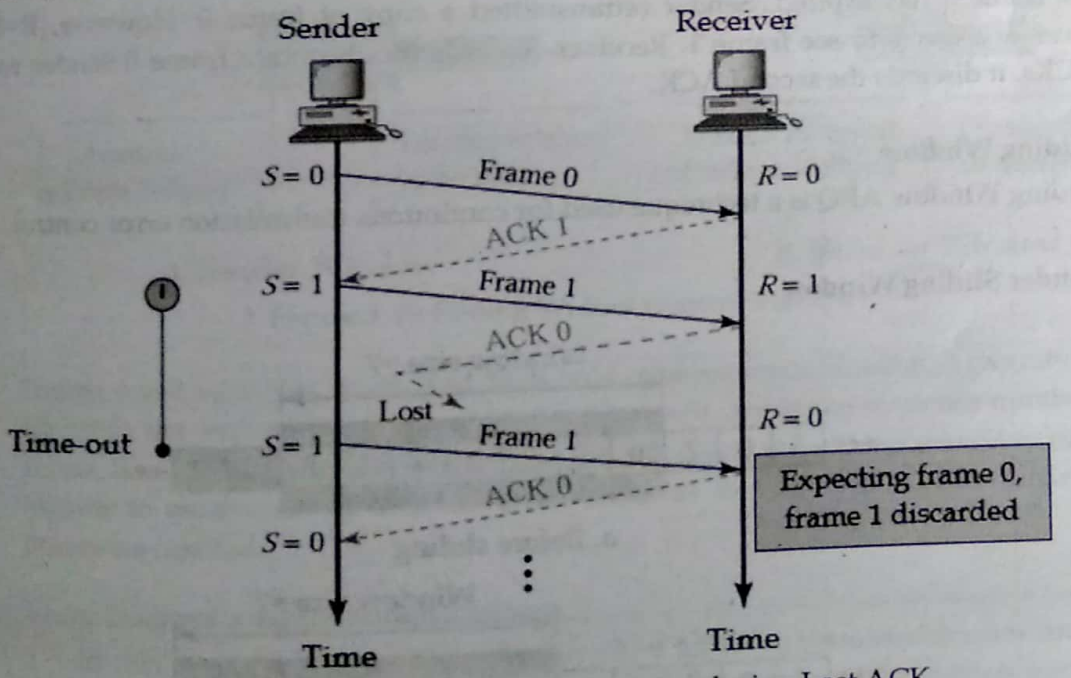


Figure 3.22: Retransmission during Lost ACK

If the sender receives a damaged ACK, it discards it. When the timer of the sender expires, the sender retransmits frame 1. Receiver has already received frame 1 and expecting to receive frame 0 (R=0). Therefore it discards the second copy of frame 1.

c. **Delayed ACK**

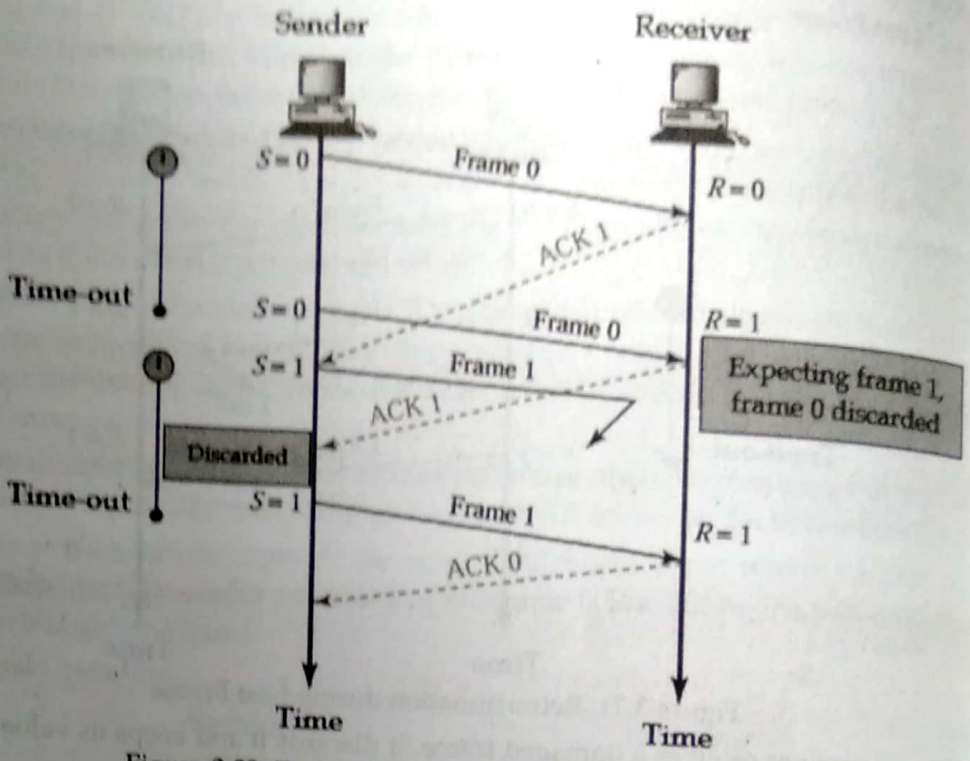


Figure 3.23: Retransmission during Delayed ACK

The ACK can be delayed at the receiver or due to some problem. It is received after the time for frame 0 has expired. Sender retransmitted a copy of frame 0. However, R=1 means receiver expects to see frame 1. Receiver discards the duplicate frame 0.Sender receives 2 ACKs, it discards the second ACK.

2. **Sliding Window**

Sliding Window ARQ is a technique used for continuous transmission error control.

Sender Sliding Window

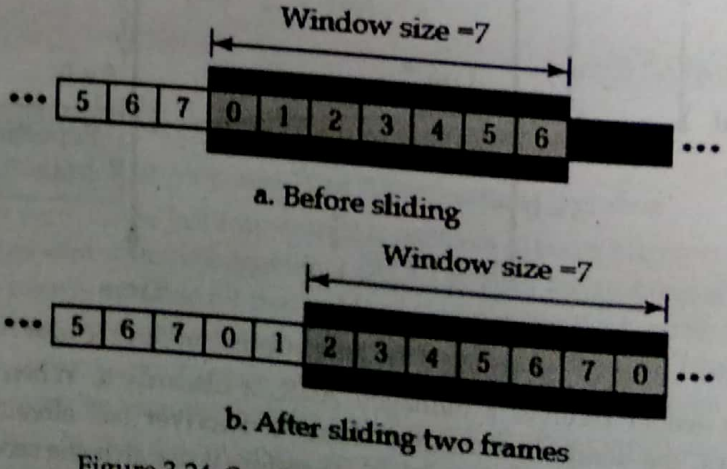


Figure 3.24: Sender Sliding Window

At the sending site, to hold the outstanding frames until they are acknowledged, we use the concept of a window. The size of the window is at most 2^m-1 where m is the number of bits for the sequence number. Size of the window can be variable, e.g. TCP. The window slides to include new unsent frames when the correct frame received.

Receive Sliding Window

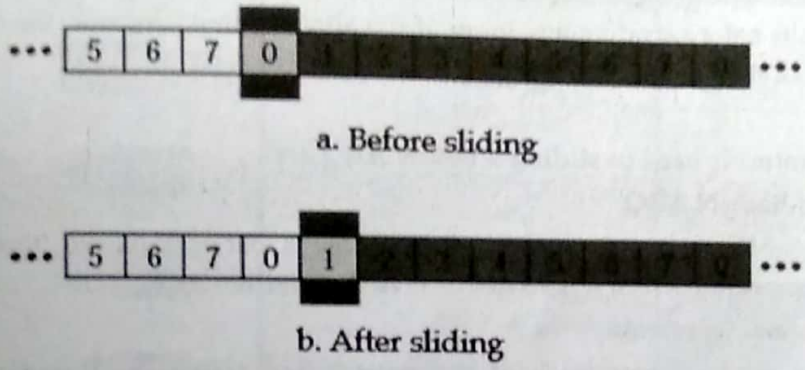


Figure 3.25: Receive Sliding Widow

Size of the window at the receiving site is always 1 in this protocol. Receiver is always looking for a specific frame to arrive in a specific order. Any frame arriving out of order is discarded and needs to be resent. Receiver window slides as shown in figure. Receiver is waiting for frame 0 in part a.

Control Variables

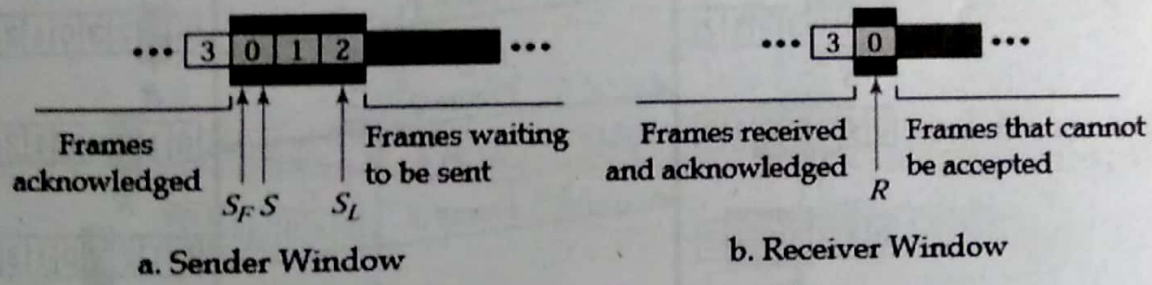


Figure 3.26: Sliding Widow Control Variables

Sender has 3 variables: **S**, **SF**, and **SL**.**S** holds the sequence number of recently send frame. **SF** holds the sequence number of the first frame.**SL** holds the sequence number of the last frame. Receiver only has the one variable, **R** that holds the sequence number of the frame it expects to receive. If the seq. no. is the same as the value of **R**, the frame is accepted, otherwise rejected.

Three Features used for retransmission:

1. In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
2. The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be

numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.

3. The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ are:

a. Go-Back-N ARQ

In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Normal Operation

The sender keeps track of the outstanding frames and updates the variables and windows as the ACKs arrive.

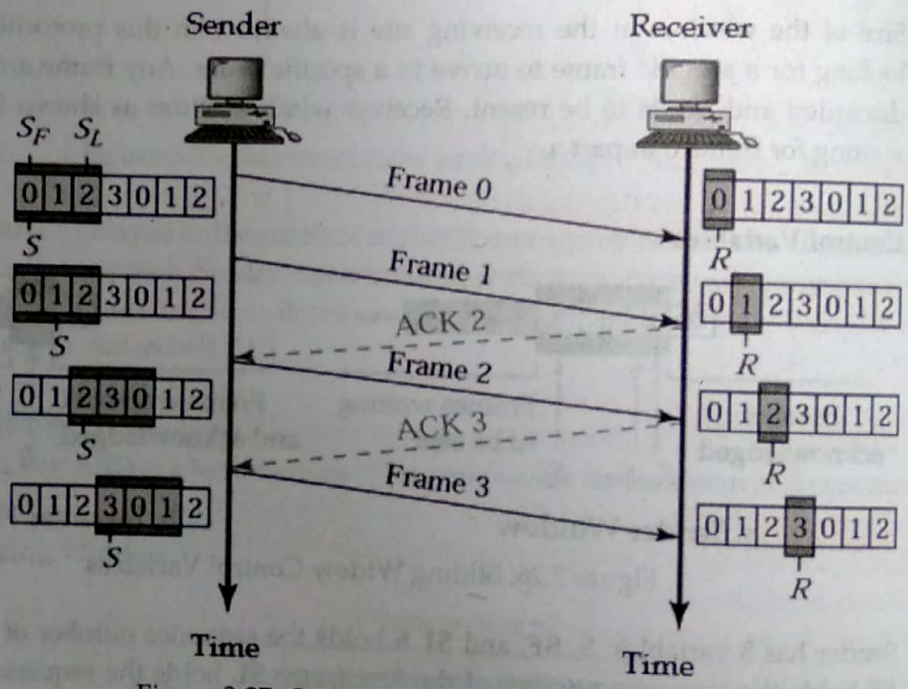


Figure 3.27: Go-Back-N ARQ Normal Operation

Lost Frame

In figure 3.28 frame 2 is lost. When the receiver receives frame 3, it discards frame 3 as it is expecting frame 2 (according to window). After the timer for frame 2 expires at the sender site, the sender sends frame 2 and 3. (Go back to 2).

In figure 3.29 Frame 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same for frame 3. Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.

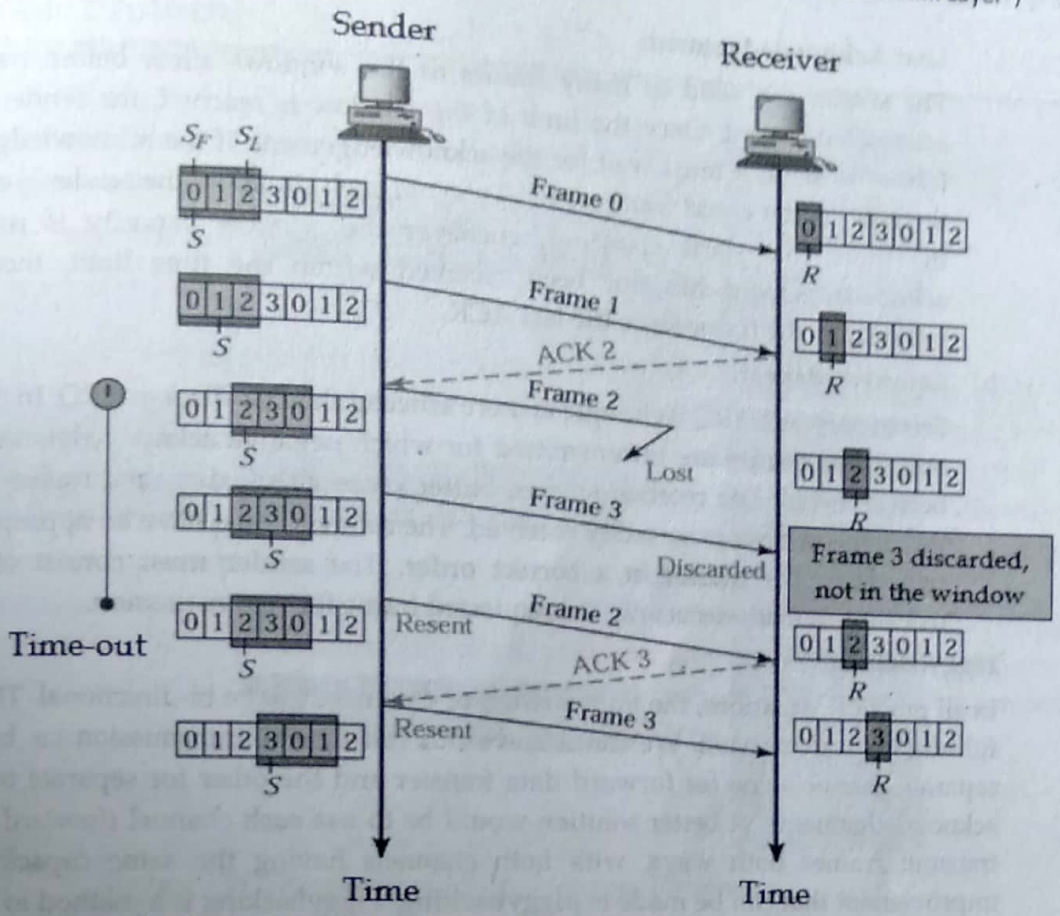


Figure 3.28: Go-Back-N ARQ lost frame and receiver window size=1

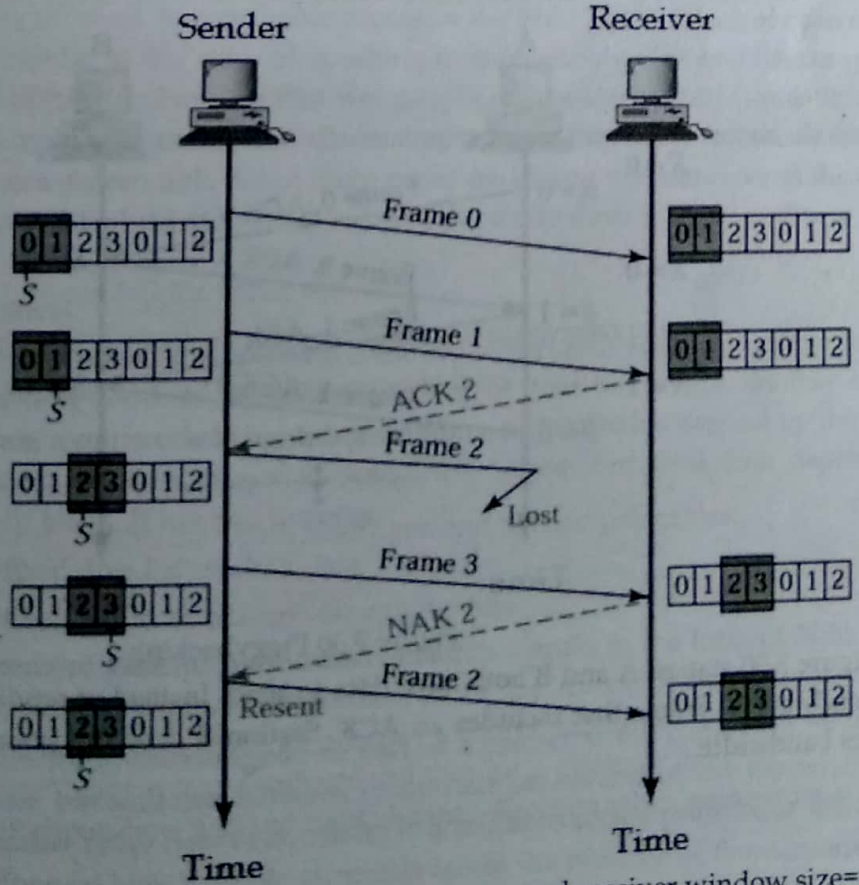


Figure 3.29: Go-Back-N ARQ lost frame and receiver window size=2

Lost Acknowledgement:

The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

b. Selective-Repeat

Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ. In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received. The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received. The receiver must have an appropriate logic for reinserting the frames in a correct order. The sender must consist of a searching mechanism that selects only the requested frame for retransmission.

Piggybacking

In all practical situations, the transmission of data needs to be bi-directional. This is called as full-duplex transmission. We can achieve this full duplex transmission i.e. by having two separate channels-one for forward data transfer and the other for separate transfer i.e. for acknowledgements. A better solution would be to use each channel (forward & reverse) to transmit frames both ways, with both channels having the same capacity. One more improvement that can be made is **piggybacking**. Piggybacking is a method to combine data frame with ACK i.e. bidirectional transmission.

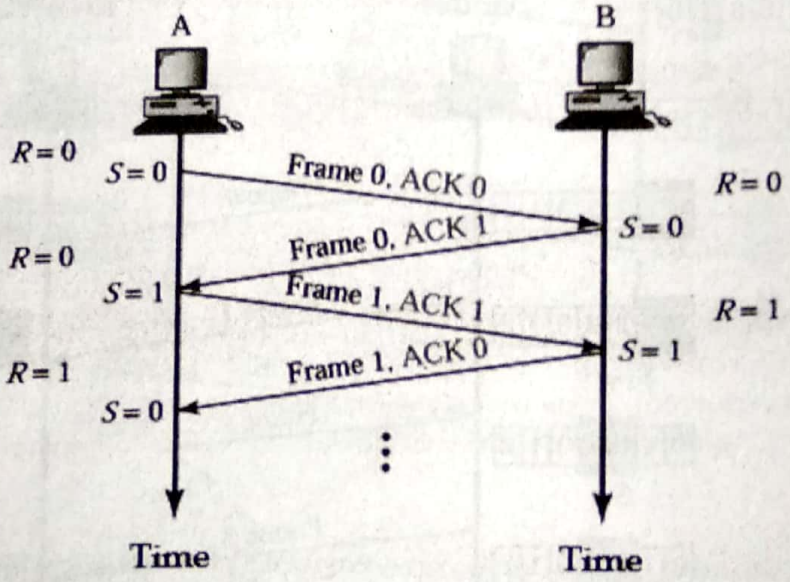


Figure 3.30 Piggybacking

In figure 3.30 station A and B both have data to send. Instead of sending separately, station A sends a data frame that includes an ACK. Station B does the same thing. Piggybacking saves bandwidth.

Multiple Access Protocol

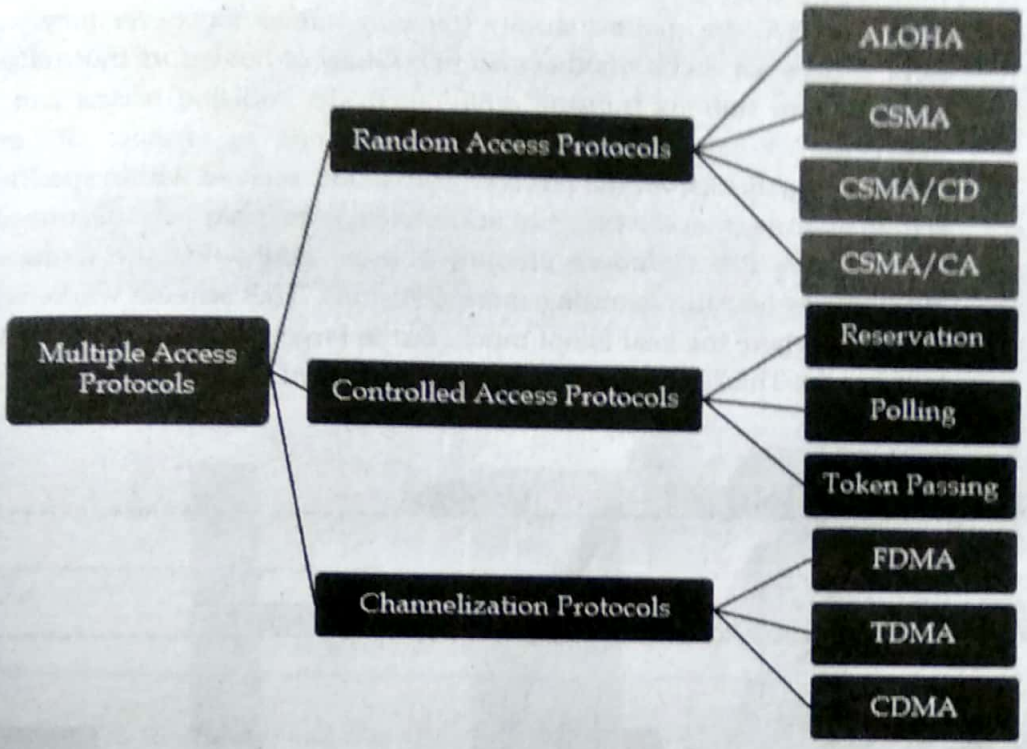


Figure 3.31 Taxonomy of Multiple-access Protocols

When nodes or stations are connected and use a common link, called a **multipoint** or **broadcast link**, we need a multiple-access protocol to coordinate access to the link. The problem of controlling the access to the medium is similar to the rules of speaking in an assembly. The procedures guarantee that the right to speak is upheld and ensure that two people do not speak at the same time, do not interrupt each other, do not monopolize the discussion, and so on. Many protocols have been devised to handle access to a shared link. All of these protocols belong to a sub-layer in the data-link layer called **Media Access Control (MAC)**. We categorize them into three groups, as shown in figure 3.31.

1. **Random Access Protocol**

   In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. Any station can send data depending on medium's state(idle or busy). It has two features:

   - There is no fixed time for sending data
   - There is no fixed sequence of stations sending data

   The random access protocols are further subdivided as:

   a) **ALOHA:**

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

- **Pure ALOHA:**

  Pure Aloha is an un-slotted, decentralized, and simple to implement protocol. In pure ALOHA, the stations simply transmit frames whenever they want data to send. It does not check whether channel is busy or not before transmitting. In case, two or more stations transmit simultaneously, collision occurs and frames are destroyed. Whenever any station transmits a frame, it expects the acknowledgement from the receiver. If it is not received within specified time, the station assumes that the frame or acknowledgement has been destroyed. Then, the station waits for a random amount of time and sends the frame again. This randomness helps in avoiding more collisions. This scheme works well in small networks where the load is not much. But in largely loaded networks, this scheme fails poorly. This led to the development of Slotted Aloha.

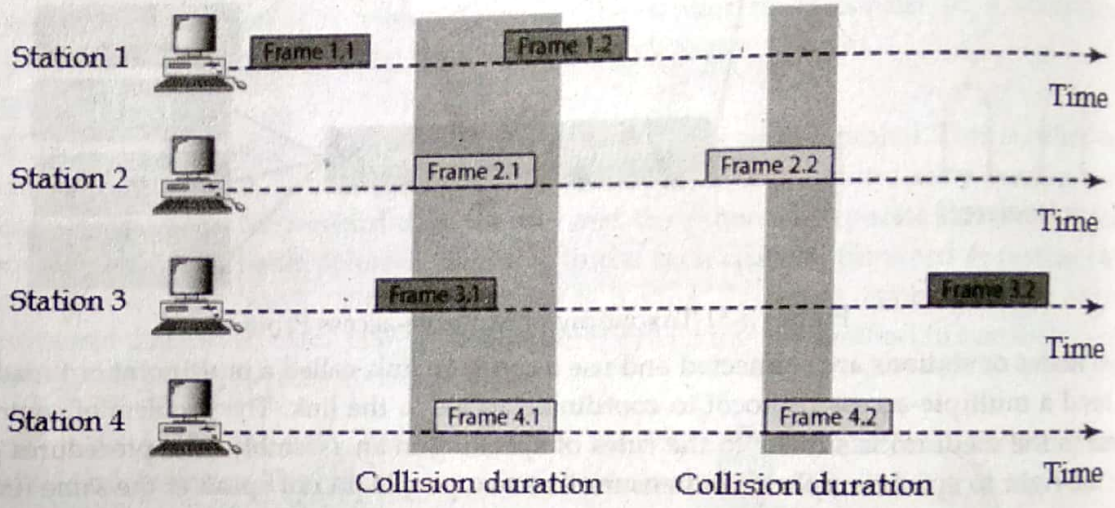


Figure 3.32 Frames in Pure ALOHA Network

To assure pure aloha: Its throughput and rate of transmission of frame to be predicted. For that to make some assumption:

i) All the frames should be the same length.

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

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

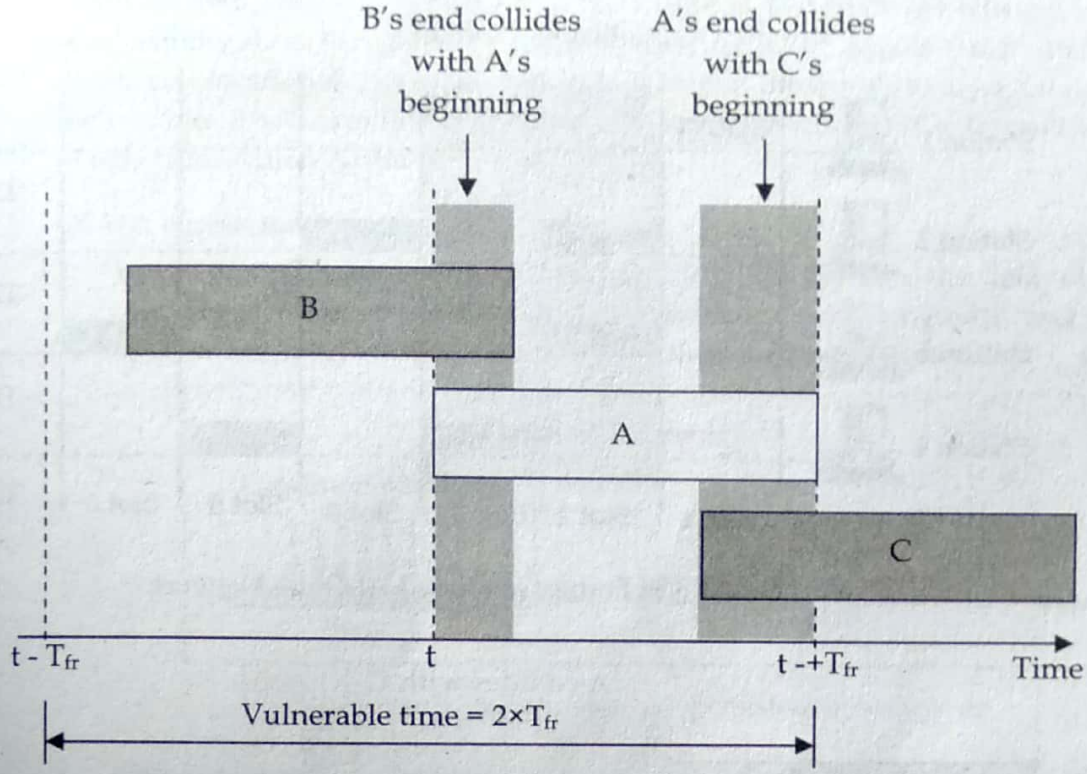


Figure 3.33 Vulnerable time for Pure ALOHA Protocol

Pure ALOHA vulnerable Time = 2 × Frame Transmission Time (T_{fr})

Throughput for pure ALOHA (Spure) = $G \times e^{-2G}$

Where G is number of stations wants to transmit in T_{fr} slot.

Maximum throughput $(Spure)_{max}$ = 0.184 for G=0.5

Which means, in Pure ALOHA, only about 18.4% of the time is used for successful transmissions.

- **Slotted ALOHA:**

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

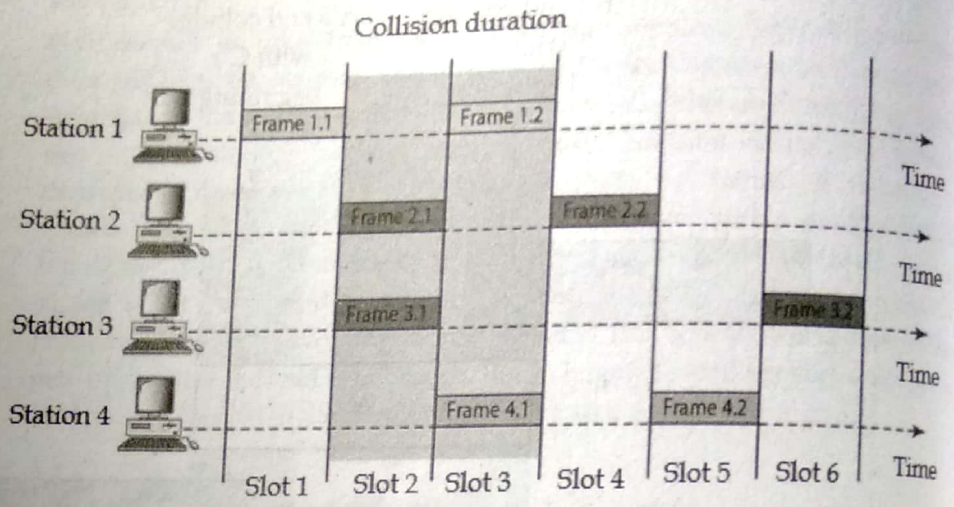


Figure 3.34 Frames in Slotted ALOHA Network

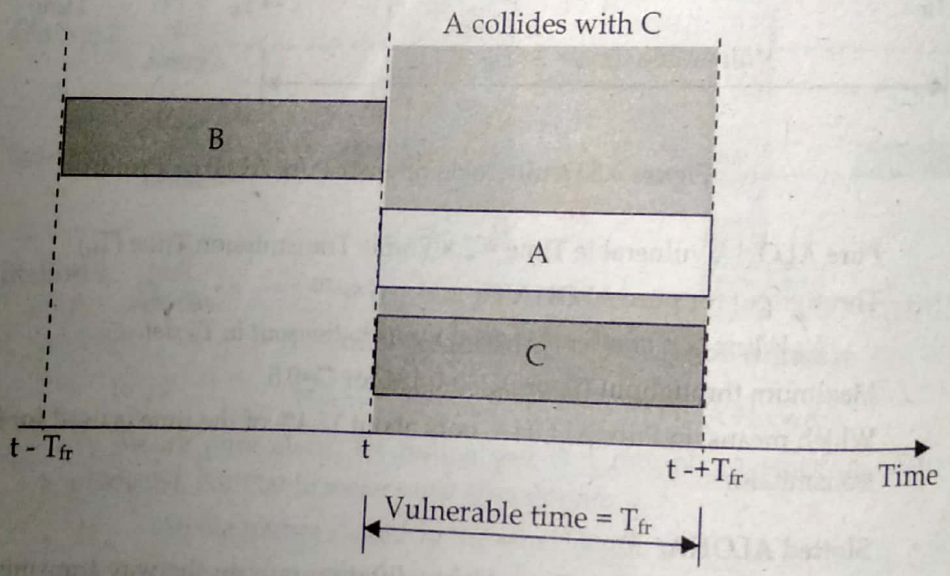


Figure 3.35: Vulnerable time for slotted ALOHA protocol

Slotted ALOHA vulnerable Time = Frame Transmission Time (T_{fr})

Throughput for Slotted ALOHA (Sslotted) = $G \times e^{-2G}$

Where G is number of stations wants to transmit in T_{fr} slot.

Maximum throughput $(Sslotted)_{max}$ = 0.368 for G=1

Which means, in slotted ALOHA, about 36.8% of the time is used for successful transmissions.

b) Carrier Sense Multiple Access (CSMA)

Carrier Sense Multiple Access (CSMA) ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A

wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes:

1. 1-persistent: The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.

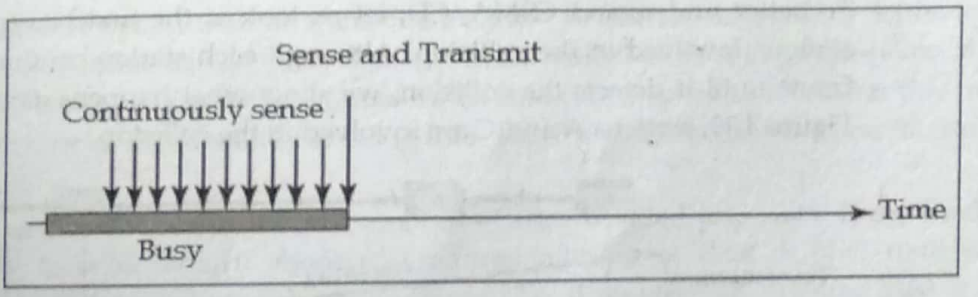


Figure 3.36: Behavior of 1-persistent access mode

2. Non-Persistent: The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.

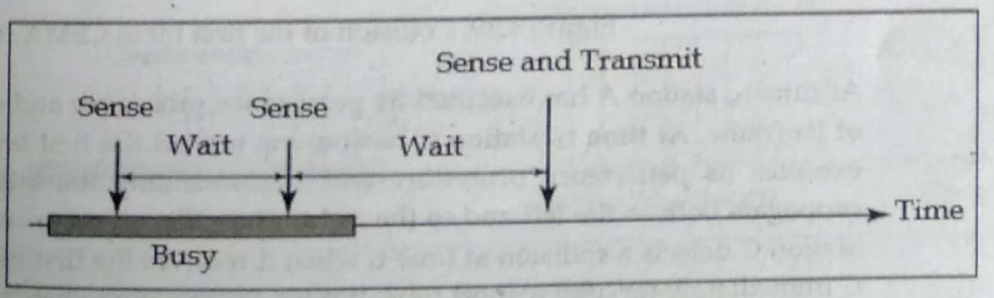


Figure 3.37: Behavior of Non-persistent access mode

3. P-persistent: The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wi-Fi and packet radio systems.

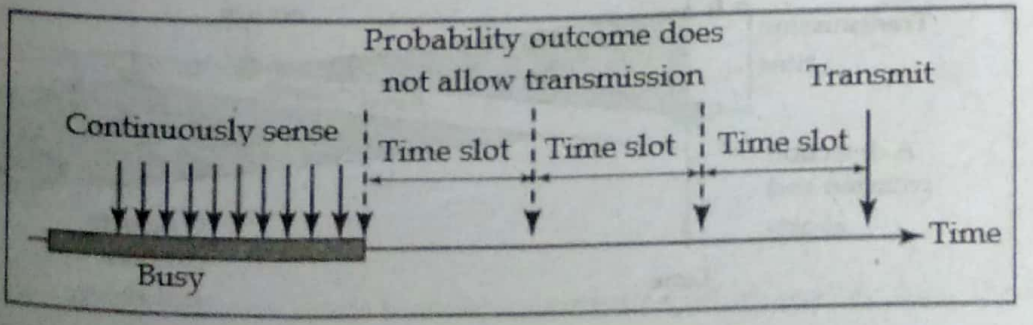


Figure 3.38: Behavior of p-persistent access mode

4. O-persistent: Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

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

The CSMA method does not tells us what to do in case there is a collision. Carrier sense multiple access with collision detection (CSMA/CD) adds on to the CSMA algorithm to deal with collision. In CSMA/CD, the size of a frame must be large enough so that collision can be detected by sender while sending the frame. So, the frame transmission delay must be at least two times the maximum propagation delay.

To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide. In Figure 3.39, stations A and C are involved in the collision.

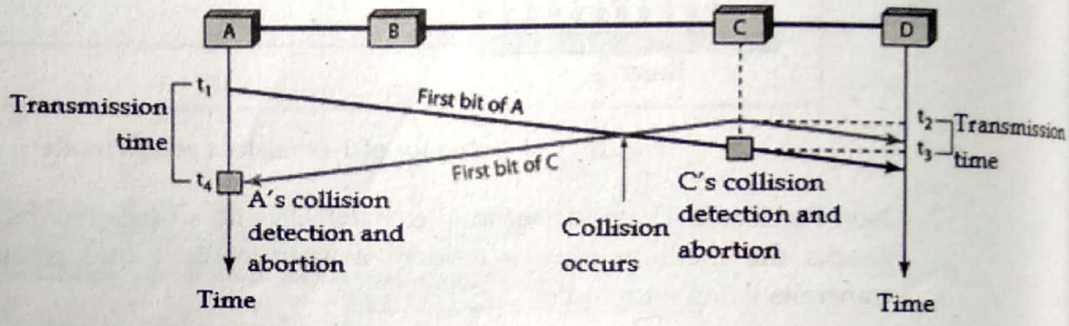


Figure 3.39: Collision of the first bit in CSMA/CD

At time t_1, station A has executed its persistence procedure and starts sending the bits of its frame. At time t_2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t_2. Station C detects a collision at time t_3 when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time t_4 when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration $t_4 - t_1$; C transmits for the duration $t_3 - t_2$.

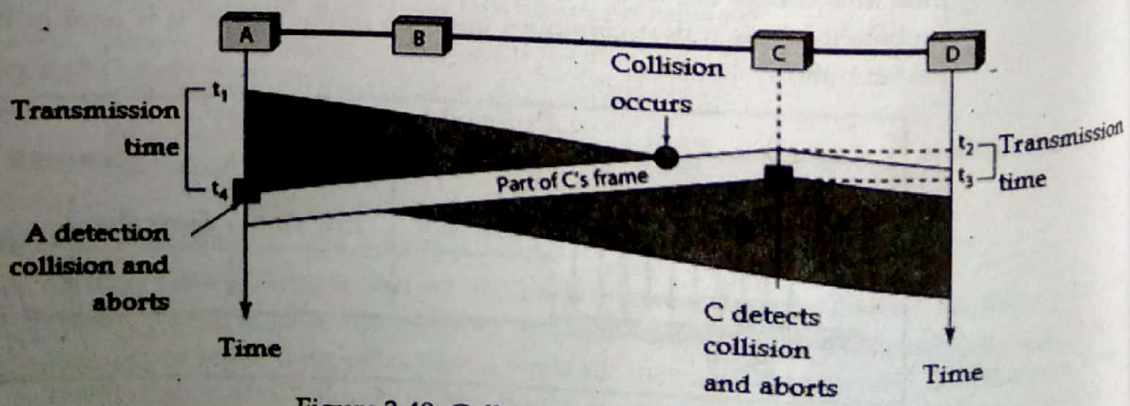


Figure 3.40: Collision and abortion in CSMA/CD

d) **Carrier Sense Multiple Access with Collision Avoidance(CSMA/CA)**

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal (its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA avoids collision by:

a) **Interframe space**: Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.

b) **Contention Window**: It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.

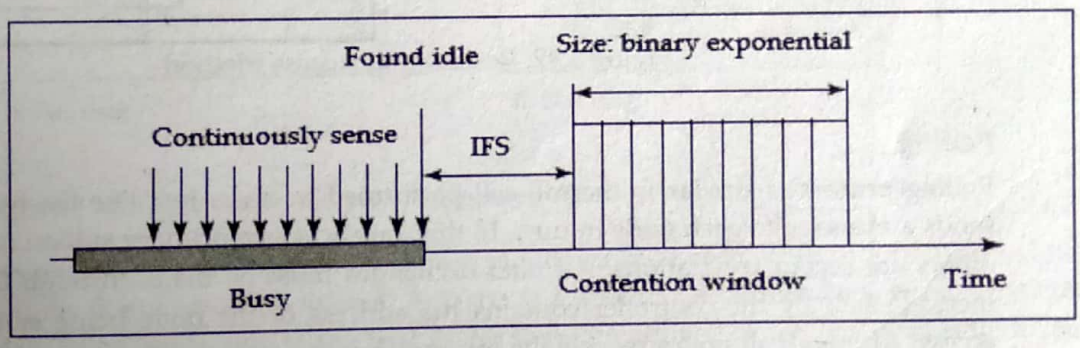


Figure 3.41: Contention Window

c) **Acknowledgement**: Sender re-transmits the data if acknowledgement is not received before time-out.

2. **Controlled Access Protocols**

In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid collision of messages on shared medium.

The three controlled-access methods are:

- Reservation
- Polling
- Token Passing

Reservation

In the reservation method, a station needs to make a reservation before sending data. The time line has two kinds of periods:

a) Reservation interval of fixed time length and
b) Data transmission period of variable frames.

If there are M stations, the reservation interval is divided into M slots, and each station has on slot. Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No othe station is allowed to transmit during this slot. In general, i^{th} station may announce that it has frame to send by inserting a 1 bit into i^{th} slot. After all N slots have been checked, each statio knows which stations wish to transmit. The stations which have reserved their slots transfe their frames in that order. After data transmission period, next reservation interval begins Since everyone agrees on who goes next, there will never be any collisions.

The following figure 3.42 shows a situation with five stations and a five slot reservation frame In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

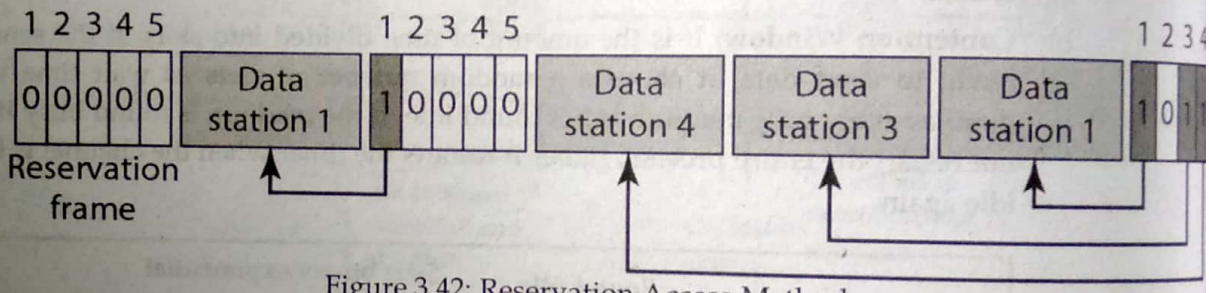


Figure 3.42: Reservation Access Method

Polling

Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn. In this, one acts as a primary station (controller) and the others are secondary stations. All data exchanges must be made through the controller. The message sent by the controller contains the address of the node being selected for granting access. Although all nodes receive the message but the addressed one responds to it and sends data, if any. If there is no data, usually a "poll reject"(NAK) message is sent back. Problems include high overhead of the polling messages and high dependence on the reliability of the controller.

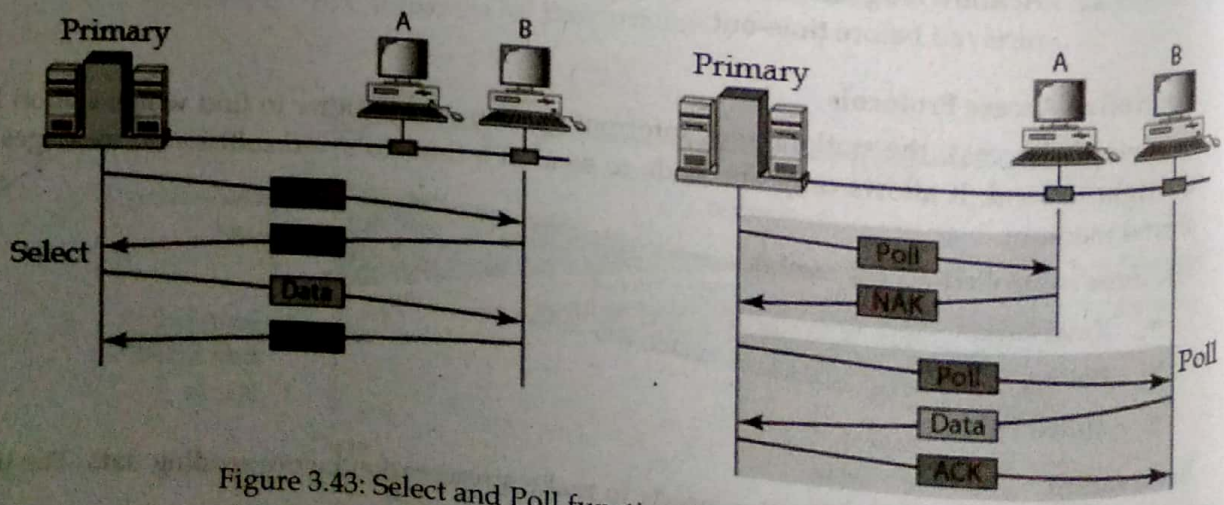


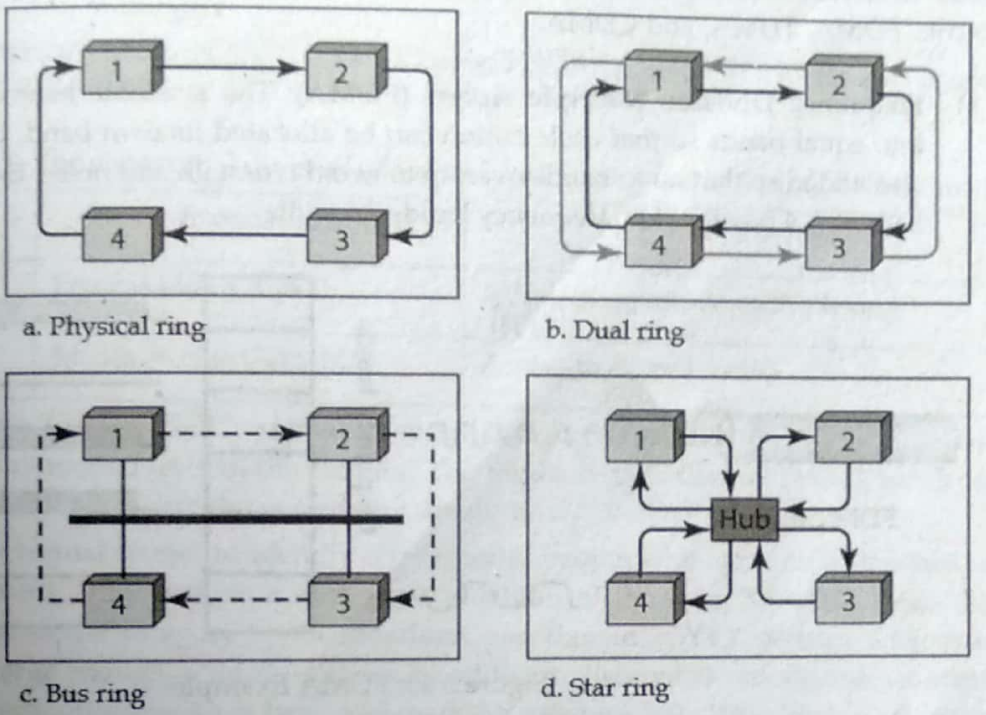
Figure 3.43: Select and Poll function in polling access method

Efficiency of Polling

Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then,

$$\text{Efficiency} = T_t/(T_t + T_{poll})$$

Token Passing



a. Physical ring

b. Dual ring

c. Bus ring

d. Star ring

Figure 3.44: Logical ring and physical topology in token-passing access method

In token passing scheme, the stations are connected logically to each other in form of ring and access of stations is governed by tokens. A token is a special bit pattern or a small message, which circulate from one station to the next in the some predefined order. In Token ring, token is passed from one station to another adjacent station in the ring whereas in case of Token bus, each station uses the bus to send the token to the next station in some predefined order. In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply. After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbors and the other N – 1 stations to send a frame, if they have one. There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.

Performance of Token Passing

Performance of token ring can be concluded by 2 parameters:

a. **Delay**, which is a measure of time between when a packet is ready and when it is delivered. So, the average time (delay) required to send a token to the next station = a/N.

b. **Throughput**, which is a measure of the successful traffic.

Throughput, $S = 1/(1 + a/N)$ for $a<1$and

$S = 1/\{a\ (1 + 1/N)\}$ for $a>1$. Where N = number of stations

$a = T_p/T_t$ [Where T_p=propagation delay and T_t=transmission delay]

3. Channelization Protocols

In this, the available bandwidth of the link is shared in time, frequency and code to multipl stations to access channel simultaneously. In this section, we discuss three channelizatio protocols: FDMA, TDMA, and CDMA.

a) **Frequency Division Multiple Access (FDMA)**: The available bandwidth is divide into equal bands so that each station can be allocated its own band. Guard bands a also added so that no to bands overlap to avoid crosstalk and noise. Example: 6-statio LAN, 1,3, 4 have packet, frequency bands 2,5,6 idle

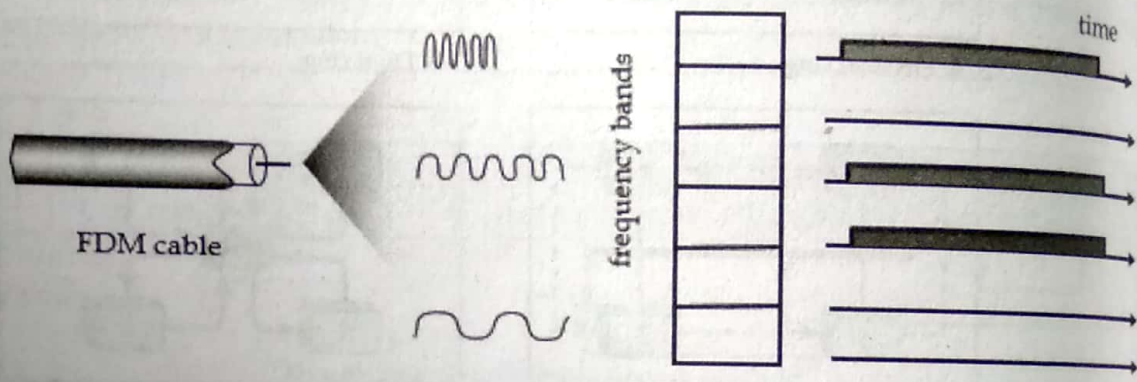


Figure 3.45: FDMA Example

b) **Time Division Multiple Access (TDMA):** In this, the bandwidth is shared betwee multiple stations. To avoid collision time is divided into slots and stations are allotte these slots to transmit data. However there is a overhead of synchronization as eac station needs to know its time slot. This is resolved by adding synchronization bits t each slot. Another issue with TDMA is propagation delay which is resolved b addition of guard bands.6-station LAN, 1,3, 4 have packet, frequency bands 2,5,6 idle

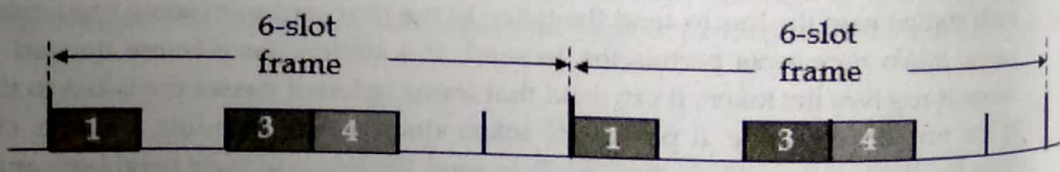


Figure 3.46: TDMA Example

c) **Code Division Multiple Access (CDMA):** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly data from different stations can be transmitted simultaneously in different code languages.

Ethernet Standards

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

IEEE 802 Model and Standards

To help characterize standards, IEEE divides Layer 2 of the protocol stack into two conceptual sub-layers, as table3.6 illustrates.

Table 3.6: The conceptual division of Layer 2 into sub-layers according to IEEE model.

Sub-Layer	Expansion	Purpose
LLC	Logical Link Control	Addressing and de-multiplexing
MAC	Media Access Control	Access to shared media

The Logical Link Control (LLC) sub-layer specifies addressing and the use of addresses for de-multiplexing as described later in the chapter. The Media Access Control (MAC) sub-layer specifies how multiple computers share the underlying medium.

Rather than use textual names to identify the group of people who work on a standard or the final standard document, IEEE assigns a multi-part identifier of the form XXX.YYY.ZZZ. The numeric value XXX denotes the category of the standard, and the suffix YYY denotes a subcategory. If a subcategory is large enough, a third level can be added to distinguish among specific standards. For example, LAN specifications have been assigned the category 802. Thus, each working group that devises a LAN standard is assigned an ID such as 802.1, 802.2, and so on. Note that neither the value 802 nor the individual suffixes convey any technical meaning – they merely identify standards. Table 3.7 lists examples of IEEE assignments.

As the figure shows, IEEE has created many working groups that are each intended to standardize one type of network technology. A group, which consists of representatives from the industrial and academic communities, meets regularly to discuss approaches and devise standards. IEEE allows a working group to remain active provided the group makes progress and the technology is still deemed important. If a working group decides that the technology under investigation is no longer relevant, the group can decide to disband. For example, a better technology might be discovered that makes further standardization pointless. Alternatively, another standards organization might produce a standard first, making an IEEE effort redundant. Thus, Table 3.7 includes topics that were once important, but have been disbanded.

Table 3.7:Examples of the identifiers IEEE has assigned to various LAN standards.

ID	Topic
802.1	Higher layer LAN protocols
802.2	Logical link control
802.3	Ethernet
802.4	Token bus (disbanded)
802.5	Token Ring

802.6	Metropolitan Area Networks (disbanded)
802.7	Broadband LAN using Coaxial Cable (disbanded)
802.9	Integrated Services LAN (disbanded)
802.10	Interoperable LAN Security (disbanded)
802.11	Wireless LAN (Wi-Fi)
802.12	Demand priority
802.13	Category 6 - 10Gb LAN
802.14	Cable modems (disbanded)
802.15	Wireless PAN, 802.15.1 (Bluetooth), 802.15.4 (ZigBee)
802.16	Broadband Wireless Access, 802.16e (Mobile) Broadband Wireless
802.17	Resilient packet ring
802.18	Radio Regulatory TAG
802.19	Coexistence TAG
802.20	Mobile Broadband Wireless Access
802.21	Media Independent Handoff
802.22	Wireless Regional Area Network

Wireless LAN: Spread Spectrum, Bluetooth, Wi-Fi

Spread Spectrum

Spread spectrum is an increasingly important form of encoding for wireless communications. It can be used to transmit either analog or digital data, using an analog signal. The basic idea of spread spectrum is to modulate the signal so as to increase significantly the bandwidth (spread the spectrum) of the signal to be transmitted. It was initially developed for military and intelligence requirements. The use of spread spectrum makes jamming and interception more difficult and provides improved reception. The first type of spread spectrum developed is known as **frequency hopping**. A more recent type of spread spectrum is **direct sequence**. Both of these techniques are used in various wireless communications standards and products.

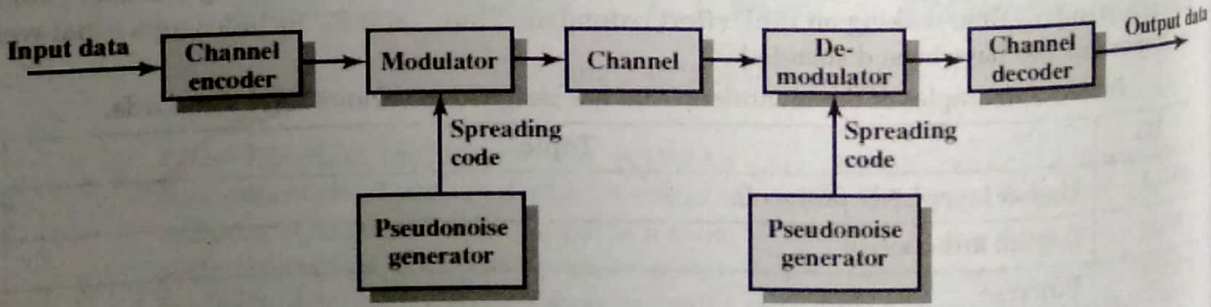


Figure 3.47: General Model of Spread Spectrum Digital Communication System

Figure 3.47 highlights the key characteristics of any spread spectrum system. Input is fed into a channel encoder that produces an analog signal with a relatively narrow bandwidth around some center frequency. This signal is further modulated using a sequence of digits known as a spreading code or spreading sequence. Typically, but not always, the spreading code is generated by a pseudo noise, or pseudorandom number, generator. The effect of this modulation is to increase significantly the bandwidth (spread the spectrum) of the signal to be transmitted. On the receiving end, the same digit sequence is used to demodulate the spread spectrum signal. Finally, the signal is fed into a channel decoder to recover the data.

Advantages

Several advantages can be gained from this apparent waste of spectrum by this approach:

- The signals gains immunity from various kinds of noise and multipath distortion. The earliest applications of spread spectrum were military, where it was used for its immunity to jamming.
- It can also be used for hiding and encrypting signals. Only a recipient who knows the spreading code can recover the encoded information.
- Several users can independently use the same higher bandwidth with very little interference. This property is used in cellular telephony applications, with a technique known as code division multiplexing (CDM) or code division multiple access (CDMA).

Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 20,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. Bluetooth was standardized as **IEEE 802.15.1**, but the standard is no longer maintained. The SIG oversees the development of the specification, manages the qualification program, and protects the trademarks. To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG. A network of patents is required to implement the technology, which is licensed only for that qualifying device.

Wi-Fi (IEEE 802.11 Wireless LAN)

Wireless communication is one of the fastest growing technologies these days. Wireless LANs are those Local Area Networks that use high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or Wi-Fi.

IEEE 802.11 Standards

In 1990, the IEEE 802 Committee formed a new working group, IEEE 802.11, specifically devoted to wireless LANs, with a charter to develop a MAC protocol and physical medium specification. The initial interest was in developing a wireless LAN operating in the ISM band. Since that time, the demand for WLANs, at different frequencies and data rates, has exploded. Keeping pace with this demand, the IEEE 802.11 working group has issued an ever-expanding list of standards, as shown in Table 3.8.

The first 802.11 standard to gain broad industry acceptance was 802.11b. Although 802.11b products are all based on the same standard, there is always a concern whether products from different vendors will successfully interoperate. To meet this concern, the Wireless Ethernet Compatibility

Alliance (WECA), an industry consortium, was formed in 1999. This organization, subsequently renamed the Wi-Fi (Wireless Fidelity) Alliance, created a test suite to certify interoperability for 802.11b products. The term used for certified 802.11b products is Wi-Fi. Wi-Fi certification has been extended to 802.11g products. The Wi-Fi Alliance has also developed a certification process for 802.11a products, called Wi-Fi5. The Wi-Fi Alliance is concerned with a range of market areas for WLANs, including enterprise, home, and hot spots.

Table 3.8: IEEE 802.11 Standards

IEEE Standard	Scope
802.11	Medium access control (MAC): One common MAC for WLAN applications
	Physical layer: Infrared at 1 and 2 Mbps
	Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
	Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
802.11a	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
802.11b	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
802.11c	Bridge operation at 802.11 MAC layer
802.11d	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains(countries)
802.11e	MAC: Enhance to improve quality of service and enhance security mechanisms
802.11f	Recommended practices for multivendor access point interoperability
802.11g	Physical layer: Extend 802.11b to data rates> 20 Mbps
802.11h	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
802.11i	MAC: Enhance security and authentication mechanisms
802.11j	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
802.11k	Radio resource measurement enhancements to provide interface to higher layers for radio and network measurements
802.11m	Maintenance of IEEE 802.11-1999 standard with technical and editorial corrections
802.11n	Physical/MAC: Enhancements to enable higher throughput
802.11p	Physical/MAC: Wireless access in vehicular environments
802.11r	Physical/MAC: Fast roaming (fast BSS transition)
802.11s	Physical/MAC: ESS mesh networking
802.11,2	Recommended practice for the evaluation of 802.11 wireless performance
802.11u	Physical/MAC: Interworking with external networks

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows

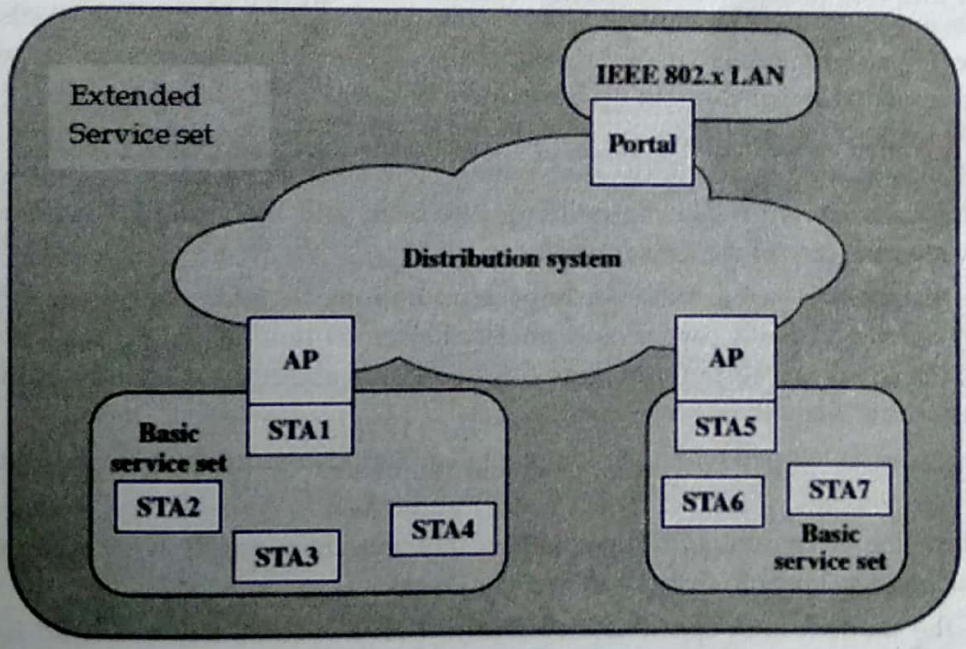
1. **Stations (STA):** Stations comprise all devices and equipment that are connected to the wireless LAN. A station can be of two types:
   a) **Wireless Access Point (WAP):** WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
   b) **Client:** Clients are workstations, computers, laptops, printers, smartphones, etc.

Each station has a wireless network interface controller.

2. **Basic Service Set (BSS):** A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:
   a) **Infrastructure BSS:** Here, the devices communicate with other devices through access points.
   b) **Independent BSS:** Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) **Extended Service Set (ESS):** It is a set of all connected BSS.

4) **Distribution System (DS):** It connects access points in ESS.



STA = station
AP = access point

Figure 3.48: IEEE 802.11 Architecture

Advantages of WLANs

1. They provide clutter free homes, offices and other networked places.
2. The LANs are scalable in nature, i.e. devices may be added or removed from the network at a greater ease than wired LANs.
3. The system is portable within the network coverage and access to the network is not bounded by the length of the cables.
4. Installation and setup is much easier than wired counterparts.
5. The equipment and setup costs are reduced.

Disadvantages of WLANs

1. Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
2. Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
3. WLANs are slower than wired LANs.

Overview of Virtual Circuit Switching, Frame Relay & ATM

Virtual Circuit Switching

A virtual circuit is a circuit or path between points in a network that appears to be a discrete, physical path but is actually a managed pool of circuit resources from which specific circuits are allocated as needed to meet traffic requirements.(See unit 2 for detail)

Frame Relay

Frame Relay is a packet switching methodology that is designed in the late 1980s and widely deployed in the 1990s. Frame Relay uses virtual circuits. These virtual circuits can be set up for each session (switched virtual circuits) or set up permanently (permanent virtual circuits). Frame relay is designed for fiber optic cables with a very low bit error rate. Frame Relay has no error recovery and no flow control. Whenever a Frame Relay switch detects an error in a packet, it just discard the data. This results in a network with a low processing overhead and high transmission rates. The end system will have to take care of the data integrity.

Frame Relay is extensively used today in large corporations to interconnect the LANs between buildings. Frame Relay offers a corporation an alternative to sending its intra IP traffic over the public Internet, for which the corporation may have concerns about the reliability or the security. In this case the virtual circuits will be permanent.

Packet switching was developed when the long distance digital communication showed a large error rate.

- To reduce the error rate, additional coding bits were introduced in each packet in order to introduce redundancy to detect and recover errors.
- But in the modem high speed telecommunication a system, this overhead is unnecessary and infect counterproductive.
- Frame relay was developed for taking the advantage of the high data rates and low error rates in the modem communication system.
- The original packet switching networks were designed with a data rate at the user end of about 64 kbps.
- But the frame relay networks are designed to operate efficiently at the user's data rates up to 2 Mbps.
- This is possible practically because most of the overhead (additional bits) are striped off.
- Frame relay is a virtual circuit wide area network which was designed in early 1990s.
- Frame relay also is meant for more efficient transmission scheme than the X.25 protocol.
- Frame Relay is used mostly to route Local Area Network protocols such as IPX or TCP/IP.

- The biggest difference between Frame Relay and X.25 is that X.25 guarantees data integrity and network managed flow control at the cost of some network delays. Frame Relay switches packets end-to-end much faster, but there is no guarantee of data integrity at all.

Features of frame relay:

- Frame relay operates at a high speed (1.544 Mbps to 44.376 Mbps).
- Frame relay operates only in the physical and data link layers. So it can be easily used in Internet.
- It allows the bursty data.
- It has a large frame size of 9000 bytes. So it can accommodate all local area network frame sizes.
- Frame relay can only detect errors (at the data link layer). But there is no flow control or error control.
- The damaged frame is simply dropped. There is no retransmission. This is to increase the speed. So frame relay needs a reliable medium and protocols having flow and error control.

Frame Format

- The DLCI length is 10 bits
- There are two EA locations. The value of the first one is fixed at 0 and the second at 1 is set in the DE (Discard Eligibility) for the part that can be discarded first when congestion occurs
- The data size may vary up to 4096 bytes.

Frame relay layers

Frame relay has only two layers i.e. physical layer and data link layer.

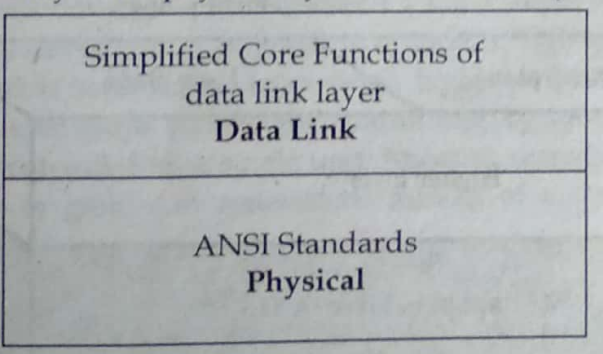


Figure 3.49: Relay Layers

Physical layer

- Frame relay supports ANSI standards.
- No specific protocol is defined for the physical layer. The user can use any protocol which is recognized by ANSI.

Data link layer

- A simplified version of HDLC is employed by the frame relay at the data link layer.
- A simpler version is used because flow control and error correction is not needed in frame relay.

Asynchronous Transfer Mode (ATM)

ATM, also known as cell relay, is a streamlined packet transfer interface which takes advantage of the reliability and fidelity of modern digital facilities to provide faster packet switching than X.25. Like packet switching and frame relay, ATM involves the transfer of data in discrete chunks, and allows multiple logical connections to be multiplexed over a single physical interface. In the case of ATM, the information flow on each logical connection is organized into fixed-size packets, called cells.

ATM is a streamlined protocol with minimal error and flow control capabilities. This reduces the overhead of processing ATM cells and reduces the number of overhead bits required with each cell, thus enabling ATM to operate at high data rates. Further, the use of fixed-size cells simplifies the processing required at each ATM node, again supporting the use of ATM at high data rates.

The standards issued for ATM by ITU-T are based on the protocol architecture shown in Figure 3.50, which illustrates the basic architecture for an interface between user and network. The physical layer involves the specification of a transmission medium and a signal encoding scheme. The data rates specified at the physical layer range from 25.6 Mbps to 622.08 Mbps. Other data rates, both higher and lower, are possible.

Two layers of the protocol architecture relate to ATM functions. There is an ATM layer common to all services that provides packet transfer capabilities, and an ATM adaptation layer (AAL) that is service dependent. The ATM layer defines the transmission of data in fixed-size cells and defines the use of logical connections. The use of ATM creates the need for an adaptation layer to support information transfer protocols not based on ATM. The AAL maps higher-layer information into ATM cells to be transported over an ATM network, then collects information from ATM cells for delivery to higher layers.

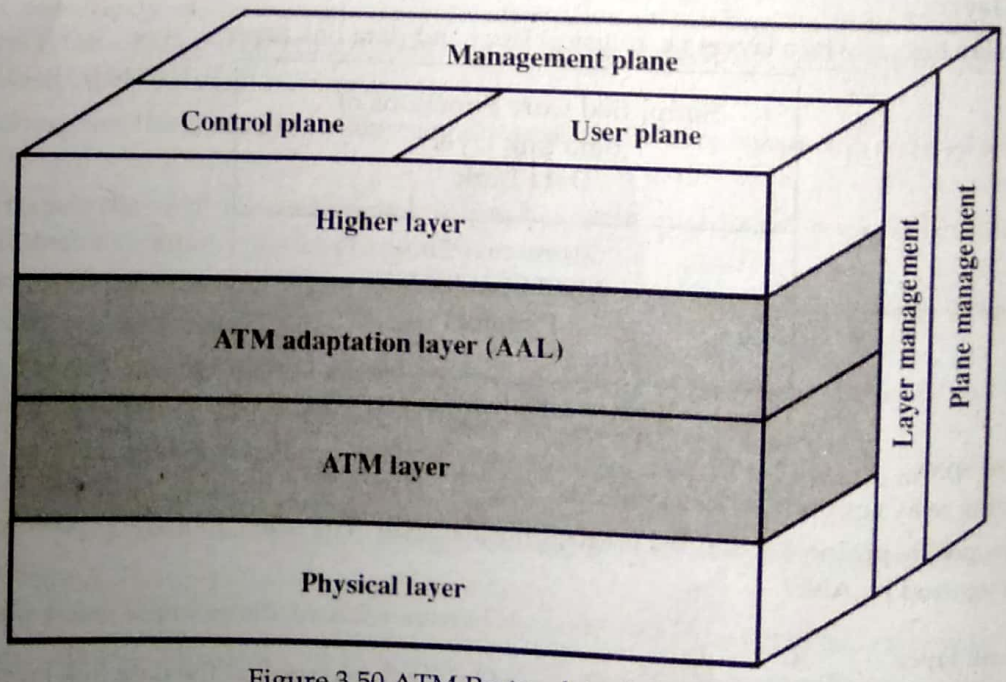


Figure 3.50 ATM Protocol Architecture

The protocol reference model involves three separate planes:

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

Asynchronous Transfer Mode (ATM)

ATM, also known as cell relay, is a streamlined packet transfer interface which takes advantage of the reliability and fidelity of modern digital facilities to provide faster packet switching than X.25. Like packet switching and frame relay, ATM involves the transfer of data in discrete chunks, and allows multiple logical connections to be multiplexed over a single physical interface. In the case of ATM, the information flow on each logical connection is organized into fixed-size packets, called cells.

ATM is a streamlined protocol with minimal error and flow control capabilities. This reduces the overhead of processing ATM cells and reduces the number of overhead bits required with each cell, thus enabling ATM to operate at high data rates. Further, the use of fixed-size cells simplifies the processing required at each ATM node, again supporting the use of ATM at high data rates.

The standards issued for ATM by ITU-T are based on the protocol architecture shown in Figure 3.50, which illustrates the basic architecture for an interface between user and network. The physical layer involves the specification of a transmission medium and a signal encoding scheme. The data rates specified at the physical layer range from 25.6 Mbps to 622.08 Mbps. Other data rates, both higher and lower, are possible.

Two layers of the protocol architecture relate to ATM functions. There is an ATM layer common to all services that provides packet transfer capabilities, and an ATM adaptation layer (AAL) that is service dependent. The ATM layer defines the transmission of data in fixed-size cells and defines the use of logical connections. The use of ATM creates the need for an adaptation layer to support information transfer protocols not based on ATM. The AAL maps higher-layer information into ATM cells to be transported over an ATM network, then collects information from ATM cells for delivery to higher layers.

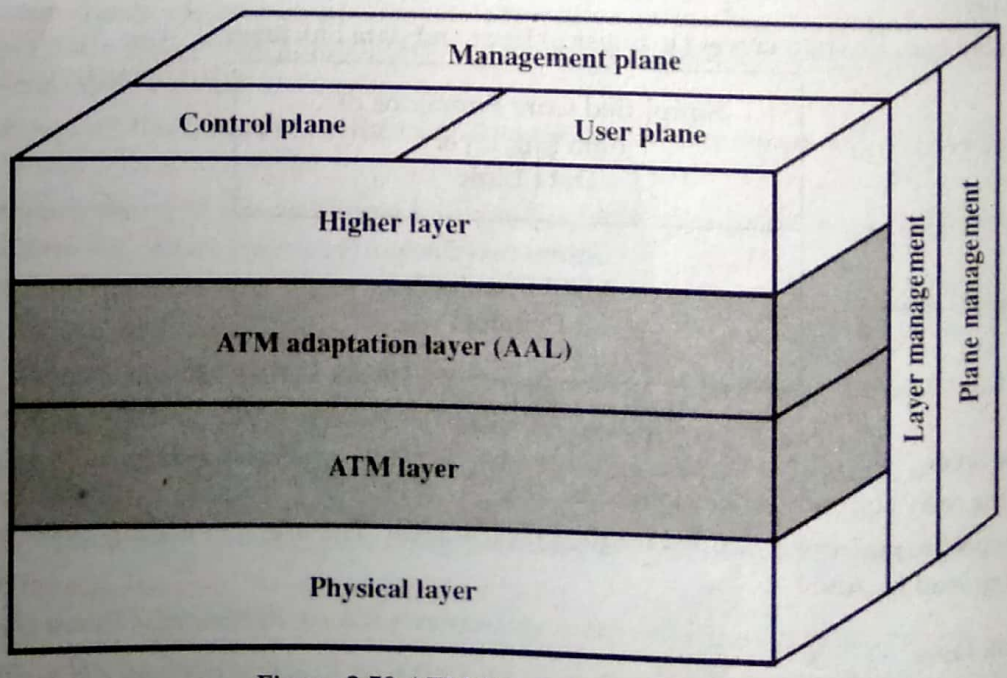


Figure 3.50 ATM Protocol Architecture

The protocol reference model involves 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

ATM Logical connections: Logical connections in ATM are referred to as virtual channel connections (VCCs). A VCC is analogous to a virtual circuit in X.25; it is the basic unit of switching in an ATM network. A VCC is set up between two end users through the network and a variable-rate, full-duplex flow of fixed-size cells is exchanged over the connection. VCCs are also used for user-network exchange (control signaling) and network-network exchange (network management and routing).

ATM Virtual Path Connection (VPC)

Figure 3.51 Virtual Connection Relationship

For ATM, a second sub-layer of processing has been introduced that deals with the concept of virtual path (Figure 11.2). 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. The virtual path concept was developed in response to a trend in high-speed networking in which the control cost of the network is becoming an increasingly higher proportion of the overall network cost. The virtual path technique helps contain the control cost by grouping connections sharing common paths through the network into a single unit. Network management actions can then be applied to a small number of groups of connections instead of a large number of individual connections.

The terminology of virtual paths and virtual channels used in the standard is a bit confusing. Whereas most of the network-layer protocols that we deal with in this book relate only to the user-network interface, the concepts of virtual path and virtual channel are defined in the ITU-T Recommendations with reference to both the user-network interface and the internal network operation.

DLL Protocol: HDLC, PPP

High-Level Data Link Control (HDLC)

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. HDLC is a synchronous Data Link layer bit-oriented protocol developed by the International Organization for Standardization (ISO). The current standard for HDLC is ISO 13239. HDLC was developed from the Synchronous Data Link Control (SDLC) standard proposed in

the 1970s. HDLC provides both connection-oriented and connectionless service. HDLC use synchronous serial transmission to provide error free communication between two points. HDL defines a Layer 2 framing structure that allows for flow control and error control through the use o acknowledgments. Each frame has the same format, whether it is a data frame or a control fram When you want to transmit frames over synchronous or asynchronous links, you must remembe that those links have no mechanism to mark the beginnings or ends of frames. HDLC uses a fram delimiter, or flag, to mark the beginning and the end of each frame.

HDLC Framing

To provide the flexibility necessary to support all the options possible in the modes and configurations just described, HDLC defines three types of frames:

1. Information frames (I-frames),
2. Supervisory frames (S-frames), and
3. Unnumbered frames (U-frames).

Each type of frame serves as an envelope for the transmission of a different type of message. I-frames are used to data-link user data and control information relating to user data (piggybacking). S-frames are used only to transport control information. U-frames are reserved for system management. Information carried by U-frames is intended for managing the link itself.

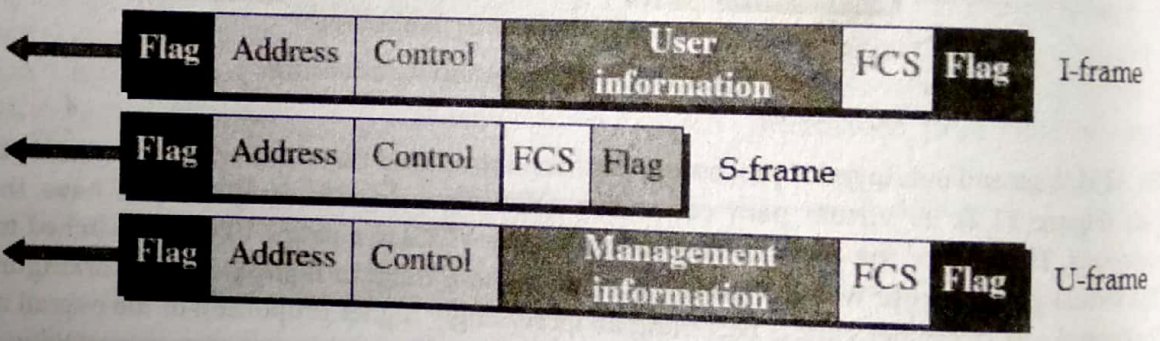


Figure 3.52: HDLC frames

Let us now discuss the fields and their use in different frame types.

- **Flag field.** This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.
- **Address field.** This field contains the address of the secondary station. If a primary station created the frame, it contains a *to* address. If a secondary station creates the frame, it contains a *from* address. The address field can be one byte or several bytes long, depending on the needs of the network.
- **Control field.** The control field is one or two bytes used for flow and error control. The interpretation of bits are discussed later.
- **Information field.** The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.
- **FCS field.** The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte CRC.

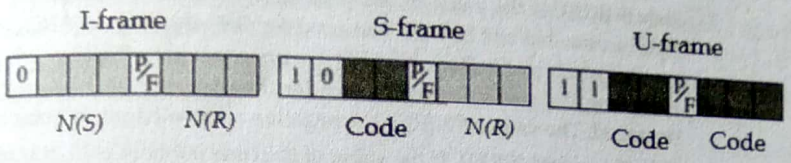


Figure 3.53: Control field format for the different frame types

I-Frame:

I-frames are designed to carry user data from the network layer. In addition, they can include flow and error control information (piggybacking).

- The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame.
- The next 3 bits, called N(S), define the sequence number of the frame. Note that with 3 bits, we can define a sequence number between and 7; but in the extension format, in which the control field is 2 bytes, this field is larger.
- The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used.
- The single bit between N(S) and N(R) is called the P/F bit. The P/F field is a single bit with a dual purpose. It has meaning only when it is set (bit = 1) and can mean poll or final. It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver). It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

S-Frame:

Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than an acknowledgment). S-frames do not have information fields.

- If the first 2 bits of the control field is 10, this means the frame is an S-frame.
- The last 3 bits, called N(R), corresponds to the acknowledgment number (ACK) or negative acknowledgment number (NAK) depending on the type of S-frame.
- The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames, as described below:

1. **Receive ready (RR).** If the value of the code subfield is 00, it is an RR S-frame. This kind of frame acknowledges the receipt of a safe and sound frame or group of frames. In this case, the value of the N(R) field defines the acknowledgment number.
2. **Receive not ready (RNR).** If the value of the code subfield is 10, it is an RNR S-frame. This kind of frame is an RR frame with additional functions. It acknowledges the receipt of a frame or group of frames, and it announces that the receiver is busy and cannot receive more frames. It acts as a kind of congestion-control mechanism by asking the sender to slow down. The value of N(R) is the acknowledgment number.

3. **Reject (REJ).** If the value of the code subfield is 01, it is an REJ S-frame. This is a NAK frame, but not like the one used for Selective Repeat ARQ. It is a NAK that can be used in Go-Back-N ARQ to improve the efficiency of the process by informing the sender, before the sender timer expires, that the last frame is lost or damaged. The value of N(R) is the negative acknowledgment number.
4. **Selective reject (SREJ).** If the value of the code subfield is 11, it is an SREJ S-frame. This is a NAK frame used in Selective Repeat ARQ. Note that the HDLC Protocol uses the term selective reject instead of selective repeat. The value of N(R) is the negative acknowledgment number.

U-Frames

Unnumbered frames are used to exchange session management and control information between connected devices. Unlike S-frames, U-frames contain an information field, but one used for system management information, not user data. As with S-frames, however, much of the information carried by U-frames is contained in codes included in the control field. U-frame codes are divided into two sections: a 2-bit prefix before the P/F bit and a 3-bit suffix after the P/F bit. Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.

Point-to-point protocol (PPP):

Although HDLC is a general protocol that can be used for both point-to-point and multi-point configurations, one of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer.

PPP provides several services:

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

On the other hand, to keep PPP simple, several services are missing:

1. PPP does not provide flow control. A sender can send several frames one after another with no concern about overwhelming the receiver.
2. PPP has a very simple mechanism for error control. A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs

to take care of the problem. Lack of error control and sequence numbering may cause a packet to be received out of order.

3. PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

PPP Framing

PPP uses a character-oriented (or byte-oriented) frame. Figure 3.54 shows the format of a PPP frame. The description of each field follows:

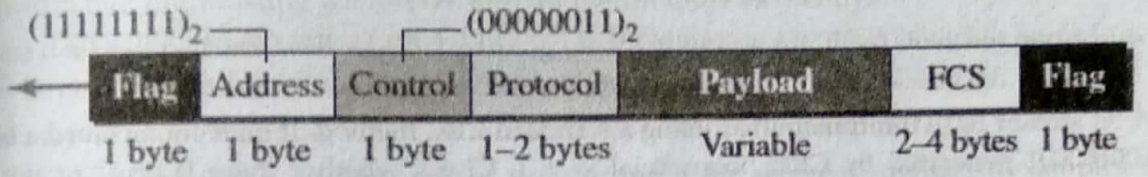


Figure 3.54: PPP frame format

- **Flag:** A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110.
- **Address:** The address field in this protocol is a constant value and set to 11111111 (broadcast address).
- **Control:** This field is set to the constant value 00000011 (imitating unnumbered frames in HDLC). As we will discuss later, PPP does not provide any flow control. Error control is also limited to error detection.
- **Protocol:** The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.
- **Payload field:** This field carries either the user data or other information that we will discuss shortly. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte-stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.
- **FCS:** The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

Byte Stuffing

Since PPP is a byte-oriented protocol, the flag in PPP is a byte that needs to be escaped whenever it appears in the data section of the frame. The escape byte is 01111101, which means that every time the flag like pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag. Obviously, the escape byte itself should be stuffed with another escape byte.

Exercise

1. Define Data link layer and list its services. Explain the responsibilities of data link layer in the internet model.
2. Define framing and the reason for its need.
3. Explain the error detection and error correction mechanism.
4. Compare and contrast flow control and error control.

Chapter 4
NETWORK LAYER

Introduction

The network layer or layer 3 is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes. It manages device addressing, tracks the location of devices on the network, and determines the best way to move data. This means that it's up to the Network layer to transport traffic between devices that aren't locally attached. Routers, which are layer 3 devices, are specified at this layer and provide the routing services within an internetwork.

This layer contains hardware devices such as routers, bridges, firewalls and switches, but it actually creates a logical image of the most efficient communication route and implements it with a physical medium. Network layer protocols exist in every host or router. The router examines the header fields of all the IP packets that pass through it. Internet Protocol and Netware IPX/SPX are the most common protocols associated with the network layer. In the OSI model, the network layer responds to requests from the layer above it (transport layer) and issues requests to the layer below it (data link layer)

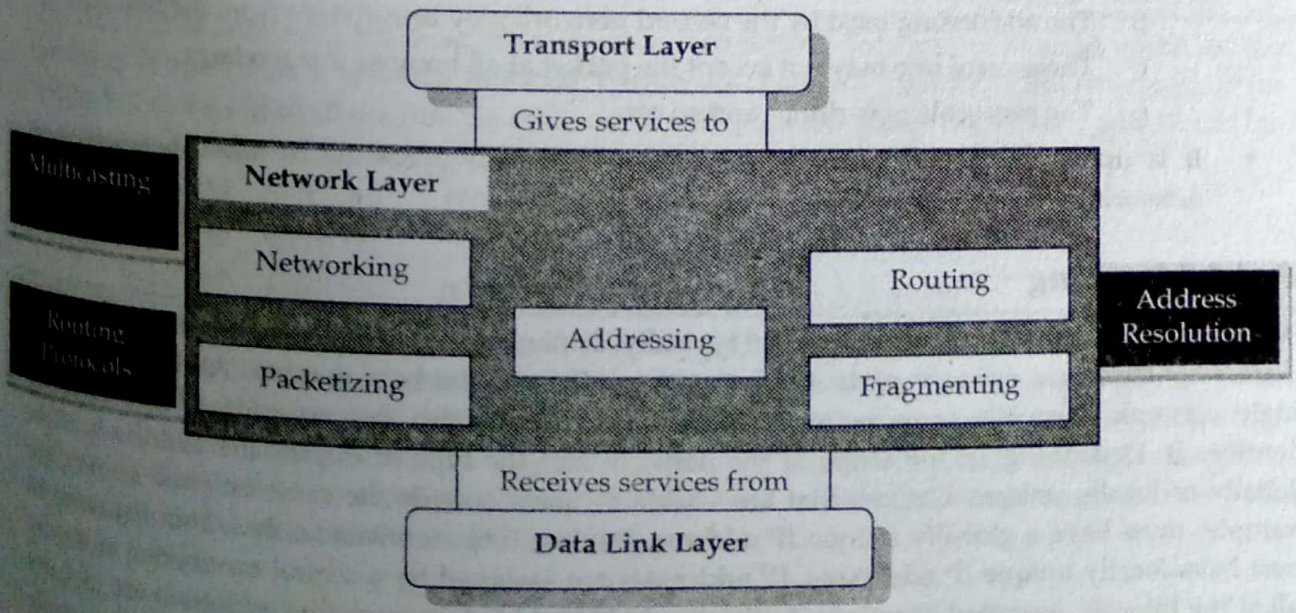


Figure 4.1: Transport layer

Working process: first, when a packet is received on a router interface, the destination IP address is checked. If the packet isn't destined for that particular router, it will look up the destination network address in the routing table. Once the router chooses an exit interface, the packet will be sent to that interface to be framed and sent out on the local network. If the router can't find an entry for the packet's destination network in the routing table, the router drops the packet.

Functions of Network Layer

1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.

Design Issues with Network Layer

- A key design issue is **determining how packets are routed from source to destination**. Routes can be based on static tables that are wired into the network and rarely changed. They can also be highly dynamic, being determined anew for each packet, to reflect the current network load.
- If **too many packets** are present in the subnet at the same time, they will get into one another's way, forming **bottlenecks**. The **control of such congestion** also belongs to the network layer.
- Moreover, the **quality of service** provided (delay, transmit time, jitter, etc) is also a network layer issue.
- When a packet has to **travel from one network to another to get to its destination**, many problems can arise such as:
    - The addressing used by the second network may be different from the first one.
    - The second one may not accept the packet at all because it is too large.
    - The protocols may differ, and so on.
- It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

IPv4 Addressing

IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number. All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it. Depending on the scope of the network and the type of device, the address is either globally or locally unique. Devices that are visible to users outside the network (web servers, for example) must have a globally unique IP address. Devices that are visible only within the network must have locally unique IP addresses. IP addresses are assigned by a central numbering authority called the Internet Assigned Numbers Authority (IANA). IANA ensures that addresses are globally unique where needed and has a large address space reserved for use by devices not visible outside their own networks. The IPv4 addressing contains the following sections:

IPv4 Classful Addressing

To provide flexibility in the number of addresses distributed to networks of different sizes, 4-octet (32-bit) IP addresses were originally divided into three different categories or classes: class A, class B, and class C. Each address class specifies a different number of bits for its network prefix and host number:

- **Class A** addresses use only the first byte (octet) to specify the network prefix, leaving 3 bytes to define individual host numbers.
- **Class B** addresses use the first 2 bytes to specify the network prefix, leaving 2 bytes to define host addresses.
- **Class C** addresses use the first 3 bytes to specify the network prefix, leaving only the last byte to identify hosts.

In binary format, with an x representing each bit in the host number, the three address classes can be represented as follows:

```
00000000 xxxxxxxx xxxxxxxx xxxxxxxx (Class A)
00000000 00000000 xxxxxxxx xxxxxxxx (Class B)
00000000 00000000 00000000 xxxxxxxx (Class C)
```

Because each bit (x) in a host number can have a 0 or 1 value, each represents a power of 2. For example, if only 3 bits are available for specifying the host number, only the following host numbers are possible:

111 110 101 100 011 010 001 000

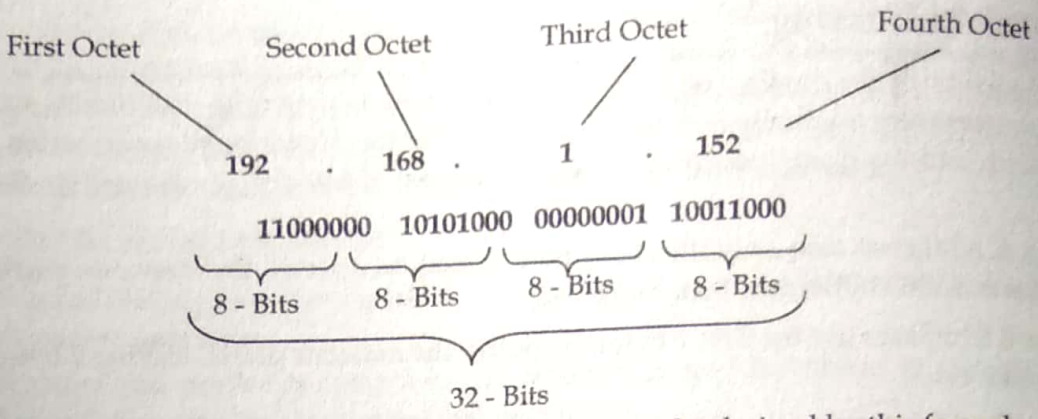
In each IP address class, the number of host-number bits raised to the power of 2 indicates how many host numbers can be created for a particular network prefix. Class A addresses have 2^{24} (or 16,777,216) possible host numbers, class B addresses have 2^{16} (or 65,536) host numbers, and class C addresses have 2^8 (or 256) possible host numbers.

IPv4 Dotted Decimal Notation

The 32-bit IPv4 addresses are most often expressed in dotted decimal notation, in which each octet (or byte) is treated as a separate number. Within an octet, the rightmost bit represents 2^0 (or 1), increasing to the left until the first bit in the octet is 2^7 (or 128). Following are IP addresses in binary format and their dotted decimal equivalents:

```
11010000 01100010 11000000 10101010 = 208.98.192.170
01110110 00001111 11110000 01010101 = 118.15.240.85
00110011 11001100 00111100 00111011 = 51.204.60.59
```

Internet protocol hierarchy contains several classes of IP addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address. Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses. The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



The number of networks and the number of hosts per class can be derived by this formula:

Number of networks = $2^{\text{network bits}}$

Number of Hosts/network = $(2^{\text{network bits}} - 2)$

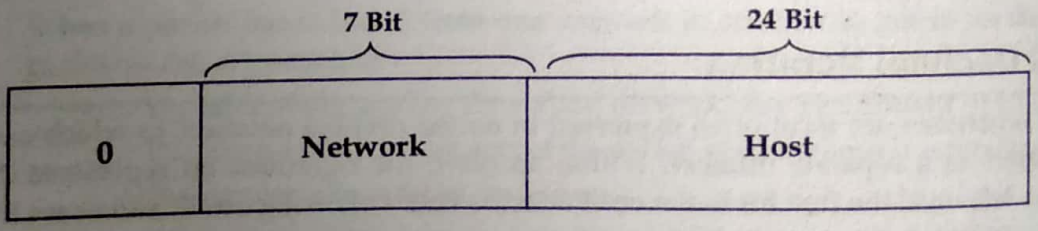
When calculating hosts' IP addresses, two IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long
- The host ID is 24 bits long

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network.



Thus the first octet ranges from 1 – 127, i.e.

00000001 - 01111111

1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses. The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2). Class A IP address format is

0NNNNNNN HHHHHHHH HHHHHHHH HHHHHHHH

Class B Address

IP addresses belonging to class B are assigned to the network that ranges from medium-sized to large-sized networks.

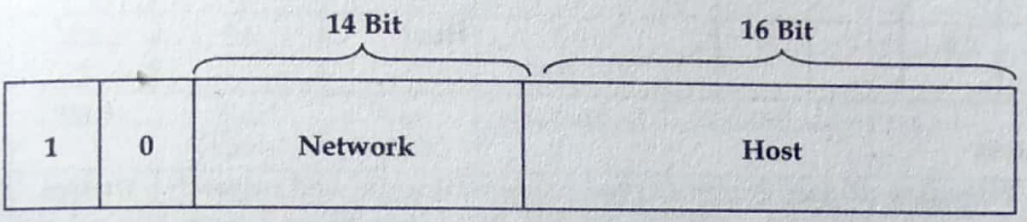
- The network ID is 16 bits long.

- The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. Class B has a total of:

2^{14} = 16384 network address

$2^{16} - 2$ = 65534 host address



Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Thus the first octet ranges from 1 – 127, i.e.

100000001 - 101111111

128 – 191

Class B IP address format is:

10NNNNNN NNNNNNNN HHHHHHHH HHHHHHHH

Class C Address

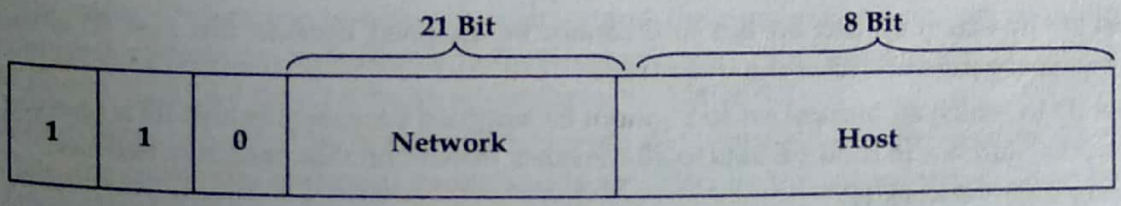
IP addresses belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long
- The host ID is 8 bits long

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

2^{21} = 2097152 network address

$2^{8} - 2$ = 254 host address



IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x. and the default subnet mask for Class C is 255.255.255.x. The first octet of Class C IP address has its first 3 bits set to 110, that is:

11000001 - 11011111

192 – 223

Class C IP address format is:

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

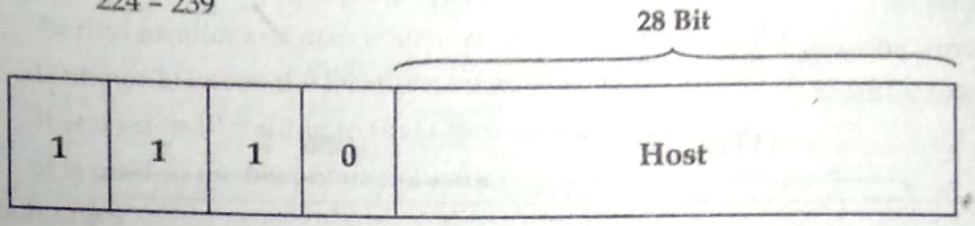
Class D Address

IP addresses belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the

address that interested hosts recognize. Class D does not have any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.

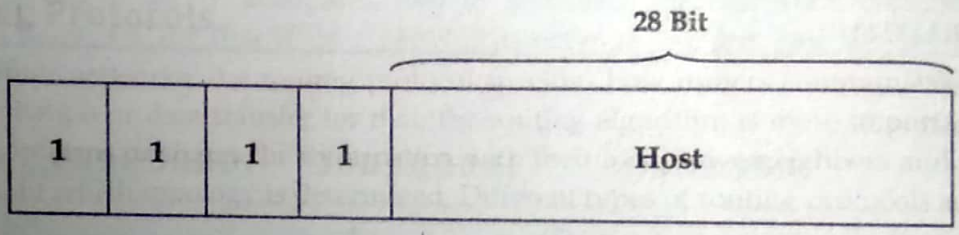
11100000 - 11101111

224 – 239



Class E Address

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Range of special IP addresses

169.254.0.0 – 169.254.0.16: Link local addresses

127.0.0.0 – 127.0.0.8: Loop-back addresses

0.0.0.0 – 0.0.0.8: used to communicate within the current network.

Rules for assigning Host ID

Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network are assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Table 4.1 Summary of Classful Addressing

Class	Leading bit	Network ID bit	Host ID bit	No. of networks	Addresses per network	Start Address	End Address
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	172.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0	239.255.255.255
CLASS E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0	255.255.255.255

Problems with Classful Addressing

The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing, and are therefore available as a single block only. Class E addresses are reserved.

Subnetting

The process of subnetting involves dividing a network up into smaller networks called subnets or sub networks. Each of these subnets has its own specific address. To create these additional networks we use a subnet mask. The subnet mask simply determines which portion of the IP address belongs to the host. The subnet address is created by dividing the host address into network address and host address.

The network address specifies the type of subnetwork in the network and the host address specifies the host of that subnet. Subnets are under local administration. As such, the outside world sees an organization as a single network and has no detailed knowledge of the organization's intema1 structure. Subnetting provides the network administrator with several benefits, including extra flexibility, more efficient use of network address and the capability to contain broadcast traffic. A given network address can be broken up into many subnetworks. For example, 172.16.1.0, 172.16.2.0, 172.16.3.0 and 172.16.4.0 are all subnets within network 171.16.0.0.

A subnet address is created by borrowing bits from the host field and designating them as subnet field. The number of bits borrowed varies and is specified by the subnet mask. Table below shows how bits are borrowed from the host address field to create the subnet address field.

Table: Subnet mask for class B address

	1st octant	2nd octant	3rd octant	4th octant
	Network	Network	Subnet	Host
Binary Representation	11111111	11111111	11111111	00000000
Dotted Decimal Representation	255. 255. 255. 0			
Bits are borrowed from the host address field to crate the subnet address field				

The subnet mask does not alter the class of the IP address; it simply "borrows" bits from the host portion and uses these to create subnets. This naturally reduces the maximum number of hosts your network can have, because you are using some of your host bits for your subnet bits.

Why use subnetting?

When a network becomes too big with too much traffic, performance can begin to suffer. Breaking the network into smaller parts can help alleviate this network congestion. A subnet allows routers to choose the right destination for packets. An Organization can use IP subnets to divide large networks for logical reasons (firewalls, etc.), or physical requirements (smaller broadcast domains etc.).In other words, routers use subnets to make routing choices. Subnetting can also improve network security. With a division between subnets, organizations can control who has access to what. With subnets, security incidents can be better contained.

How to create subnets?

Creating subnetworks is essentially the act of taking bits from the host portion of the address and reserving them to define the subnet address instead. Clearly this will result in fewer bits being available for defining your hosts, which is something you'll always want to keep in mind.

To create a subnet, we'll start by fulfilling these three steps:

1. Determine the number of required network IDs:
   - One for each LAN subnet
   - One for each wide area network connection
2. Determine the number of required host IDs per subnet:
   - One for each TCP/IP host
   - One for each router interface
3. Based on the previous requirements, create the following:
   - A unique subnet mask for your entire network
   - A unique subnet ID for each physical segment
   - A range of host IDs for each subnet

Subnet Mask

For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. This condition is met by assigning a subnet mask to each machine. A subnet mask is a 32-bit value that allows the device that's receiving IP packets to distinguish the network ID portion of the IP address from the host ID portion of the IP address. The 32-bit subnet mask is composed of 1s and0s, where the 1s represent the positions that refer to the network subnet addresses. Not all networks need subnets, and if not, it really means that they are using the default subnet mask, which is basically the same as saying that a network doesn't have a subnet address. Table below shows the default subnet masks for Classes A, B, and C.

Table 4.2 Default Subnet Mask

Class	Format	Default Subnet Mask
A	network.host.host.host	255.0.0.0
B	network.network.host.host	255.255.0.0
C	network.network.network.host	255.255.255.0

Although you can use any mask in any way on an interface, typically it's not usually good to mess with the default masks. In other words, you don't want to make a Class B subnet mask read 255.0.0.0, and some hosts won't even let you type it in. But these days, most devices will. For a Class A network, you wouldn't change the first byte in a subnet mask because it should read 255.0.0.0 at a minimum. Similarly, you wouldn't assign 255.255.255.255 because this is all 1s, which is a broadcast address. A Class B address starts with 255.255.0.0, and a Class C starts with 255.255.255.0, and for the CCNA especially, there is no reason to change the defaults.

Type of Subnetting

There are two types of Subnetting FLSM and VLSM. In FLSM, all subnets have equal number of host addresses and use same Subnet mask. In VLSM, subnets have flexible number of host addresses and use different subnet mask. FLSM is easy in implementation and simple in operation but wastes a lot of IP addresses. VLSM is hard in implementation and complex in operation but utilizes maximum IP addresses.

Classless Inter-Domain Routing (CIDR)

Another term you need to familiarize yourself with is Classless Inter-Domain Routing (CIDR). It's basically the method that Internet service providers (ISPs) use to allocate a number of addresses to a company, a home—their customers. They provide addresses in a certain block size.

When you receive a block of addresses from an ISP, what you get will look something like this: 192.168.10.32/28. This is telling you what your subnet mask is. The slash notation (/) means how many bits are turned on (1s). Obviously, the maximum could only be /32 because a byte is 8 bits and there are 4 bytes in an IP address: (4 × 8 = 32). But keep in mind that regardless of the class of address, the largest subnet mask available relevant to the Cisco exam objectives can only be a /30 because you've got to keep at least 2 bits for host bits.

Take, for example, a Class A default subnet mask, which is 255.0.0.0. This tells us that the first byte of the subnet mask is all ones (1s), or 11111111. When referring to a slash notation, you need to count all the 1 bits to figure out your mask. The 255.0.0.0 is considered a /8 because it has 8 bits that are 1s - that is, 8 bits that are turned on. A Class B default mask would be 255.255.0.0, which is a /16 because 16 bits are ones (1s): 11111111 11111111 00000000 00000000. Table 4.3 has a listing of every available subnet mask and its equivalent CIDR slash notation.

Table 4.3 Available subnet mask

Subnet Mask	CIDR Value
255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17

255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

The /8 through /15 can only be used with Class A network addresses. /16 through /23 can be used by Class A and B network addresses. /24 through /30 can be used by Class A, B, and C network addresses. This is a big reason why most companies use Class A network addresses. Since they can use all subnet masks, they get the maximum flexibility in network design.

Subnetting Class C Addressing

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 move to the right, without skipping bits. This means that the only Class C subnet masks can be the following:

Table 4.4 Class C subnet masks

Binary	Decimal Dotted	CIDR
00000000	255.255.255.0	/24
10000000	255.255.255.128	/25
11000000	255.255.255.192	/26
11100000	255.255.255.224	/27
11110000	255.255.255.240	/28
11111000	255.255.255.248	/29
11111100	255.255.255.252	/30

We can't use a /31 or /32 because, as I've said, we must have at least 2 host bits for assigning IP addresses to hosts. But this is only mostly true. Certainly we can never use a /32 because that would mean zero host bits available, yet Cisco has various forms of the IOS, as well as the new Cisco Nexus switches operating system, that support the /31 mask.

Subnetting a Class C Address-The Fast Way!

When you've chosen a possible subnet mask for your network and need to determine the number of subnets, valid hosts, and the broadcast addresses of a subnet that mask will provide, 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?
- What's the broadcast address of each subnet?
- What are the valid hosts in each subnet?

Here's how you arrive at the answers to those five big questions:

- **How many subnets?**
  2^x = number of subnets. x is the number of masked bits, or the 1s. For example, in 11000000, the number of 1s gives us 2^2 subnets. So in this example, there are 4 subnets.
- **How many hosts per subnet?**
  $2^y - 2$ = number of hosts per subnet. y is the number of unmasked bits, or the 0s. For example, in 11000000, the number of 0s gives us $2^6 - 2$ hosts, or 62 hosts per subnet. You need to subtract 2 for the subnet address and the broadcast address, which are not valid hosts.
- **What are the valid subnets?**
  256 - Subnet mask = block size, or increment number. An example would be the 255.255.255.192 mask, where the interesting octet is the fourth octet (interesting because that is where our subnet numbers are). Just use this math: **256 – 192 = 64.** The block size of a 192 mask is always 64. Start counting at zero in blocks of 64 until you reach the subnet mask value and these are your subnets in the fourth octet: 0, 64, 128, 192.
- **What's the broadcast address for each subnet?**
  Now here's the really easy part. Since we counted our subnets in the last section as 0, 64, 128, and 192, the broadcast address is always the number right before the next subnet. For example, the 0 subnet has a broadcast address of 63 because the next subnet is 64. The 64 subnet has a broadcast address of 127 because the next subnet is 128, and so on. Remember, the broadcast address of the last subnet is always 255.
- **What are the valid hosts?**
  Valid hosts are the numbers between the subnets, omitting the all-0s and all-1s. For example, if 64 is the subnet number and 127 is the broadcast address, then 65–126 is the valid host range. Your valid range is always the group of numbers between the subnet address and the broadcast address.

Practice Example Class C Address: 255.255.255.128 (/25)

Since 128 is 10000000 in binary, there is only 1 bit for subnetting and 7 bits for hosts. We're going to subnet the Class C network address 192.168.10.0.

192.168.10.0 = Network address
11111111 11111111 11111111 10000000 = Subnet mask in binary
255.255.255.128 = Subnet mask in decimal dotted

Now, let's answer our big five:

- **How many subnets?** Since 128 is 1 bit on (10000000), the answer would be $2^1 = 2$.
- **How many hosts per subnet?** We have 7 host bits off (10000000), so the equation would be $2^7 - 2 = 126$ hosts. Once you figure out the block size of a mask, the amount of hosts is always the block size minus 2. No need to do extra math if you don't need to!

- **What are the valid subnets?** 256 – 128 = 128. Remember, we'll start at zero and count in ou block size, so our subnets are 0, 128. By just counting your subnets when counting in you block size, you really don't need to do steps 1 and 2. We can see we have two subnets, an in the step before this one, just remember that the amount of hosts is always the block siz minus 2, and in this example, that gives us 2 subnets, each with126 hosts.
- **What's the broadcast address for each subnet?** The number right before the value of th next subnet is all host bits turned on and equals the broadcast address. For the zero subne the next subnet is 128, so the broadcast of the 0 subnet is 127.
- **What are the valid hosts?** These are the numbers between the subnet and broadcast addres The easiest way to find the hosts is to write out the subnet address and the broadca address, which makes valid hosts completely obvious. The following table shows the 0 an 128 subnets, the valid host ranges of each, and the broadcast address of both subnets:

Subnet (Network IP)	Usable IP Pool (first host to last host)		Broadcast IP
	First host	Last host	
192.168.10.0	192.168.10.1	192.168.10.126	192.168.10.127
192.168.10.128	192.168.10.129	192.168.10.254	192.168.10.255

Example Question: If 200.100.10.66/26 is IPv4 address then answer the following questions:

a. Is this a host, network, or broadcast address?
b. What is the subnet mask in dotted decimal?
c. What is the network address?
d. What is the broadcast address?
e. What is the first usable host address?
f. What is the last usable host address?
g. How many usable hosts are in the network?
h. What is the next available network address?

Solution:

IP address: 200.100.10.66/26

Subnet Mask: 11111111 11111111 11111111 11000000 = 255.255.255.192

Total Subnets = $2^2 = 4$

Total hosts = $2^6 = 64$

Usable hosts = $2^6 - 2 = 64 - 2 = 62$

Valid Subnets (4^{th} octet) = 256 – 192= 64

Subnet (Network IP)	Usable IP Pool (first host to last host)		Broadcast IP
	First host	Last host	
200.100.10.0	200.100.10.1	200.100.10.62	200.100.10.63
200.100.10.64	200.100.10.65	200.100.10.126	200.100.10.127
200.100.10.128	200.100.10.129	200.100.10.190	200.100.10.191
200.100.10.192	200.100.10.193	200.100.10.254	200.100.10.255

a. Is this a host, network, or broadcast address?
→It is host address
b. What is the subnet mask in dotted decimal?
→255.255.255.192
c. What is the network address?
→200.100.10.64/26
d. What is the broadcast address?
→200.100.10.127/26
e. What is the first usable host address?
→200.100.10.65/26
f. What is the last usable host address?
→200.100.10.126/26
g. How many usable hosts are in the network?
→62
h. What is the next available network address?
→200.100.10.128/26

What do we know?

When you see a subnet mask or slash notation (CIDR), you should know the following:

CIDR	Net Mask	Bits	Block size	Remark
/25	128	x= 1, y=7	128	2 subnets, each with 126 hosts
/26	192	x= 2, y=6	64	4 subnets, each with 62 hosts
/27	224	x= 3, y=5	32	8 subnets, each with 30 hosts
/28	240	x= 4, y=4	16	16 subnets, each with 14 hosts
/29	248	x= 5, y=3	8	32 subnets, each with 6 hosts
/30	252	x= 6, y=2	4	64 subnets, each with 2 hosts

Regardless of whether you have a Class A, Class B, or Class C address, the /30 mask will provide you with only two hosts, ever. As suggested by Cisco, this mask is suited almost exclusively for use on point-to-point links.

Subnetting Class B Addresses

Before we dive into this, let's look at all the possible Class B subnet masks first. Notice that we have a lot more possible subnet masks than we do with a Class C network address:

Table 4.5 Class B subnet masks

Binary (3rd and 4th octet)	Decimal Dotted	CIDR
00000000 00000000	255.255.0.0	/16
10000000 00000000	255.255.128.0	/17
11000000 00000000	255.255.192.0	/18
11100000 00000000	255.255.224.0	/19
11110000 00000000	255.255.240.0	/20
11111000 00000000	255.255.248.0	/21

11111100 00000000	255.255.252.0	/22
11111110 00000000	255.255.254.0	/23
11111111 00000000	255.255.255.0	/24
11111111 10000000	255.255.255.128	/25
11111111 11000000	255.255.255.192	/26
11111111 11100000	255.255.255.224	/27
11111111 11110000	255.255.255.240	/28
11111111 11111000	255.255.255.248	/29
11111111 11111100	255.255.255.252	/30

The process of subnetting a Class B network is pretty much the same as it is for a Class C, except that you have more host bits and you start in the third octet. Use the same subnet numbers for the third octet with Class B that you used for the fourth octet with Class C, but add a zero to the network portion and a 255 to the broadcast section in the fourth octet.

Example Question: If 172.16.0.0/17 is IPv4 address then answer the following questions:

a. Is this a host, network, or broadcast address?
b. What is the subnet mask in dotted decimal?
c. What is the network address?
d. What is the broadcast address?
e. What is the first usable host address?
f. What is the last usable host address?
g. How many usable hosts are in the network?
h. What is the next available network address?

Solution:

IP address: If 172.16.0.0/17

Subnet Mask: 11111111 11111111 10000000 00000000 = 255.255.128.0

Total Subnets = $2^1 = 2$

Total hosts = $2^{15} = 32768$

Usable hosts = $2^{15} - 2 = 32768 - 2 = 32766$

Valid Subnets (3^{rd} octet) = 256 – 128= 128

Valid Subnets (4^{th} octet) = 256 – 0= 256

Subnet (Network IP)	Usable IP Pool (first host to last host)		Broadcast IP
	First host	Last host	
172.16.0.0	172.16.0.1	172.16.127.254	172.16.127.255
172.16.128.0	172.16.128.1	172.16.255.254	172.16.255.255

a. **Is this a host, network, or broadcast address?**
→It is network address
b. **What is the subnet mask in dotted decimal?**

→255.255.128.0

c. What is the network address?
→172.16.0.0/17

d. What is the broadcast address?
→172.16.127.255/17

e. What is the first usable host address?
→172.16.0.1/17

f. What is the last usable host address?
→172.16.127.254/17

g. How many usable hosts are in the network?
→32766

h. What is the next available network address?
→172.16.128.0/17

Subnetting Class A Address

You don't go about Class A subnetting any differently than Classes B and C, but there are24 bits to play with instead of the 16 in a Class B address and the 8 in a Class C address. Let's start by listing all the Class A masks:

Table 4.6 Class A subnet mask

Binary (2nd, 3rd and 4th octet)	Subnet Mask	CIDR Value
00000000 00000000 00000000	255.0.0.0	/8
10000000 00000000 00000000	255.128.0.0	/9
11000000 00000000 00000000	255.192.0.0	/10
11100000 00000000 00000000	255.224.0.0	/11
11110000 00000000 00000000	255.240.0.0	/12
11111000 00000000 00000000	255.248.0.0	/13
11111100 00000000 00000000	255.252.0.0	/14
1111110 00000000 00000000	255.254.0.0	/15
11111111 00000000 00000000	255.255.0.0	/16
11111111 10000000 00000000	255.255.128.0	/17
11111111 11000000 00000000	255.255.192.0	/18
11111111 11100000 00000000	255.255.224.0	/19
11111111 11110000 00000000	255.255.240.0	/20
11111111 11111000 00000000	255.255.248.0	/21
11111111 11111100 00000000	255.255.252.0	/22
11111111 11111110 00000000	255.255.254.0	/23
11111111 11111111 00000000	255.255.255.0	/24
11111111 11111111 10000000	255.255.255.128	/25

11111111 11111111 11000000	255.255.255.192	/26
11111111 11111111 11100000	255.255.255.224	/27
11111111 11111111 11110000	255.255.255.240	/28
11111111 11111111 11111000	255.255.255.248	/29
11111111 11111111 11111100	255.255.255.252	/30

That's it. You must leave at least 2 bits for defining hosts. I hope you can see the pattern by no Remember, we're going to do this the same way as a Class B or C subnet. It's just that, again, simply have more host bits and we just use the same subnet numbers we used with Class B and but we start using these numbers in the second octet. However, the reason Class A addresses are popular to implement is because they give the most flexibility.

Example Question: If 10.1.0.0/9 is IPv4 address then find all network address, broadcast address, usable host, last usable host, total no. of subnets, total no. of hosts, valid subnets.

Solution:

IP address: If 10.1.0.0/9

Subnet Mask: 11111111 10000000 00000000 00000000 = 255.128.0.0

Total Subnets = $2^1 = 2$

Total hosts = $2^{23} = 8388608$

Usable hosts = $2^{23} - 2 = 8388606$

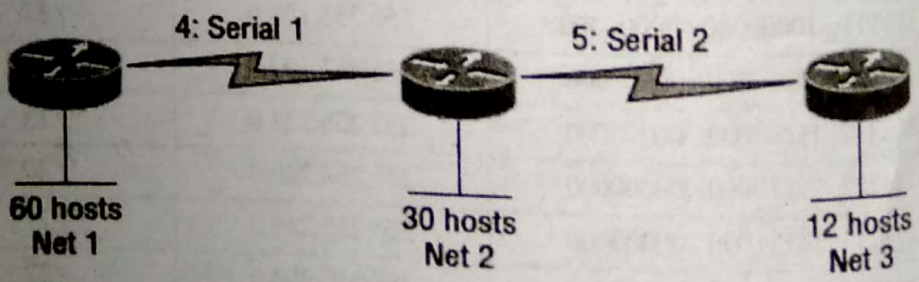
Valid Subnets (2^{nd}octet) = 256 – 128 = 128

Valid Subnets (3^{rd} octet) = 256 – 0 = 256

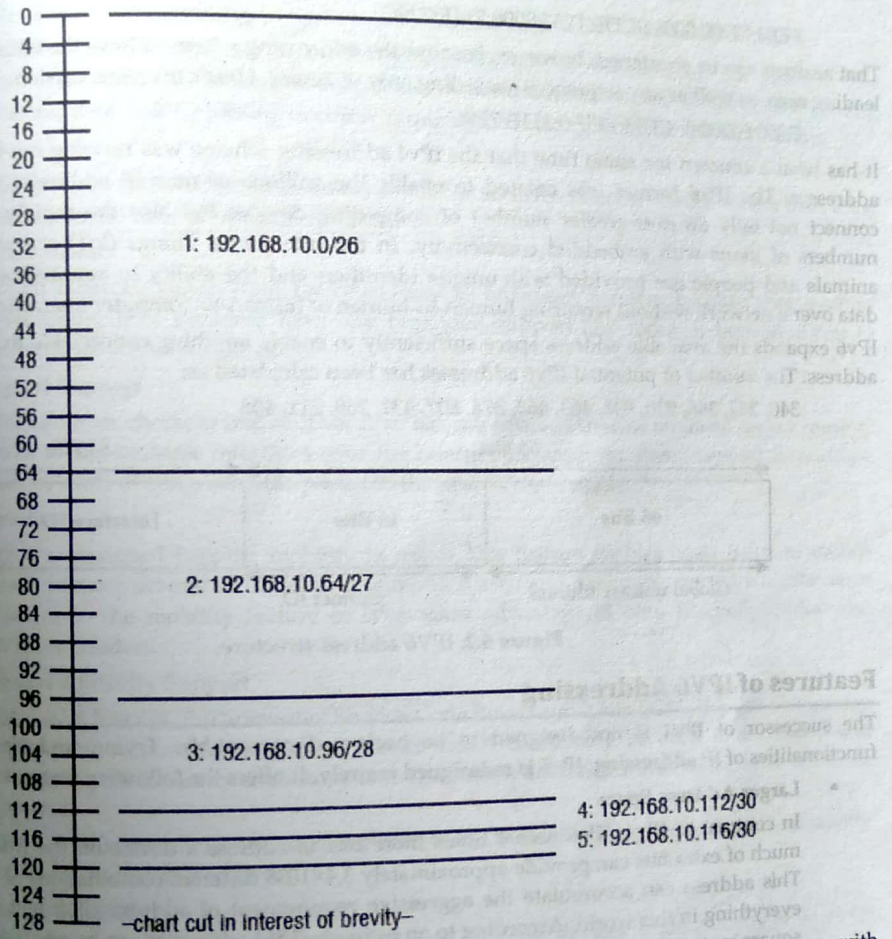
Valid Subnets (4^{th} octet) = 256 – 0 = 256

Subnet (Network IP)	Usable IP Pool (first host to last host)		Broadcast IP
	First host	Last host	
10.0.0.0	10.0.0.1	10.127.255.254	10.127.255.255
10.128.0.0	10.128.0.1	10.255.255.254	10.255.255.255

Example: VLSM



Solution:



This solution began at subnet 0, and we used the block size of 64. Clearly, we didn't have to go with a block size of 64 because we could've chosen a block size of 4 instead. But we didn't because we usually like to start with the largest block size and move to the smallest. With that done, we have added the block sizes of 32 and 16 as well as the two block sizes of 4. This solution is optimal because it still leaves lots of room to add subnets to this network.

IPv6 Addressing and its Features

Internet Protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on the Network Layer (Layer-3). Along with its offering of an enormous amount of logical address space, this protocol has ample features to which address the shortcoming of IPv4.

An IPv6 address is a 128-bit alphanumeric string that identifies an endpoint device in the Internet Protocol Version 6 (IPv6) addressing scheme.

In more precise terms, an IPv6 address is 128 bits long and is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits and the groups are separated by colons. Here's an example of a full IPv6 address:

FE80:CD00:0000:0CDE:1257:0000:211E:729C

That address can be shortened, however, because the addressing scheme allows the omission of any leading zero, as well as any sequences consisting only of zeroes. Here's the short version:

FE80:CD00:0: CDE: 1257:0:211E:729C

It has been a concern for some time that the IPv4 addressing scheme was running out of potential addresses. The IPv6 format was created to enable the trillions of new IP addresses required to connect not only an ever-greater number of computing devices but also the rapidly expanding numbers of items with embedded connectivity. In the Internet of Things (IoT) scenario, objects, animals and people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction.

IPv6 expands the available address space sufficiently to enable anything conceivable to have an IP address. The number of potential IPv6 addresses has been calculated as:

340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456

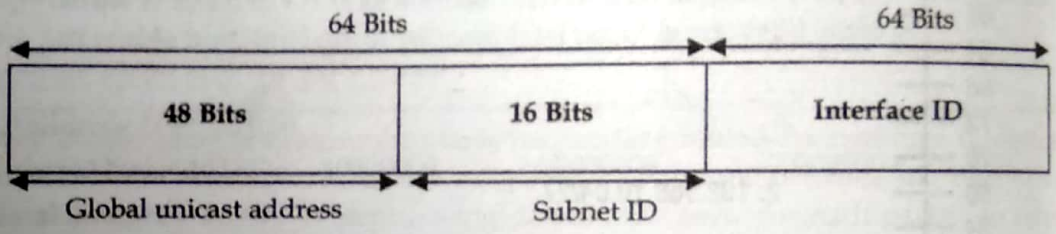


Figure 4.2: IPV6 address structure.

Features of IPV6 Addressing

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:

- **Larger Address Space**

  In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×1038 different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

- **Simplified Header**

  IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 provided the fact that IPv6 address is four times longer.

- **End-to-end Connectivity**

  Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.

- **Auto-configuration**

  IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.

Simplified information contained in the first part of the header is adequate for a router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.

- **IPSec**
  Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.
- **No Broadcast**
  Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.
- **Anycast Support**
  This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.
- **Mobility**
  IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.
- **Enhanced Priority Support**
  IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it.
  In IPv6, Traffic class and Flow label are used to tell the underlying routers how to efficiently process the packet and route it.
- **Smooth Transition**
  Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This mechanism saves IP addresses and NAT is not required. So devices can send/receive data among each other, for example, VoIP and/or any streaming media can be used much efficiently.
  Other fact is, the header is less loaded, so routers can take forwarding decisions and forward them as quickly as they arrive.
- **Extensibility**
  One of the major advantages of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

IPv4 Datagram Formats

Packets in the network (internet) layer are called datagrams. A datagram is a variable-length packet consisting of two parts: **header and data**. The header is 20 to 60 bytes in length and contains information essential to routing and delivery. It is customary in TCP/IP to show the header in 4-byte sections. The following Figure shows the IP datagram format.

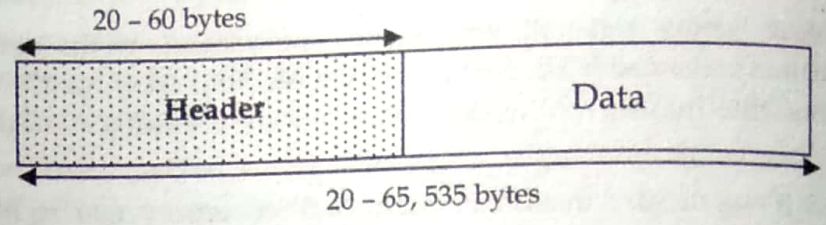


Figure 4.3: IP Datagram

Version (4 Bits)	Header length (4 Bits)	Type of service (8 Bits)	Total length (16 Bits)
Identification (16 Bits)		Flags (3 Bits)	Fragmentation offset (13 Bits)
Time to Live (8 Bits)	Upper layer protocol (8 Bits)		Header checksum (16 Bits)
Source IP address (16 Bits)			
Destination IP address (16 Bits)			
Options + Padding (0 to 40 bytes)			
Data (16 Bits)			

Figure 4.4 Header format of IPv4

Version Number

These 4 bits specify the IP protocol version of the datagram. By looking at the version number, the router can determine how to interpret the remainder of the IP datagram. Different versions of IP use different datagram formats.

Header Length

Because an IPv4 datagram can contain a variable number of options (which are included in the IPv4 datagram header), these 4 bits are needed to determine where in the IP datagram the data actually begins. Most IP datagrams do not contain options, so the typical IP datagram has a 20-byte header.

Type of Service

The type of service (TOS) bits were included in the IPv4 header to allow different types of IP datagrams (for example, datagrams particularly requiring low delay, high throughput, or reliability) to be distinguished from each other. For example, it might be useful to distinguish real-time datagrams from non-real-time traffic (for example, FTP). The specific level of service to be provided is a policy issue determined by the router's administrator.

Datagram Length

This is the total length of the IP datagram (header plus data), measured in bytes. Since this filed is 16 bits long, the theoretical maximum size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 1,500 bytes.

Length of data = total length - header length

Identification

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

Flags

As required by the network resources, if IP Packet is too large to handle, these flags tells if they can be fragmented or not. The first bit is reserved (not used). The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If its value is 0, the datagram can be fragmented if necessary. The third bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment. If its value is 0, it means this is the last or only fragment.

Fragment Offset

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

Time-to-live

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

Protocol

This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport-layer protocol to which the data portion of this IP datagram should be passed. For example, a value of 6 indicates that the data portion is passed to TCP, while a value of 17 indicates that the data is passed to UDP.

Header Checksum

This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.

Source Address

This 32-bit field define the address of the Sender (or source) of the packet.

Destination Address

This 32-bit field define the address of the Receiver (or destination) of the packet.

Options

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

Data (Payload)

Finally, we come to the last and most important field. In most circumstances, the data field of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination. However, the data field can carry other types of data, such as ICMP messages.

Problem no 1: An IP packet has arrived with the first 8 bits as shown: 01000010

The receiver discards the packet. Why?

Solution: There is an error in this packet. The 4 left-most bits (0100) show the version, which is correct. The next 4 bits (0010) show the wrong header length (2* 4 = 8). The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

Problem no 2: In an IP packet, the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet?

Solution: The HLEN value is 8, which means the total number of bytes in the header is 8* 4 or 32 bytes. The first 20 bytes are the base header; the next 12 bytes are the options.

Problem no 3: In an IP packet, the value of HLEN is 516 and the value of the total length field is 002816. How many bytes of data are being carried by this packet?

Solution: The HLEN value is 5, which means the total number of bytes in the header is 5* 4 or 20 bytes (no options). The total length is 40 bytes, which means the packet is carrying 20 bytes of data (40 - 20).

Problem no 4: An IP packet has arrived with the first few hexadecimal digits as shown: 45000028000100000102. How many hops can this packet travel before being dropped? The data belong to what upper layer protocol?

Solution: To find the time-to-live field, we skip 8 bytes (16 hexadecimal digits). The time-to-live field is the ninth byte, which is 01. This means the packet can travel only one hop. The protocol field is the next byte (02), which means that the upper layer protocol is IGMP.

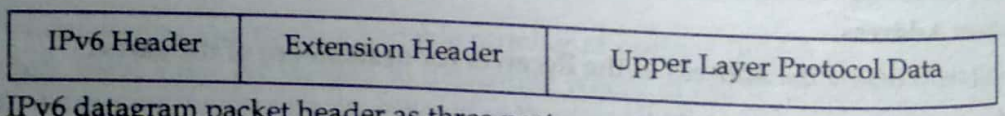
Problem no 5: A packet has arrived in which the offset value is 100, the value of HLEN is 5 and the value of the total length field is 100. What is the number of the first byte and the last byte?

Solution: The first byte number is 100 × 8 = 800. The total length is 100 bytes and the header length is 20 bytes (5 × 4), which means that there are 80 bytes in this datagram. If the first byte number is 800, the last byte number must be 879.

IPv6 Datagram Formats

An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

IPv6 has a much simpler packet header compared with IPv4, by including only the information needed for forwarding the IP datagram. IPv4 has a fixed length header of size 40 bytes. Fixed length IPv6 header allows the routers to process the IPv6 datagram packets more efficiently. The following figure shows the structure of IPv6 datagram packet.



We may divide IPv6 datagram packet header as three parts.

- IPv6 datagram packet header
- Extension Header
- Upper Layer Protocol Data.

IPv6 datagram packet has also extension headers of varying lengths. If extension headers are present in IPv6 datagram packet, a Next Header field in the IPv6 header points the first extension header. Each extension header contains another Next Header field, pointing the next extension header. The last IPv6 datagram packet extension header points the upper layer protocol header (Transmission

Control Protocol (TCP), User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMPv6)). There is no '**options**' in IPv6 datagram packet header, which was present in IPv4 header.

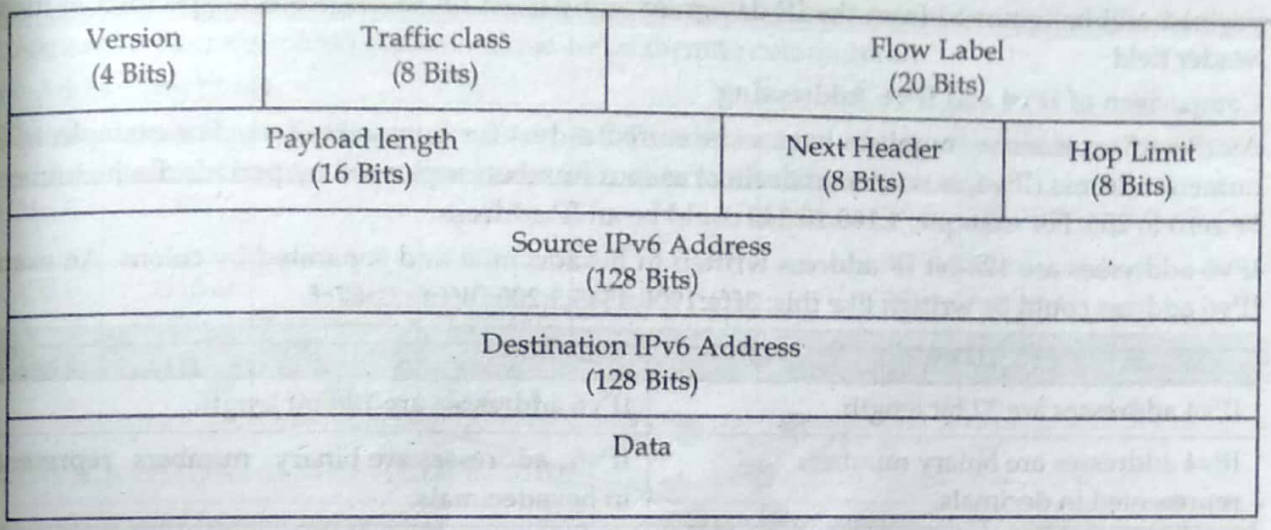


Figure 4.5: Header format of IPv6

Version (4-bits)

It represents the version of Internet Protocol, i.e. 0110.

Traffic Class (8-bits)

These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

Flow Label (20-bits)

This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.

Payload Length (16-bits)

This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.

Next header (8-bits)

This field identifies the protocol to which the contents (data field) of this datagram will be delivered (for example, to TCP or UDP). The filed uses the same values as the protocol field in the IPv4 header.

Hop Limit (8-bits)

This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.

Source Address (128-bits)

This field indicates the address of originator of the packet.

Destination Address (128-bits)

This field provides the address of intended recipient of the packet.

Data

This is the payload portion of the IPv6 datagram. When the datagram reaches its destination, the payload will be removed from the IP datagram and passed on to the protocol specified in the next header field.

Comparison of IPv4 and IPv6 Addressing

An IP address is binary numbers but can be stored as text for human readers. For example, a 32-bit numeric address (IPv4) is written in decimal as four numbers separated by periods. Each number can be zero to 255. For example, **1.160.10.240** could be an IP address.

IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons. An example IPv6 address could be written like this: **3ffe:1900:4545:3:200:f8ff:fe21:67cf**.

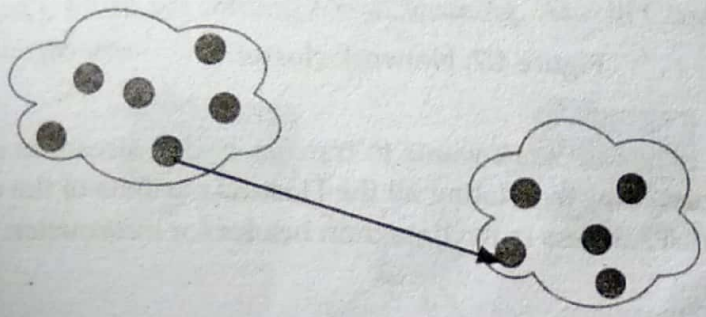
IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPSec support is only optional.	Inbuilt IPSec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.
No packet flow identification.	Packet flow identification is available within the IPv6 header using the Flow Label field.
Checksum field is available in IPv4 header	No checksum field in IPv6 header.
Options fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	Broadcast messages are not available. Instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality.
Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required to configure IPv4 addresses.	Auto-configuration of addresses is available.
It can generate 4.29 x 109 addresses.	It can produce quite a large number of addresses, i.e., 3.4 x 1038.
It can generate 4.29 x 109 addresses.	It can produce quite a large number of addresses, i.e., 3.4 x 1038.

Example Addresses: Unicast, Multicast and Broadcast

IPv4 supports three different types of addressing modes namely unicast, multicast and broadcast. The cast term here signifies some data (stream of packets) is being transmitted to the recipient from client side over the communication channel that helps them to communicate.

Unicast Addressing Mode

In this mode, data is sent only to one destined host. The destination address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server.



Network B

This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short you can term it as a one-to-one transmission. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream (data packets) to the device with IP address 20.12.4.2 in the other network, and then unicast comes into picture. This is the most common form of data transfer over the networks.

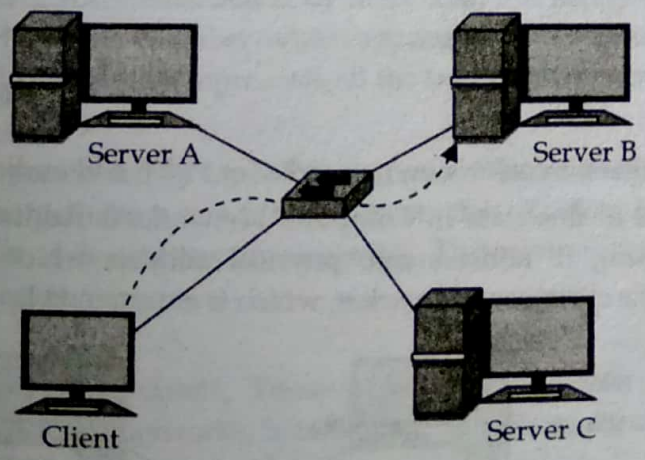


Figure: 4.6: Unicast addressing

Broadcast Addressing Mode

Broadcasting transfer (one-to-all) techniques can be classified into two types:

Limited Broadcasting

Suppose you have to send stream of packets to all the devices over the network that you reside, this broadcasting comes handy. For this to achieve, it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as limited broadcast address in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.

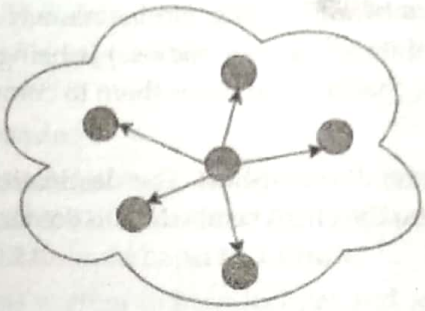
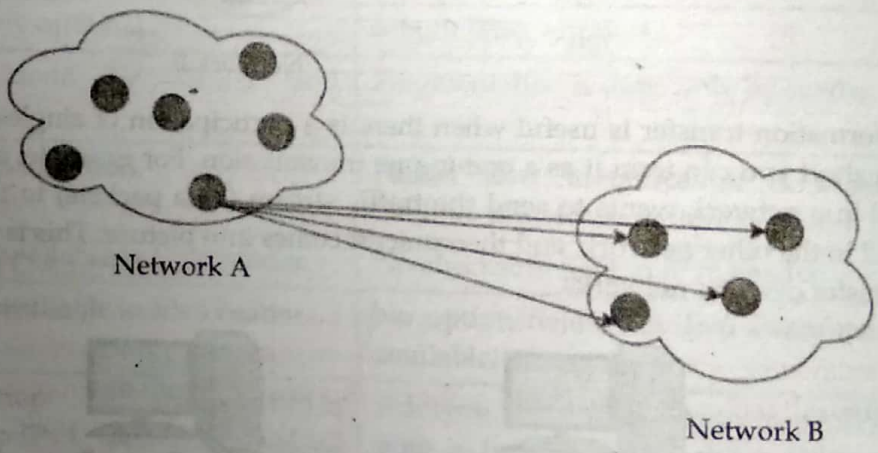


Figure 4.7: Network cluster

Direct Broadcasting

This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1, referred as Direct Broadcast Address in the datagram header for information transfer.



This mode is mainly utilized by television networks for video and audio distribution.

One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) that is used for resolving IP address into physical address which is necessary for underlying communication. Here the client sends a packet, which is entertained by all the Servers:

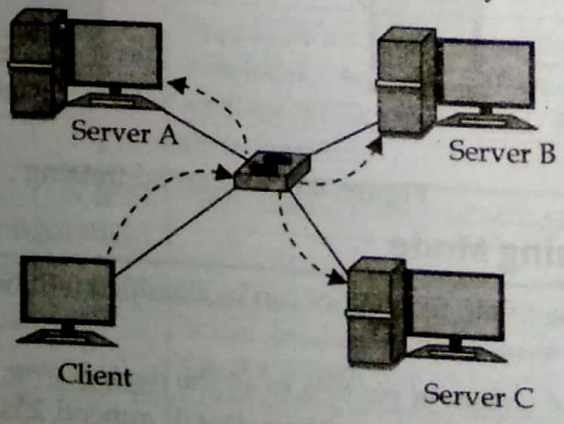


Figure 4.8: Direct broadcasting

Multicast Addressing Mode

This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.

In multicasting, one or more senders and one or more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server's direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also in Classful IP addressing **Class D** is reserved for multicast groups.

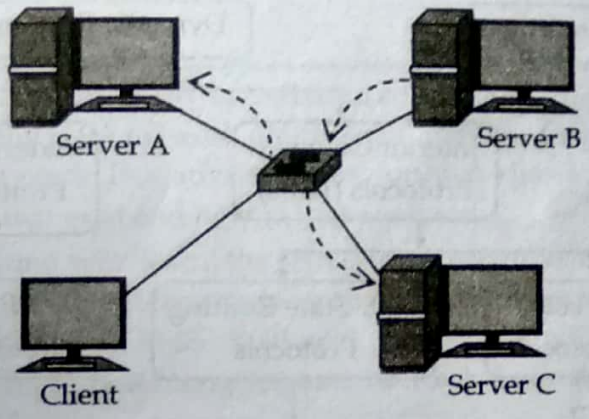


Figure 4.9: Multicast addressing.

Here a server sends packets which are entertained by more than one server. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

Routing

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another. Routing is the path that network data or a packet takes to reach its destination on a network. The network router is what decides the best route for each network packet.

Types of Routing

Routing protocols were created for routers. These protocols have been designed to allow the exchange of routing tables, or known networks, between routers. There are a lot of different routing protocols, each one designed for specific network sizes.

Two main types of routing:

- Static routing
- Dynamic routing

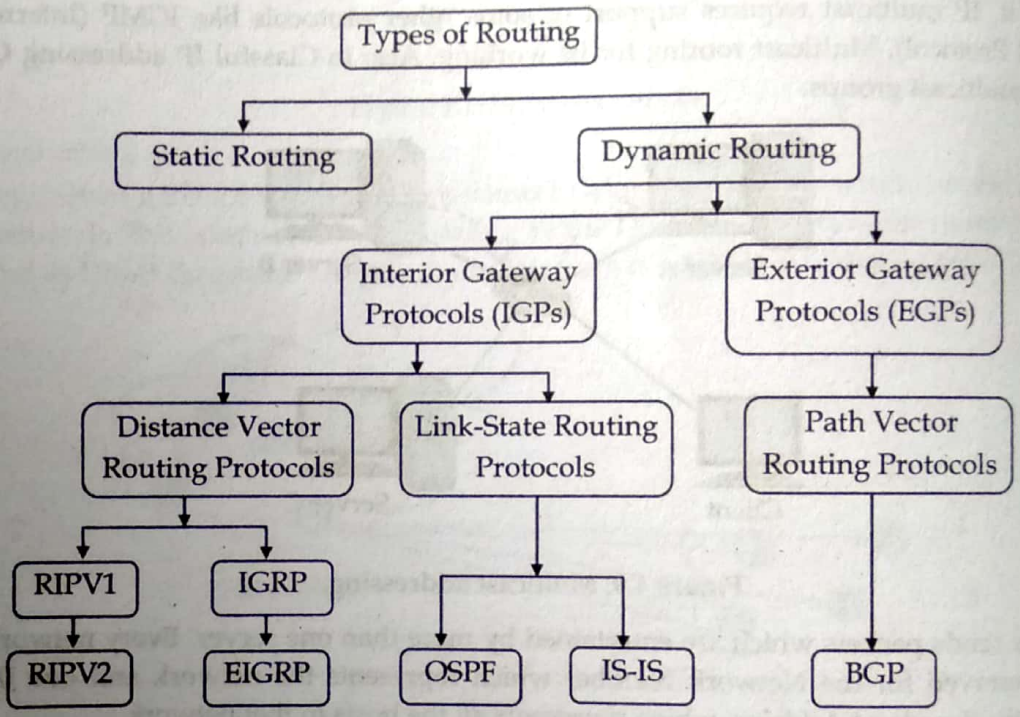
The router learns about remote networks from neighbor routers or from an administrator. The router then builds a routing table. If the network is directly connected then the router already knows how to get to the network. If the networks are not attached, the router must learn how to get to the remote network with either static routing (administrator manually enters the routes in the router's table) or dynamic routing (happens automatically using routing protocols like EIGRP, OSPF, etc.).

The routers then update each other about all the networks they know. If a change occurs e. g a router goes down, the dynamic routing protocols automatically inform all routers about the change. If static

routing is used, then the administrator has to update all changes into all routers and therefore routing protocol is used.

There are 3 types of Dynamic routing protocols, these are differing by the way that discover and make calculations about routes;

- Distance Vector
- Link State
- Hybrid



Static vs. Dynamic Routing

Static Routing

Static routing is not really a routing protocol. Static routing is simply the process of manual entering routes into a device's routing table via a configuration file that is loaded wh the routing device starts up. As an alternative, these routes can be entered by a netwo administrator who configures the routes manually. Since these manually configured routes do change after they $A = \pi r^2$ configured (unless a human changes them) they are called 'static' route Static routing is the simplest form of routing, but it is a manual process.

Use static routing when you have very few devices to configure and when you know the routes w probably never change. Static routing also does not handle failures in external networks well becau any route that is configured manually must be updated or reconfigured manually to fix or repair a lost connectivity.

Static Routing Advantages and Disadvantages

Advantages

- Easily implemented in a small network.
- No overheads are produced on router CPU.
- Secure because the routes are managed statically.

- It is predictable as the route to the destination is fixed.
- Extra resources (such as CPU and memory) are not required as update mechanisms are not needed.
- Bandwidth usage is not required between routers.

Disadvantages

- Unsuitable for complex topologies and large networks.
- Large networks increase configuration complexity and time consumption.
- Link failure can hinder traffic rerouting.
- The administrator must be extra careful while configuring the routes.

Dynamic Routing

Dynamic routing protocols are supported by software applications running on the routing device (the router) which dynamically learn network destinations and how to get to them and also advertise those destinations to other routers. This advertisement function allows all the routers to learn about all the destination networks that exist and how to those networks.

A router using dynamic routing will 'learn' the routes to all networks that are directly connected to the device. Next, the router will learn routes from other routers that run the same routing protocol (RIP, RIP2, EIGRP, OSPF, IS-IS, BGP etc). Each router will then sort through its list of routes and select one or more best routes for each network destination the router knows or has learned.

Dynamic routing protocols will then distribute this best route information to other routers running the same routing protocol, thereby extending the information on what networks exist and can be reached. This gives dynamic routing protocols the ability to adapt to logical network topology changes, equipment failures or network outages on the fly..

Dynamic Routing Advantages and Disadvantages

Advantages

- Suitable for all the topologies.
- Network size doesn't affect the router operations.
- Topologies are adapted automatically to reroute the traffic.

Disadvantages

- Initially, it could be complicated to implement.
- The broadcasting and multicasting of routing updates make it less secure.
- Routes rely on current topologies.
- Additional resources are required such as CPU, memory and link bandwidth.

Key Differences between Static and Dynamic Routing

- The routers are configured manually, and the table is also created manually in static routing whereas in dynamic routing the configuration and table creation is automatic and router driven.
- In static routing, the routes are user-defined while in dynamic routing the routes are updated as topology changes.
- Static routing does not employ complex algorithms. As against, dynamic routing uses the complex algorithm for calculating shortest path or route.

- Dynamic routing is suitable for large networks where the number of hosts is high. Conversely, static routing can be implemented in a small network.
- When a link fails in static routing, the rerouting is discontinued and requires manual intervention to route traffic. In contrast, link failure in dynamic routing does not disrupt rerouting.
- The message broadcast and multicast in dynamic routing makes it less secure. On the other hand, static routing does not involve advertisement which makes it more secure.
- Dynamic routing involves protocols such as RIP, EIGRP, BGP, etc. Inversely, static routing does not require such protocols.
- Static routing does not need any additional resources while dynamic routing requires additional resources such as memory, bandwidth, etc.

Unicast vs. Multicast

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.

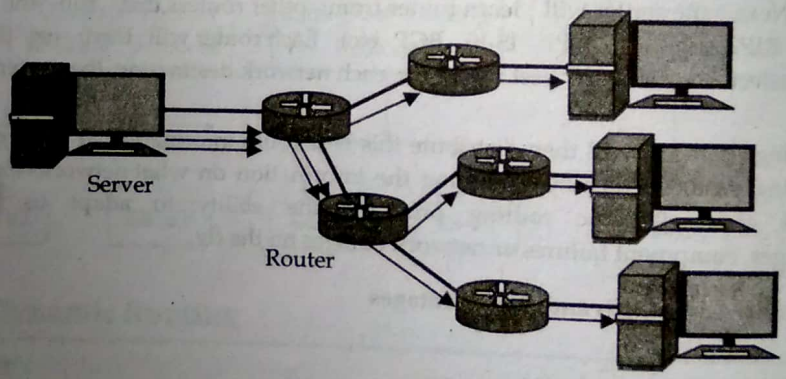


Figure 4.10: Unicast

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing the data is sent to only nodes which wants to receive the packets.

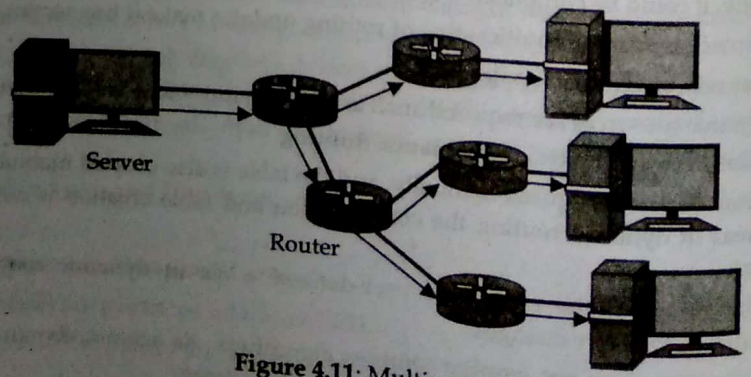


Figure 4.11: Multicast

The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping. Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

Key Differences between Unicast and Multicast

- The basic difference that distinguishes unicast from multicast is that in unicast, there is only one sender and only one receiver. But, in multicast there is a single sender but, multiple receivers.
- When we want to send the data to multiple people then using unicast will waste lots of bandwidth but, multicasting will utilize the bandwidth more efficiently.
- Unicast does not perform well while streaming media whereas; multicast does not perform well across large networks.
- Unicast is one to one mapping whereas, multicast is one-to-many mapping.
- An example of unicast is surfing web or transferring a file whereas, multicast examples are multimedia delivery, stock exchange.

Link State vs. Distance Vector dynamic routing protocol

Distance Vector Routing Protocols

It is a dynamic routing algorithm in which each router computes distance between itself and each possible destination i.e. its immediate neighbors. The router shares its knowledge about the whole network to its neighbors and accordingly updates table based on its neighbors. The sharing of information with the neighbors takes place at regular intervals. It makes use of Bellman Ford Algorithm for making routing tables.

The vector shows the direction to that specific network. Distance vector protocols send their entire routing table to directly connected neighbors. Examples of distance vector protocols include RIP - Routing Information Protocol and IGRP - Interior Gateway Routing Protocol.

Link State Routing Protocols

It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network. A router sends its information about its neighbors only to all the routers through flooding. Information sharing takes place only whenever there is a change. It makes use of Dijkstra's Algorithm for making routing tables. Link state protocols are also called shortest-path-first protocols. Link state routing protocols have a complete picture of the network topology. Hence they know more about the whole network than any distance vector protocol. Three separate tables are created on each link state routing enabled router. One table is used to hold details about directly connected neighbors, one is used to hold the topology of the entire internetwork and the last one is used to hold the actual routing table.

Link state protocols send information about directly connected links to all the routers in the network. Examples of Link state routing protocols include OSPF - Open Shortest Path First and ARE-IS - Intermediate System to Intermediate System.

Comparison between Distance Vector Routing and Link State Routing

If all routers were running a Distance Vector protocol, the path or route chosen would be from A to B directly over the ISDN serial link, even though that link is about 10 times slower than the indirect route from A→C→D →B.

A Link State protocol would choose the A→ C→ D→ B path because it's using a faster medium (100 Mb Ethernet). In this example, it would be better to run a Link State routing protocol, but if all the links in the network are the same speed, then a Distance Vector protocol is better.

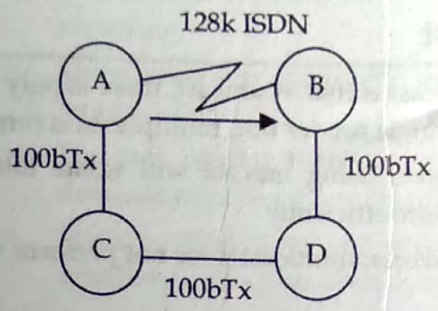


Figure 4.12: Distance Vector

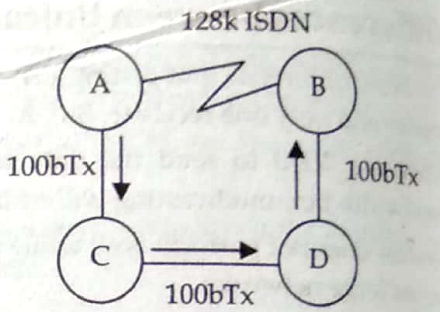


Figure 4.13: Link State

Distance Vector Routing	Link State Routing
Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
Based on local knowledge since it updates table based on information from neighbors.	Based on global knowledge i.e. it have knowledge about entire network.
Make use of Bellman Ford algorithm	Make use of Dijkstra's algorithm.
Traffic is less	Traffic is more
Converges slowly i.e. good news spread fast and bad news spread slowly.	Converges faster.
Count to infinity problem	No count to infinity problem.
Persistent looping problem i.e. loop will there forever.	No persistent loops, only transient loops.
Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.
Configurations for distance vector routing is easy	Configurations for link state routing is difficult.
It doesn't has hierarchical structure	It has hierarchical structure
Utilization of CPU and memory in distance vector routing is lower than link state routing.	Utilization of CPU and memory in link state routing is faster than distance vector.

Interior vs. exterior dynamic routing

The names interior and exterior are very descriptive. Interior routing protocols are designed for use within a contained network of limited size, whereas exterior routing protocols are designed to link multiple networks together. They can be used in combination in order to simplify network administration. For example, a network can be built with only border routers of a network running the exterior routing protocol, while all the routers on the network run the interior protocol, which prevents them from connecting outside the network without passing through the border. Exterior routers in such a configuration must have both exterior and interior protocols, to communicate with

the interior routers and outside the network. Nearly all routing protocols are interior routing protocols. Only BGP is commonly used as an exterior routing protocol.

You may see interior gateway protocol (IGP) used to refer to interior routing protocols, and exterior gateway protocol (EGP) used to refer to interior routing protocols.

Path Computation Algorithms

Multipath computation algorithms are useful to enable multipath routing and so providing reliability and efficiency. According to the objective (e.g., load balancing or fast rerouting) and the forwarding context (e.g., hop by hop, tunneling...), there exists several shortest paths algorithms to perform multiple paths computation. In order to evaluate several existing approaches and algorithms, we have developed a tool analyzing a bunch of pertinent indicators (e.g., the computation time, the coverage...). Our tool allows for analyzing various path computation methods depending on a large set of parameters.

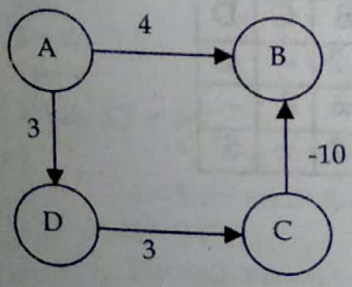
Bellman Ford Algorithm

The **Bellman–Ford algorithm** is an algorithm that computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph. It is slower than Dijkstra's algorithm for the same problem, but more versatile, as it is capable of handling graphs in which some of the edge weights are negative numbers.

Bellman-Ford algorithm returns a Boolean value indicating whether or not there is a negative-weight cycle that is reachable from the source. If there is such a cycle, the algorithm indicates that no solution exists. If there is no such cycle, the algorithm produces the shortest paths and their weights.

The algorithm initializes the distance to the source to 0 and all other nodes to infinity. Then for all edges, if the distance to the destination can be shortened by taking the edge, the distance is updated to the new lower value. At each iteration i that the edges are scanned, the algorithm finds all shortest paths of at most length i edges. Since the longest possible path without a cycle can be v-1 edges, the edges must be scanned v-1 times to ensure the shortest path has been found for all nodes. A final scan of all the edges is performed and if any distance is updated then a path of length |v| edges has been found which can only occur if at least one negative cycle exists in the graph.

Example: Find shortest path of following graph by using Bellman Ford algorithm

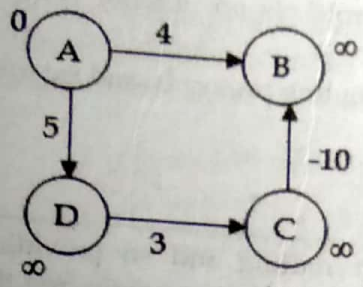


Solution: Let's choose processing edge list as,

(C, B) (D, C) (A, D) (A, B)

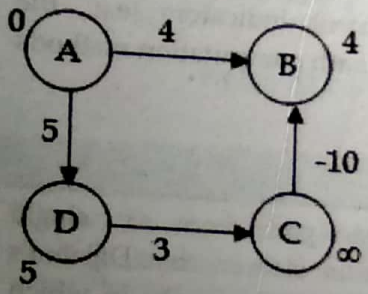
Since there are four number of vertices i.e. n=4 so number of iterations for solving problem is (n-1) = (4-1) = 3

Step 1: Let's choose vertex 'A' as starting vertex then,



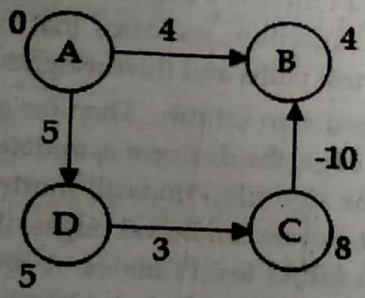
	A	B	C	D
C	∞	∞	-	∞
D	∞	∞	∞	-
A	0	∞	∞	∞

Step 2: Iteration 1



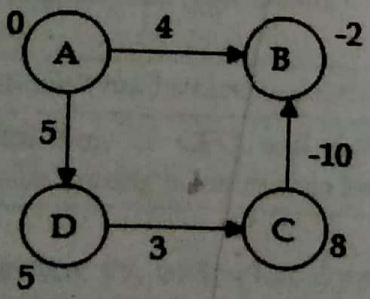
	A	B	C	D
C	∞	∞	-	∞
D	∞	∞	∞	-
A	0	4	∞	5

Step 3: Iteration 2



	A	B	C	D
C	∞	∞	-	∞
D	∞	∞	8	-
A	0	4	∞	5

Step 4: Iteration 3



	A	B	C	D
C	∞	-2	-	∞
D	∞	∞	8	-
A	0	-2	∞	5

Thus final shortest path form,

A to A = 0

A to B = -2

A to C = 8

A to D = 5

Advantages of Bellman Ford Algorithm

- Cost is minimized when building a network using Bellman Ford Algorithm.

- Maximizes the performance of the system. Also finds min path weight.
- It allows splitting of traffic between several paths. It thus increases system performance.

Dijkstra's Algorithm

This is another approach of getting single source shortest paths. In this algorithm it is assumed that there is no negative weight edge. Dijkstra's algorithm works using greedy approach, as we will see later. Dijkstra's algorithm finds the shortest path from one vertex v_0 to each other vertex in a digraph. When it has finished, the length of the shortest distance from $v0$ to v is stored in the vertex v, and the shortest path from v_0 to v is recorded in the back pointers of v and the other vertices along that path.

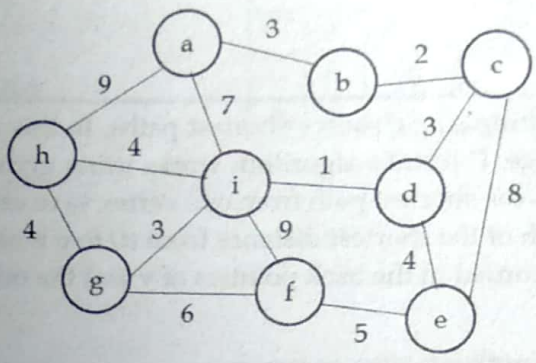
Steps in Dijkstra's algorithm

Precondition: G = (V, w) is a weighted graph with initial vertex v_0 then it holds following steps:

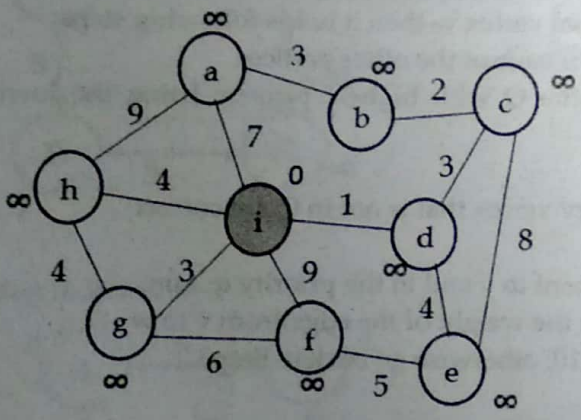
1. Initialize the distance field to 0 for v_0 and to for each of the other vertices.
2. Enqueue all the vertices into a priority queue Q with highest priority being the lowest distance field value.
3. Repeat steps 4–10 until Q is empty.
4. The distance and back reference fields of every vertex that is not in Q are correct
5. Dequeue the highest priority vertex into v.
6. Do steps 7–10 for each vertex w that are adjacent to v and in the priority queue.
7. Let S be the sum of the v's distance field plus the weight of the edge from v to w.
8. If s is less than w's distance field, do steps 9–10; otherwise go back to Step3.
9. Assign s to w's distance field.
10. Assign v to w's back reference field.

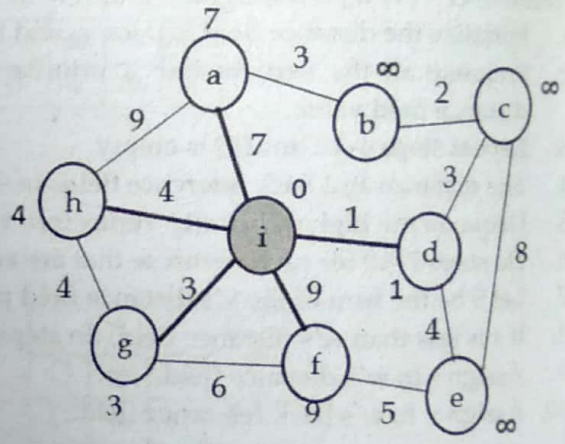
gorithm

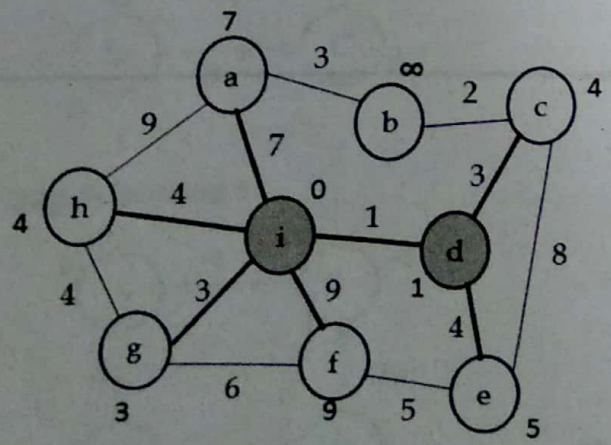
Example Find the shortest paths from the source node 'i' to all other vertices using Dijkstra's algorithm.

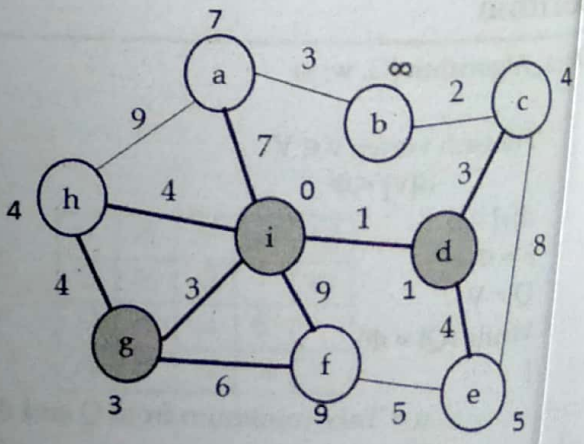


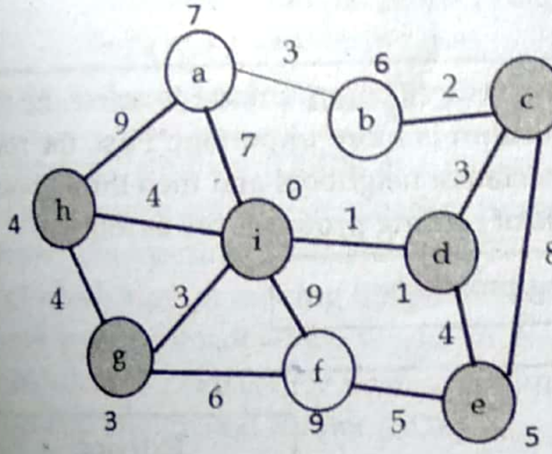
Solution

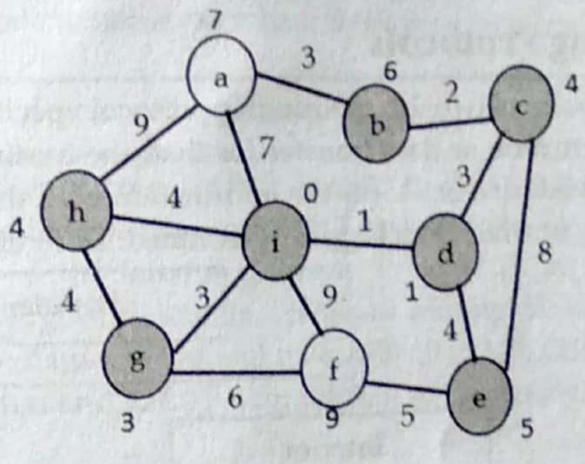


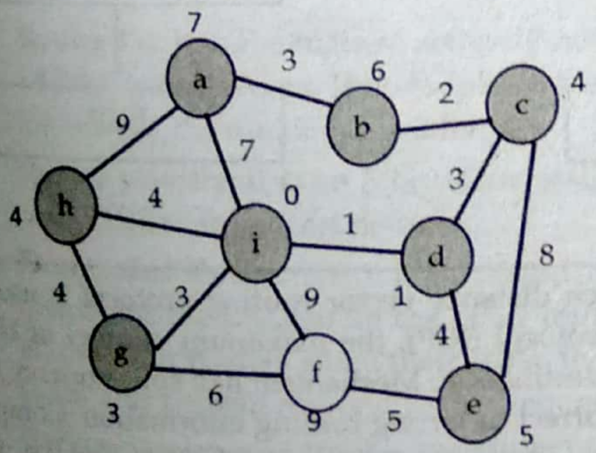


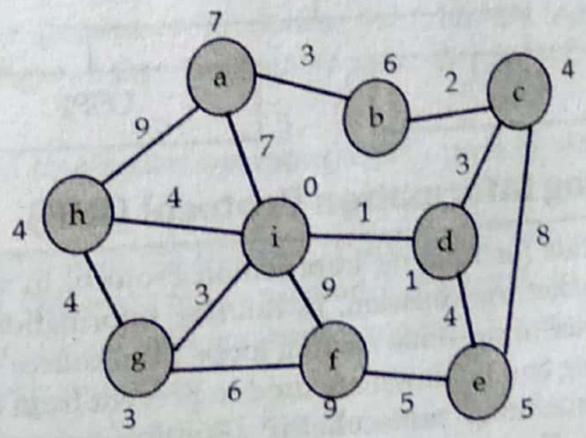












Thus, the shortest path from vertex i to a=7
The shortest path from vertex i to b=6
The shortest path from vertex i to c=4
The shortest path from vertex i to d=1
The shortest path from vertex i to e=5
The shortest path from vertex i to f=9
The shortest path from vertex i to g=3
The shortest path from vertex i to h=4
The shortest path from vertex i to i=0

Advantage and Disadvantage of Dijkstra's Algorithm

Advantages

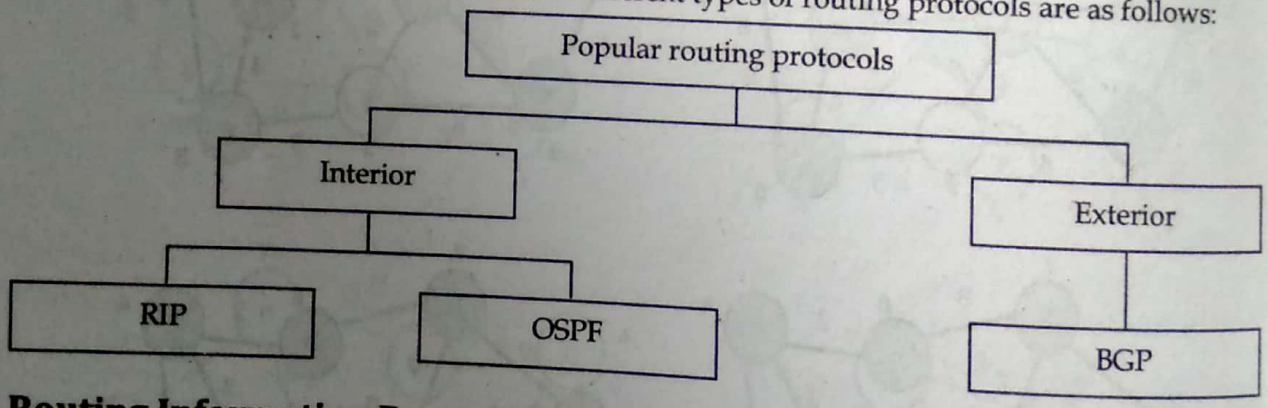
- It is used in Google Maps, geographical Maps etc.
- To find locations of map which refers to vertices of graph
- Distance between the locations refers to edges.
- It is used in IP routing to find Open shortest Path First.
- It is used in the telephone network.

Disadvantages

- It do blind search so wastes lot of time while processing.
- It cannot handle negative edges.
- This leads to acyclic graphs and most often cannot obtain the right shortest path.

Routing Protocols

In computer networks, the routing protocol specifies how routers communicate to select the routes for information or data transfer for that, the routing algorithm is more important. First, the routing protocol informs or shares the information with their associative neighbors and then throughout the network, in which topology is determined. Different types of routing protocols are as follows:



Routing Information Protocol (RIP)

RIP stands for Routing Information Protocol in which distance vector routing protocol is used for data/packet transmission. In Routing Information protocol (RIP), the maximum number of Hop is 15, because it prevents routing loops from source to destination. Mechanism like split horizon, route poisoning and holdown are used to prevent from incorrect or wrong routing information. Compared to other routing protocol, RIP (Routing Information Protocol) is poor and limit size i.e. small network. The main advantage of using RIP is it uses the UDP (User Datagram Protocol) and reserved port is 520.

Routing Information Protocol (RIP) is a dynamic protocol used to find the best route or path from end-to-end (source to destination) over a network by using a routing metric/hop count algorithm. This algorithm is used to determine the shortest path from the source to destination, which allows the data to be delivered at high speed in the shortest time.

In brief the RIP protocol works as follows

- Each router initializes its routing table with a list of locally connected networks.
- Periodically, each router advertises the entire contents of its routing table over all of its RIP-enabled interfaces.

- Whenever a RIP router receives such an advertisement, it puts all of the appropriate routes into its routing table and begins using it to forward packets. This process ensures that every network connected to every router eventually becomes known to all routers.
- If a router does not continue to receive advertisements for a remote route, it eventually times out that route and stops forwarding packets over it. In other words, RIP is a "soft state" protocol.

- Every route has a property called a metric, which indicates the distance to the route's destination.
  - Every time a router receives a route advertisement, it increments the metric.
  - Routers prefer shorter routes to longer routes when deciding which of two versions of a route to program in the routing table.
  - The maximum metric permitted by RIP is 16, which means that a route is unreachable. This means that the protocol cannot scale to networks where there may be more than 15 hops to a given destination.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e. the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router (DR)/Backup Designated Router (BDR).

OSPF terms

1. **Router I'd:** It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. **Router priority:** It is an 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.
3. **Designated Router (DR):** It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers share their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.
4. **Backup Designated Router (BDR):** BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) are the core routing protocol of the internet and responsible to maintain a table of Internet protocol networks which authorize network reaching capability between AS. The Border Gateway Protocol (BGP) expressed as path vector protocol. It doesn't employ conventional IGP metrics but making routing judgment based on path, network policies. It is created to replace the Exterior Gateway Protocol (EGP) routing protocol to permit completely decentralized routing in order to permit the removal of the NSF Net which consent to internet to turn into a truly

decentralized system. The fourth version of Border Gateway Protocol (BGP) has been in use since 1994 and 4th version from 2006.

BGP is relevant to network administrators of large organizations which connect to two or more ISPs, as well as to Internet Service Providers (ISPs) who connect to other network providers. If you are the administrator of a small corporate network, or an end user, then you probably don't need to know about BGP.

BGP basics

- The current version of BGP is BGP version 4, based on RFC4271.
- BGP is the path-vector protocol that provides routing information for autonomous systems on the Internet via its AS-Path attribute.
- BGP is a Layer 4 protocol that sits on top of TCP. It is much simpler than OSPF, because it doesn't have to worry about the things TCP will handle.
- Peers that have been manually configured to exchange routing information will form a TCP connection and begin speaking BGP. There is no discovery in BGP.
- Medium-sized businesses usually get into BGP for the purpose of true multi-homing for their entire network.
- An important aspect of BGP is that the AS-Path itself is an anti-loop mechanism. Routers will not import any routes that contain themselves in the AS-Path.

Comparison of OSPF and BGP Routing Protocols

OSPF	BGP
The OSPF will always search for the fastest route, and not the shortest, in spite of its name.	BGP focuses in determining the best path for a datagram.
OSPF is an internal gateway protocol	BGP is an external gateway protocol
OSPF is mainly used on smaller scale networks that are centrally administered.	The BGP protocol is mainly used on very large-scale networks, like the internet.
OSPF is comparatively easy to implement	BGP is comparatively complex to implement
OSFP doesn't scale up well as Routers using the OSPF protocol will verify the status of the other routers to which they have access, frequently sending a message	BGP scales up well because it sends a complete route update only once when a session is established
Dijkstra's algorithm is suitable to implement OSPF routing protocol	Best path algorithm is suitable to implement BGP routing protocol.
Port number 89 used	Port number 179 used
IP protocol is used	TCP protocol is used

Overview of IPv4 to IPv6 Transition Mechanisms

Here are a couple of main methods that can be used when transitioning a network from IPv4 to IPv6; these include:

- **Dual Stack**: Running both IPv4 and IPv6 on the same devices
- **Tunneling**: Transporting IPv6 traffic through an IPv4 network transparently
- **Translation:** Converting IPv6traffic to IPv4 traffic for transport and vice versa.

Dual Stack

The simplest approach when transitioning to IPv6 is to run IPv6 on all of the devices that are currently running IPv4. If this is something that is possible within the organizational network, it is very easy to implement. However, for many organizations, IPv6 is not supported on all of the IPv4 devices; in these situations other methods must be considered.

Tunneling

Most people with some networking knowledge are familiar with the concept of tunneling; a given packet is encapsulated into a wrapper than enables its transport from a source to destination transparently where it is decapsulated and retransmitted. There are a number of different tunneling methods that exist for IPv6, many that are integrated as part of Cisco and other manufactures certification tests. The following list shows the different available tunneling methods:

- **Manual IPv6 Tunnels** – A manually created IPv6 tunnel is configured between two routers that each must support both IPv4 and IPv6. Incoming traffic that is destined for networks on the other side of the tunnel is encapsulated on the source router and tunneled through IPv4.
- **Generic Routing Encapsulation (GRE) IPv6 tunnels** – GRE is a protocol that was developed by Cisco and for the purposes of IPv6 tunneling operates and is configured very much the same as manual tunnels. GRE itself is able to be used to tunnel over a diverse number of network layer protocols other than IPv4. When dealing with IPv6, a GRE tunnel can be used to tunnel IPv6 over IPv4 or IPv4 over IPv6. As with manual tunnels, when configuring GRE tunnels both the source and destination must be manually configured and each must support both IPv4 and IPv6.
- **6 to 4 Tunnels** – As the name suggest a 6to4 tunnel allows IPv6 to be tunneled via IPv4. Unlike the previously discussed tunneling methods, the 6to4 method is automatically set up using the 2002:/16 IPv6 address space. The IPv4 address for the edge routers is embedded in an IPv6 address that is created.
- **IPv6 rapid deployment (6rd)** – The 6rd method was derived from the 6to4 method but allows the implementer to use the IPv6 block that was assigned to it.
- **IPv4 Compatible Tunnels** – The IPv4 Compatible tunneling method is very similar to 6to4 tunneling; both provide a mechanism to tunnel IPv6 over IPv4. The major difference is how the IPv4 address is embedded inside the IPv6 address that is used by the edge device. IPv4 Compatible tunnels have been depreciated but are still covered in some certification exams (including the current Cisco ROUTE exam).
- **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Tunnels** – Again, like the other tunneling mechanisms, the ISATAP method transport IPv6 traffic over IPv4; unlike other methods the ISATAP method is intended for use inside a site and not between two dual stacked edge devices. Communications between IPv6 hosts is handled through a central IPv6 capable device.

Translation

Unlike the above discussed tunneling methods, a translation method provides a way to translate IPv6 to IPv4 traffic and vice versa. When using translation, the traffic is not encapsulated but is converted to the destination type (be that IPv4 or IPv6). There are two methods that are typically used with translated IPv6 networks; these include:

- **Network Address Translation**: Protocol Translation (NAT-PT) – The NAT-PT method enables the ability to either statically or dynamically configure a translation of a IPv4

network address into an IPv6 network address and vice versa. For those familiar with more typically NAT implementations, the operation is very similar but includes a protocol translation function. NAT-PT also ties in an Application Layer Gateway (ALG) functionality that converts Domain Name System (DNS) mappings between protocols.

- **NAT64**: One of the main limitations to NAT-PT was that it tied in ALG functionality; this was considered a hindrance to deployment. With NAT64 also came DNS64, both of which are configured and implemented separately; when these were defined and accepted the use of NAT-PT was depreciated. NAT64 offers both a stateless and stateful option when deploying, the later that keeps track of bindings and enables 1-to-N functionality.

Overview of ICMP/ICMPv6

The IP protocol alone provides no direct way to do the following:

- For an end system to learn the fate of IP packets that fail to make it to their destinations.
- For obtaining diagnostic information (e.g., which routers are used along a path or a method to estimate the round-trip time).

To address these deficiencies, a special protocol called the **Internet Control Message Protocol** (ICMP) is used in conjunction with IP to provide diagnostics and control information related to the configuration of the IP protocol layer and the disposition of IP packets.

ICMP provides for the delivery of error and control messages that may require attention. ICMP messages are usually acted on by:

- The IP layer itself,
- Higher-layer transport protocols (TCP or UDP),
- User applications.

ICMP does not provide reliability for IP; it indicates certain classes of failures and configuration information. The most common cause of packet drops (buffer overrun at a router) does not elicit any ICMP information. Other protocols, such as TCP, handle such situations.

Because of the ability of ICMP to affect the operation of important system functions and obtain configuration information, hackers have used ICMP messages in a large number of attacks. As a result of concerns about such attacks, network administrators often arrange to block ICMP messages with firewalls, especially at border routers. If ICMP is blocked, however, a number of common diagnostic utilities (e.g., ping, traceroute) do not work properly.

The term ICMP refers to ICMP in general, and the terms ICMPv4 and ICMPv6 to refer specifically to the versions of ICMP used with IPv4 and IPv6, respectively. ICMPv6 plays a far more important role in the operation of IPv6 than ICMPv4 does for IPv4.

Overview of NATing

Network Address Translation (NAT) is a mechanism to translate the IP address of a computer or group of computers into a single public address when the packets are sent out to the internet. By translating the IP address, only one IP address is publicized to the outside network. Since only one IP address is visible to the outside world, NAT provides additional security and it can have only one public address for the entire network instead of having multiple IP addresses.

The following types of NAT are supported on Juniper Networks devices:

- Static NAT
- Destination NAT
- Source NAT

Overview of Network Traffic Analysis

Network traffic analysis is the process of recording, reviewing and analyzing network traffic for the purpose of performance, security and/or general network operations and management. It is the process of using manual and automated techniques to review granular-level detail and statistics within network traffic.

Security Concepts: Firewall & Router Access Control

A **firewall** is a hardware device or software application installed on the borderline of secured networks to examine and control incoming and outgoing network communications. As the first line of network defense, firewalls provide protection from outside attacks, but they have no control over attacks from within the corporate network. Some firewalls also block traffic and services that are actually legitimate.

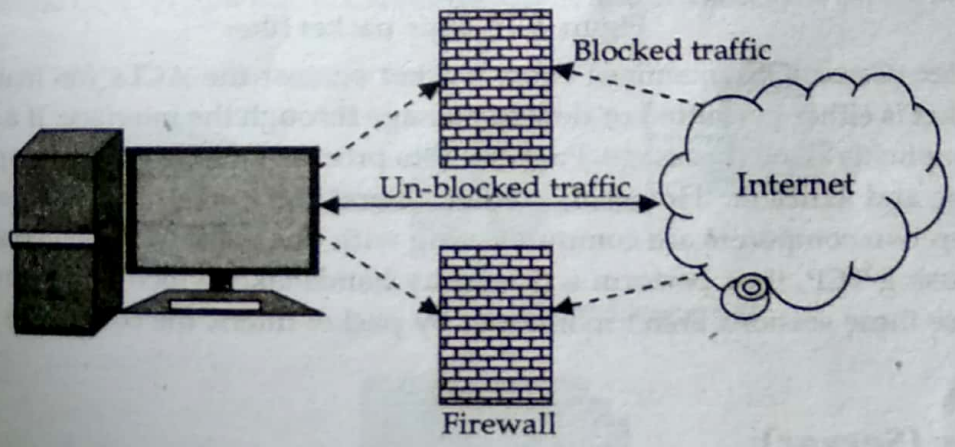


Fig 4.14 Firewall

Types of Firewall Filtering Technologies

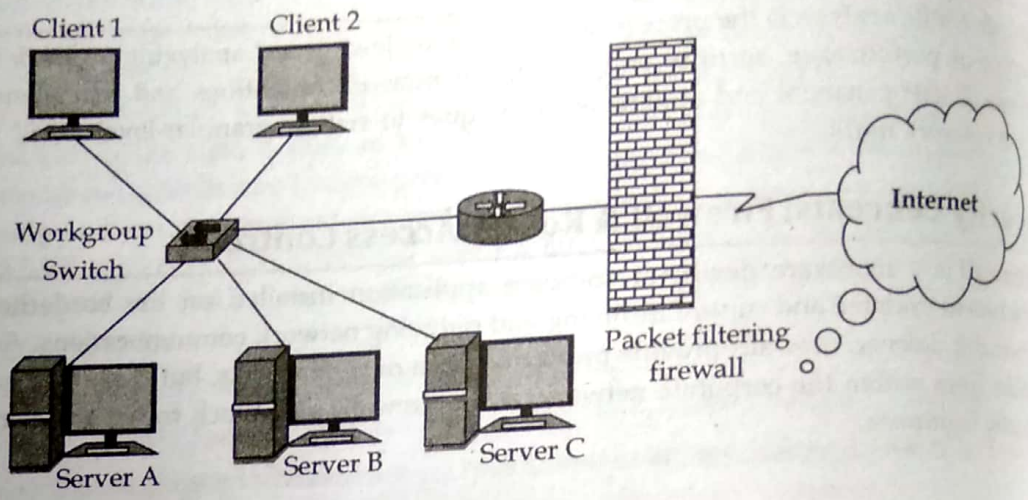


Figure 4.15 Basic packet filter

The packet filter (Cisco IOS) examines every packet against the ACLs for matches. If a match is found, the packet is either permitted or denied passage through the interface. If a match is not found, the packet is implicitly denied passage. Packet filters process information only up to layer 4, making them very fast and efficient. However, packet filters don't track the TCP session information generated when two computers are communicating with one another. When computers first start to communicate using TCP, they perform a three-way handshake, which is used to establish the TCP session. Because these sessions aren't monitored by packet filters, the computers become vulnerable to spoofing.

Proxy Filter (Server)

Proxy filters, also known as application proxy servers, extend beyond the reach of packet filters by examining information from layers 4–7. A proxy server sits between the client and the destination working as a middleman between the two communicating parties. It requires the client to establish a session with the proxy itself, which in turn creates a second session between itself and the destination. Consider, for instance, a client computer that requests information from a remote Web site. The client creates a session with the proxy server, which can then authenticate the user for valid access to the Internet before creating a second session between the Web site and itself. As the information comes back from the Web site, the proxy server examines layers 4–7 for a valid connection to the inside network.

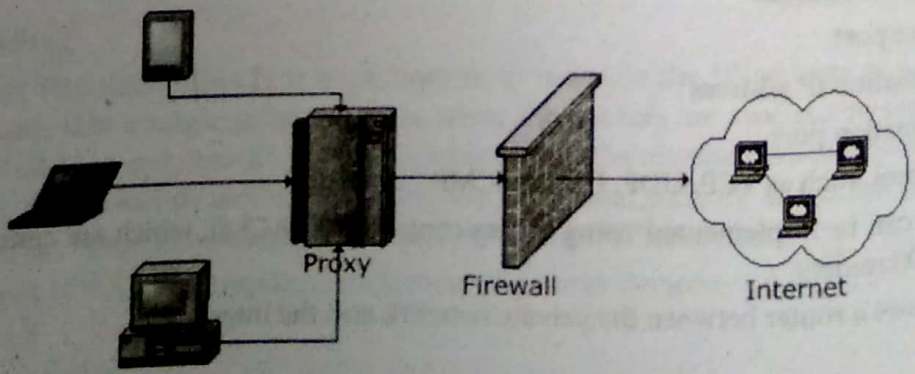


Figure 4.16 Proxy server sessions

Although proxies can provide some of the most effective measures of protection, they can introduce speed and performance issues, particularly when a large number of sessions are being simultaneously negotiated. They are also built on general-purpose operating systems such as UNIX, Linux, or Microsoft Windows, which can make them vulnerable to OS-related attacks

Stateful Packet Filter—Stateful Inspection

This type of firewall combines the speed of packet filters with the enhanced security of stored session information typified by proxies. While traffic is being forwarded through the firewall, stateful inspections of the packets create slots in session flow tables. These tables contain source and destination IP addresses, port numbers, and TCP protocol information. Before traffic can travel back through the firewall, stateful inspections of the packets are cross-referenced to the session flow tables for an existing connection slot. If a match is found in the tables, the packets are forwarded; otherwise, the packets are dropped or rejected. The Cisco PIX firewall uses stateful inspection as its primary method to control traffic flow. Figure below shows the client and session flow tables being used.

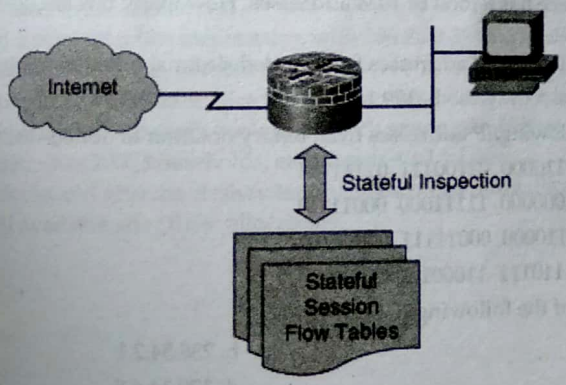


Figure 4.17 Stateful inspections

Exercise

1. What is the difference between the delivery of a frame in the data link layer and the delivery of a packet in the network layer?
2. Explain the Network Service Model.
3. Discuss the importance of routing algorithm. Discuss distance vector routing algorithm. Compare it with link state routing.
4. What is multicast routing? Discuss.
5. What do you mean by routing algorithm? How adaptive routing differs with non-adaptive routing?
6. What do you mean by hierarchical routing?
7. Discuss distance vector routing algorithm and link state routing algorithm in detail.
8. Explain the Internet Control Message Protocol (ICMP).
9. Explain IPv4 addressing.
10. List the fields of IPv4 header. What is the main function of time to live (TTL) field?
11. What do you mean by IP datagram fragmentation?

Chapter 5

TRANSPORT LAYER

Introduction

The transport layer is the layer in the open system interconnection (OSI) model responsible for end-to-end communication over a network. It provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components.

The transport layer is also responsible for the management of error correction, providing quality and reliability to the end user. This layer enables the host to send and receive error corrected data, packets or messages over a network and is the network component that allows multiplexing.

Various responsibilities of a Transport Layer:

- **Process to Process Delivery**

  While Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source- destination hosts to correctly deliver a frame and Network layer requires the IP address for appropriate routing of packets, in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A **port number** is a 16 bit address used to identify any client-server program uniquely.

- **End-to-end Connection between Hosts**

  Transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection- orientated protocol which uses a handshake protocol to establish a robust connection between two end- hosts. TCP ensures reliable delivery of messages and is used in various applications. UDP on the other hand is a stateless and unreliable protocol which ensures best-effort delivery. It is suitable for the applications which have little concern with flow or error control and requires sending bulk of data like video conferencing. It is a often used in multicasting protocols.

- **Multiplexing and De-multiplexing**

  Multiplexing allows simultaneous use of different applications over networks which are running on a host. Transport layer provides this mechanism which enables us to send

packet streams from various applications simultaneously over a network. Transport layer accepts these packets from different processes differentiated by their port numbers and passes them to network layer after adding proper headers. Similarly De-multiplexing is required at the receiver side to obtain the data coming from various processes. Transport receives the segments of data from network layer and delivers it to the appropriate process running on the receiver's machine.

- **Congestion Control**

  Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occur. As a result retransmission of packets from the sources increases the congestion further. In this situation Transport layer provides Congestion Control in different ways. It uses **open loop** congestion control to prevent the congestion and **closed loop** congestion control to remove the congestion in a network once it occurred. TCP provides AIMD- additive increase multiplicative decrease, leaky bucket technique for congestion control.

- **Data integrity and Error Correction**

  Transport layer checks for errors in the messages coming from application layer by using error detection codes, computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data is arrived or not and checks for the integrity of data.

- **Flow Control**

  Transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents the data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by receiver by sending a window back to the sender informing the size of data it can receive.

Functions of Transport Layer

1. **Service Point Addressing:** Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
2. **Segmentation and Reassembling:** A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
3. **Connection Control:** It includes 2 types:
   - Connectionless Transport Layer: Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
   - Connection Oriented Transport Layer: Before delivering packets, connection is made with transport layer at the destination machine.
4. **Flow Control:** In this layer, flow control is performed end to end.

5. **Error Control:** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.

Transport Protocols

The Internet provides a way to get packets from any host computer to one or more other host computers. However, the network protocols make no guarantees about delivering a packet. In fact, a packet may get lost, may arrive after others sent later or may be distorted. A packet might even arrive that simply wasn't sent.

To counter this, host computers incorporate transport protocols, which use the Internet to carry the application information around, but also send a variety of other information to provide checking and correction or recovery from such errors. There is a spectrum of complexity in transport protocols, depending on the application requirements. The three representative ones are:

- The User Datagram Protocol, or UDP
- The Reliable Data Protocol, or RDP
- The Transmission Control Protocol, or TCP

Transmission Control Protocol (TCP)

TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet.

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control, and because it is meant to provide error-free data transmission handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive.

For example, when a Web server sends an HTML file to a client, it uses the HTTP protocol to do so. The HTTP program layer asks the TCP layer to set up the connection and send the file. The TCP stack divides the file into packets, numbers them and then forwards them individually to the IP layer for delivery. Although each packet in the transmission will have the same source and destination IP addresses, packets may be sent along multiple routes. The TCP program layer in the client computer waits until all of the packets have arrived, then acknowledges those it receives and asks for the retransmission on any it does not (based on missing packet numbers), then assembles them into a file and delivers the file to the receiving application.

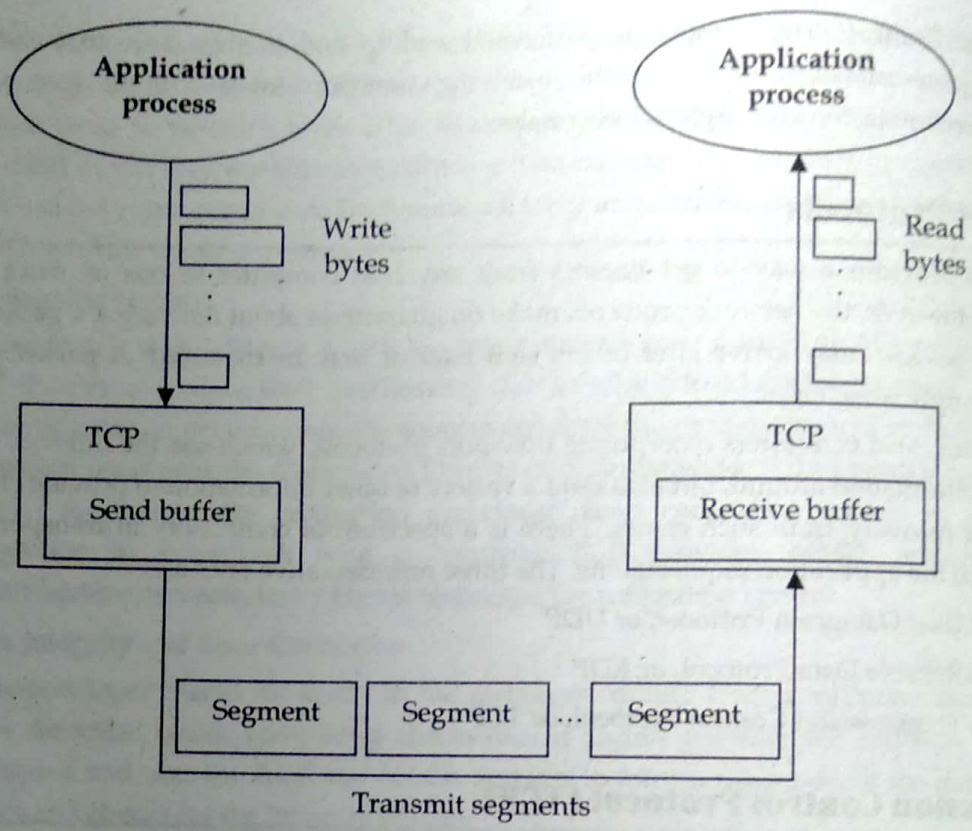


Figure 5.1 TCP

Features of TCP

- **Stream Data transfer:** Applications working at the application layer transfers a continuous stream of bytes to the bottom layers. It is the duty of TCP to pack this byte stream to packets, known as TCP segments, which are passed to the IP layer for transmission to the destination device. The application does not have to bother to chop the byte stream data packets.
- **Reliability:** The most important feature of TCP is reliable data delivery. In order to provide reliability, TCP must recover from data that is damaged, lost, duplicated, or delivered out of order by the network layer. TCP assigns a sequence number to each byte transmitted, and expects a positive acknowledgment (ACK) from the receiving TCP layer. If the ACK is not received within a timeout interval, the data is retransmitted. The receiving TCP uses the sequence numbers to rearrange the TCP segments when they arrive out of order, and to eliminate duplicate TCP segments.
- **Flow control:** Network devices operate at different data rates because of various factors like CPU and available bandwidth. It may happen a sending device to send data at a much faster rate than the receiver can handle. TCP uses a sliding window mechanism for implementing flow control. The number assigned to a segment is called the sequence number and this numbering is actually done at the byte level. The TCP at the receiving device, when sending an ACK back to the sender, also indicates to the TCP at the sending device, the number of bytes it can receive without causing serious problems in its internal buffers.
- **Multiplexing:** Multitasking achieved through the use of port numbers.
- **Connections:** Before application processes can send data by using TCP, the devices must establish a connection. The connections are made between the port numbers of the sender and the receiver devices. A TCP connection identifies the end points involved in the connection. A

hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.

- **Control Flags**

  These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:

  - ✓ **URG:** Urgent pointer is valid
  - ✓ **ACK**: Acknowledgement number is valid(used in case of cumulative acknowledgement)
  - ✓ **PSH:** Request for push
  - ✓ **RST:** Reset the connection
  - ✓ **SYN:** Synchronize sequence numbers
  - ✓ **FIN:** Terminate the connection

- **Window Size**

  This field tells the window size of the sending TCP in bytes.

- **Checksum**

  This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

- **Urgent Pointer**

  This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

TCP Connection Establishment using Three-way Handshaking

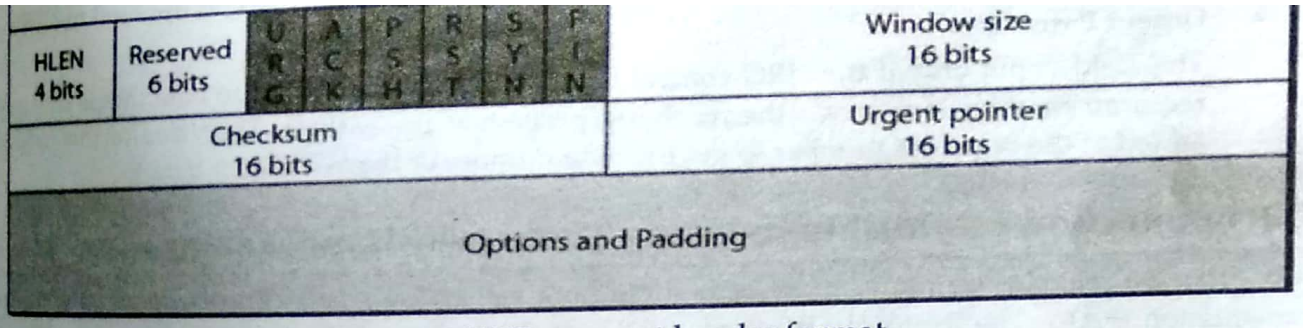


Figure 5.2 TCP segment header format

The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, header is of 20 bytes else it can be of upmost 60 bytes. Header fields:

- **Source Port Address**

  16 bit field that holds the port address of the application that is sending the data segment.

- **Destination Port Address**

  16 bit field that holds the port address of the application in the host that is receiving the data segment.

- **Sequence Number**

  It is a 32 bit field that holds the sequence number, i.e., the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end if the segments are received out of order.

- **Acknowledgement Number**

  It is a 32 bit field that holds the acknowledgement number, i.e., the byte number that the receiver expects to receive next. It is an acknowledgment for the previous bytes being received successfully.

- **Header Length (HLEN)**

  This is a 4 bit field that indicates the length of the TCP header by number of 4-byte words in the header, i.e, if the header is of 20 bytes (min length of TCP header), then this field will

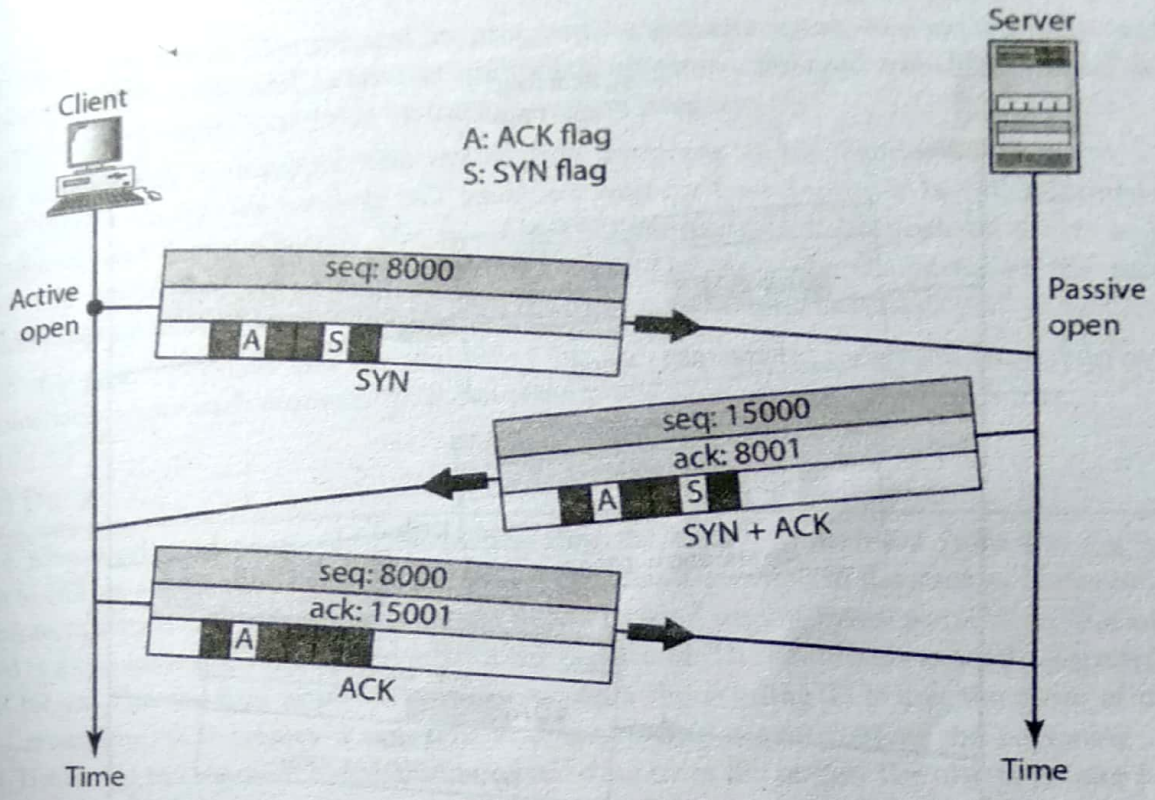


Figure 5.3 Connection establishment using three-way handshaking

- **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.

Data Transfer

During data transmission, each segment sent has to be acknowledged. When a segment is sent a retransmission timer is started, and if the timeout interval expires before the segment is acknowledged, the sender will retransmit. Segments must be delivered in the correct order and the simplest approach if a timeout occurs is to adopt a go-back-N strategy. When acknowledging incoming segments, an entity may elect to wait for a returning segment on which to piggyback an acknowledgement. A TCP entity sending a segment with next expected sequence number, i, implicitly acknowledges all bytes received up to i+1, so it is not actually necessary to send an ACK for every segment which arrives.

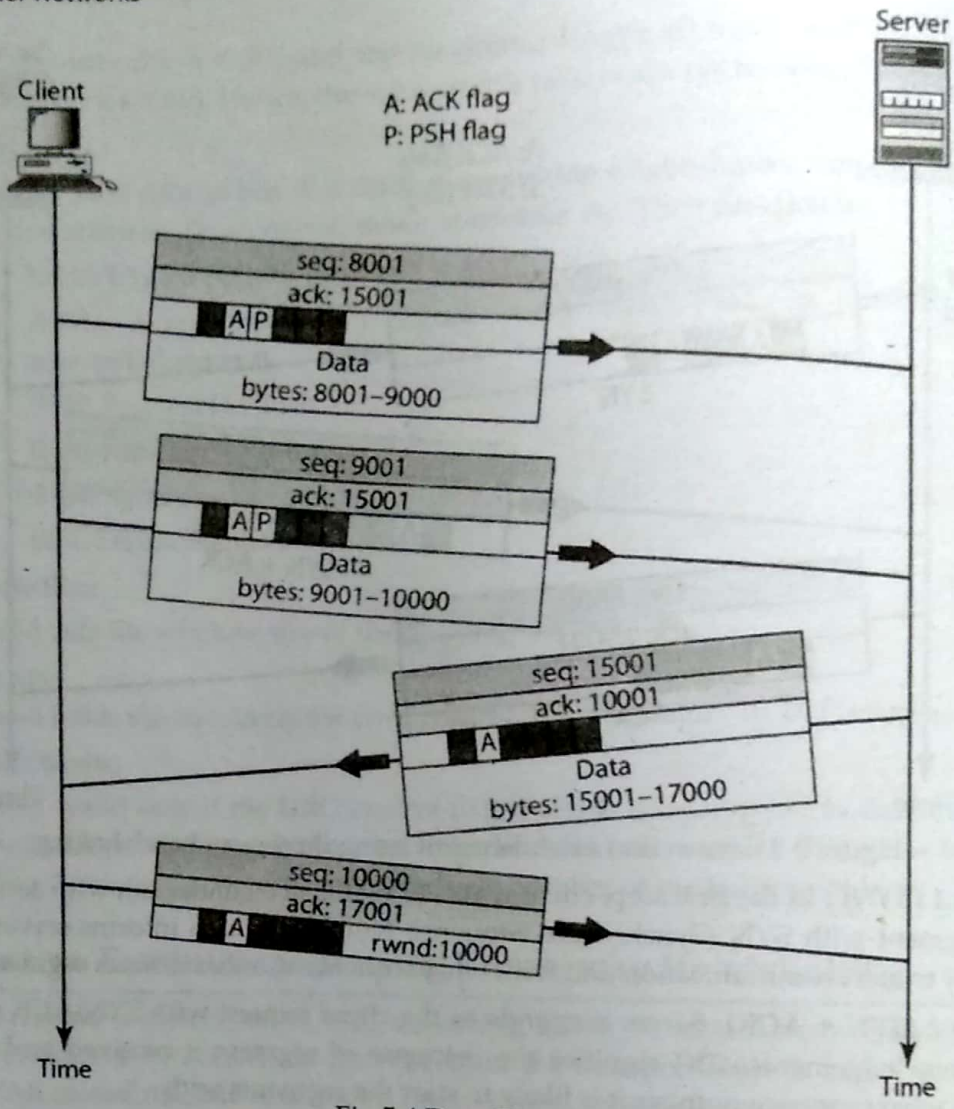


Fig 5.4 Data Transfer

In this example, after a connection is established, the client sends 2,000 bytes of data in two segments. The server then sends 2,000 bytes in one segment. The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgment because there is no more data to be sent. Note the values of the sequence and acknowledgment numbers. The data segments sent by the client have the PSH (push) flag set so that the server TCP tries to deliver data to the server process as soon as they are received. We discuss the use of this flag in more detail later. The segment from the server, on the other hand, does not set the push flag. Most TCP implementations have the option to set or not set this flag.

Pushing Data

We saw that the sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size. The receiving TCP also buffers the data when they arrive and delivers them to the application program when the application program is ready or when it is convenient for the receiving TCP. This type of flexibility increases the efficiency of TCP.

However, there are occasions in which the application program has no need for this flexibility. For example, consider an application program that communicates interactively with another application

program on the other end. The application program on one site wants to send a keystroke to the application at the other site and receive an immediate response. Delayed transmission and delayed delivery of data may not be acceptable by the application program.

TCP can handle such a situation. The application program at the sender can request a push operation. This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. The sending TCP must also set the push bit (PSH) to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come.

Although the push operation can be requested by the application program, most current TCP implementations ignore such requests. TCP can choose whether or not to use this feature.

Urgent Data

TCP is a stream-oriented protocol. This means that the data is presented from the application program to TCP as a stream of bytes. Each byte of data has a position in the stream. However, there are occasions in which an application program needs to send urgent bytes, some bytes that need to be treated in a special way by the application at the other end. The solution is to send a segment with the URG bit set. The sending application program tells the sending TCP that the piece of data is urgent. The sending TCP creates a segment and inserts the urgent data at the beginning of the segment. The rest of the segment can contain normal data from the buffer. The urgent pointer field in the header defines the end of the urgent data (the last byte of urgent data).

When the receiving TCP receives a segment with the URG bit set, it informs the receiving application of the situation. How this is done, depends on the operation system. It is then to the discretion of the receiving program to take an action. It is important to mention that TCP's urgent data is neither a priority service nor an expedited data service. Rather, TCP urgent mode is a service by which the application program at the sender side marks some portion of the byte stream as needing special treatment by the application program at the receiver side.

Thus, signaling the presence of urgent data and marking its position in the data stream are the only aspects that distinguish the delivery of urgent data from the delivery of all other TCP data. For all other purposes, urgent data is treated identically to the rest of the TCP byte stream. The application program at the receiver site must read every byte of data exactly in the order it was submitted regardless of whether or not urgent mode is used. The standard TCP, as implemented, does not ever deliver any data out of order.

Connection Termination

Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. Most implementations today allow two options for connection termination: **three-way handshaking** and **four-way handshaking** with a half-close option. Most implementations today allow three-way handshaking for connection termination as shown in Figure 5.5 below.

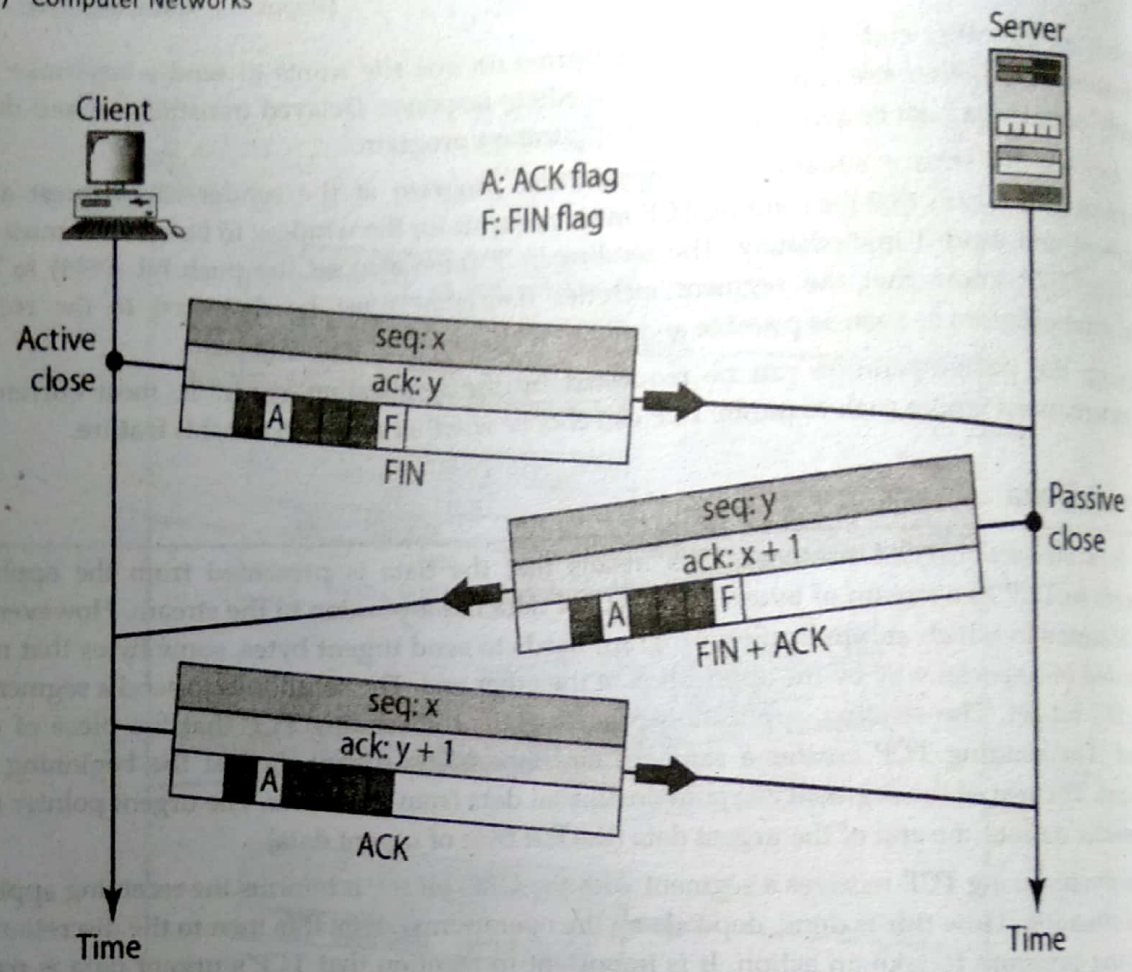


Figure 5.5: Connection Termination using Three-way Handshaking

1. In a common situation, the client TCP, after receiving a close command from the client process sends the first segment, a FIN segment in which the FIN flag is set. Note that a FIN segment can include the last chunk of data sent by the client or it can be just a control segment as shown in the figure. If it is only a control segment, it consumes only one sequence number.
2. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN+ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.
3. The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is one plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers.

User Datagram Protocol (UDP)

UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol (TCP) used primarily for establishing low-latency and loss-tolerating connections between applications on the internet.

User datagram protocol is an open systems interconnection (OSI) transport layer protocol for client-server network applications. UDP uses a simple transmission model but does not employ handshaking dialogs for reliability, ordering and data integrity. The protocol assumes that error-checking and correction is not required, thus avoiding processing at the network interface level. UDP is widely used in video conferencing and real-time computer games. The protocol permits individual packets to be dropped and UDP packets to be received in a different order than that in which they were sent, allowing for better performance. UDP network traffic is organized in the form of datagrams, which comprise one message units. The first eight bytes of a datagram contain header information, while the remaining bytes contain message data. A UDP datagram header contains four fields of two bytes each:

- Source port number
- Destination port number
- Datagram size
- Checksum

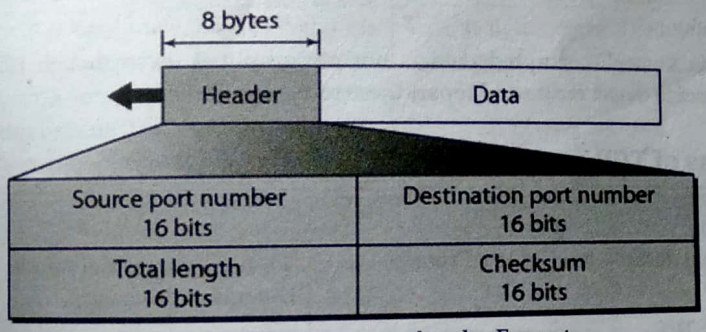


Figure 5.6 User Datagram header Format

- **Source Port:** Source Port is 2 Byte long fields used to identify port number of source.
- **Destination Port:** It is 2 Byte long fields, used to identify the port of destined packet.
- **Length:** Length is the length of UDP including header and the data. It is 16-bits field.
- **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

User datagram protocol features

The user datagram protocol has attributes that make it advantageous for use with applications that can tolerate lost data.

- It allows packets to be dropped and received in a different order than they were transmitted, making it suitable for real-time applications where latency might be a concern.
- It can be used for transaction-based protocols, such as DNS or Network Time Protocol.
- It can be used where a large number of clients are connected and where real-time error correction isn't necessary, such as gaming, voice or video conferencing, and streaming media.
- Provides connectionless, unreliable service. So UDP faster than TCP.
- Adds only checksum and process-to-process addressing to IP.
- Used when socket is opened in datagram mode.

- It sends bulk quantity of packets.
- No acknowledgment.
- 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.
- It has no handshaking or flow control.
- It not even has windowing capability.
- It is a fire and forgets 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 establishments 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).

Comparisons of TCP and UDP

	TCP	UDP
Acronym for	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
Function	As a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Use by other protocols	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because error recovery is not attempted. It is a "best effort" protocol.

Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header Size	TCP header size is 20 bytes	UDP Header size is 8 bytes.
Common Header Fields	Source port, Destination port, Check Sum	Source port, Destination port, Check Sum
Streaming of data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.
Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control
Error Checking	TCP does error checking and error recovery. Erroneous packets are retransmitted from the source to the destination.	UDP does error checking but simply discards erroneous packets. Error recovery is not attempted.
Fields	Sequence Number, Data offset, Reserved, Control bit, Window, Urgent Pointer Options, Padding, Check Sum, Source port, Destination port etc.	Length, Source port, Destination port, Check Sum etc.
Acknowledgement	Acknowledgement segments	No Acknowledgment
Handshake	SYN, SYN-ACK, ACK	No handshake (connectionless protocol)

Connection Oriented and Connectionless Services

When one computer wants to send a packet to another computer connected to the internet, umbersome operations are executed including establishing the connection between sender and eceiver. These operations are governed by the set of rules called protocol. The services provided by ese protocols are of two types- Connection-oriented and connectionless services. Each has its own dvantages and disadvantages.

Connection-oriented

It requires a session connection (analogous to a phone call) be established before any data can be sent. This method is often called a "reliable" network service. It can guarantee that data will arrive in the same order. Connection-oriented services set up virtual links between end systems through a network. There is a sequence of operation to be followed by the users of connection oriented service. These are:

a. Connection is established
b. Information is sent
c. Connection is released

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection. Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

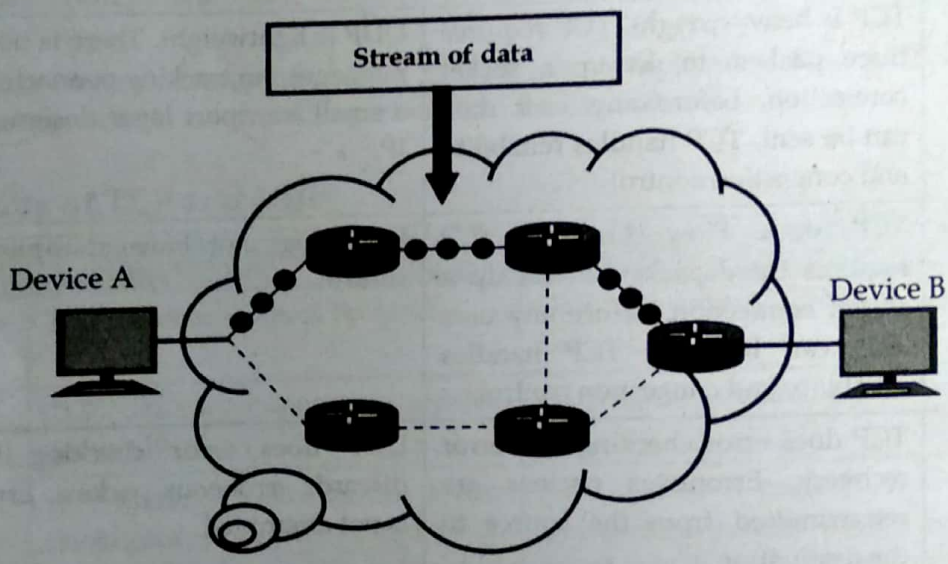


Figure 5.7: Connect-oriented service

If we need reliable communication between sender and receiver, connection-oriented services are more useful.

Example: We use email for communication. If we are sending an email to another recipient, it should be delivered. In this case, the connection-oriented protocol is more reliable to use.

Advantages and Disadvantages of Connection-Oriented Service

Advantages

- It is reliable
- All the packets follow the same path to the destination

Disadvantages

- Handshaking is required before sending an actual data packet over the internet
- Requires additional header parameter to ensure reliable communication between sender and receiver. So, it has extra overhead
- Header size of the packet is bigger than connectionless protocol

Connectionless

It does not require a session connection between sender and receiver. The sender simply starts sending packets (called datagrams) to the destination. This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers. Neither system must maintain state information for the systems that they send transmission to or receive transmission from. A connectionless network provides minimal services. It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received. In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

If we are more concern about the packet transmission speed than reliability, connectionless service is more useful.

Example: If we are developing video streaming website, we need a faster connection to stream without buffer delay. In this case, the connectionless protocol is more useful. Domain name server (DNS) uses connectionless service protocol (UDP) for the domain and IP resolution.

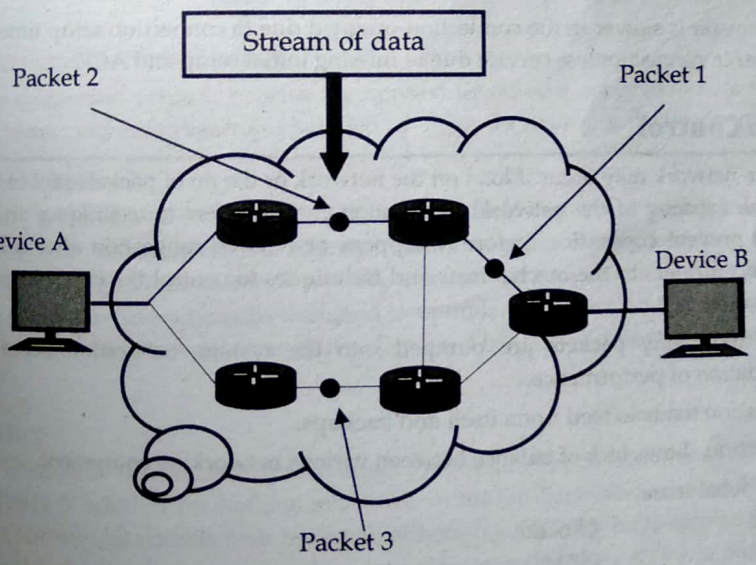


Figure 5.8: Connect less service

Advantages and Disadvantages of Connectionless protocol

Advantages

- It sends the packet without handshaking
- It is faster than connection-oriented protocol
- The header size of the packet is smaller as compared to the packets in connection-oriented services

Disadvantages

- It is not reliable and cannot ensure the data transmission to the destination
- Packets decide the route while transmission based on the network congestion

- It does not have a fixed path
- Different packets do not necessarily follow the same path

Difference between connection-oriented and connectionless service

- A prior connection setup is needed in connection-oriented service but not in connectionless service.
- Connection-oriented service guarantees reliability but not connectionless service.
- Congestion is very unlikely in connection-oriented service but not in connectionless.
- Lost data retransmission is possible in connection-oriented service but not in connectionless service.
- Connection-oriented is suitable for long connection while connectionless is suitable for bursty connection
- Packets reach the destination following the same route in connection-oriented service, but for connectionless, the packets can take different paths.
- Resource allocation is needed in the connection-oriented but not in the case of connectionless service.
- The transfer is slower in the connection-oriented due to connection setup time and ACK but is faster in connectionless service due to missing initial setup and ACK.

Congestion Control

Congestion in a network may occur if load on the network or the no of packets sent to the network is greater than the capacity of the network. Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens or remove congestion after it has happened. 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 to degradation of performance.
- Congestion tends to feed upon itself and backups.
- Congestion shows lack of balance between various networking equipment.
- It is a global issue.

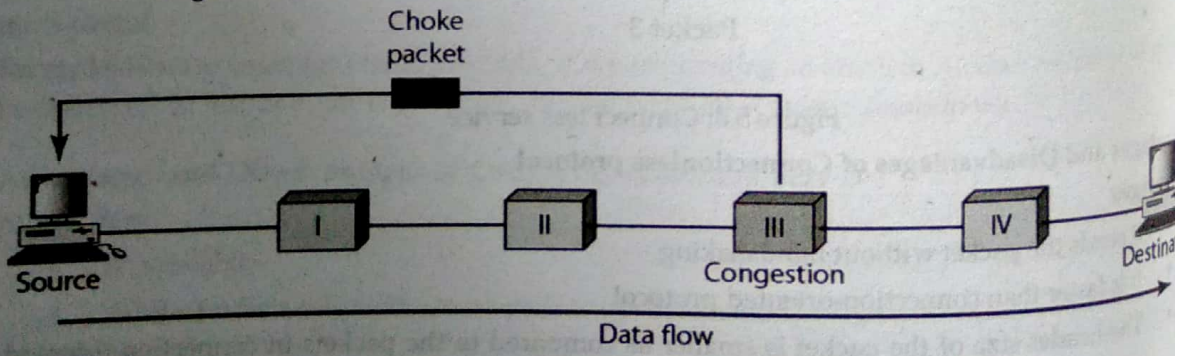
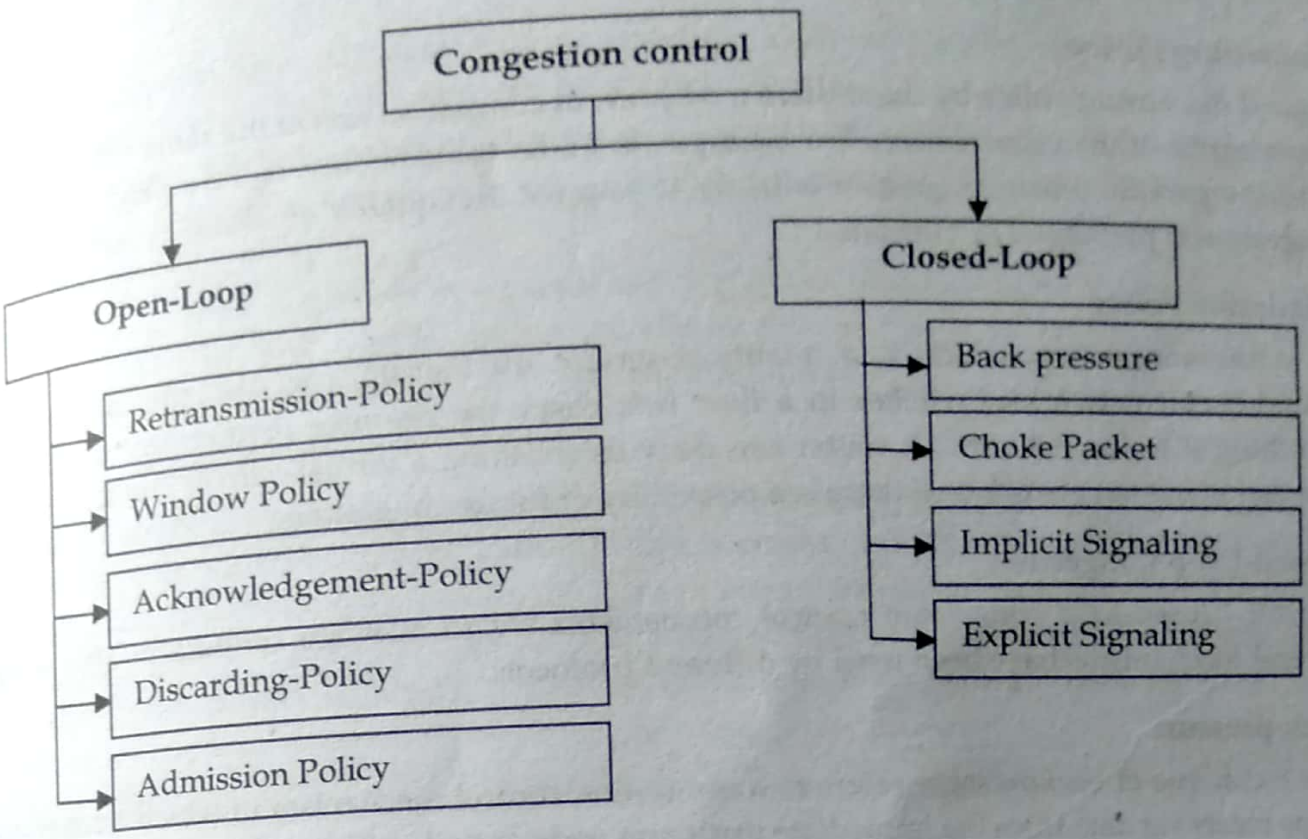


Figure 5.9

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 fig below:



Open-loop congestion control policy

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.

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.

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.

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 [illegible] to acknowledge only N packets at [illegible]

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.

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.

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.

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.

Implicit Signaling

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a 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.

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.

TCP Congestion Control

Transmission Control Protocol (TCP) uses a network congestion-avoidance algorithm that includes various aspects of an additive increase/multiplicative decrease (AIMD) scheme, with other schemes such as slow start and congestion window to achieve congestion avoidance. The TCP congestion-avoidance algorithm is the primary basis for congestion control in the Internet. Per the end-to-end principle, congestion control is largely a function of internet hosts, not the network itself. TCP's general policy for handling congestion consists of following three phases:

- Slow start
- Congestion avoidance
- Congestion detection

Slow Start Phase

Slow start is part of the congestion control strategy used by TCP in conjunction with other algorithms to avoid sending more data than the network is capable of forwarding, that is, to avoid causing network congestion. Initially, sender sets congestion window size = Maximum Segment Size (1 MSS). After receiving each acknowledgment, sender increases the congestion window size by 1 MSS. In this phase, the size of congestion window increases exponentially. The formula is,

Congestion window size = Congestion window size + Maximum segment size

Steps for working mechanism of slow start policy for TCP congestion control are listed below;

- A sender attempts to communicate to a receiver. The sender's initial packet contains a small congestion window, which is determined based on the sender's maximum window.
- The receiver acknowledges the packet and responds with its own window size. If the receiver fails to respond, the sender knows not to continue sending data.
- After receiving the acknowledgement, the sender increases the next packet's window size. The window size gradually increases until the receiver can no longer acknowledge each packet, or until either the sender or the receiver's window limit is reached.

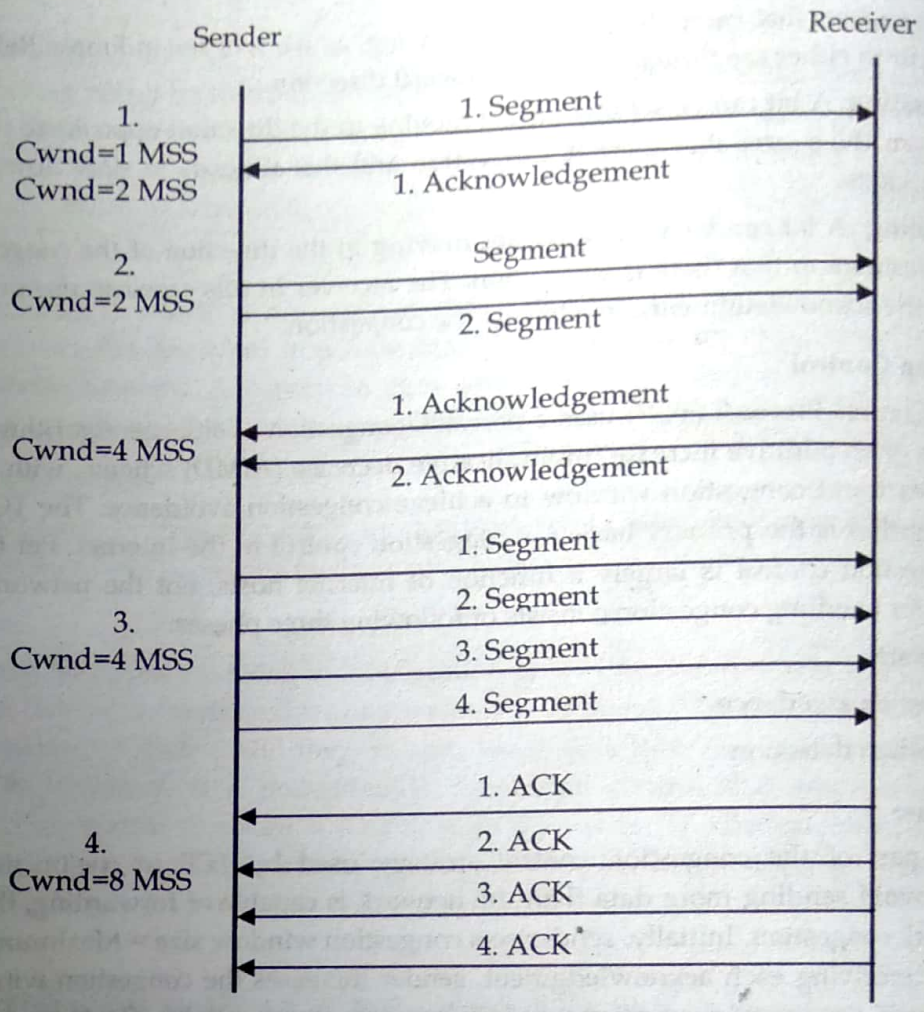


Figure 5.10

In this phase after every RTT the congestion window size increments exponentially.

Initially cwnd = 1

After 1 RTT, cwnd = $2^1 = 2$

2 RTT, cwnd = $2^2 = 4$

3 RTT, cwnd = $2^3 = 8$

Congestion Avoidance Phase

It is also called additive increment. This phase starts after the threshold value also denoted as ssthresh. The size of cwnd (congestion window) increases additive.

After each RTT cwnd = cwnd + 1.

Initially cwnd = i

After 1 RTT, cwnd = i+1

2 RTT, cwnd = i+2

3 RTT, cwnd = i+3

Congestion detection

It is also called multiplicative decrement. If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has occurred is the need to retransmit a

segment. Retransmission is needed to recover a missing packet which is assumed to have been dropped by a router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

Case 1: Retransmission due to Timeout – In this case congestion possibility is high.

- ssthresh is reduced to half of the current window size.
- Set cwnd = 1
- Start with slow start phase again.

Case 2: Retransmission due to 3 Acknowledgement duplicates – In this case congestion possibility is less.

- ssthresh value reduces to half of the current window size.
- Set cwnd= ssthresh
- Start with congestion avoidance phase

Traffic Shaping Algorithms

Traffic shaping is a bandwidth management technique used on computer networks which delays some or all datagrams to bring them into compliance with a desired traffic profile. Traffic shaping is used to optimize or guarantee performance, improve latency, or increase usable bandwidth for some kinds of packets by delaying other kinds. Traffic Shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Approach of congestion management is called Traffic shaping. Traffic shaping helps to regulate rate of data transmission and reduces congestion. There are 2 types of traffic shaping algorithms:

- Leaky Bucket
- Token Bucket

Traffic shaping is used for a number of purposes:

- Time-sensitive data may be given priority over traffic that can be delayed briefly with little-to-no ill effect.
- A large ISP (Internet service provider) may shape the traffic of an independent reseller.
- In a corporate environment, business-related traffic may be given priority over other traffic.
- An ISP may limit bandwidth consumption for certain applications to reduce costs and create the capacity to take on additional subscribers. This practice can effectively limit a subscriber's "unlimited connection" and is often imposed without notification.
- Traffic shaping could be an integral component of the proposed two-tiered Internet, in which certain customers or services would get traffic priority for a premium charge.

Leaky Bucket & Token Bucket

Leaky Bucket

The leaky Bucket algorithm used to control rate in a network. It is implemented as a single server queue with constant service time. If the bucket overflows then packets are discarded. In this algorithm the input rate can vary but the output rate remains constant. This algorithm saves busty traffic into fixed rate traffic by averaging the data rate.

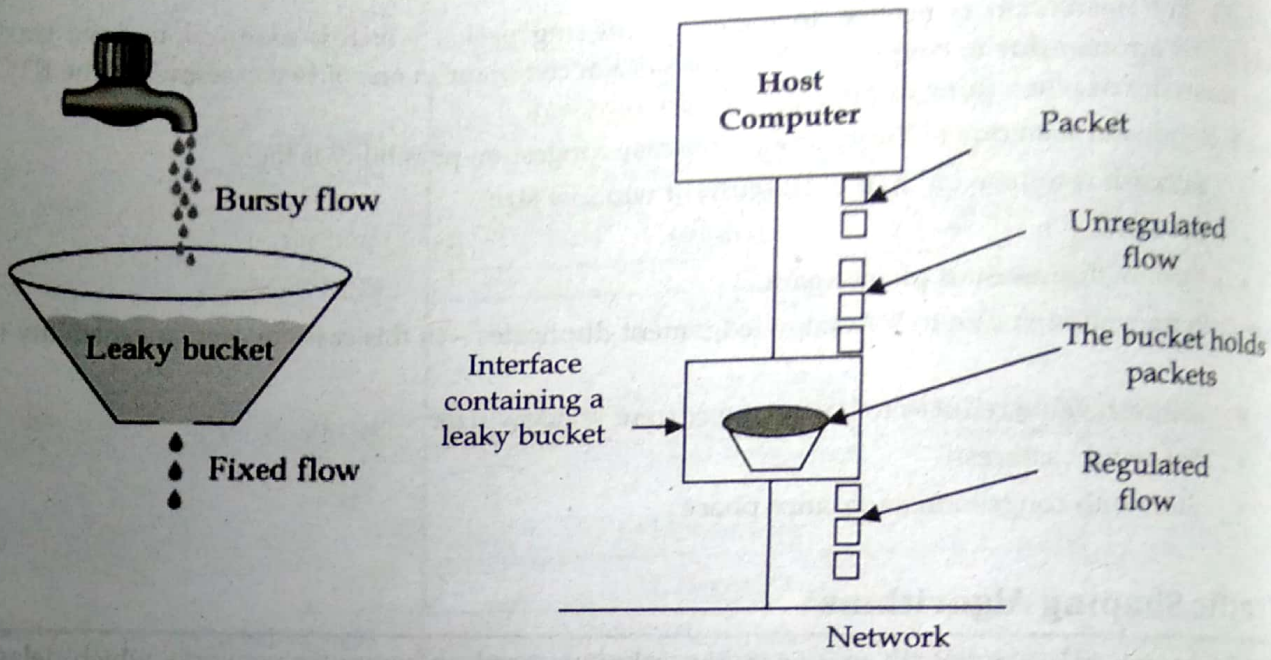


Figure 5.11: A leaky bucket with packets

Algorithm

Step 1: Initialize the counter to 'n' at every tick of clock

Setp 2: If n is greater than the size of packet in the front of queue send the packet into the network and derement the counter by size of packet. Repeat the step until n is less than the size of packet.

Step 3: Reset the counter and go to step-1.

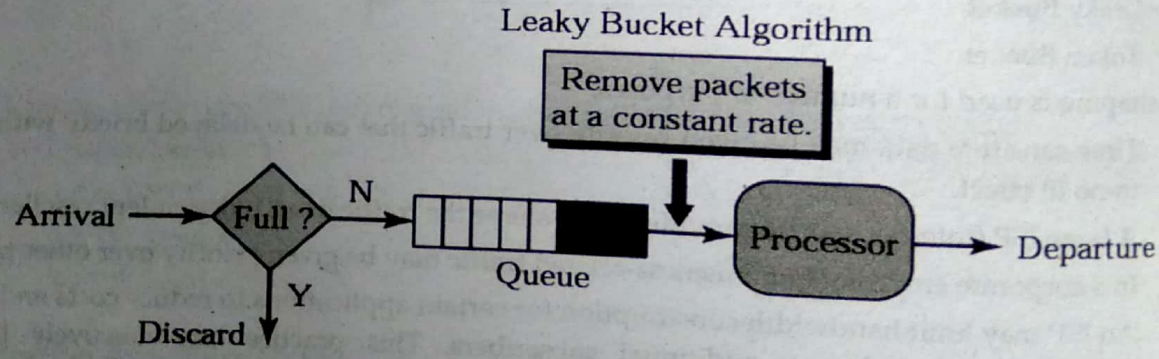


Figure 5.12

Token Bucket

The token bucket algorithm compare to Leaky Bucket Algorithm allow the output rate vary depending on the size of burst. In this algorithm the bucket holds token to transmit a packet, the host must capture and destroy one token. Token are generated by a clock at the rate of one token every second.

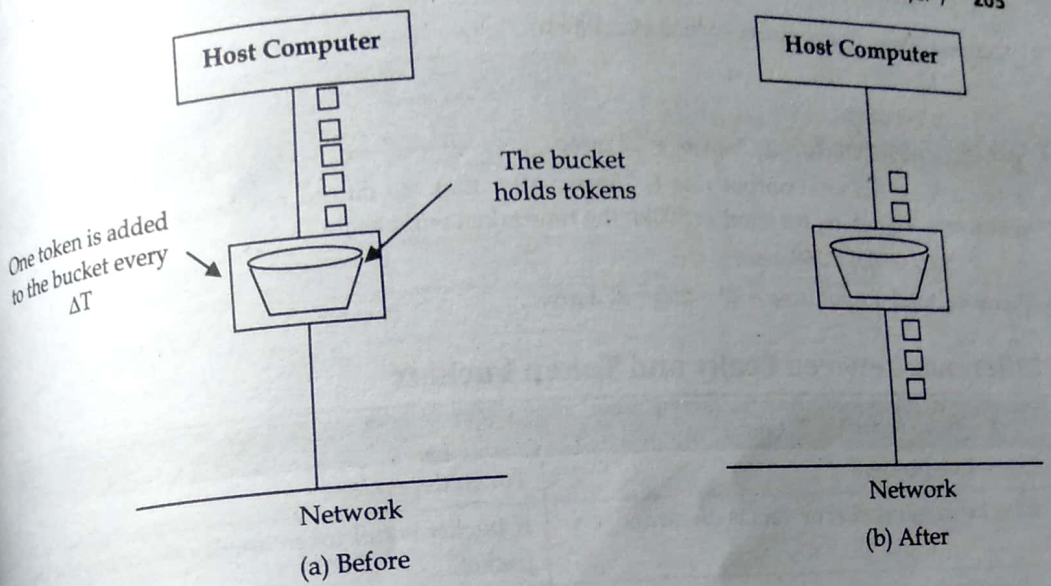


Figure 5.13

Algotithm

Setp-1: A token is added at every Δt time.

Setp-2: The bucket can hold b-token. If a token arrive when bucket is full it is discarded.

Step 3: when a packet of m bytes arrived m tokens are removed from the bucket and the packet is sent to the network.

Step 4: If less than n tokens are available no tokens are removed from the buckets and the packet is considered to be non conformant.

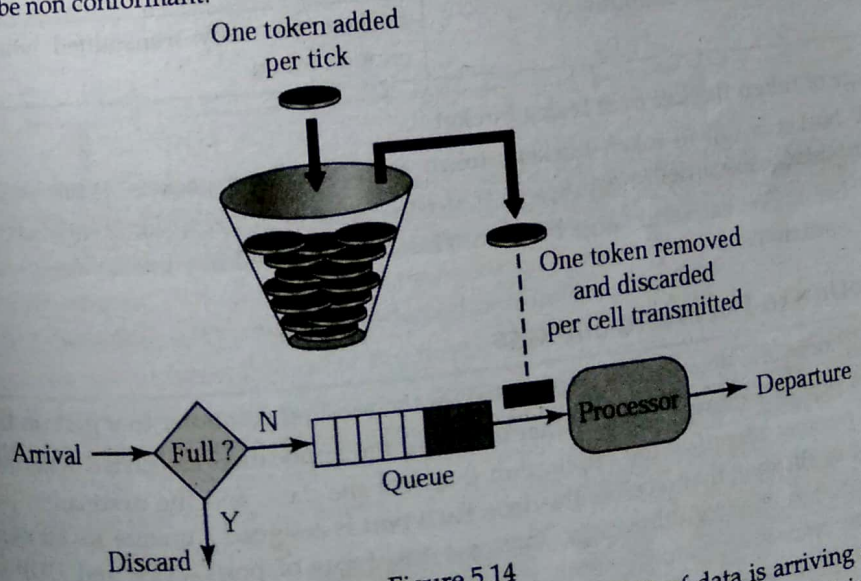


Figure 5.14

Example: Consider a frame relay network having a capacity of 1Mb of data is arriving at the rate of 25mbps for 40msec. The token arrival rate is 2mbps and the capacity of bucket is 500kb with maximum output rate 25mbps. Calculate 1). The Burst length 2). Total output time.

Solution: Here, C is capacity of bucket = 500kb

M = 25 mbps

ρ = 2 mbps

1. S = 500/((25-2)*1000) = 21.73msec = 22 msec
2. For 22msec the total output rate is 25msec after that the output rate becomes 2mbps i.e. token arrival rate. Therefore, for another 500kb the time taken will be,

500/(2000) = 250 msec

Therefore, total output time = 22 + 250 = 272 msec.

Difference between Leaky and Token buckets

	Token Bucket
Token Independent	Token dependent
If bucket is full packet or data is discarded.	If bucket is full token are discarded, but not the packet.
When the host has to send a packet, packet is thrown in bucket.	In this leaky bucket holds tokens generated at regular intervals of time.
Bucket leaks at constant rate	Bucket has maximum capacity.
Queue outputs at finite rate queue outputs at finite rate.	If there is a no token in bucket, packet cannot be send.
It does not save token	It saves token to send large bursts.
It sends the packet at constant rate	It allows large bursts to be sent faster rate after that constant rate.
Packets are transmitted continuously	Packets can only transmitted when there are enough token

Advantage of token Bucket over leaky bucket

- If bucket is full in token Bucket , token are discard not packets. While in leaky bucket, packets are discarded.
- Token Bucket can send Large bursts can faster rate while leaky bucket always sends packets at constant rate.

Introduction to Ports and Sockets

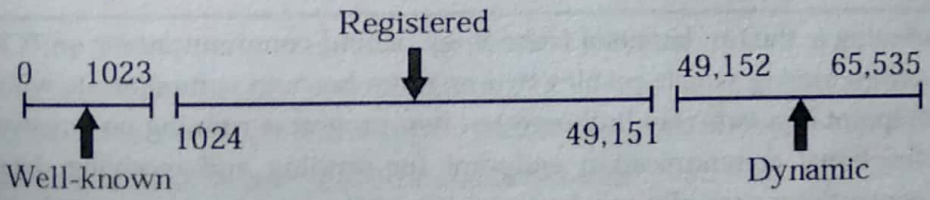
On a TCP/IP network, data travels from a port on the sending computer to a port on the receiving computer. A port is a numerical value that identifies the application associated with the data. The source port number identifies the application that sent the data, and the destination port number identifies the application that receives the data. Each port is assigned a unique 16- bit number in the range of 0 through 65535. Additionally, there are two types of ports—TCP and UDP—which are based on their respective protocols. Both TCP and UDP maintain a separate list of used (reserved and allocated) port numbers. This allows them both to make sure no port is duplicated within each list.

The well-known port numbers for common protocols are tabulated below:

Port	Protocol
UDP port 15	NETSTAT
TCP port 20	FTP Data
TCP port 21	FTP control
TCP port 22	SSH
TCP port 23	Telnet
TCP port 25	SMTP
TCP port 53	DNS zone transfers
UDP port 69	TFTP
TCP port 70	Gopher
TCP port 79	Finger

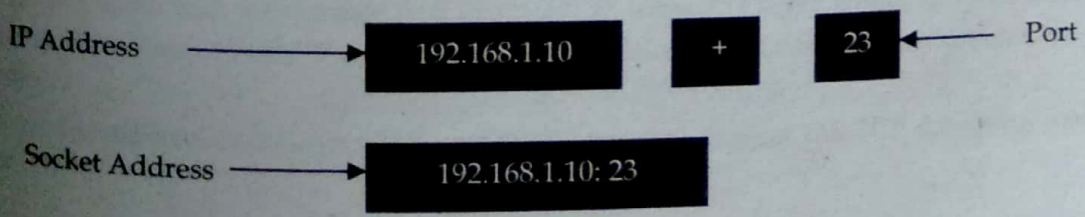
Port numbers are divided into ranges as follows:

- **Port numbers 0-1023 (Well-known ports)**: These are allocated to server services by the Internet Assigned Numbers Authority (IANA). E.g. Web servers normally use port 80 and SMTP servers use port 25.
- **Ports 1024-49151(Registered Port):** these can be registered for services with the IANA and should be treated as semi-reserved. User written programs should not use these ports.
- **Ports 49152-65535**: These are used by client programs and you are free to use these in client programs. When a web browser connects to a web server the browser will allocate itself a port in this range. Also known as ephemeral ports.



The combination of an IP address (more on IP addresses in a moment) and a port number is known as a ***socket***. A socket identifies a single network process in terms of the entire internet or other end to end IP-based internetwork. Two sockets one on the sending system and one on the receiving host are needed to define a connection for connection-oriented protocols, such as TCP.

A network socket is one endpoint in a statement flow in the middle of two programs running over a network, also it is maintaining and allow communication between two different processes on the same or different machines. In networking, a socket is used to allow many processes within a single or different host to use TCP communication simultaneously. The socket is formed by including the IP address with the port number to uniquely identify each separate data stream.



Differences between port and socket

Port is a number used by a particular software. The same port may be used in different computers/servers running same software.	Socket is a combination of port and IP-address to identify particular software and particular computer/server.
A port is a logical data connection that can be used to exchange data without the use of a temporary file or storage.	A socket is an end point of a bidirectional communication that occurs in a computer network that is based on the internet protocol.
A port is a numerical value that is assigned to an application in an endpoint of communication	A socket is an internal endpoint for sending and receiving data within a node on a computer network.
Port helps to identify a specific application or a process.	socket works as the interface to send and receive data through a specific port
Port operates at the transport layer of the OSI.	Sockets are a means of plugging the application layer.
A port functions like a telephone number, identifying the machine and giving the socket an area to connect.	While the socket functions like a cord that ties the computers together.
A port is request running on that socket and port uses socket to deliver the packet to correct application.	A socket is the way a server and a client keep track of request.

Socket Programming

Sockets programming is the fundamental technology behind communications on TCP/IP networks. It is a field of programming which enables two or more hosts to communicate with each other. A socket is one endpoint of a two-way link between two programs running on a network. The socket provides a bidirectional communication endpoint for sending and receiving data with another socket. Socket connections normally run between two different computers on a local area network (LAN) or across the internet, but they can also be used for inter-process communication on a single computer.

Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket (node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server. Socket programming usually pertains to the basic communication protocols like TCP/UDP and raw sockets like ICMP. These protocols have a small communication overhead when compared to underlying protocols such as HTTP/DHCP/SMTP etc.

Chapter 6
APPLICATION LAYER

Introduction

The application layer is a layer in the Open Systems Interconnection (OSI) seven-layer model and in the TCP/IP protocol suite. It consists of protocols that focus on process-to-process communication across an IP network and provides a firm communication interface and end-user services. The application layer provides full end-user access to a variety of shared network services for efficient OSI model data flow. This layer has many responsibilities, including error handling and recovery, data flow over a network and full network flow. It is also used to develop network-based applications. More than 15 protocols are used in the application layer, including File Transfer Protocol, Telnet, Trivial File Transfer Protocol and Simple Network Management Protocol.

A user may or may not directly interact with the applications. Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of Transport and all layers below it to communicate or transfer its data to the remote host. When an application layer protocol wants to communicate with its peer application layer protocol on remote host, it hands over the data or information to the Transport layer. The transport layer does the rest with the help of all the layers below it.

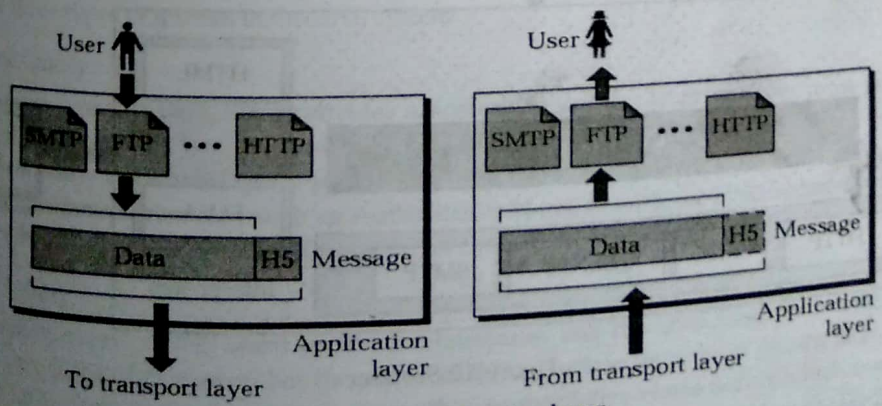


Figure 6.1 Application layer

Functions of Application layer

- **File Transfer:** It allows a user to access, retrieve and manage files in a remote computer.
- **Mail services:** It provides the basis for email forwarding and storage facilities.
- **Directory services:** It provides distributes database sources and access for glo information about various objects and services.

Web & HTTP

The World Wide Web (WWW), or the Web, is a repository of information spread all over the wo and linked together. The WWW has a unique combination of flexibility, portability, and us friendly features that distinguish it from other services provided by the Internet. The WWW toda a distributed client-server service, in which a client using a browser can access a service usin server. However, the service provided is distributed over many locations called websites.

The WWW uses the concept of hypertext and hypermedia. In a hypertext environment, informati is stored in a set of documents that are linked together using the concept of pointers. An item can associated with another document using a pointer. The reader who is browsing through document can move to other documents by choosing (clicking) the items that are linked to ot documents. To use WWW, we need three components: a browser, a web server, and a protocol cal the Hypertext Transfer Protocol (HTTP).

Browser

A variety of vendors offer commercial browsers that interpret and display a web document, and of them use nearly the same architecture. Each browser usually consists of three parts: a controll client programs, and interpreters. The controller receives input from the keyboard or the mouse a uses the client programs to access the document. After the document has been accessed, controller uses one of the interpreters to display the document on the screen. The client program c be one of the protocols described previously such as FTP, or TELNET, but it is usually HTTP. T interpreter is a language used today on the Internet such as HTML or Java

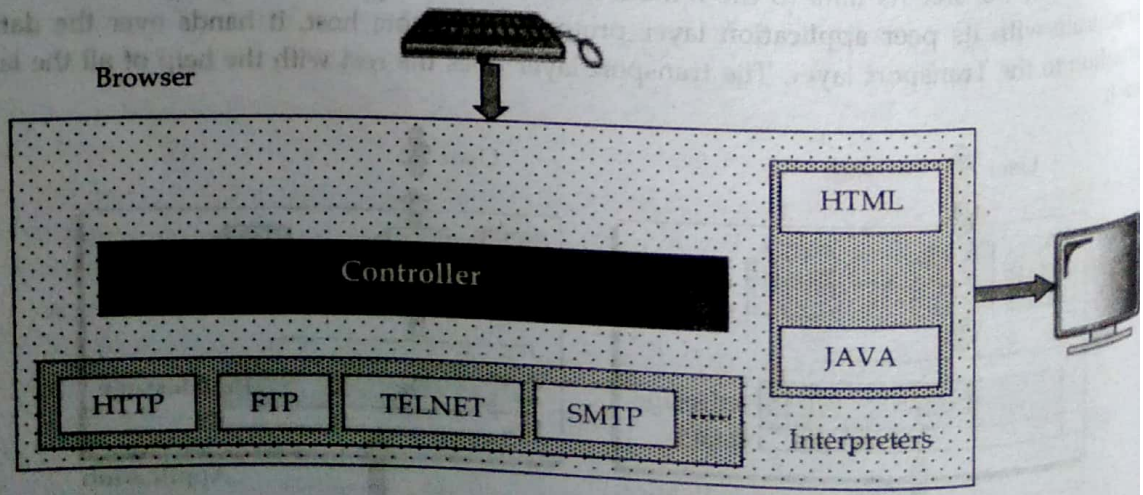


Figure 6.2 Browser

Server

The server stores all pages belonging to the site.

Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. The protocol transfers data in the form of plain text, hypertext, audio, video, and so on. It is called the Hypertext Transfer Protocol because its efficiency allows its use in a hypertext environment where there are rapid jumps from one document to another.

The idea of HTTP is very simple. A client sends a request, which looks like mail, to the server. The server sends the response, which looks like a mail reply, to the client. The request and response messages carry data in the form of a letter with MIME-like format.

The commands from the client to the server are embedded in a letter like request message. The contents of the requested file or other information are embedded in a letter like response message.

DNS and the Query Types

DNS is a global system for translating IP addresses to human-readable domain names. When a user tries to access a web address like "example.com", their web browser or application performs a DNS Query against a DNS server, supplying the hostname. The DNS server takes the hostname and resolves it into a numeric IP address, which the web browser can connect to.

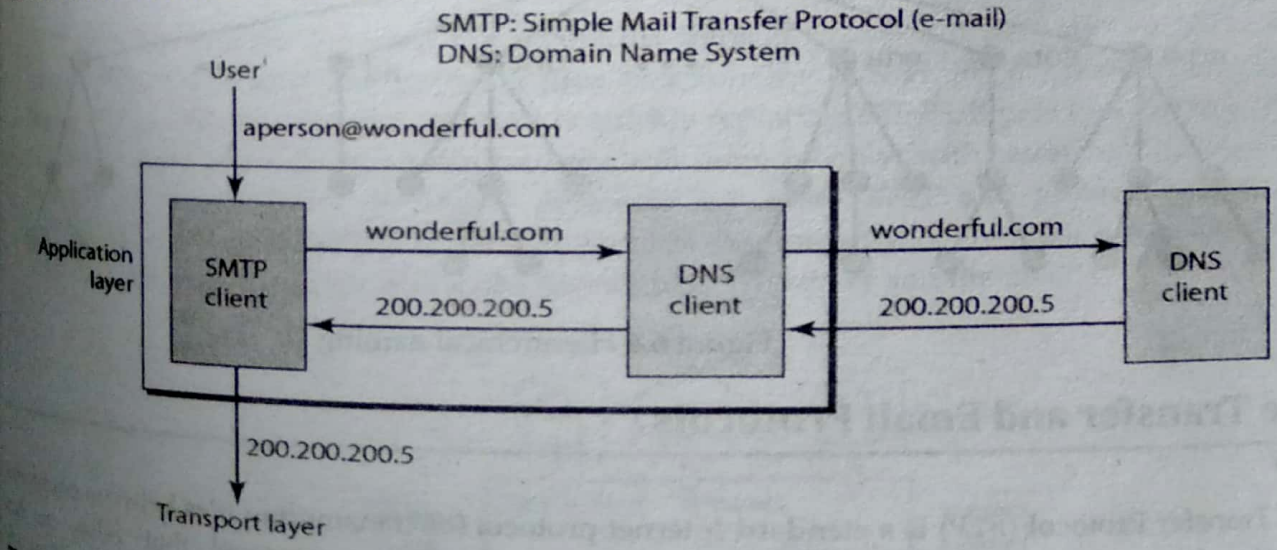


Figure 6.3 DNS service

There are three types of queries in the DNS system:

Recursive Query

In a recursive query, a DNS client provides a hostname, and the DNS Resolver must provide an answer—it responds with either a relevant resource record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS Root Server, until it finds the Authoritative Name Server (for more on Authoritative Name Servers see DNS Server Types below) that holds the IP address and other information for the requested hostname.

Iterative Query

In an iterative query, a DNS client
answer it can. If
refers

Non-Recursive Query

A non-recursive query is a query in which the DNS Resolver already knows the answer. It either immediately returns a DNS record because it already stores it in local cache, or queries a DNS Name Server which is authoritative for the record, meaning it definitely holds the correct IP for that hostname. In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client.

DNS name space and domain name space

To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses

- Flat Name Space and
- Hierarchical 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.

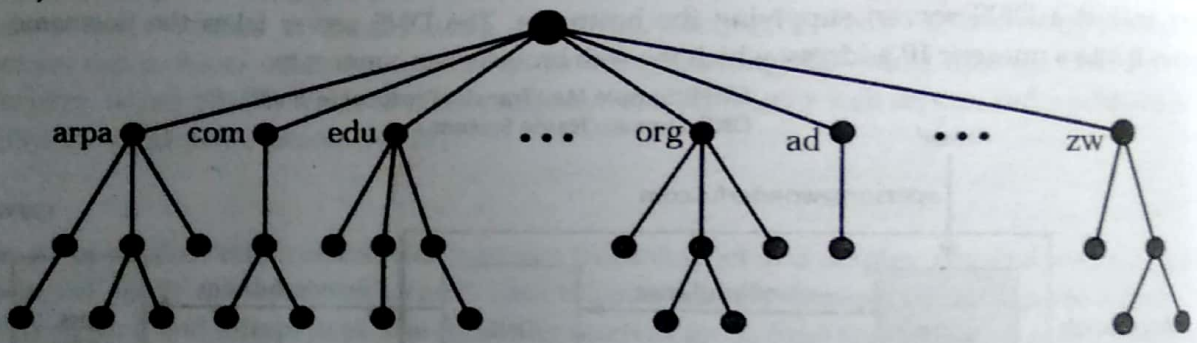


Figure 6.4 Hierarchical naming

File Transfer and Email Protocols

FTP

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections. FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.

File Transfer Protocol (FTP) is the standard mechanism for one of the most common tasks on the Internet, copying a file from one computer to another. Although file transfer from one system to another seems simple and straight- forward, some problems must be dealt with first. For example, two systems may use different file name conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. All of these problems have been solved by FTP in a very simple and elegant approach.

FTP differs from other client-server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication. We need to transfer only a line of command or

a line of response at a time. The data connection, on the other hand, needs more complex rules due to the variety of data types transferred.

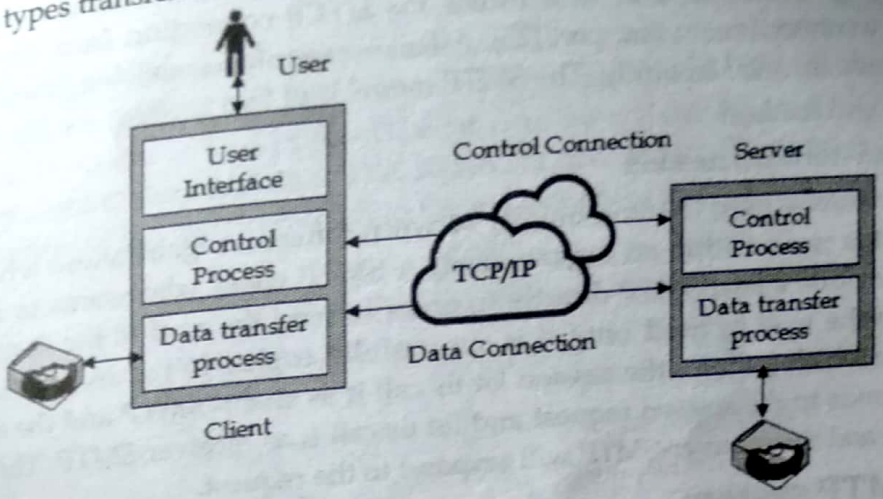


Figure 6.5 Control and data connection in FTP

SFTP

SFTP (SSH File Transfer Protocol) is a secure file transfer protocol. It runs over the SSH protocol. It supports the full security and authentication functionality of SSH. SFTP has pretty much replaced legacy FTP as a file transfer protocol, and is quickly replacing FTP/S. It provides all the functionality offered by these protocols, but more securely and more reliably, with easier configuration. There is basically no reason to use the legacy protocols any more. SFTP also protects against password sniffing and man-in-the-middle attacks. It protects the integrity of the data using encryption and cryptographic hash functions, and authenticates both the server and the user.

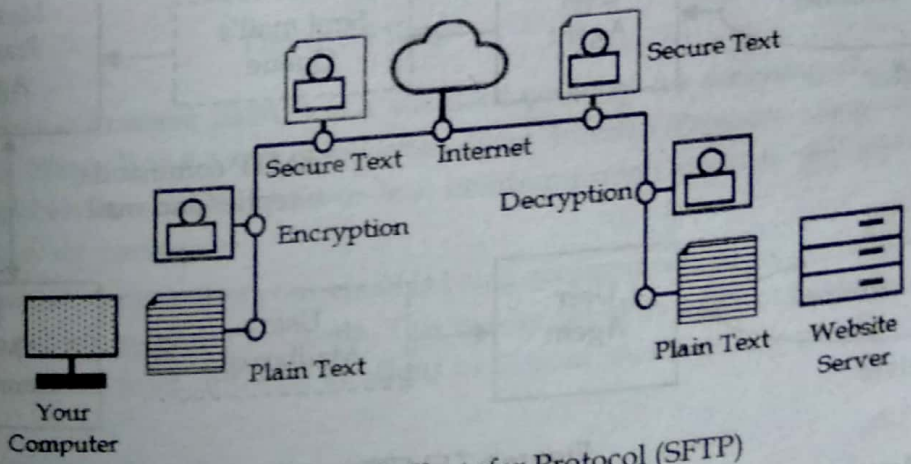


Figure 6.6 Secure File Transfer Protocol (SFTP)

SMTP

SMTP stands for "Simple Mail Transfer Protocol." It is a connection-oriented, text-based network protocol from the internet protocol family and is located on the seventh layer of the OSI model: the application layer. Just like any other network protocol, it contains rules for correct communication between computers in a network. SMTP is responsible for feeding and forwarding e-mails from sender to recipient.

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly. The SMTP model is of two types:

1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method is used within an organization. A SMTP client who wants to send the mail will contact the destination's host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP. The client SMTP is the one which initiates the session let us call it as client- SMTP and the server SMTP is the one which responds to the session request and let us call it as receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

Model of SMTP system

In the SMTP model user deals with the user agent (UA) for example Microsoft outlook, Netscape, Mozilla etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the Message Transfer Agent (MTA) it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.

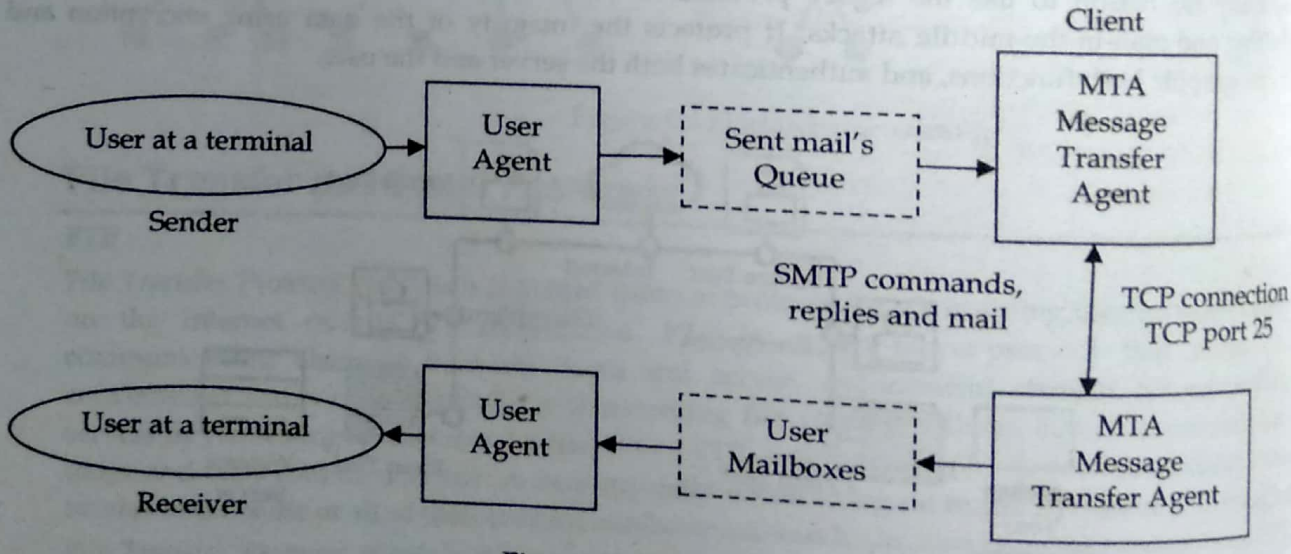


Figure 6.7 SMTP system

Internet Message Access Protocol (IMAP)

IMAP (Internet Message Access Protocol) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device. This allows users to organize messages into folders, have multiple client applications know which messages have been read, flag messages for urgency or follow-up and save draft messages on the server.

with another client/server email protocol, Post Office Protocol 3 (POP3). ...for the end user in a single mailbox on the server and moved to the end ...e mail client opens. While POP3 can be thought of as a "store-and-forward" ...ought of as a remote file server. Most implementations of IMAP support ...ows the end user to simultaneously connect to the email server with different ...e end user could connect to the mail server with his Outlook iPhone app and ...ers at the same time. The details for how to handle multiple connections are ...t are instead left to the developers of the mail client.

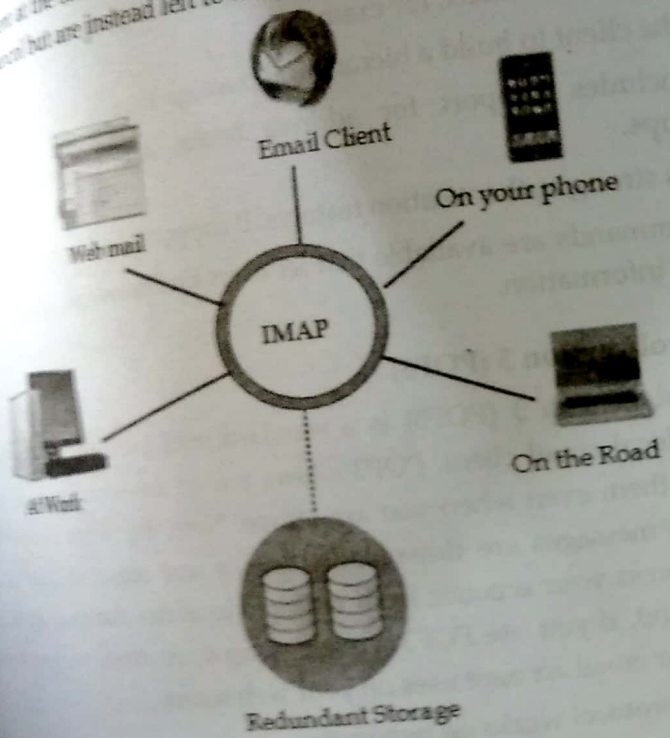


Figure 6.8 Scope of IMAP

...Access Protocol (IMAP) is a standard protocol for accessing email on a remote ...a mail client. IMAP is an application layer Internet Protocol using the underlying ...protocols to establish host-to-host communication services for applications like ...a remote mail server.

...protocol assumes that your email is being accessed only from one application. IMAP ...access by multiple clients. This is why IMAP is more suitable for you if you ...your email from different locations or if your messages are managed by multiple ...

...IMAP protocol works on two ports:

- ...is the default IMAP non-encrypted port
- ...is the port you need to use if you want to connect using IMAP securely.

...enables users to send and receive emails through a remote server. ...a particular device. This type of email access is ideal for business users ...from their home desktop or office computer.

...available with IMAP that are not available in POP are described here.

- Clients can selectively download only the mail they want to read from the server by reviewing message headers.
- Clients may choose to download only part of a message. This is useful if a message has a large attachment and the user is working on a slow link. The attachment can be downloaded later.
- Shared mailboxes are available for workgroup use. All members of the workgroup are allowed to post and receive mail from the shared mailbox. The minutes of a meeting could be posted in the mailbox, for example.
- Allows the client to build a hierarchical message store on the server for storing messages.
- IMAP includes support for address books, and links to documents and USENET newsgroups.
- IMAP has strong authentication features. It supports Kerberos and other security protocols.
- Search commands are available that let users find messages based on their header, subject, or content information.

Post Office Protocol version 3 (POP3)

Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server. This means that if you access your account from multiple locations that may not be the best option for you. On the other hand, if you use POP3, your messages are stored on your local computer, which reduces the space your email account uses on your web server.

By default, the POP3 protocol works on two ports:

- **Port 110:** this is the default POP3 non-encrypted port
- **Port 995:** this is the port you need to use if you want to connect using POP3 securely

Post Office Protocol (POP) is simple but limited in functionality. The client POP soft- ware is installed on the recipient computer; the server POP software is installed on the mail server. Mail access starts with the client when the user needs to download the received email from the mailbox on the mail server. The client (user agent) sends the user name and password to access the mailbox. The user can then list and retrieve the mail messages, one by one. Figure below shows an example of downloading using POP.

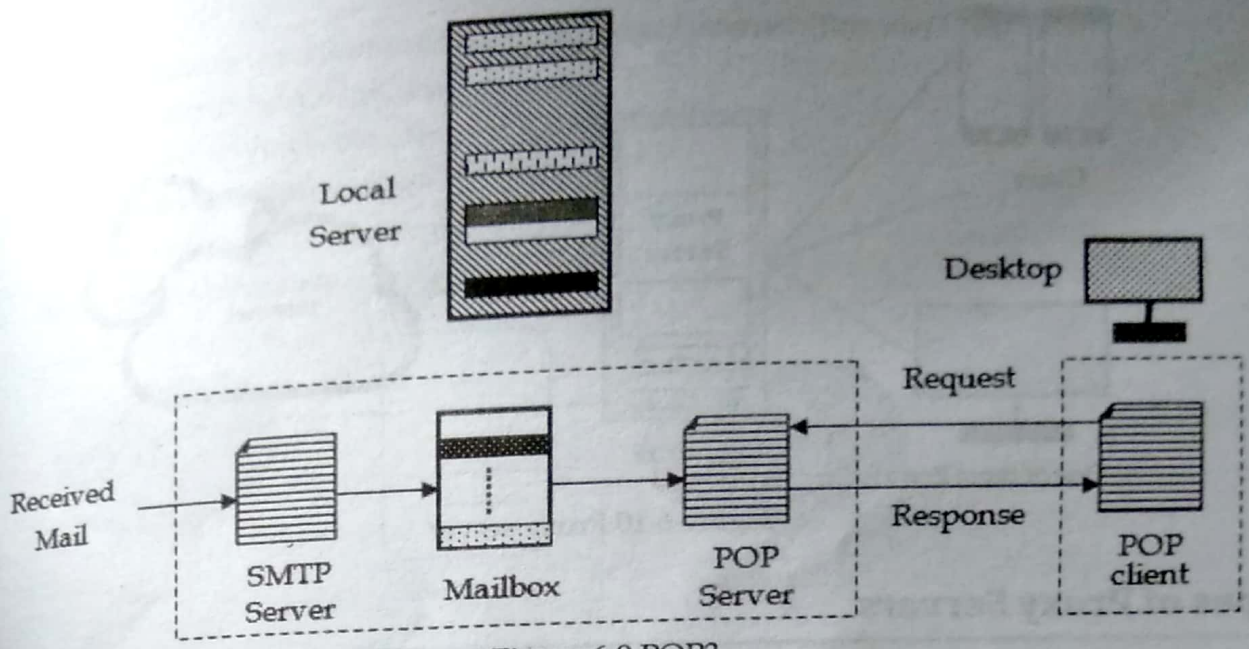


Figure 6.9 POP3

Overview of Application Server Concepts

An application server is a component-based product that resides in the middle-tier of a server centric architecture. It provides middleware services for security and state maintenance, along with data access and persistence.

An application server is a server program in a computer in a distributed network that provides the business logic for an application program. The application server is frequently viewed as part of a three-tier application, consisting of a graphical user interface (GUI) server, an application (business logic) server, and a database and transaction server. More descriptively, it can be viewed as dividing an application into:

- A first-tier, front-end, Web browser-based graphical user interface, usually at a personal computer or workstation
- A middle-tier business logic application or set of applications, possibly on a local area network or intranet server
- A third-tier, back-end, database and transaction server, sometimes on a mainframe or large server

Proxy Application Server

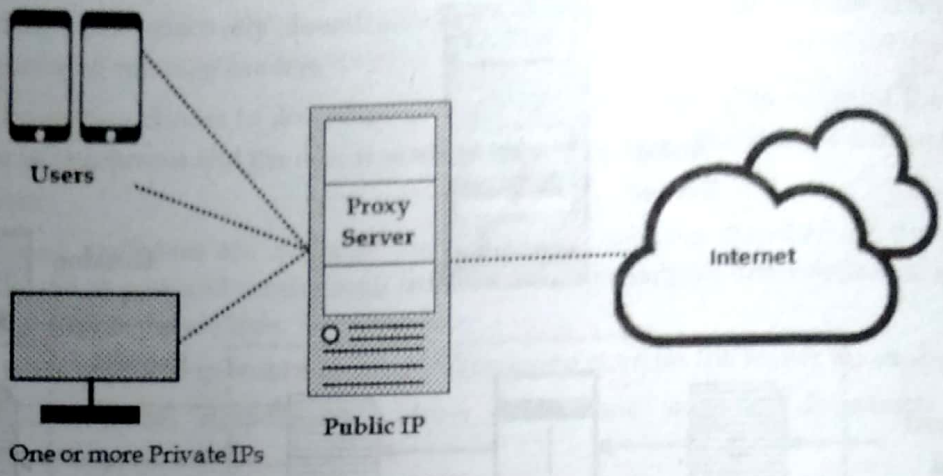


Figure 6.10 Proxy server

Types of Proxy Servers

Not all proxy servers work the same way. It's important to understand exactly what functionality you're getting from the proxy server, and ensure that the proxy server meets your use case. Following table briefly describes the type of proxies:

Forward Proxies

In this the client requests its internal network server to forward to the internet. **Forward proxy can be used by the client to** bypass firewall restrictions in order to visit websites that are blocked by school, government, company etc. If a website blocked an IP range from visiting the website, then a person in that IP range can use forward proxy to hide the real IP of the client so that person can visit the website and maybe leave some spam comments. There are some paid proxy service that has numerous proxy systems around the world so that they can change your IP address every time your visit a new web page and this makes it harder for website administrators to detect.

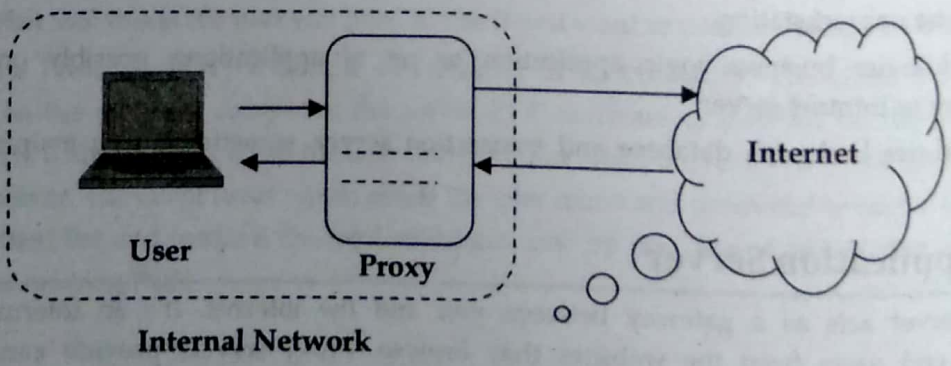


Figure 6.11 Forward proxy example

Open Proxies

Open Proxies helps the clients to conceal their IP address while browsing the web. An **open proxy** is a **proxy** server that is accessible by any Internet user. Generally, a **proxy** server only allows users within a network group (i.e. a closed **proxy**) to store and forward Internet services such as DNS or web pages to reduce and control the bandwidth used by the group. Following are the some list of open proxies

- http://directory.google.com/Top/Computers/Internet/Proxies/Free/?il=1
- http://tools.rosinstrument.com/proxy/
- http://www.stayinvisible.com/
- http://www.multiproxy.org/
- http://www.openproxies.com/
- http://www.blackcode.com/proxy/

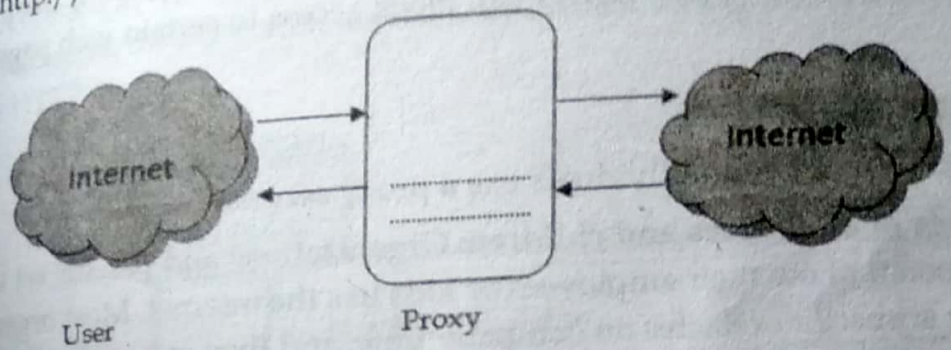
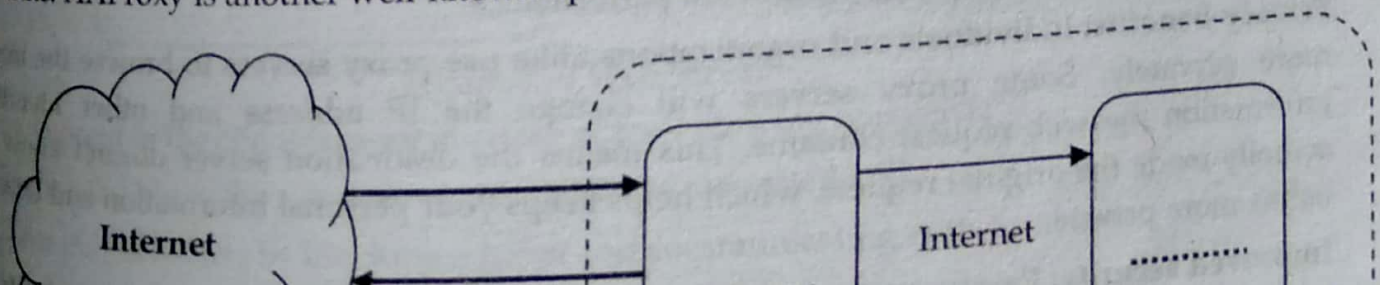


Figure 6.12 Open proxy example

Reverse Proxies

In this the requests are forwarded to one or more proxy servers and the response from the proxy server is retrieved as if it came directly from the original Server.

Reverse proxy is mainly used by server admin to achieve load balancing and high availability. A website may have several web servers behind the reverse proxy. The reverse proxy server takes requests from the Internet and forwards these requests to one of the web servers. Most visitors don't know websites are using reverse proxy because they usually lack the knowledge and tools to detect it or they simply don't care about it. Nginx can be acting both a web server and a reverse proxy at the same time. HAProxy is another well-known open-source reverse proxy software.



A proxy server is basically a computer on the internet with its own IP address that your computer knows. When you send a web request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the web server, and forwards you the web page data so you can see the page in your browser.

When the proxy server forwards your web requests, it can make changes to the data you send and still get you the information that you expect to see. A proxy server can change your IP address, so the web server doesn't know exactly where you are in the world. It can encrypt your data, so your data is unreadable in transit. And lastly, a proxy server can block access to certain web pages, based on IP address.

Why Should You Use a Proxy Server?

There are several reasons organizations and individuals use a proxy server.

- **To control internet usage of employees and children:** Organizations and parents set up proxy servers to control and monitor how their employees or kids use the internet. Most organizations don't want you looking at specific websites on company time, and they can configure the proxy server to deny access to specific sites, instead redirecting you with a nice note asking you to refrain from looking at said sites on the company network. They can also monitor and log all web requests, so even though they might not block the site, they know how much time you spend cyber loafing.
- **Bandwidth savings and improved speeds:** Organizations can also get better overall network performance with a good proxy server. Proxy servers can cache (save a copy of the website locally) popular websites so when you ask for www.youtube.com, the proxy server will check to see if it has the most recent copy of the site, and then send you the saved copy. What this means is that when hundreds of people hit www.youtube.com at the same time from the same proxy server, the proxy server only sends one request to youtube.com. This saves bandwidth for the company and improves the network performance.
- **Privacy benefits:** Individuals and organizations alike use proxy servers to browse the internet more privately. Some proxy servers will change the IP address and other identifying information the web request contains. This means the destination server doesn't know who actually made the original request, which helps keeps your personal information and browsing habits more private.
- **Improved security:** Proxy servers provide security benefits on top of the privacy benefits. You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions. You can also prevent known malware sites from any access through the proxy server. Additionally, organizations can couple their proxy server with a Virtual Private Network (VPN), so remote users always access the internet through the company proxy. A VPN is a direct connection to the company network that companies provide to external or remote users. By using a VPN, the company can control and verify that their users have access to the resources (email, internal data) they need, while also providing a secure connection for the user to protect the company data.
- **Get access to blocked resources:** Proxy servers allow users to circumvent content restrictions imposed by companies or governments. Is the local sports ball team's game blacked out online? Log into a proxy server on the other side of the country and watch from there. The proxy server makes it look like you are in California, but you actually live in North Carolina. Several governments around the world closely monitor and restrict access to the internet, and proxy servers offer their citizens access to an uncensored internet.

Web Application Server

Web server is a computer where the web content is stored. Basically web server is used to host the web sites but there exists other web servers also such as gaming, storage, FTP, email etc. Web site is collection of web pages while web server is software that responds to the request for web resources. When client sends request for a web page, the web server search for the requested page if requested page is found then it will send it to client with an HTTP response. If the requested web page is not found, web servers will the send an **HTTP response: Error 404 not found.** If client has requested for some other resources then the web server will contact to the application server and data store to construct the HTTP response.

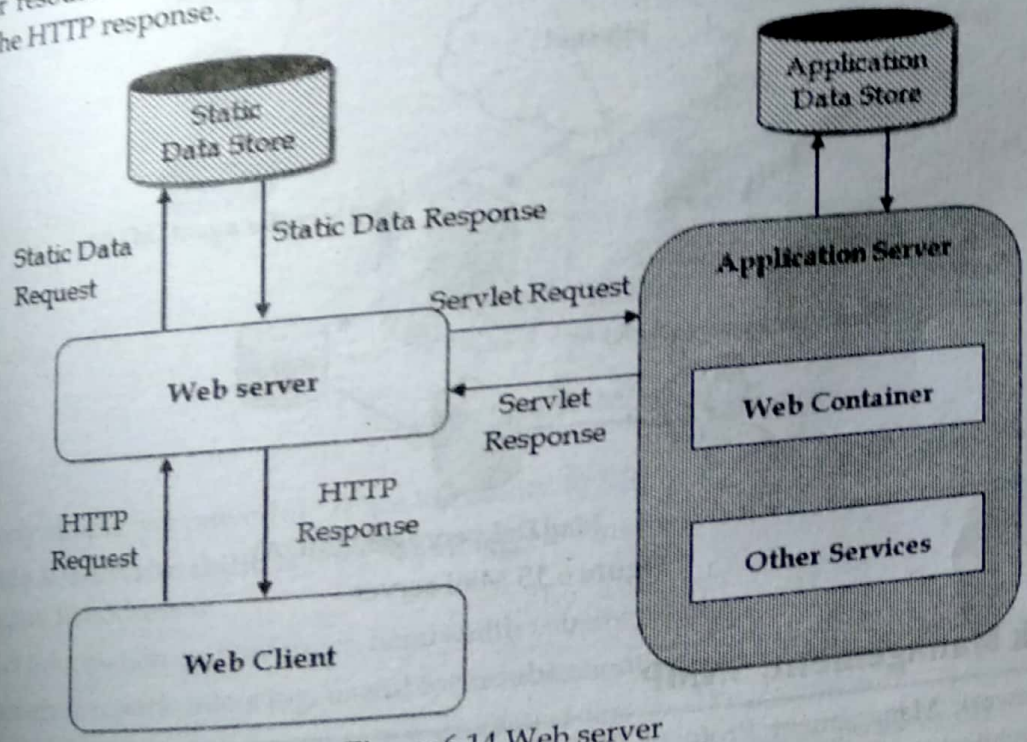


Figure 6.14 Web server

Web server respond to the client request in either of the following two ways:

- Sending the file to the client associated with the requested URL.
- Generating response by invoking a script and communicating with database

Mail Application Server

A mail server (also known as a mail transfer agent or MTA, a mail transport agent, a mail router or an Internet mailer) is an application that receives incoming e-mail from local users (people within the same domain) and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. Microsoft Exchange, sendmail, qmail are some common mail server programs.

The mail server works in conjunction with other programs to make up what is sometimes referred to as a messaging system. A messaging system includes all the applications necessary to keep e-mail moving as it should. When you send an e-mail message, your e-mail program, such as Outlook or Eudora, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a **message store** to be forwarded later

Mail servers can be broken down into two main categories: outgoing mail servers and incoming mail servers. Outgoing mail servers are known as SMTP, or Simple Mail Transfer Protocol, servers.

Incoming mail servers come in two main varieties. POP3, or Post Office Protocol, version 3, servers are best known for storing sent and received messages on PCs' local hard drives. IMAP, or Internet Message Access Protocol, servers always store copies of messages on servers. Most POP3 servers can store messages on servers, too, which is a lot more convenient.

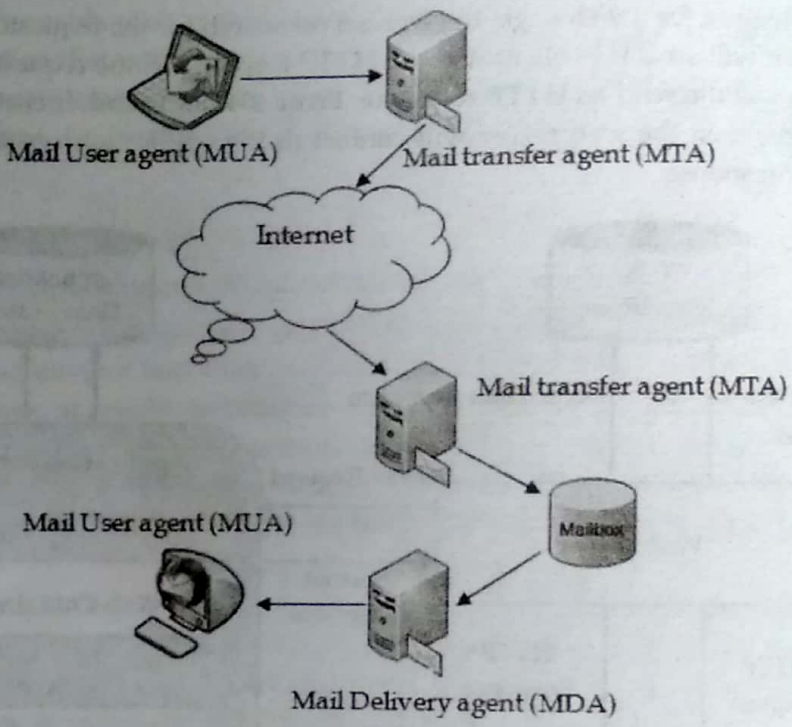


Figure 6.15 Mail server

Network Management: SNMP

Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol (TCP/IP) protocol suite. SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the professional-grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the network management system (NMS).

Simple Network Management Protocol (SNMP) is a set of protocols for network management and monitoring. These protocols are supported by many typical network devices such as routers, hubs, bridges, switches, servers, workstations, printers, modem racks and other network components and devices. Supported devices are all network-attached items that must be monitored to detect conditions. These conditions must be addressed for proper, appropriate and ongoing network administration. SNMP standards include an application layer protocol, a set of data objects and a methodology for storing, manipulating and using data objects in a database schema.

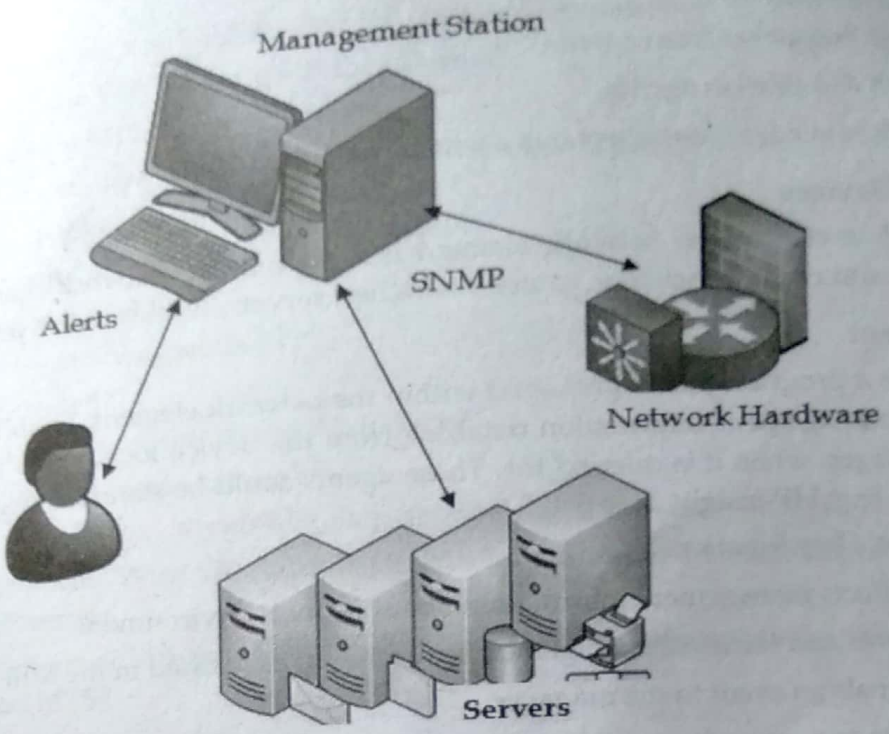


Figure 6.16 SNMP example

SNMP is very simple, yet powerful. It has the ability to help you manage your network by:

- **Provide Read/Write abilities –** for example you could use it to reset passwords remotely, or re-configure IP addresses.
- Collect information on how much bandwidth is being used.
- Collect error reports into a log, useful for troubleshooting and identifying trends.
- Email an alert when your server is low on disk space.
- Monitor your servers' CPU and Memory use, alert when thresholds are exceeded.
- Page or send an SMS text-message when a device fails.
- Can perform active polling, i.e. Monitoring station asks devices for status every few minutes.
- **Passive SNMP** – devices can send alerts to a monitoring station on error conditions.

SNMP basic components and their functionalities

SNMP consists of following four components:

- SNMP Manager
- Managed devices
- SNMP agent
- Management Information Database or Management Information Base (MIB)

SNMP Manager

A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager's key functions

- Queries agents
- Gets responses from agents
- Sets variables in agents
- Acknowledges asynchronous events from agents

Managed Devices

A managed device or the network element is a part of the network that requires some form of monitoring and management e.g. routers, switches, servers, workstations, printers, UPSs, etc...

SNMP Agent

The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (e.g. Net-SNMP) or specific to a vendor (e.g. HP insight agent)

SNMP agent's key functions

- Collects management information about its local environment
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non-SNMP manageable network node.

Management Information database or Management Information Base (MIB)

Every SNMP agent maintains an information database describing the managed device parameters. The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the Network Management System (NMS). This commonly shared database between the Agent and the Manager is called Management Information Base (MIB). Typically these MIB contains standard set of statistical and control values defined for hardware nodes on a network. SNMP also allows the extension of these standard values with values specific to a particular agent through the use of private MIBs.

In briefly, MIB files are the set of questions that a SNMP Manager can ask the agent. Agent collects these data locally and stores it, as defined in the MIB. So, the SNMP Manager should be aware of these standard and private questions for every type of agent.

Exercise

1. In the client-server model, what is the role of the client program? What is the role of the server program?
2. What application program allows connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system?
3. How is TFTP different from FTP?
4. What is the function of SMTP?
5. What is the difference between a user agent (UA) and a mail transfer agent (MTA)?
6. How does MIME enhance SMTP?

Chapter 7

MULTIMEDIA AND FUTURE NETWORKING

Overview Multimedia Streaming Protocols

We use the term multimedia to refer to data that contains audio or video, and may include text. The phrase real-time multimedia refers to multimedia data that must be reproduced at exactly the same rate that it was captured (e.g., a television news program that includes audio and video of an actual event).

Instead of requiring the underlying networks to handle real-time transmission, the Internet uses additional protocol support. Interestingly, the most significant problem to be handled is jitter, not packet loss. To see why, consider a live webcast. If a protocol uses timeout-and-retransmission to resend the packet, the retransmitted packet will arrive too late to be useful — the receiver will have played the video and audio from successive packets and it makes no sense to insert a snippet of the webcast that was missed earlier.

Stream Control Transmission Protocol (SCTP)

The Stream Control Transmission Protocol (SCTP) is a computer networking communications protocol which operates at the transport layer and serves a role similar to the popular protocols TCP and UDP. It is standardized by IETF in RFC 4960. SCTP provides some of the features of both UDP and TCP: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP. It differs from those protocols by providing multi-homing and redundant paths to increase resilience and reliability. SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users:

- Acknowledged error-free non-duplicated transfer of user data.
- Data fragmentation to conform to discovered path MTU size.
- Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages.
- Optional bundling of multiple user messages into a single SCTP packet.

- Network-level fault tolerance through supporting of multi-homing at either or both ends of an association.

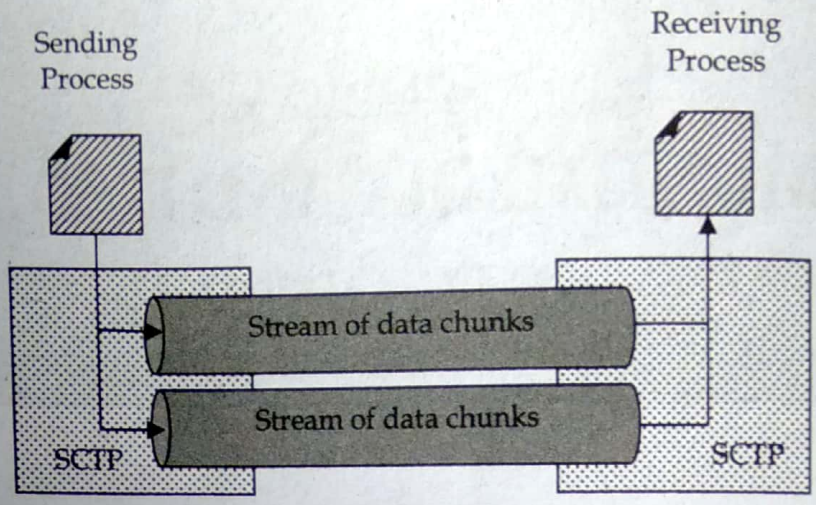


Figure 7.1: SCTP

Features of SCTP

- Multi homing support in which one or both endpoints of a connection can consist of more than one IP address, enabling transparent failover between redundant network paths.
- Delivery of chunks within independent streams eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.
- Path selection and monitoring to select a primary data transmission path and test the connectivity of the transmission path.
- Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks

Overview of Software-defined networking (SDN)

Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The Open Flow protocol is a foundational element for building SDN solutions.

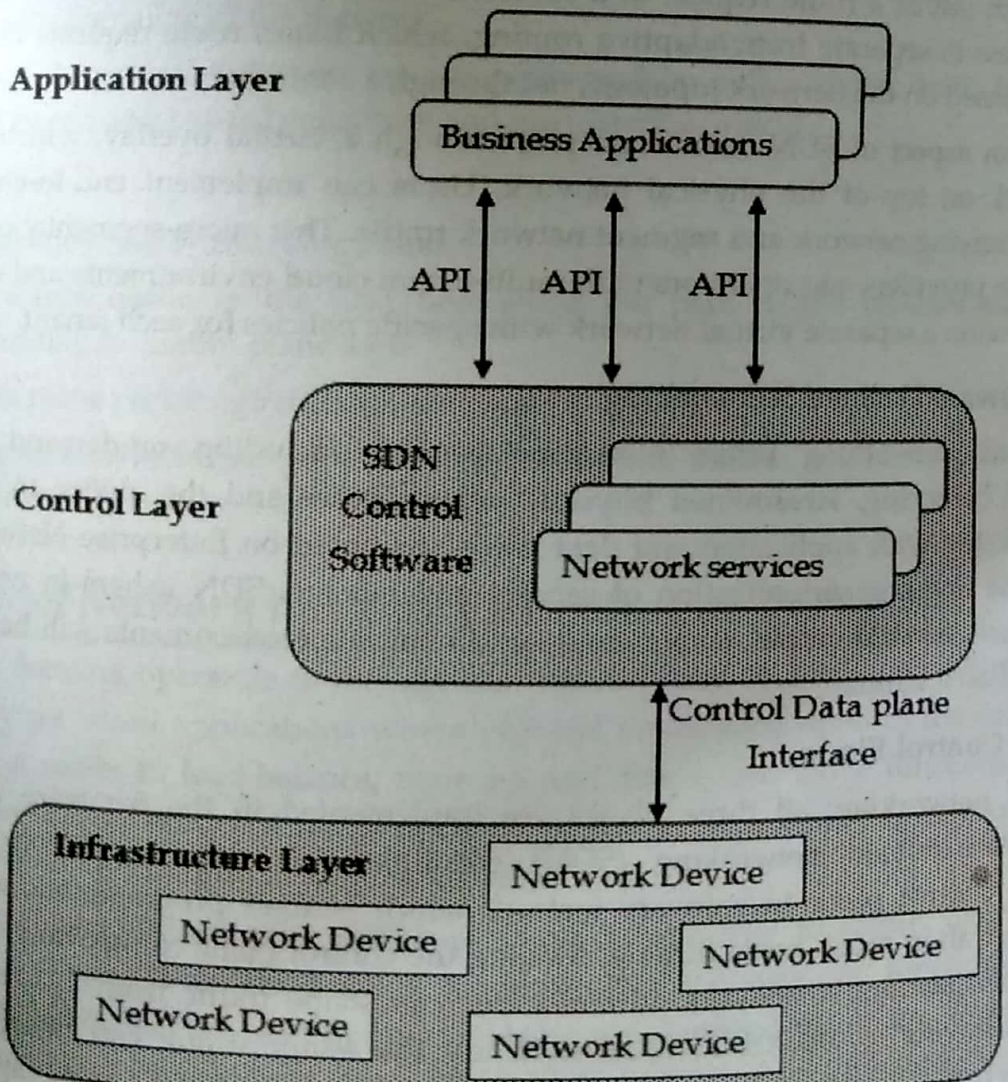
In a software-defined network, a network engineer or administrator can shape traffic from a centralized control console without having to touch individual switches in the network. The centralized SDN controller directs the switches to deliver network services wherever they're needed, regardless of the specific connections between a server and devices. This process is a move away from traditional network architecture, in which individual network devices make traffic decisions based on their configured routing tables.

SDN architecture

A typical representation of SDN architecture comprises three layers: the application layer, the control layer and the infrastructure layer.

The application layer, not surprisingly, contains the typical network applications or functions organizations use, which can include intrusion detection systems, load balancing or firewalls. Where a traditional network would use a specialized appliance, such as a firewall or load balancer, a software-defined network replaces the appliance with an application that uses the controller to manage data plane behavior.

The control layer represents the centralized SDN controller software that acts as the brain of the software-defined network. This controller resides on a server and manages policies and the flow of traffic throughout the network. The infrastructure layer is made up of the physical switches in the network.



decisions about how packets should flow through the network, the data plane actually moves packets from place to place.

In a classic SDN scenario, a packet arrives at a network switch, and rules built into the switch's proprietary firmware tell the switch where to forward the packet. These packet-handling rules are sent to the switch from the centralized controller.

The switch -- also known as a data plane device -- queries the controller for guidance as needed, and it provides the controller with information about traffic it handles. The switch sends every packet going to the same destination along the same path and treats all the packets the exact same way.

Software-defined networking uses an operation mode that is sometimes called adaptive or dynamic, in which a switch issues a route request to a controller for a packet that does not have a specific route. This process is separate from adaptive routing, which issues route requests through routers and algorithms based on the network topology, not through a controller.

The virtualization aspect of SDN comes into play through a virtual overlay, which is a logically separate network on top of the physical network. Users can implement end-to-end overlays to abstract the underlying network and segment network traffic. This micro-segmentation is especially useful for service providers and operators with multi-tenant cloud environments and cloud services, as they can provision a separate virtual network with specific policies for each tenant.

Benefits of Software Defined Networking

Software defined networking offers numerous benefits including on-demand provisioning, automated load balancing, streamlined physical infrastructure and the ability to scale network resources in lockstep with application and data needs. As noted on Enterprise Networking Planet, coupled with the ongoing virtualization of servers and storage, SDN ushers in no less than the completely virtualized data center, where end-to-end compute environments will be deployed and decommissioned on a whim.

SDN Data and Control Plane

In conventional networking, all three planes are implemented in the firmware of routers and switches. Software-defined networking (SDN) decouples the data and control planes and implements the control plane in software instead, which enables programmatic access to make network administration much more flexible. Moving the control plane to software allows dynamic access and administration. A network administrator can shape traffic from a centralized control console without having to touch individual switches. The administrator can change any network switch's rules when necessary -- prioritizing, de-prioritizing or even blocking specific types of packets with a very granular level of control.

Conceptually, data plane is the part where all the packet processing and forwarding logic is there. Data plane decides what to do with the packet, where to transfer, whether to encapsulate or encapsulate the packet. It is also known as forwarding plane. Control plane provides the management interface through which network can be configured.

Generally, these control plane and data plane are tightly coupled. For example, network admin can assign VLANs or he can fill the forwarding entries in the in the forwarding tables. But he can configure particular classification rules or cannot control how packets are handled. So we need to decouple the vendor's control plane with customized version and we should be able to control the packet processing and forwarding from this control system.

Difference between control plane & data plane

Control Plane

- Makes decisions about where traffic is sent
- Control plane packets are destined to or locally originated by the router itself
- The control plane functions include the system configuration, management, and exchange of routing table information
- The route controller exchanges the topology information with other routers and constructs a routing table based on a routing protocol, for example, RIP, OSPF or BGP
- Control plane packets are processed by the router to update the routing table information.
- It is the Signaling of the network
- Since the control functions are not performed on each arriving individual packet, they do not have a strict speed constraint and are less time-critical

Data Plane

- Also known as Forwarding Plane
- Forwards traffic to the next hop along the path to the selected destination network according to control plane logic
- Data plane packets go through the router
- The routers/switches use what the control plane built to dispose of incoming and outgoing frames and packets

Overview of Network function virtualization (NFV)

NFV allows network operators to manage and expand their network capabilities on demand using virtual, software based applications where physical boxes once stood in the network architecture. This makes it easier to load-balance, scale up and down, and move functions across distributed hardware resources. With continual updates, operators can keep things running on the latest software without interruption to their customers.

Network functions virtualization (NFV) provides a new way to create, distribute, and operate networking services. It is the process of decoupling the network functions from proprietary hardware appliances so they can run in software on standardized hardware. These functions (such as firewall, deep packet inspection, and intrusion prevention) become virtual network functions (VNF).

NFV is designed to consolidate and deliver the networking components needed to support an infrastructure totally independent from hardware. These components include virtual compute, storage and network functions. NFV utilizes standard IT virtualization technologies that run on off-the-shelf hardware like commodity x86 servers. It is applicable to any data plane processing or control plane function in both wired and wireless network infrastructures.

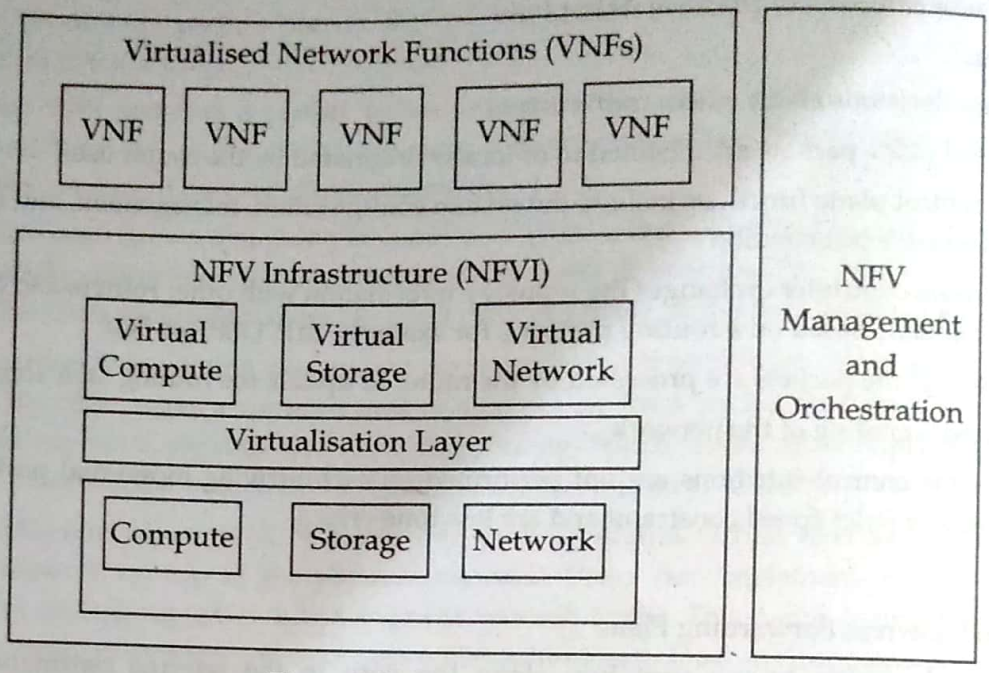


Figure 7.3: Components of NFV

The Benefits of NFV

NFV virtualizes network services via software to enable operators to:

- Reduce CapEx by reducing the need to purchase purpose-built hardware and using pay-as-you-grow models to eliminate wasteful over-provisioning.
- Reduce OpEX by reducing space, power and cooling requirements of equipment and simplifying the rollout and management of network services.
- Accelerate time-to-market by reducing the time required to deploy new networking services to support changing business requirements, new market opportunities, and return on investment of new services. NFV lowers the risks associated with rolling out new services, allowing providers to easily trial and evolve services to determine what best meets the needs of customers.
- Deliver agility and flexibility to quickly scale services up or down to address changing demands; services can be delivered via software on any industry-standard server hardware.

Differences between SDN and Network Functions Virtualization

Network functions virtualization and software defined networking are very closely linked, but they are not the same. Often the terms are incorrectly used synonymously. The main points of each are summarized below so that both SDN and NFV can be evaluated with their similarities and differences.

1. **The Basic Idea**

   SDN separates control and data and centralizes control and programmability of the network.

   NFV transfers network functions from dedicated appliances to generic servers.

2. **Areas of Operation**

   SDN operates in a campus, data center and/or cloud environment

   NFV targets the service provider network

The **next-generation network** (**NGN**) is a body of key architectural changes in telecommunication core and access networks. The general idea behind the NGN is that one network transports all information and services (voice, data, and all sorts of media such as video) by encapsulating these into IP packets, similar to those used on the Internet. NGNs are commonly built around the Internet Protocol, and therefore the term all IP is also sometimes used to describe the transformation of formerly telephone-centric networks toward NGN.

Next Generation Network (NGN) is a term that describes the evolution and migration of fixed and mobile network infrastructures from distinct proprietary networks to converged networks based on IP. It is conceived to be an interworking environment of heterogeneous networks of wired and wireless access networks, PSTN, satellites, broadcasting, etc. The concept of this network will not only bring wide range of possibilities to introduce new and existing technologies in field of information transmission and processing, but also many possibilities especially in the branch of network services.

Architecture of NGN

The complete Next Generation Networks are divided into two typical constituents those are Access and Core networks. The Fig below shows the two network components. The end users have direct access to the Access network that is shown by an external circle in the figure and it provides a common service to both the wire line and wireless service users. The core networks take care to carry the data across the network. They include legacy technologies such as Asynchronous Transport Mode (ATM) and the modern family of IP based core. IP based technologies such as Multi-Protocol Label Switching (MPLS) possess two QoS models standardized by IETF, the Differentiated Services and the Integrated Services models. NGN provides end-to-end communication and employs multiple services at a time.

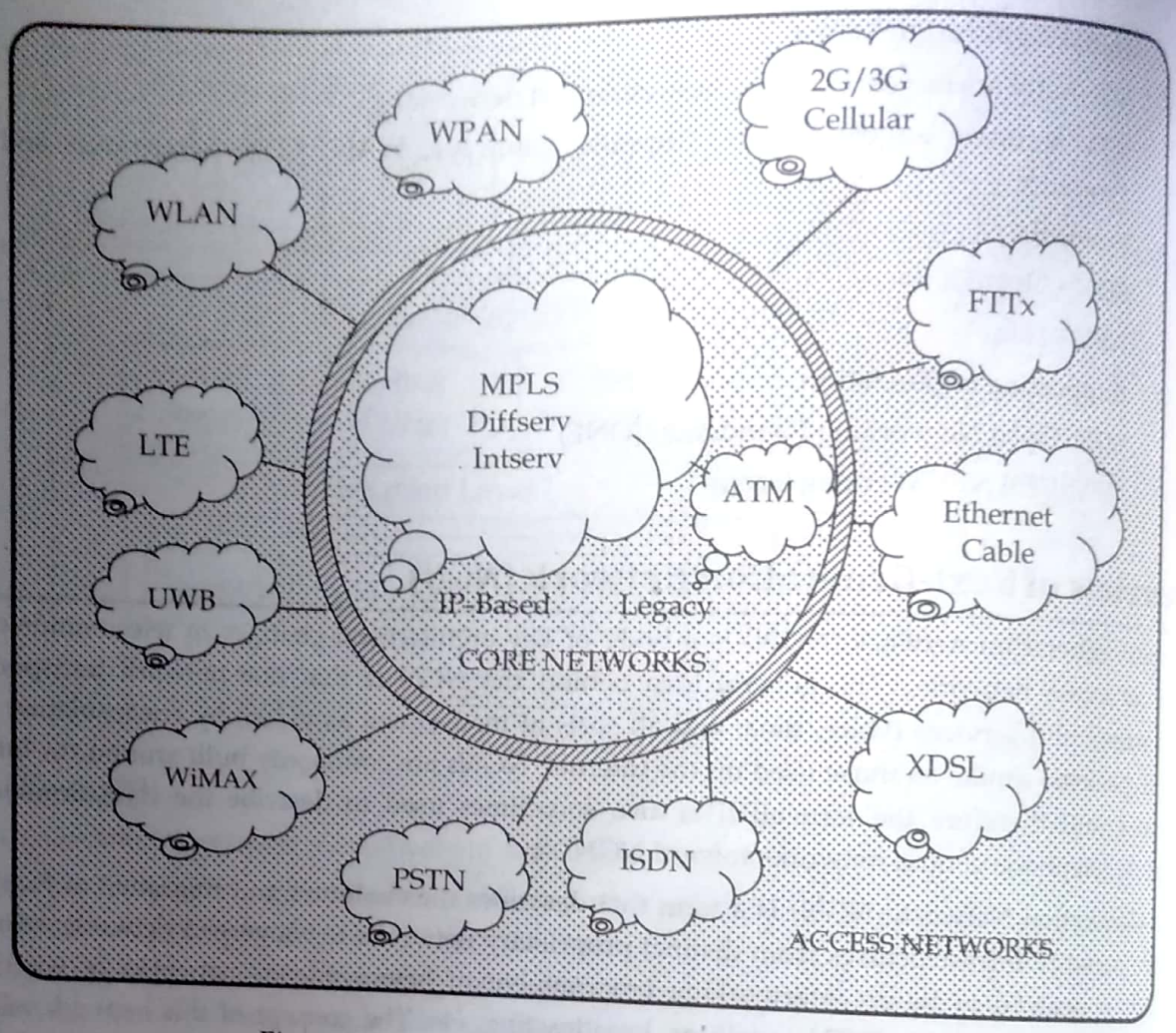


Figure 7.4: Access and Core Networks of NGN

But, this multi-tasking feature of NGN makes it somewhat complex network with the requirement to provide proper internetworking and interconnection between the different users and telecommunication operators. With the aim to create a logical framework for NGN, the functional model is mainly organized in three layers: the Transport layer, the Service Control layer and the Application layer are described below:

Transport Layer: Transport Layer of NGN is based on IP and can utilize the advantage of MPLS. Transport Layer forms the core of the Network. It basically consists of an assembly of Routers with optical network, which are responsible for carrying traffic originated by access layer. As the same core network is going to be used for all kinds of subscribers enjoying different kind of real time and non real time services, it should be able to make use of bandwidth policies and QoS policies. Operator has to think of managed Network for its subscribers. The underlying packet transport and media infrastructure are grouped under Transport layer which also interworks with circuit-switched (PSTN) network through Media Gateways so that existing networks can co-exist and need not be scrapped.

Service Control Layer: It consists of call servers where all information of the network resides and these servers are responsible for call setting up and routing, modifying, charging, tear down of the calls and controls some other activities within NGN environment. The Service Control layer consisting of Soft Switches, Media Gateway Controllers and IMS performs the functions of

authentication, accounting, maintaining QoS, security and network management. NGN may work on soft switch principle. It consists of MGC (Media Gateway Controller) as an overall controller and MGs (Media Gateway) for termination of traffic. MGC is basically a server and it is having all the necessary information of network. MGC instructs MGs for establishing the call. Under the control of MGC, MG performs different call related tasks such as connection, modification and termination of media streams, packetization of media etc.

Application Layer: The Application layer makes use of the capabilities provided by other functional layers to provide multimedia services and applications based on Open Architecture of Application Programming Interfaces (APIs). The enhanced services to the subscribers will be provided with the help of application servers. It may include prepaid servers, Announcement servers, Service servers etc. Hence NGN is making service separation from Network. Any service can be introduced with the help of server at any time without any modifications in the control, transport or access layers.

Features of NGN

- NGN works on Packet based transferring.
- There is an automatic separation of control functions among bearer capabilities, call/session and application/service.
- Decoupling of service provision from network and provision of open interface is also available under NGN.
- It supports a wide range of services, applications and mechanisms based on service building blocks.
- The network has Broadband capabilities with end to-end QoS and transparency.
- This network also has a feature of interworking with legacy networks via open interfaces.
- It provides the advantage of general mobility.
- It provides unrestricted access by users to different service providers.
- It also provides variety of identification schemes which can be resolved to IP addresses for the purpose of routing in IP network.
- It is composed of Unified service characteristics for the same services as perceived by the user.

Applications of NGN

The various applications of NGN are explained below:

- Voice Telephone services
- Multimedia services
- Data services
- Push to talk over NGN (PoN)
- Content delivery services
- Global mobility services
- Virtual Private Services (VPNs)
- Broadcasting/Multicast services
- E- commerce and M- commerce

- Session Controller based Internet services
- Third party/OSA based services
- 3D Imaging
- Machine to Machine communication
- Data Augmentation

Advantages of NGN

NGN makes use of the best of both the worlds i.e. flexibility, efficiency & innovativeness of IP and QoS, Security, Reliability, Customer-friendly features of proven PSTN. Besides this it has following advantages:

- It generates additional revenue streams for new IP/Ethernet services.
- It fulfils customer's demand for high bandwidth, Ethernet/ IP solutions.
- It diminishes expertise in legacy.
- It gives End of Life/ End of Service vendor notification.
- Users can choose multiple service providers to take maximum advantage of competitive offers but may get single bill.

Disadvantage of Next Generation Network

Though having huge advantages and applications, NGN is having some major loopholes which are stated as follows:

- Migration complexities
- Not all legacy services can be replaced with new alternatives
- Not all existing infrastructure can be shut down
- Regulatory restrictions for critical services
- NGN technology is still under research and development.
- Lack of Standardization and governing body.
- Difficult to make it work with existing technology and convert the whole system as well

Exercise

1. Define multimedia data. What are the two techniques used to overcome jitter?
2. Explain how a jitter buffer permits the playback of an audio stream even if the Internet introduces jitter.
3. What is NGN? Describe their features.
4. What is the use of SDN? Describe their uses in computer network.
5. Describe the Overview of Network function virtualization in computer network.
6. What is the purpose of multimedia in computer network? Explain.
7. Describe advantages and disadvantages of NGN.
8. Compare SDN and NFV with suitable example.
9. Differentiate between SDN, NFV and NFN with comparison chart.