Networks

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

Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: **point-to-point** and **multipoint**.

1. *Point-to-Point Connection*:

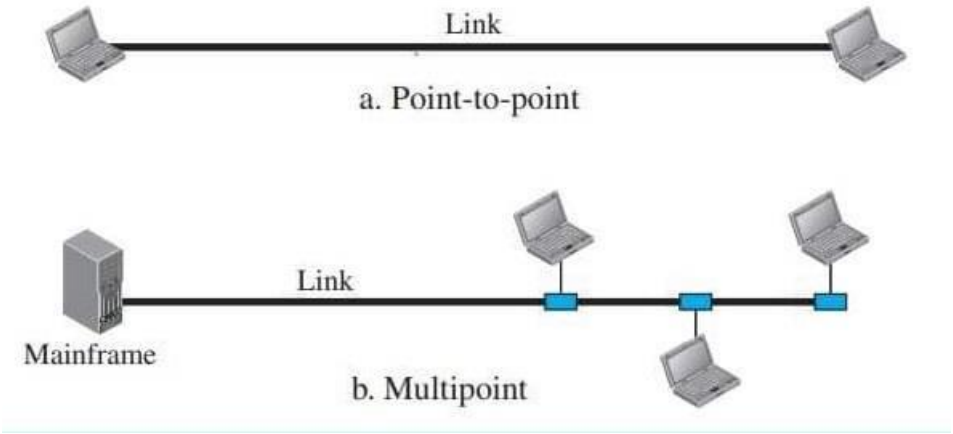
A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

When new change television channels by infrared remote control, we a re establishing a point-to-point connection between the remote control and the control system of the television.

2. *Multipoint Connection:*

A multipoint (also called **multidrop**) connection is one in which more than two specific devices share a single link. In a multipoint connection, the capacity of the channel is shared either **spatially or temporally**. If several devices can use the link simultaneously, it is a **spatially shared connection**. If users must take turns, it is a **time-shared connection**.

Figure 1: Types of connections: point-to-point and multipoint



Categories of Networks / Network Models

The category into which a network falls is determined by its **size**. Based on their size, networks are basically classified into the following three **categories or models**:

1. **Local Area Network (LAN)**
2. **Wide Area Network (WAN)**
3. **Metropolitan Area Network (MAN)**

A **LAN** normally covers an area *less than 2 miles*; a **WAN** can be *worldwide*. Networks of a size in between these two are normally referred to as **metropolitan area networks** (**MAN**) and span *tens of miles*.

Local Area Network (LAN)

A LAN is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in an office/home, or it can extend throughout a company and include audio and video peripherals. LAN size is limited to a few kilometers.

LANs are designed **to allow resources to be shared between personal computers or workstations**. The resources to be shared can include **hardware, software, or data**. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, **a given LAN will use only one type of transmission medium**. The most common LAN **topologies** are **bus, ring, and star**.

Advantages of Local Area Network

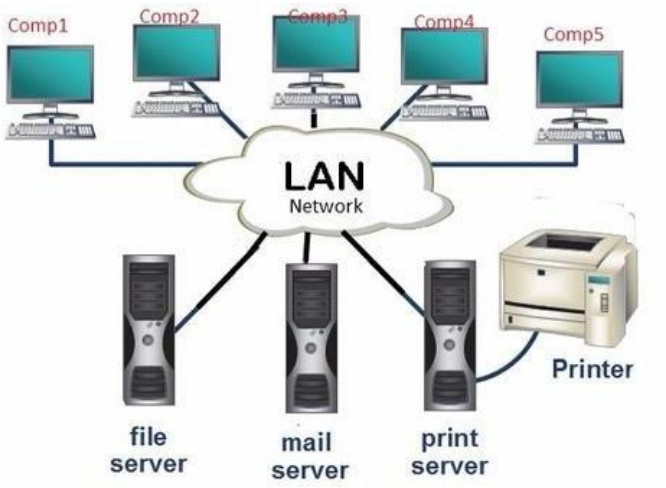
1. **Resource Sharing:** LAN provides resource sharing such as computer resources like printers, scanners, modems, DVD-ROM drives, and hard disks can be shared within the connected devices. This reduces cost and hardware purchases.
2. **Software Applications Sharing:** In a Local Area Network, it is easy to use the same software in a number of computers connected to a network instead of purchasing the separately licensed software for each client a network.

3. **Easy and Cheap Communication:** Data and messages can easily be shared with the other computer connected to the network.
4. **Centralized Data:** The data of all network users can be stored on a hard disk of the central/server computer. This help users to use any computer in a network to access the required data.
5. **Data Security:** Since data is stored on the server computer, it will be easy to manage data at only one place and the data will be more secure too.
6. **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In school labs and internet Cafes, single internet connection is used to provide internet to all connected computers.

Disadvantages of Local Area Network

1. **High Setup Cost:** The initial setup costs of installing Local Area Networks is high because there is special software required to make a server. Also, communication devices like an ethernet cable, switches, hubs, routers, cables are costly.
2. **Privacy Violations:** The LAN administrator can see and check personal data files of each and every LAN user. Moreover, he can view the computer and internet history of the LAN user.
3. **Data Security Threat:** Unauthorized users can access important data of an office or campus if a server hard disk is not properly secured by the LAN administrator.
4. **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because there are problems such as software installations, program faults or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is required to maintain these issues.
5. **Covers Limited Area:** LANs are restricted in size they cover a small area like a single office, single building or a group of nearby buildings

Figure 2: A typical LAN

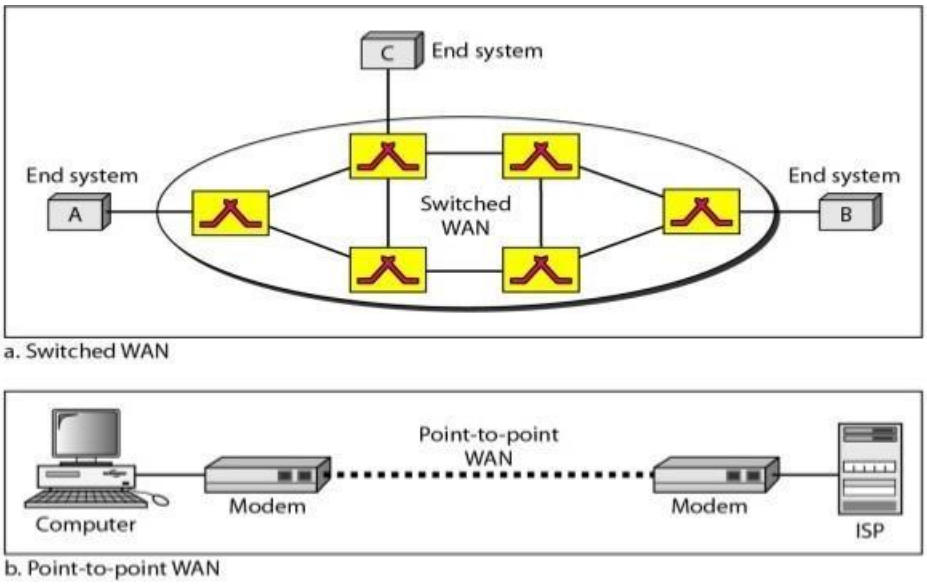


Wide Area Network (WAN)

A Wide Area Network **provides long-distance transmission of data, image, audio, and video information over large geographic areas**. WAN can be of two types**: switched WAN, and point-to-point WAN**. Switched WANs are as complex as the backbones that connect the internet, whereas point-to-point WANs are as simple as a dial-up line that connects a home computer to the internet.

The switched WAN connects the end systems, which usually comprise a router that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a LAN to an Internet Service Provider (ISP). This type of WAN is often used to provide internet access.

Figure 3: Types of WAN: Switched WAN and Point-to-Point-to-Point WAN



Advantages of Wide Area Network

1. **Covers large geographical area**: Wide area network covers a large geographical area of more than 1000km. If your office is in different cities or countries then you can connect your office branches through Wide Area Network.
2. **Centralized data:** Wide area networks also provide you the facility of sharing the data to all of your connected devices in a network.For example, through WAN connection all office branches can share the data through the head office server. You can get back up, support, and other useful data from the head office and all data are synchronized with all other office branches.
3. **Get updated files and data:** Wide Area Networks provide you the facility of getting updated files and data from the server. If a server is updated with new data then all connecting devices receive that updated data within seconds.
4. **Sharing of software and resources:** Like LANs, we can share software applications and other resources with other users on the internet.
5. **High bandwidth:** WANs covers a large geographical area of more than 1000km. therefore WANs have high bandwidth compared to LANs and MANs.

Disadvantages of Wide Area Network

1. **Security problems:** Wide Area Networks faces more security problem as compared to LANs and MANs. One of the key disadvantages of WANs is a security issue when many different people have the ability to use information from other computers.
2. **Needs firewall and antivirus software:** As it faces security issue, therefore it is a basic need of WANs to use firewalls and antivirus software to protect data transfer on the internet which can be accessed and changed by hackers. Also, some people can inject a virus into the computers so antivirus software is also needed to install.
3. **The setup cost is high:** A WAN network covers a large geographical area, it is very expensive to setup in the initial stage. It may involve purchasing different networking devices, i.e routers, switches, and extra security software.
4. **Troubleshooting problems:** A WAN network covers large geographical areas, so fixing the problem in a network is a very difficult job. Most of WANs wires go into the sea and if those wires get broken. It involves a lot of hard work to fix those lines under the sea.
5. **Maintenance Issues:** Once set up, maintaining a WAN network is a full-time job which requires high tech skills of network supervisors and technicians

Metropolitan Area Network (MAN)

A Metropolitan Area Network is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the internet, and have endpoints spread over a city.

A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network which is capable of providing high-speed data connection to the internet, today.

Network Criteria

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

Performance

Performance can be measures in many ways, including transit time and response time. **Transit time** is the amount of time required for a message to travel from one device to another. **Response time** is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: **throughput** and **delay**. We often need more throughput and less delay. However, if we try to send more data to the network, we may increase throughput, but we increase the delay because of traffic congestion in the network.

Reliability

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

Security

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

Network Topology

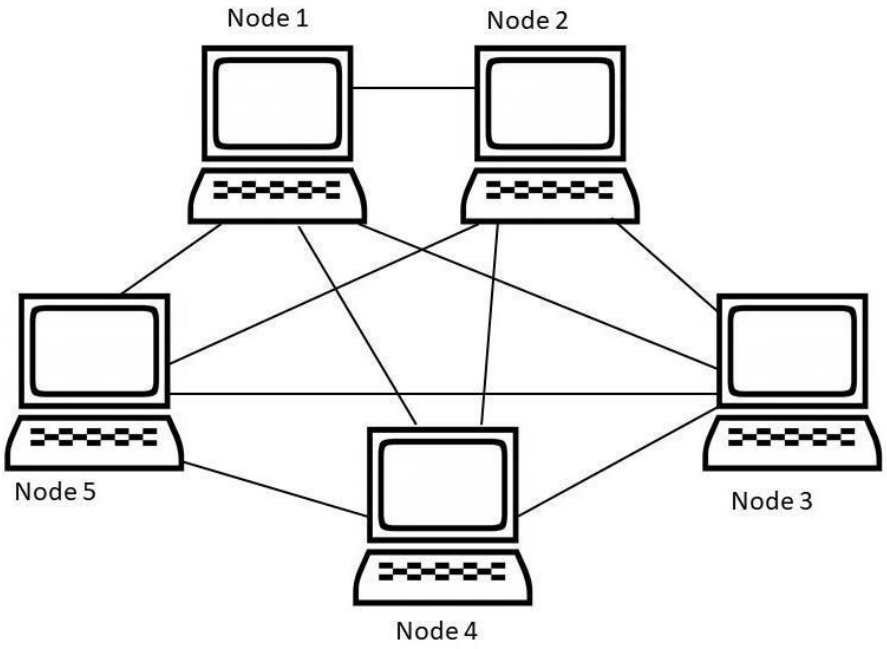
The term **physical topology** refers to **the way in which a network is laid out physically**. Two or more devices connect to a link; two or more links form a topology. The **topology of network** is the **geometric representation of the relationship of all the links and linking devices** (nodes) to one another. There are four basic topologies possible: **mesh, star, bus, and ring**.

Mesh Topology

In a mesh topology, **every device has a dedicated point-to-point link to every other device**. The term dedicated means that **the link carries traffic only between the two devices it connects**. To find the number of physical links in a fully connected mesh network with '**n' nodes**, we first consider that **each node must be connected to every other node**. Node 1 must be connected to n-1 nodes, node 2 must be connected to n -1 nodes, and finally node n must be connected to n-1 nodes. **We need n(n-1) physical links**. However, if each physical link allows communication in both directions, we can divide the number of links by 2. We can say that in a mesh topology, we need **n(n-1)/2 duplex-mode links**.

To accommodate that many links, **every node on the network must have n-1 input/output ports** to be connected to the other n-1 stations.

Figure: Mesh topology



Advantages

- The use of dedicated links guarantees that each connection can carry its own data load, thus **eliminating the traffic problems** that can occur when links must be shared by multiple devices.
- A mesh topology is **robust**. If one link becomes unusable, it does not incapacitate the entire system.
- Mesh topology offers **privacy or security**. When every message travel along a dedicated line, **only the intended recipient** sees it. **Physical boundaries** prevent the other users from gaining access to the message.
- The point-to-point links make **fault identification and fault isolation easy**. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to **discover the precise location of the fault** and helps in finding its cause and solution.

Disadvantages

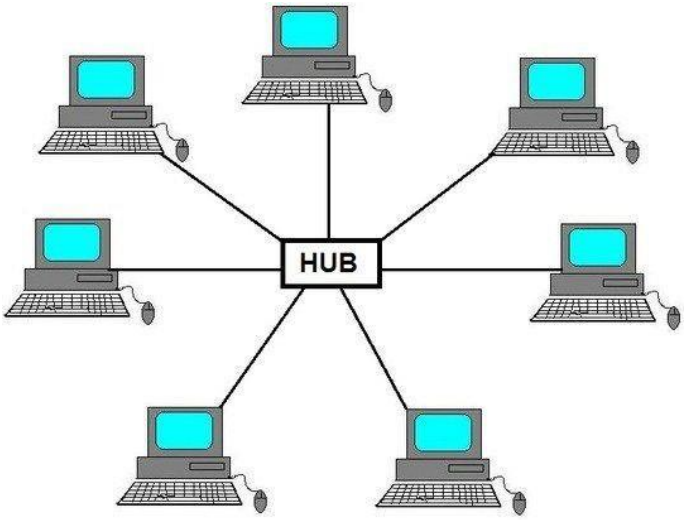
- Because every device must be connected to every other device, **installation and reconnection are difficult**.
- The **space requirement for wiring** can greater than the available space can accommodate.
- The hardware required to link each device (I/O ports and cable) can be **expensive**.

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

Star Topology

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

Figure: Star topology



Advantages

- A star topology is **less expensive than a mesh topology**.
- In star topology, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it **easy to install and reconfigure**. Far **less cabling** needs to be done, and additions, moves, and deletions involve only one connection: between that device and the hub.
- Star topology is **robust**. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to **easy fault identification and fault isolation**.
- As long as the hub is working, it can be used to **monitor link problems and bypass defective links**.

Disadvantages

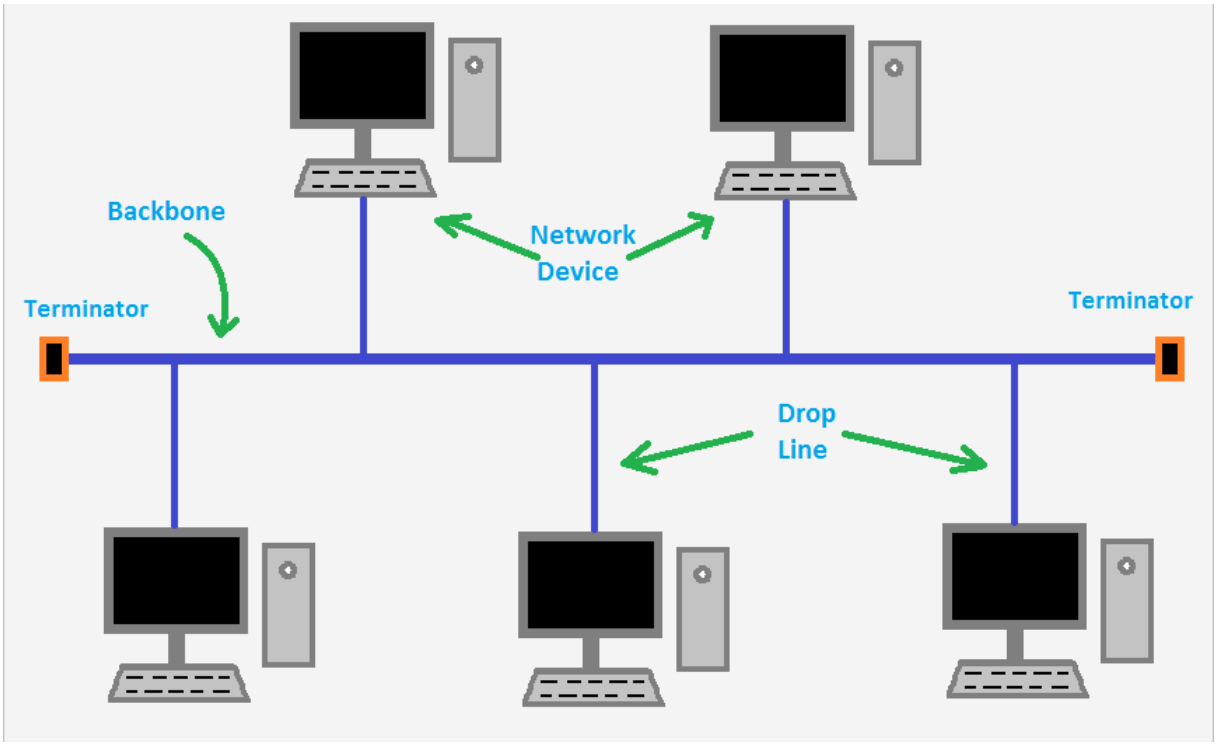
- The whole topology is **dependent on one single point**: the hub. If the hub goes down, the whole system is dead.
- Although a star topology requires far less cabling than a mesh, **each node must be linked to a central hub**. For this reason, often **more cabling is required in a star topology than in some other topologies like ring and bus**.

Bus Topology

Bus topology offers a **multipoint connection**. In bus topology, **one long cable acts as a backbone to link all the devices in a network.** Nodes are connected to the bus cable by **drop lines and taps**. A **drop line** is a connection running between the device and the main

cable. A **tap** is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into **heat**. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason, there is a **limit on the number of taps a bus can support and on the distance between those taps**.

Figure: Bus topology



Advantages

- Bus topology is **easy to install**. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
- Bus topology uses **less cabling than mesh or star topologies**. For instance, four devices in the same room require four lengths of cable reaching all the way to the hub, in star topology. In bus topology, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

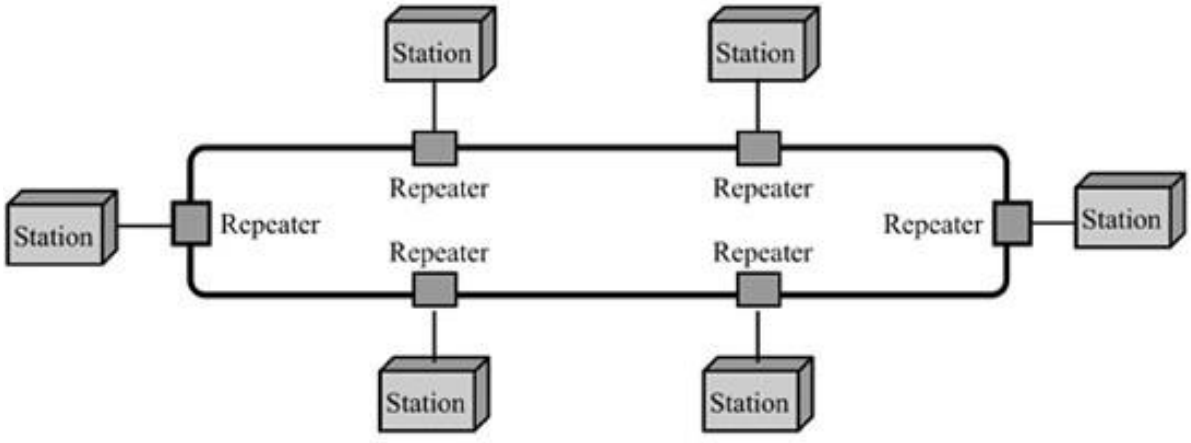
Disadvantages

- **Reconnection and fault isolation are difficult** in a bus topology. A bus is usually designed to be optimally efficient at installation. It can therefore be **difficult to add new devices**.
- **Signal reflection at the taps** in the bus topology can cause **degradation in quality**. This degradation can be controlled by **limiting the number and spacing of devices connected to a given length of cable**. Adding new devices may therefore require modification or replacement of backbone.
- **A fault or break in the bus cable stops all transmission**, even between devices on the same side of the problem. The damages area reflects signals back in the direction of origin, creating **noise** in both directions.

Ring Topology

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

Figure: Ring topology



Advantages

- A ring is **relatively easy to install and reconfigure**. Each device is linked to only its immediate neighbours. To add or remove a device requires changing only two connections.

- **Fault isolation is simplified**. Generally, in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantage

- Ring topology **supports only unidirectional traffic**. In a simple ring, a break in the ring can disable the entire network. This weakness can be solved by using a **dual ring or a switch** capable of closing off the break.

The Internet History

A network is a group of connected communicating devices such as computers and printers. An internet is two or more networks that can communicate with each other. 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.

In the mid-1960s, mainframe computers in research organizations were standalone 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 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 would be attached to a specialized computer, called an **Interface Message Processor** (**IMP**). The IMPs, in turn, would be connected to one another. 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 IMPs to form a network. Software called the **Network Control Protocol** (**NCP**) provided communication between the hosts.

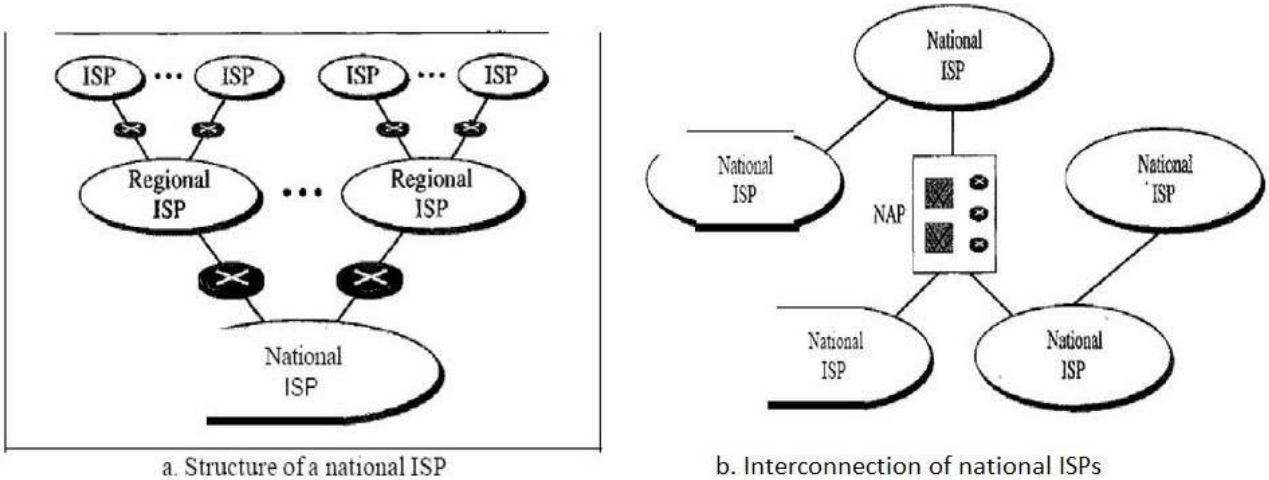
In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the **Internetting Project.** Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on **Transmission Control Protocol** (**TCP**) included concepts such as **encapsulation**, the **datagram,** and the **functions of a gateway**.

Shortly thereafter, authorities made a decision to split TCP into two protocols: **Transmission Control Protocol** (**TCP**) and **Internetworking Protocol** (**IP**). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The Internetworking Protocol became known as **TCP/IP**.

The Internet Today

The Internet has come a long way since the 1960s. 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 continually changing - new networks are being added, existing networks are adding addresses, and networks of several companies are being removed. Today most end users who want Internet connection use the services of Internet Service Providers (lSPs). 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. The following figure shows a conceptual view of the Internet.

Figure: Hierarchical Organization of the Internet



a. Structure of a national ISP

b. Interconnection of national ISPs

Internet Service Providers

International Internet Service Providers

At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers

The national Internet service providers are **backbone networks** created and maintained by specialized companies. 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 national ISP networks are also connected to one another by private switching stations called **peering points**.

Regional Internet Service Providers

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

Local Internet Service Providers

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

Protocols and Standards

Protocols

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when itis communicated. The key elements of a protocol are syntax, semantics, and timing.

Syntax: The term syntax refers to the structure or format of the data, meaning the order in which they are presented. 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.

Semantics*:* The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?

Timing: The term timing refers to two characteristics: **when data should be sent** and **how fast they can be sent**. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1Mbps, the transmission will overload the receiver and some data will be lost.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guideline to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. 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 who seek to define the functionality of a new product or technology.

- **De jure**: Those standards that have been legislated by an officially recognized body are de jure standards

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

- ***International Organization for Standardization (ISO)***:

The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.

- ***International Telecommunication Union-Telecommunication 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 Telecommunication 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 for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).

- ***American National Standards Institute (ANSI):***

Despite its name, the American National Standards Institute 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.

- ***Institute of Electrical and Electronics Engineers (IEEE):***

The Institute of Electrical and Electronics Engineers 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 communications.

- ***Electronic Industries Association (EIA):***

Aligned with ANSI, the Electronic Industries Association 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 communication.

Connecting Devices

The connecting devices are divided into five different categories based on the layer in which they operate in a network. The **five categories** contain devices which can be defined as:

1. Those which operate below the physical layer such as a passive hub
2. Those which operate at the physical layer (a repeater or an active hub)
3. Those which operate at the physical and data link layers (a bridge or a two-layer switch)
4. Those which operate at the physical, data link, and network layers (a router or a three-layer switch)
5. Those which can operate at all five layers (a gateway)

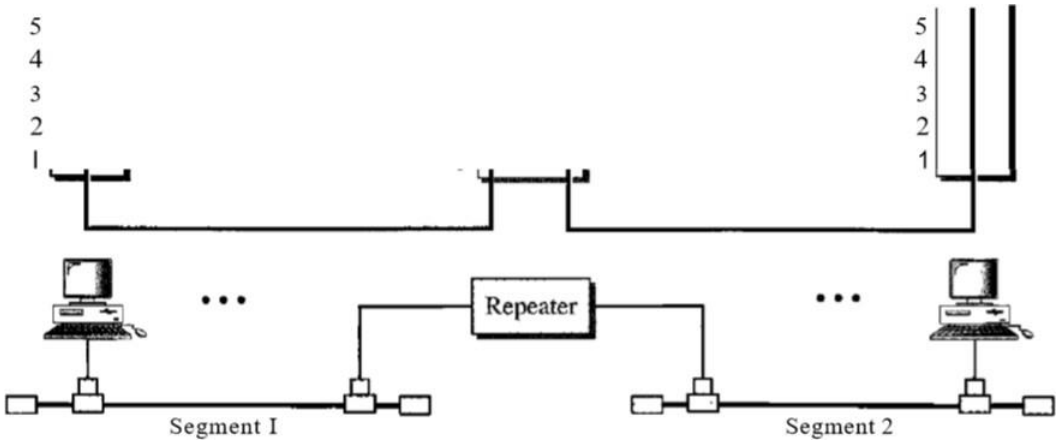
Passive Hubs

A passive hub is **just a connector.** It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the **collision point**. This type of a hub is part of the media; its location in the Internet model is below the physical layer.

Repeaters

A repeater is a device that **operates only in the physical layer**. Signals that carry information within a network can travel a fixed distance before **attenuation endangers the integrity of the data**. A repeater receives a signal and, before it becomes too weak or corrupted, **regenerates the original bit pattern**. The repeater then **sends the refreshed signal**. A repeater **can extend the physical length of a LAN**, as shown in the following figure:

Figure: A repeater connecting two segments of a LAN



A repeater **does not actually connect two LANs**; it **connects two segments of the same LAN.** The segments connected are still part of one single LAN. **A repeater is not a device that can connect two LANs of different protocols**.

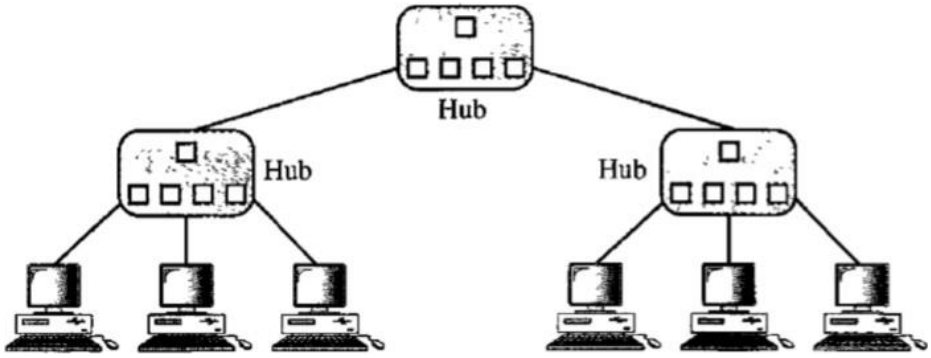
Functions of a repeater:

- A repeater connects segments of a LAN
- A repeater forwards every frame; it has no filtering capability
- A repeater is a regenerator, not an amplifier

Active Hubs

An active hub is actually a **multipart repeater**. It is normally **used to create connections between stations in a physical star topology**. However, hubs can also be **used to create multiple levels of hierarchy**, as shown in the following figure:

Figure: Hierarchy of Hubs



Bridges

A bridge **operates in both the physical and the data link layer**. As a physical layer device, it **regenerates the signal** it receives. As a data link layer device, the bridge **can check the physical (MAC) addresses** (source and destination) contained in the frame.

Filtering

There is a major **difference in the functionality of a bridge and a repeater**. A **bridge has filtering capability**. It can check the destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision must specify the port. A bridge has a table that maps addresses to ports.

Switches

We can have a **two-layer switch** or a **three-layer switch**. The two-layer switch performs at the **physical and data link layers**. A two-layer switch is a **bridge**, a bridge with **many ports** and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be **able to allocate a unique port to each station**, with each station on its own independent entity. This means that, there is **no possibility for competing traffic**.

A two-layer switch, as a bridge does, makes a **filtering decision based on the MAC address** of the frame it received. However, a two-layer switch can be **more sophisticated**. It can have a **buffer to hold the frames** for processing. It can have a switching factor that forwards the frames faster. Some new two-layer switches, called **cut-through switches**, have been designed to **forward the frame as soon as they check the MAC addresses in the header of the frame**.

A **three-layer switch** is used at the **network layer**; it is a kind of router (but a faster and more sophisticated one). The switching fabric in a three-layer switch allows faster table lookup and forwarding.

Routers

A router is a **three-layer device** that routes packets based on their **logical addresses** (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a **routing table** that is used for making **decisions** about the route. The routing tables are normally **dynamic** and are **updated using routing protocols**.

Gateway

A gateway is normally a computer that **operates in all five layers of the Internet or seven layers of OSI model**. A gateway **takes an application message, reads it, and interprets it**. This means that it can be used as a **connecting device between two internetworks that use different models**. For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message. Gateways can provide security.

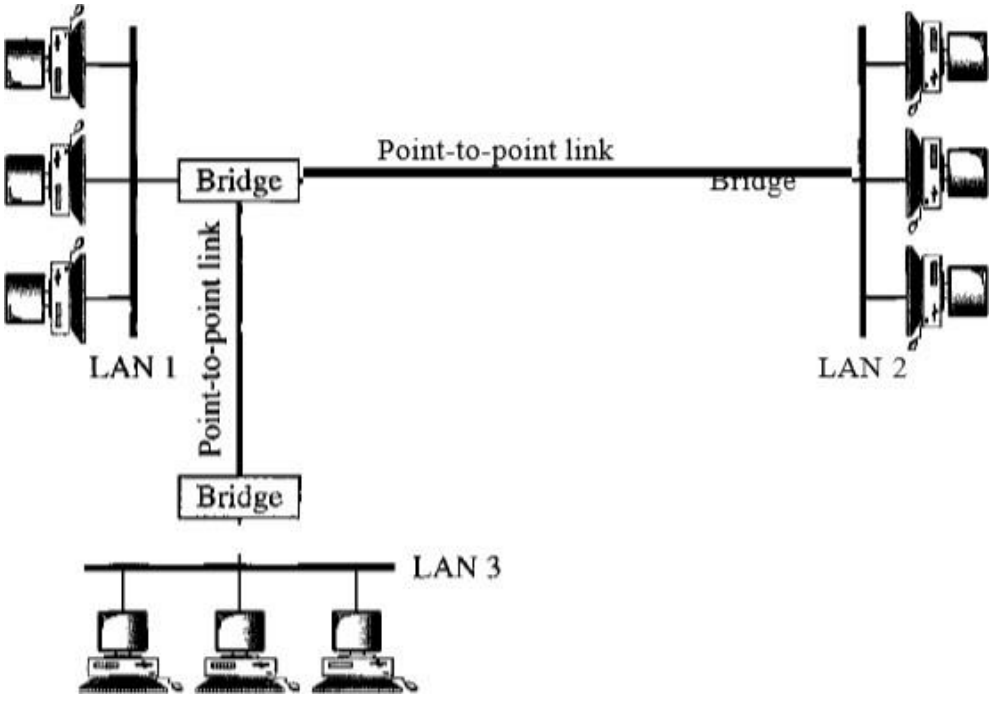
Connecting Remote LANs

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

A common **application** for a backbone network is to **connect remote LANs**. This type of backbone network is useful when a company has several offices with LANs and needs to connect them. The **connection can be done through bridges**, sometimes called **remote bridges**. The bridges act as connecting devices, connecting LANs and point-to-point networks, such as leased telephone lines or ADSL lines. The point-to-point network in this case is considered a LAN without stations.

The following figure shows a backbone connecting remote LANs.

Figure: Connecting Remote LANs



Computer Network Models

A **computer network** consists of software and hardware that is used to send and receive data from one device to another. The role of hardware is to prove the physical equipment that are required in order to send and receive data while software defines the set of instructions that uses the hardware equipments for data transmission.

A simple transmission of data consists of several steps at various layers of computer network. In computer network models we will discuss the models in detail to **understand how the data is actually transferred and received at a computer level**.

Before we discuss the computer network models, let's have a discussion on the layers that a computer model consists. Let's have a basic idea of layers involved in data communication.

Layers of a computer network models

1. The main purpose of having several layers in a computer network model is to divide a process of sending and receiving data into small tasks.

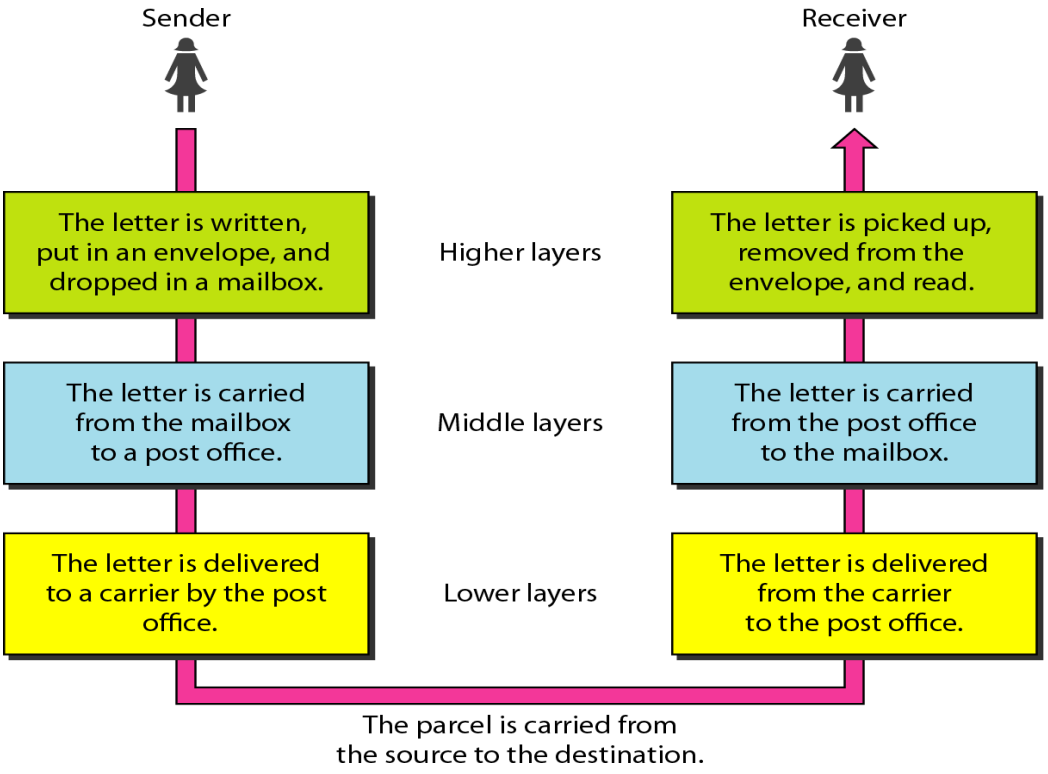
2. These layers are connected with each other, each layer provide certain data to itsimmediate higher and immediate lower layer and receives certain data from the same.

3. Dividing a model is layers make the structure quite simple that makes it easy to identify the issue if it occurs. There are three main components of a computer network model. Sender, receiver and carrier.

LAYERED TASKS EXAMPLE

Let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office.

Tasks involved in sending a letter



At sender Side:

Higher layer: Higher layer serves the middle layer, directs the message (or data) to middle layer

Middle layer: Middle layer picks up the data from higher layer and transfer it to the lower layer

Lower layer: The data is transmitted to the lower layer of the receiver side.

At receiver Side:

Lower layer: Receives the data from the lower layer of sender side and transfer it to middle layer.

Middle layer: Middle layer picks up the data from lower layer and transfer to higher layer.

Higher layer: Higher layer transfers the data to the receiver.

We will discuss more than one computer models here; each model has different set and design of layers.

The most important computer network models are:

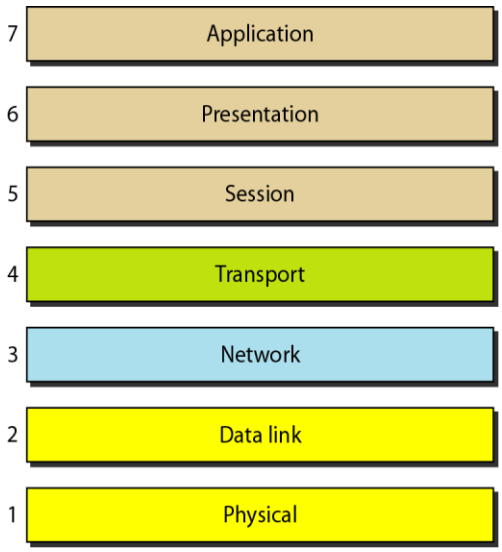
1. OSI Model

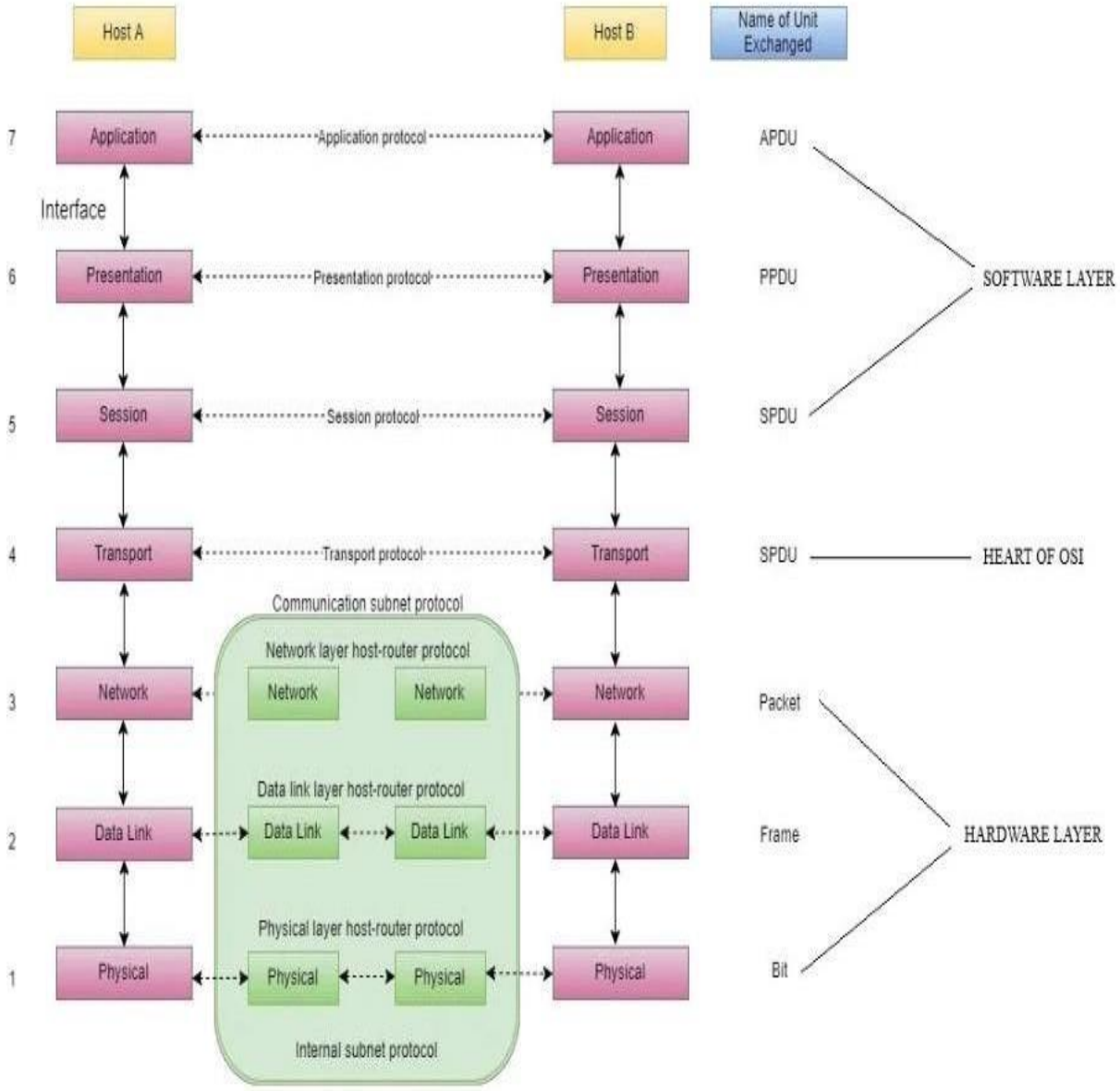
2. TCP/IP Model

THE OSI MODEL

- **OSI Model** stands for **Open System Interconnection** model.
- **OSI Model** defines how data is transferred from one computer to anothercomputer.
- In a very basic scenario two computers connected with a LAN and connectors transfer data using the NIC (Network Interface Controller). This forms a computer network, however if both the system uses different operating systems, for example one system runs on windows and other one runs on MacOS then how can data be transferred between these two different systems, here comes the role of a OSI model which is a seven layered model that defines how a data can be transferred between different systems.
- **OSI model** was introduced by International Organisation for standardisation(ISO) in 1984.
- There are **seven layers** in a OSI model

Seven layers of the OSI model

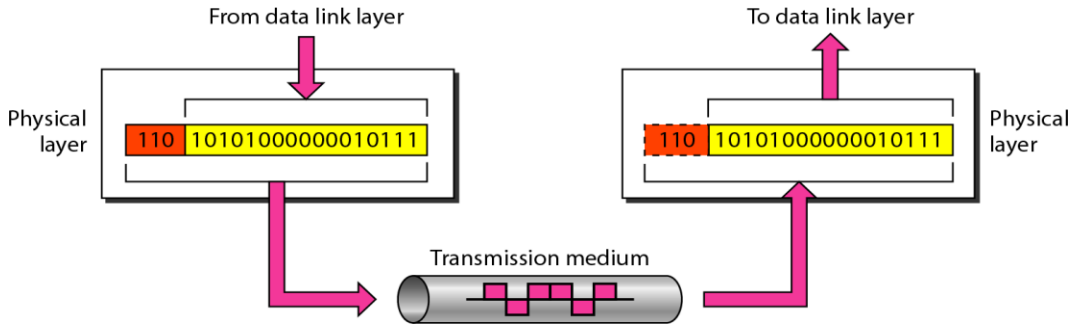




Physical layer

Physical layer converts binary sequences into signals and transfer it through a transmission media such as cables. At the physical layer, communication is direct.

The signals generated by physical layer are based on the transmission media. For example an electrical signal is generated if the media is copper cable, light signal if media is optical fiber and radio signal in case of transmission media is air. This generated signal is received by the physical layer at the receiver side and converts it into bits.



The main functions of physical layer:

- **Physical characteristics of interfaces and medium** - The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

- **Representation of bits** - The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and Is are changed to signals).

- **Data rate** - The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer definesthe duration of a bit, which is how long it lasts.

- **Synchronization of bits** - The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

- **Line configuration** - The physical layer is concerned with the connectionof devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

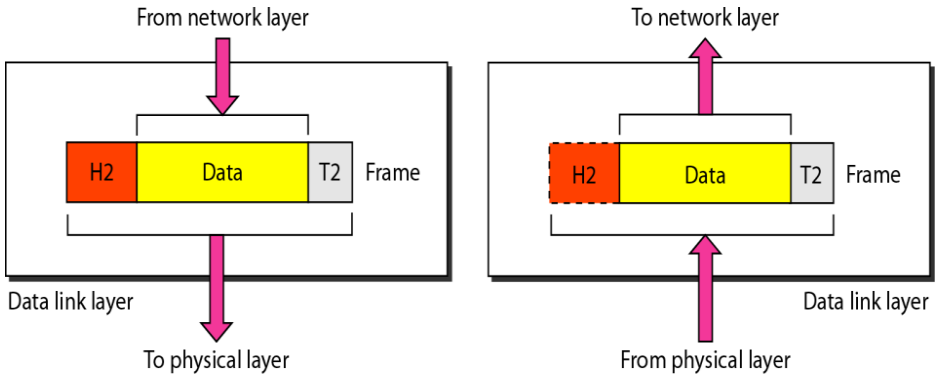
- **Physical topology** - The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every devices connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is acombination of two or more topologies).

- **Transmission mode** - The physical layer also defines the direction oftransmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the

other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

Data link layer

The data link layer is responsible for moving frames from one hop (node) to the next.



Other responsibilities of data link layer:

1. **Framing**. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

2. **Physical addressing**. If frames are to be distributed to different systems on then network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

3. **Flow control**. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

4. **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

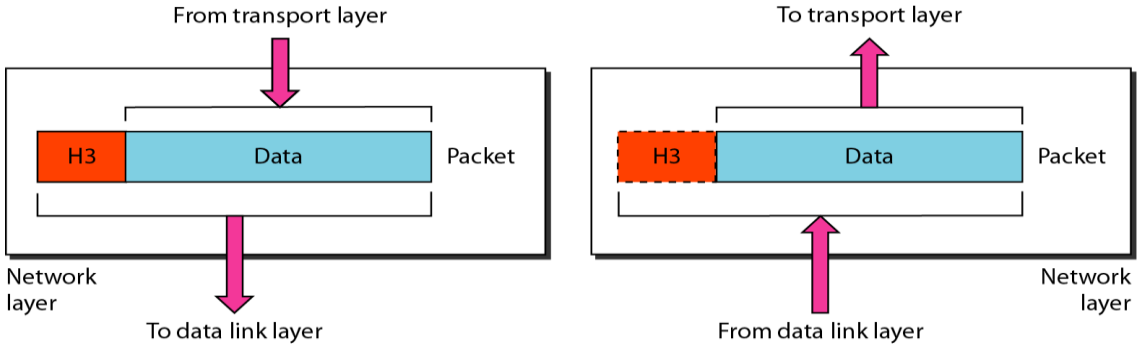
5. **Access control**. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device hascontrol over the link at any given time.

Network layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links).

The network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a 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.



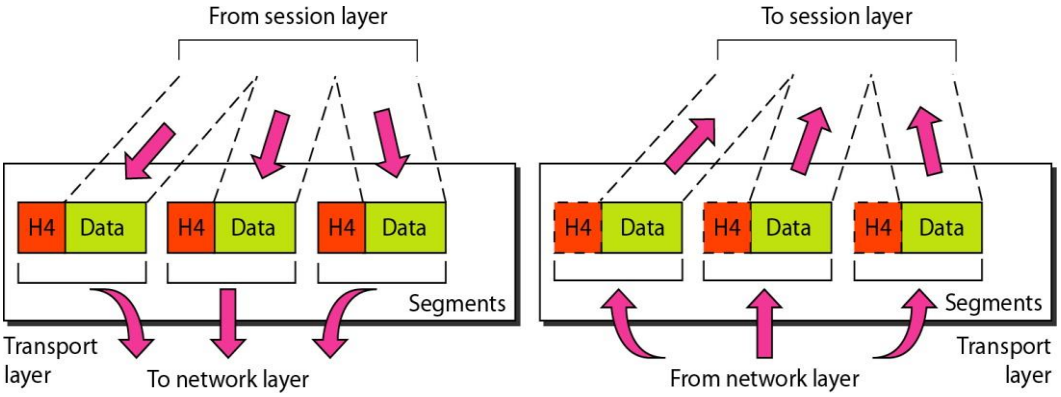
The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Other responsibilities of the network layer include the following:

1. **Logical addressing.** The physical addressing implemented by the datalink layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer addsa header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
2. **Routing**. When independent networks or links are connected to create *internetworks* (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Transport layer

The transport layer is responsible for the delivery of a message from one process to another (A process is an application program running on a host). The basic function is to accept data from above, split it up into smaller units if needed, pass these to the network layer, and ensure all the pieces arrive correctly at the other end.



Other responsibilities of the transport layer include the following:

1. **Service-point addressing**.

   Computers often run several programs at the same time.

   For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on theother.

   The transport layer header must therefore include a type of address called a service-point address (or port address).

   The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

2. **Segmentation and reassembly**.

   A message is divided into transmittable segments, with each segment containing a sequence number.

   These numbers enable the transport layer to reassemble the messagecorrectly upon arriving at the destination and to identify and replace packets that were lost in transmission.

3. Connection control.

The transport layer can be either connectionless or connection oriented.

A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated

4. Flow control.

Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link

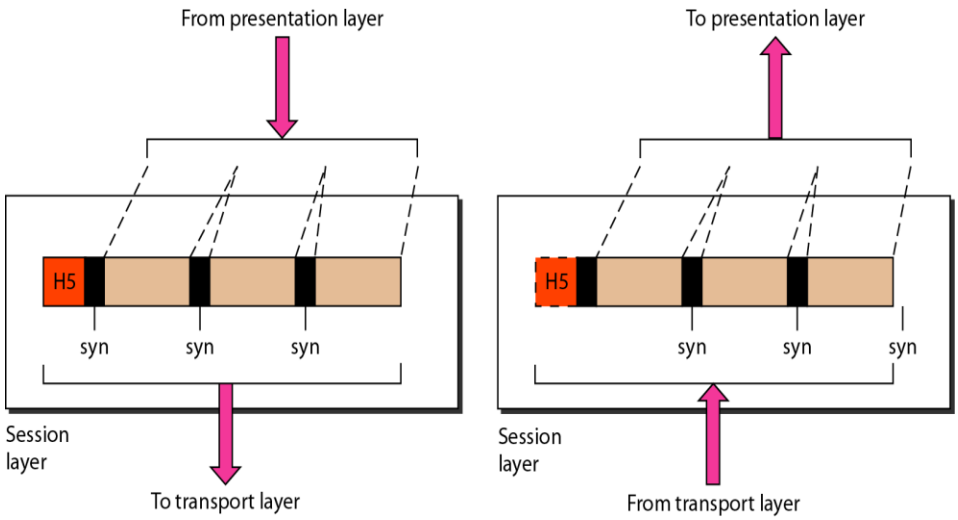
5. Error control.

Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).

Error correction is usually achieved through retransmission.

Session layer

- Session layer manages and synchronize the conversation between two different applications.
- The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.
- The session layer is responsible for dialog control and synchronization.



Specific responsibilities of the session layer include the following:

1. Dialog control.

The session layer allows two systems to enter into a dialog.

It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.

2. Synchronization.

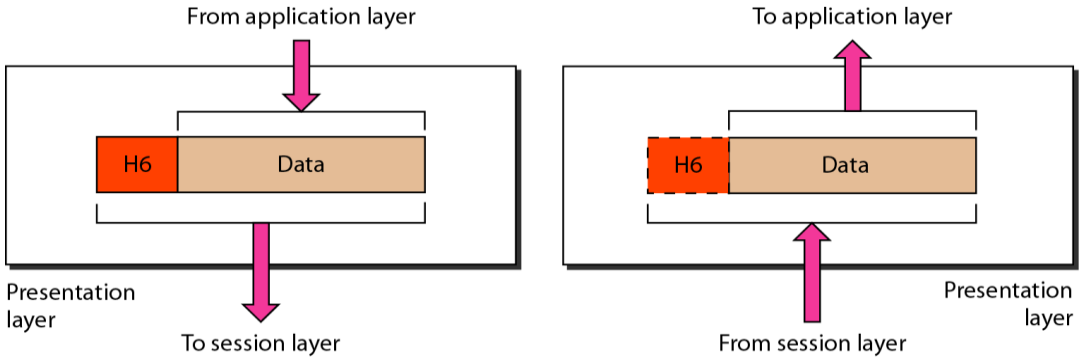
The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently.

In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Presentation layer

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



The presentation layer is responsible for translation, compression,and encryption.

Specific responsibilities of the presentation layer include the following:

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

   The presentation layer at the receiving machine changes thecommon format into its receiver-dependent format.

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

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

Application layer

It is the top most layer of OSI Model. The application layer enables the user, whether human or software, to access the network.

Manipulation of data (information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring files, distributing the results to user, directory services, network resources, etc.

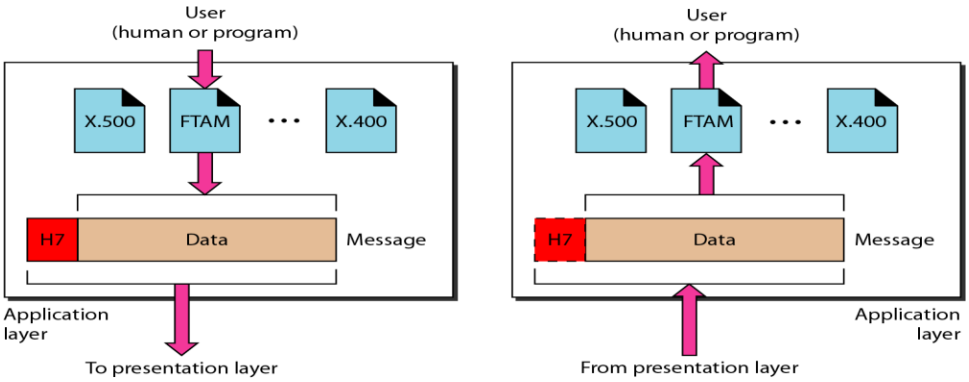
The Application Layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is **HTTP (Hypertext Transfer Protocol)**, which is the basis for the World Wide Web. When a browser wants a web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back.

Other Application protocols that are used are: **File Transfer Protocol(FTP), Trivial File Transfer Protocol (TFTP)**, **Simple Mail Transfer Protocol (SMTP)**, **TELNET**, **Domain Name System (DNS)** etc.

The application layer is responsible for providing services to the user.

Functions of Application Layer

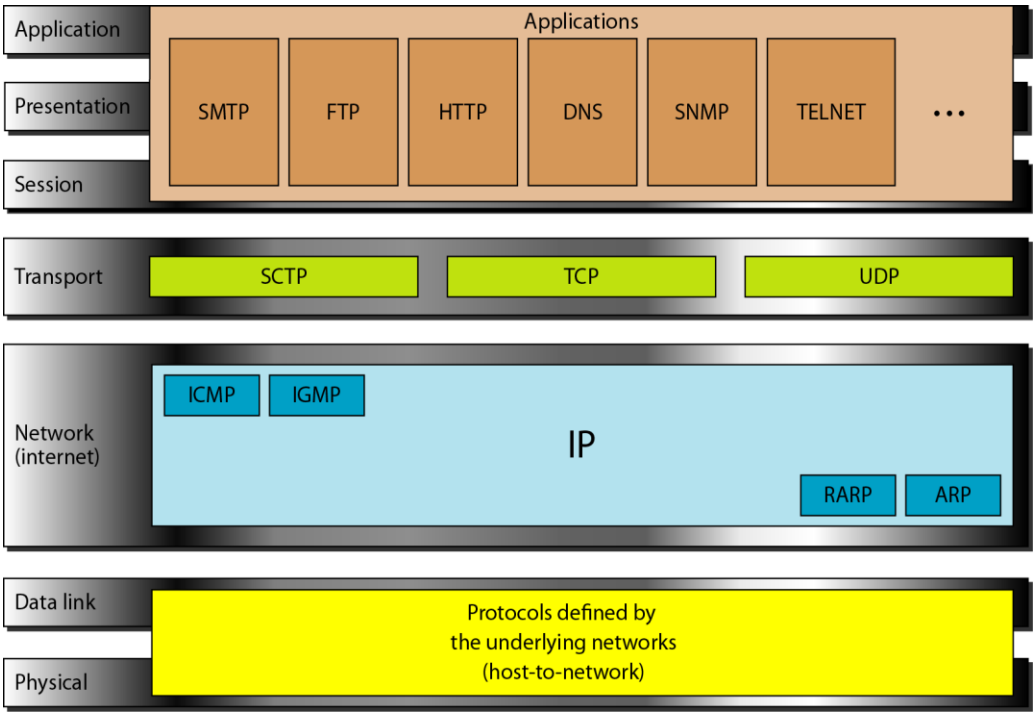
1. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal:** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
3. **Directory Services:** This layer provides access for global information about various services.
4. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.


User
(human or program)
X.500
FTAM
X.400
H7
Data
Message
Application
layer
To presentation layer
User
(human or program)
X.500
FTAM
X.400
H7
Data
Message
Application
layer
From presentation layer

TCP/IP PROTOCOL SUITE

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.

TCP/IP and OSI model



Physical and Data Link Layers

TCP/IP does not define any specific protocol at these layers. It supports all the standard and proprietary protocols. A network in a TCPIIP internetwork can be a local-area network or a wide-area network.

Network Layer

At the network layer, TCP/IP supports the following protocols:

- **Internetworking Protocol (IP)** - IP is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a best-effort

delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. IP transports data in packets called datagram's, each of which is transported separately. Datagram's can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagram's once they arrive at their destination. IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

- **Address Resolution Protocol (ARP)** - is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

- **Reverse Address Resolution Protocol (RARP)** – It allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

- **Internet Control Message Protocol (ICMP)** - is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

- **Internet Group Message Protocol (IGMP)** - is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

At the transport layer, TCP/IP defines three protocols, TCP, UDP and SCTP. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

- User Datagram Protocol (UDP)

  The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It is a process-to-process protocol that adds only port

addresses, checksum error control, and length information to the data from the upper layer.

- Transmission Control Protocol (TCP)

  TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.

  At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagram's. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

- Stream Control Transmission Protocol(SCTP)

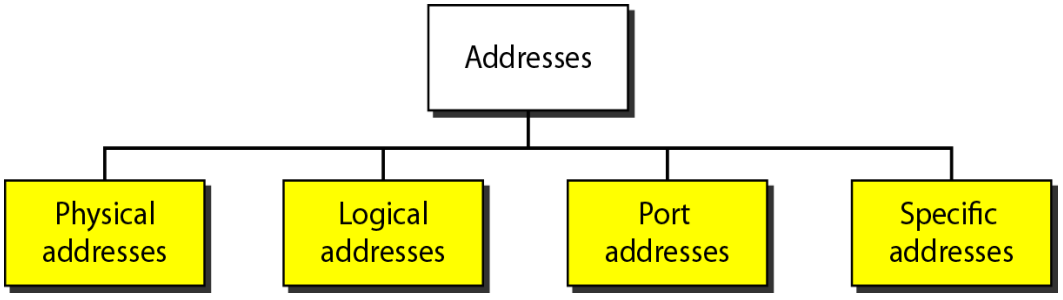
  The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

Application Layer

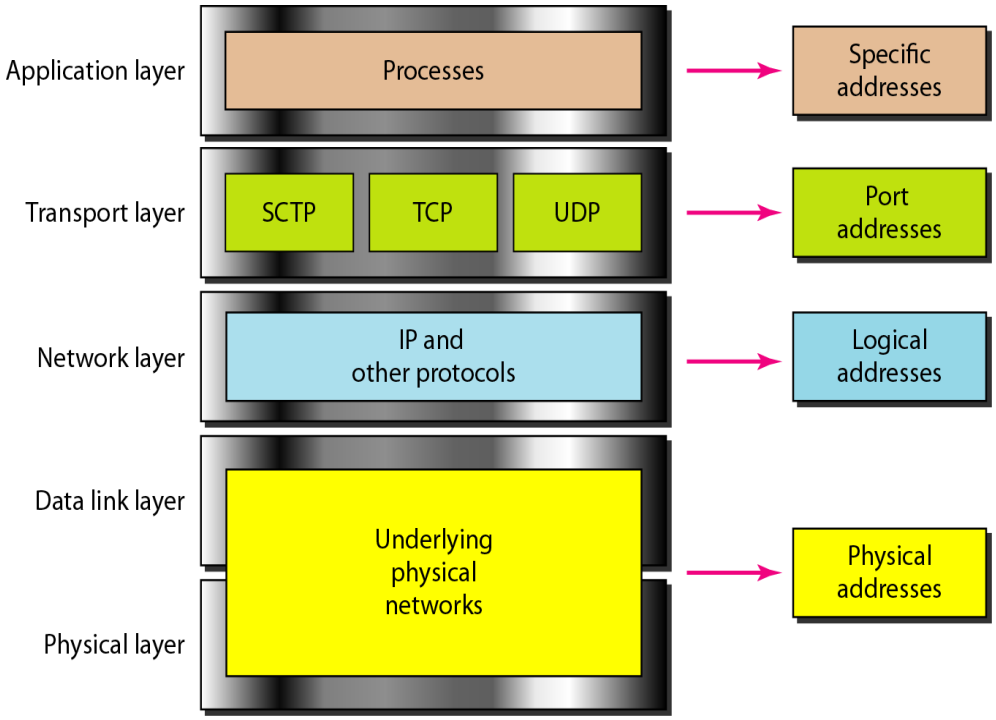
The application layer in TCP/IP is equivalent to the combined session, presentation and application layers in the OSI model. Many protocols are defined at this layer. SMTP, FTP, TELNET, HTTP, DNS etc.

ADDRESSING

Four levels of addresses in TCP/IP



Relationship of layers and addresses in TCP/IP



Physical Addresses

- It is also known as the link address.
- It is the address of a node as defined by its LAN or WAN
- It is included in the frame used by the data link layer.
- It is the lowest level address.
- The size and format of these addresses vary depending on the network.

Logical Addresses

Logical addresses are necessary for universal communications that are independent of underlying physical networks. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-

bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Port Addresses

Computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process.

For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes.

In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

The physical address will change from node to node
but the logical and port addresses usually remain the same.

Specific Addresses (Application Addresses)

Some applications have user-friendly addresses that are designed for that specific address.

Example:-

E-mail address (for example, forozan@fhda.edu)

Universal Resource Locator (URL) (for example, www.mhhe.com)

Data Link Layer

Error Detection and Correction

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.

Data can be corrupted during transmission.

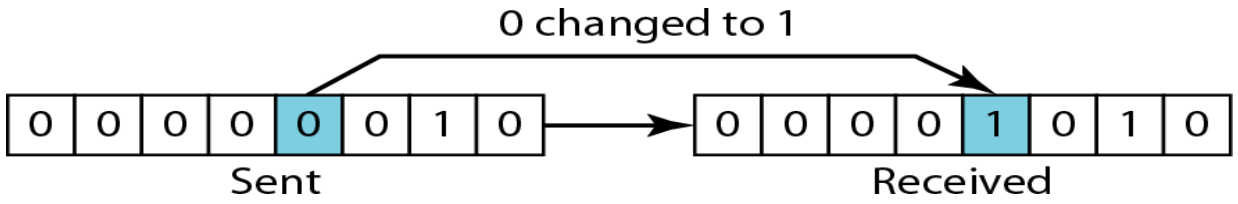
Some applications require that errors be detected and corrected.

Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interface can change the shape of the signal.

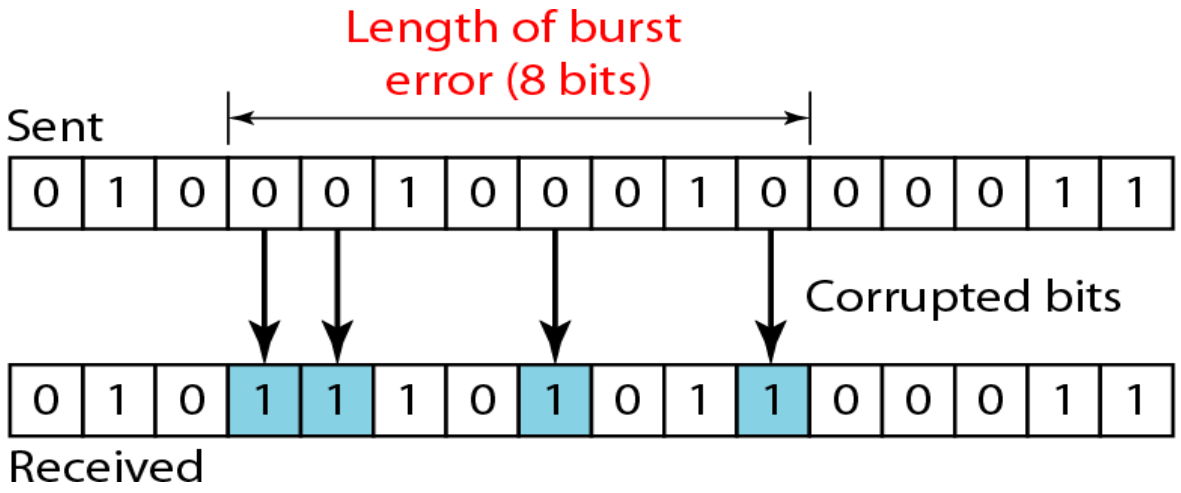
Single-Bit Error

In a single-bit error, only 1 bit in the data unit has changed. That is only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1.



Burst Error

The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



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.

Detection versus Correction

The correction of errors is more difficult than the detection. In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of errors. A single-bit error is the same for us as a burst error.

In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message. The number of the errors and the size of the message are important factors.

Forward Error Correction versus Retransmission

There are two main methods of error correction.

Forward error correction is the process in which the receiver tries to guess the message by using redundant bits. This is possible, if the number of errors is small.

Correction by retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free.

Coding

Redundancy is achieved through various coding schemes. The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits. The receiver checks the relationships between the two sets of bits to detect or correct the errors.

BLOCK CODING

In block coding, we divide our message into blocks, each of *k* bits, called **datawords**. We add *r* redundant bits to each block to make the length $n = k + r$.

The resulting *n-bit* blocks are called **code words**.

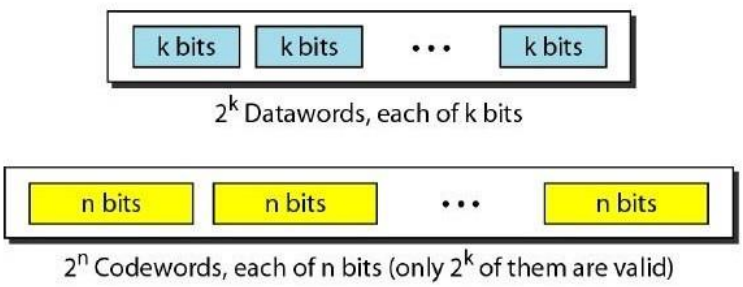
For the moment, it is important to know that we have a set of data words,each of size *k*, and a set of code words, each of size of *n*.

With *k* bits, we can create a combination of 2^k data words; with *n* bits, we cancreate a combination of 2^n code words.

Since $n > k$, the number of possible code words is larger than the number of possible data words.

The block coding process is one-to-one; the same data word is always encoded as the same codeword. This means that we have $2n - 2k$ codewords that are not used. We call these code words invalid or illegal.

Figure 10.5 *Datawords and codewords in block coding*



10.14

Error Detection

How can errors be detected by using block coding? If the following two conditions are met, the receivercan detect a change in the original codeword.

1. The receiver has (or can find) a list of valid code words.
2. The original codeword has changed to an invalid one.

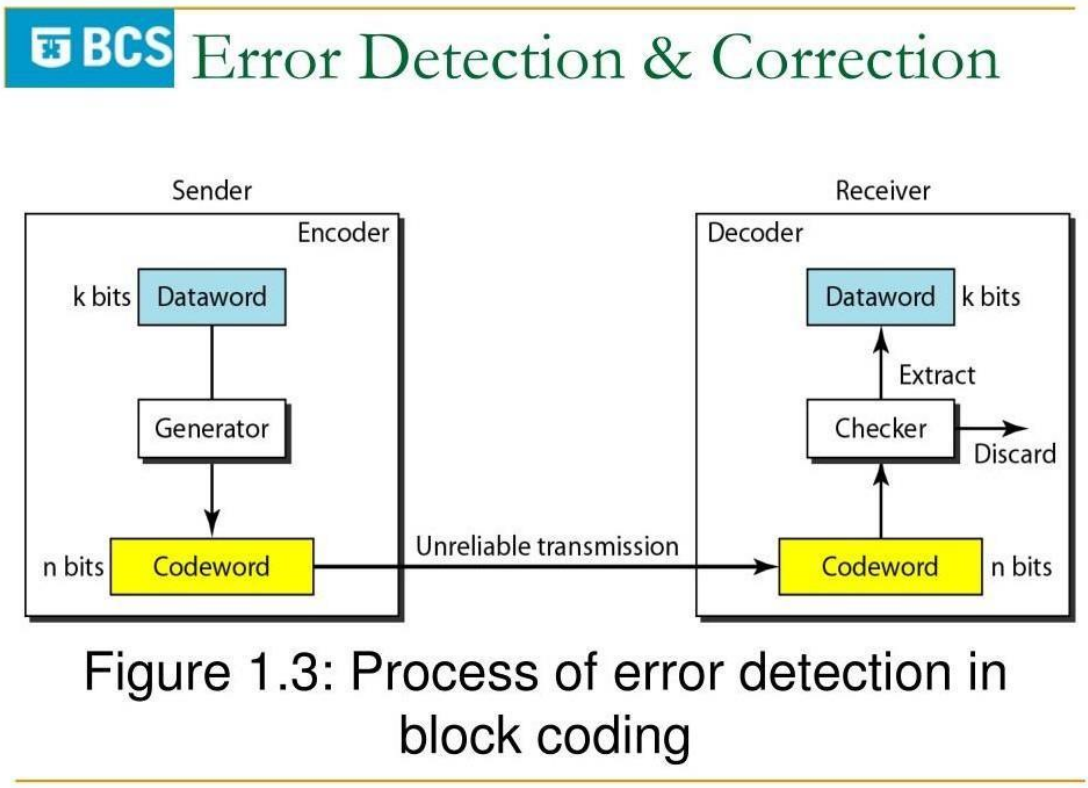


Figure 1.3: Process of error detection in block coding

The sender creates code words out of data words by using a generator that applies the rules and procedures of encoding each codeword sent to the receiver may change during transmission.

If the received codeword is the same as one of the valid code words, the word is accepted; the corresponding data word is extracted for use.

If the receiver code word is not valid, it is discarded. However, if the codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected.

This type of coding can detect only single errors. Two or more errors may remain undetected.

Example 10.2
Let us assume that *k* =2 and *n* =3. Table 10.1 shows the list of data words andcode words.
A code for error detection

Data words	*Code words*
00	000
01	011
10	101
11	110

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

1. The receiver receives 011. It is a valid codeword. The receiver extracts thedata word 01 from it.
2. The code word is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is discarded.
3. The codeword is corrupted during transmission, and 000 is received (the right two bits are corrupted). This is a valid codeword. The receiver incorrectly extracts the data word 00.

Two corrupted bits have made the error undetectable.
An error-detecting code can detect only the types of errors for which it is designed; other types of errors may remain undetected.

Error Correction

Error correction is much more difficult than error detection. In error detection, the receiver needs to know only that the received codeword is invalid; in error correction the receiver needs to find (or guess) the original codeword sent. We can say that we need more redundant bits for error correction than for error detection.
Let us add more redundant bits to Example 10.2 to see if the receiver can correctan error without knowing what was actually sent. We add 3 redundant bits to the 2-bit data word to make 5-bit code words.

Table 10.2 *A code for error correction (Example 10.3)*

Data word	*Code word*
00	00000
01	01011
10	10101
11	11110

The received code word is 01001.This is not a valid code word.

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

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

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

Hamming Distance

One of the central concepts in coding for error control is the idea of the Hammingdistance.
The Hamming distance between two words (of the same size) is the number ofdifferences between the corresponding bits. We show the Hamming distance between two words *x* and *y* as *d(x, y).*

The Hamming distance can easily be found if we apply the XOR operation on the two words and count the number of I's in the result.

Note that the Hamming distance is a value greater than zero.

The Hamming distance between two words is the number of differences betweencorresponding bits.

Example 10.4

Let us find the Hamming distance between two pairs of words.

1. The Hamming distance *d(OOO,* 011) is 2 because 000 XOR 011 is 011 (twoIs).
2. The Hamming distance *d(10101,* 11110) is 3 because 10101 XOR 11110 is01011 (three 1s)

Minimum Hamming Distance

Although the concept of the Hamming distance is the central point in dealing with error detection and correction codes, the measurement that is used for designing a code is the minimum Hamming distance.

In a set of words, the minimum Hamming distance is the smallest Hammingdistance between all possible pairs. We use $\mathbf{d_{min}}$ to define the minimum hamming distance in a coding scheme.

To find this value, we find the Hamming distances between all words and select the smallest one.

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

Example

Find the minimum Hamming distance of the coding scheme in Table 10.1.

Data words	*Code words*
00	000
01	011
10	101
11	110

Solution:

We first find all Hamming distances.

d (OOO, 011) =2

d (Oll,110)=2

The $\boldsymbol{d_{min}}$ in this case is 2.

Hamming Distance and Error

When a codeword is corrupted during transmission, the Hamming distance between the

sent and received code words is the number of bits affected by theerror.

In other words, the Hamming distance between the received codeword and the sent codeword is the number of bits that are corrupted during transmission.

For example, if the codeword 00000 is sent and 01101 is received, 3 bitsare in error and the Hamming distance between the two is

d(OOOOO, 01101) =3.

Minimum Distance for Error Detection

If s errors occur during transmission, the Hamming distance between thesent codeword and received codeword is s.

If our code is to detect up to s errors, the minimum distance between the validcodes must be s + 1, so that the received codeword does not match a valid codeword. .

To guarantee the detection of up to *s* errors in all cases, the minimum Hamming distance in a block code must be $d_{min} = S + 1$.

LINEAR BLOCK CODES

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

Minimum Distance for Linear Block Codes

It is simple to find the minimum Hamming distance for a linear block code. The minimum Hamming distance is the number of 1s in the nonzero valid codeword with the smallest number of 1s.

Some Linear Block Codes

1. *Simple Parity-Check Code*

A simple parity-check code is a single-bit error-detecting code in which $n = k + 1$with $d_{min} = 2$. In this code, a *k-bit* data word is changed to an n-bit codeword where $n = k + 1$. The extra bit, called the parity bit, is selected to make the totalnumber of I's in the codeword even.

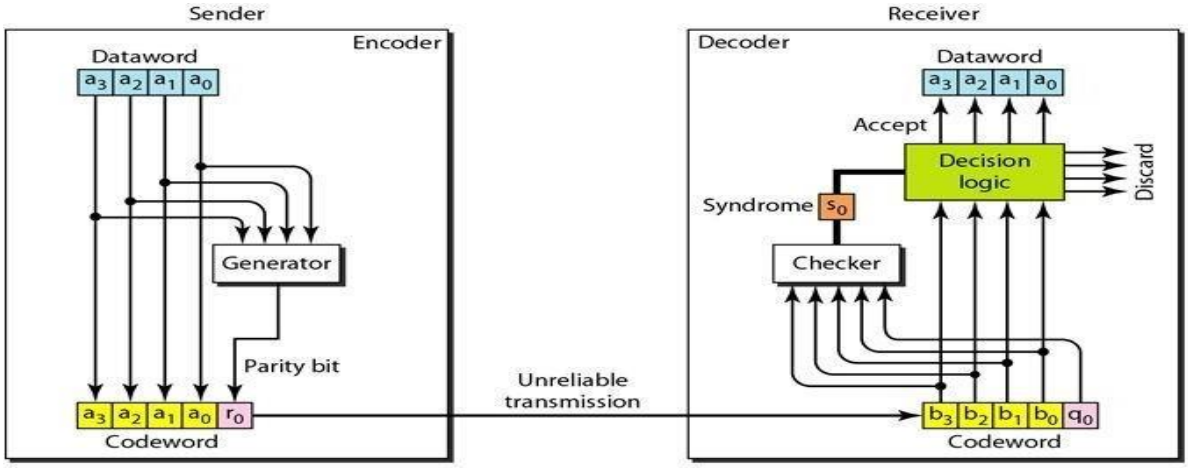
The encoder uses a generator that takes a copy of a 4-bit data word *(ao,* aI' *a2'* and *a3)* and generates a parity bit *ro.* The data word bits and the parity bit create

the 5-bit codeword. The parity bit that is added makes the number of 1's in thecodeword even.

Simple parity-check code C(5, 4)

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

Encoder and decoder for simple parity-check code



This is normally done by adding the 4 bits of the data word (modulo-2); the result is the parity bit.

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

The sender sends the codeword which may be corrupted during transmission. The receiver receives a 5-bit word. The checker at the receiver does the same thing as the generator in the sender with one exception: The addition is doneover all 5 bits. The result, which is called the syndrome, is just 1 bit. The syndrome is 0 when the number of I's in the received codeword is even; otherwise, it is 1.

The syndrome is passed to the decision logic analyzer. If the syndrome is 0, there is no

$$s_0 = b_3 + b_2 + b_1 + b_0 + q_0 \qquad \text{(modulo-2)}$$

error in the received codeword; the data portion of the received codeword is accepted as the data word; if the syndrome is 1, the data portion of the received codeword is discarded. The data word is not created.

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

CYCLIC CODES

Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.For example, if 1011000 are a codeword and we cyclically left-shift, then 0110001 is also a codeword.

In this case, if we call the bits in the first word a_0 to a_6' and the bits in the secondword b_0 to b_6, we can shift the bits by using the following:

$$b_1 = a_0 \quad b_2 = a_1 \quad b_3 = a_2 \quad b_4 = a_3 \quad b_5 = a_4 \quad b_6 = a_5 \quad b_0 = a_6$$

In the rightmost equation, the last bit of the first word is wrapped around andbecomes the first bit of the second word.

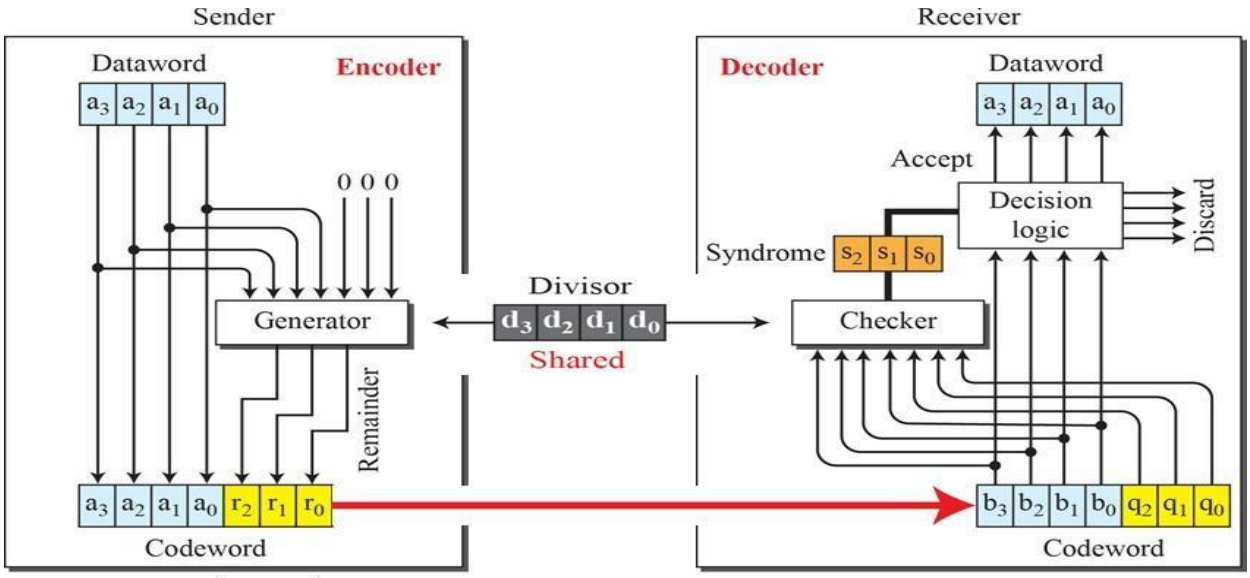
Cyclic Redundancy Check

CRC is a block code invented by W. Wesley Peterson in 1961.

It is commonly used to detect accidental changes to data transmission.

CRC involves binary division of the data bits being sent by a predetermined divisor agreed upon by the communicating system.

The divisor is generated using polynomials. So, CRC is also called polynomial code checksum.



$$r_0 = a_2 + a_1 + a_0$$
$$r_1 = a_3 + a_2 + a_1$$
$$r_2 = a_1 + a_0 + a_2$$

Encoding using CRC

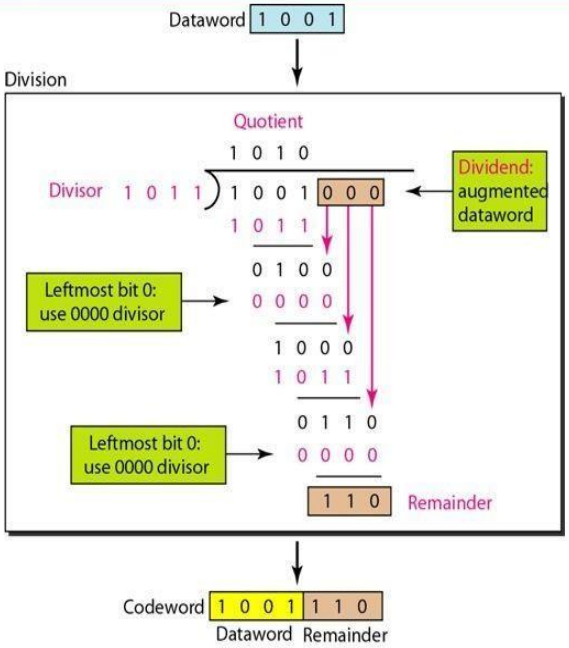
- The communicating parties agree upon the size of message block and the CRC divisor. For example, the block chosen may be CRC (7, 4), where 7is the total length of the block and 4 is the number of bits in the data segment. The divisor chosen may be 1011.
- The sender performs binary division of the data segment by the divisor.
- It then appends the remainder called CRC bits to the end of data segment. This makes the resulting data unit exactly divisible by the divisor.

Decoding

- The receiver divides the incoming data unit by the divisor.
- If there is no remainder, the data unit is assumed to be correct and is accepted.
- Otherwise, it is understood that the data is corrupted and is therefore rejected. The receiver may then send an erroneous

acknowledgement back to the sender for retransmission.

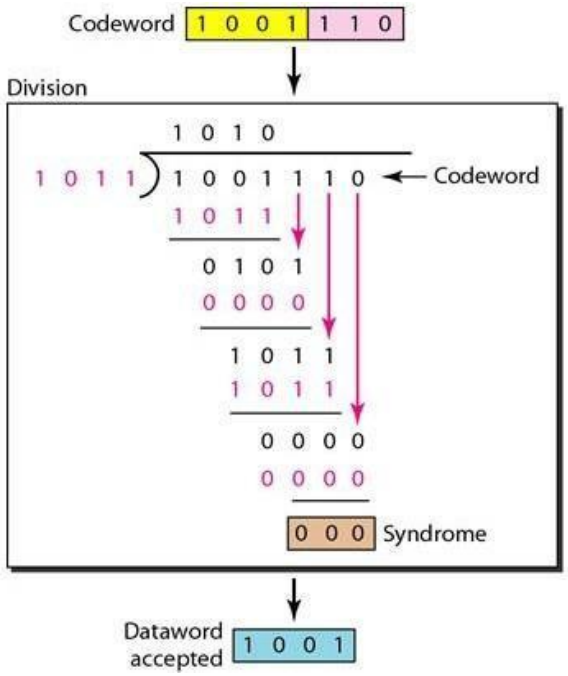
Figure 10.15 *Division in CRC encoder*

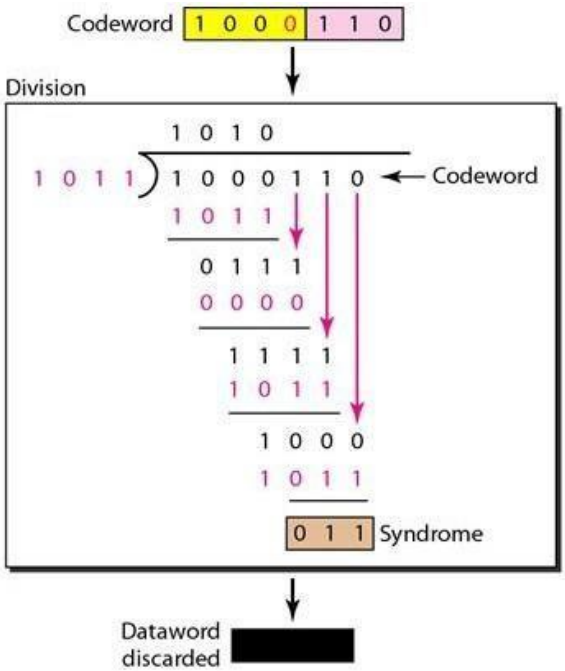


The division is done to have the most left bit 0, and is done from left to right like a regular division. The division is done until the quotient has as many bits as the dividend. The new codeword is the dataword extended by the remainder.

The divisor (generator) is agreed upon.

10.53





Cyclic codes Advantages

- Cyclic codes have a very good performance in detecting single bit errors, two bit errors and odd number of errors.
- They can easily be implemented in hardware and software
- They are especially fast when implemented in hardware.
- They are easy to encode.

Checksums

This is a block code method where a checksum is created based on the data values in the data blocks to be transmitted using some algorithm and appended to the data.

When the receiver gets this data, a new checksum is calculated and compared with the existing checksum. A non-match indicates an error.

Error Detection by Checksums

For error detection by checksums, data is divided into fixed sized frames orsegments.

Sender's End − The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.

Receiver's End − The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.

If the result is zero, the received frames are accepted; otherwise they are discarded.

Example

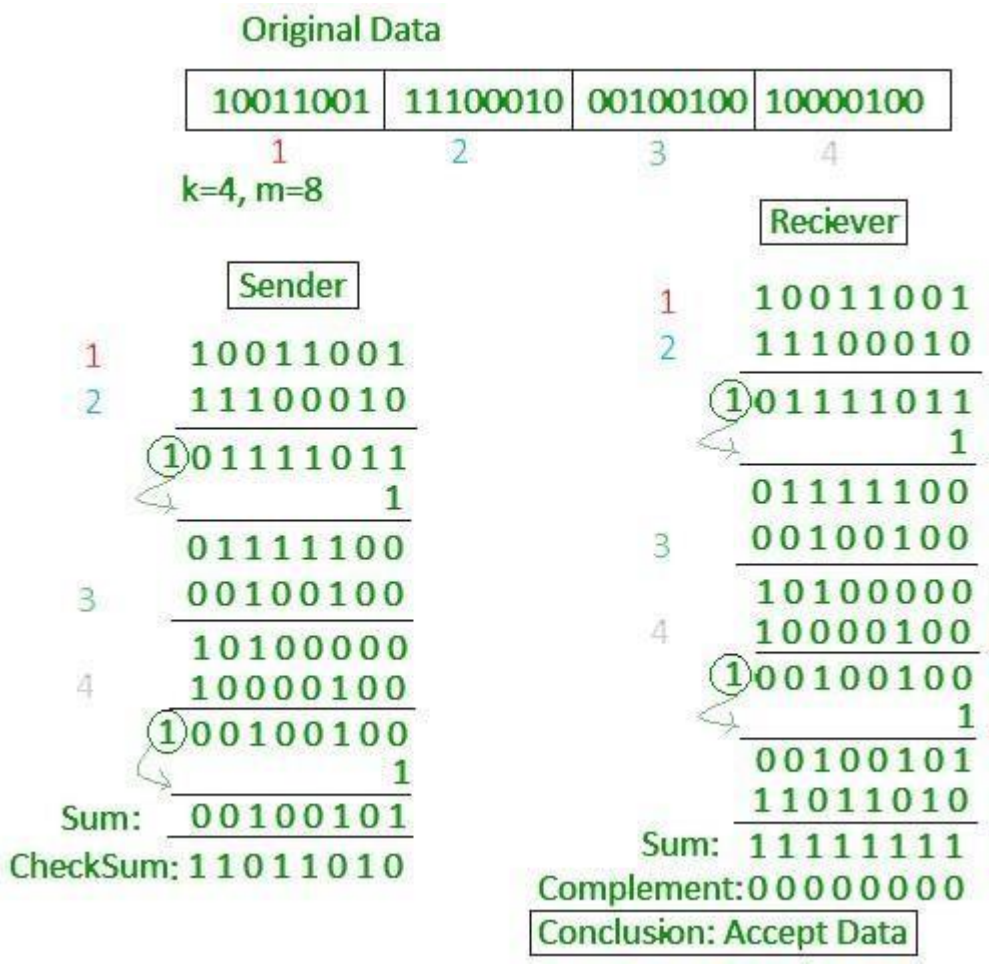
Suppose that the sender wants to send 4 frames each of 8 bits, where the frames are 11001100, 10101010, 11110000 and 11000011.

The sender adds the bits using 1s complement arithmetic. While adding two numbers using 1s complement arithmetic, if there is a carry over, it

is added to the sum.

After adding all the 4 frames, the sender complements the sum to get the checksum, 11010011, and sends it along with the data frames.

The receiver performs 1s complement arithmetic sum of all the frames including the checksum. The result is complemented and found to be 0. Hence, the receiver assumes that no error has occurred.



Framing

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.

Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Frames can be of **fixed** or **variable size**. In **fixed-size framing**, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. In **variable-size framing**, we need a way to define the end of the frame and the beginning of the next.

The two types of variable - sized framing are −

- **Character-oriented framing** - In character - oriented framing, data is transmitted as a sequence of bytes, from an 8-bit coding system like ASCII.
- **Bit - oriented framing** - In bit-oriented framing, data is transmitted as a sequence of bits that can be interpreted in the upper layers both as text as well as multimedia data.

Flow and Error Control

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

Flow Control

- Flow control coordinates the amount of data that can be sent before receiving acknowledgement.
- It is one of the most important functions of data link layer.
- Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.
- Receiver has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.

- Receiver must inform the sender before the limits are reached and request that the transmitter to send fewer frames or stop temporarily.
- Since the rate of processing is often slower than the rate of transmission, receiver has a block of memory (buffer) for storing incoming data until they are processed.

Error Control

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

Noiseless Channels

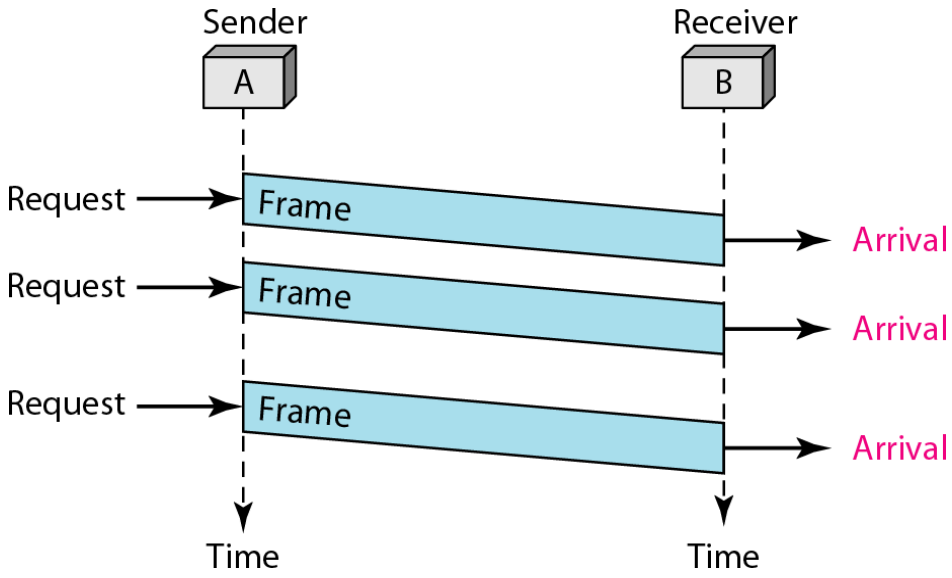
Let us first assume we have an ideal channel in which no frames are lost, duplicated, or corrupted. We introduce two protocols for this type of channel.

- Simplest Protocol
- Stop-and-Wait Protocol

Simplest Protocol

- In simplest protocol, there is no flow control and error control mechanism. It is a **unidirectional protocol** in which data frames travel in only one direction (from sender to receiver).
- Also, the receiver can immediately handle any received frame with a processing time that is small enough to be negligible.
- The protocol consists of two distinct procedures: a sender and receiver. The sender runs in the data link layer of the source machine and the receiver runs in the data link layer of the destination machine. No sequence number or acknowledgements are used here.

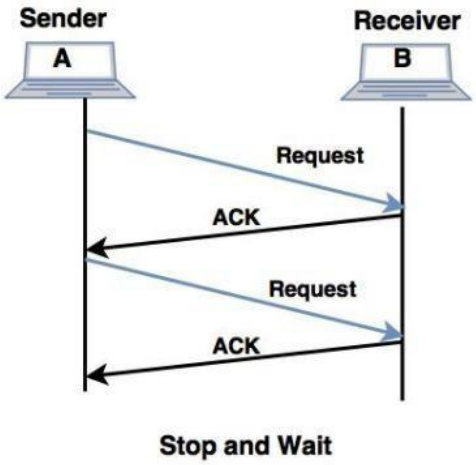
Flow diagram



Stop and Wait Protocol

- The simplest retransmission protocol is stop-and-wait.
- Transmitter (Station A) sends a frame over the communication line and then waits for a positive or negative acknowledgement from the receiver (station B).
- If no error occurs in the transmission, station B sends a positive acknowledgement (ACK) to station A.
- Now, the transmitter starts to send the next frame. If frame is received at station B with errors, then a negative acknowledgement (NAK) is sent to station A. In this case, station 'A' must retransmit the old packet in a new frame.
- There is also a possibility that the information frames or ACKs may get lost.
- Then, the sender is equipped with a timer. If no recognizable acknowledgement is received when the timer expires at the end of time out interval, the same frame is sent again.
- The sender which sends one frame and then waits for an acknowledgement before process is known as **stop and wait.**

Flow diagram



Noisy Channels

Although the Stop-and-Wait Protocol gives us an idea of how to add flow control to its predecessor, noiseless channels are nonexistent. We discuss three protocols in this section that use error control.

Stop and Wait Automatic Repeat Request (Stop and Wait ARQ)

Stop-and-Wait Automatic Repeat Request (Stop-and Wait ARQ), adds a simple error control mechanism to the Stop-and-Wait Protocol.

Detection and correction of Error:

- To detect and correct corrupted frames, redundancy bits are added to our data frame
- When the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded.
- The detection of errors in this protocol is manifested by the **silence of the receiver**.

Identification of a frame:

- Lost frames are more difficult to handle than corrupted ones. In our previous protocols, there was no way to identify a frame. The received frame could be the correct one, or a duplicate, or a frame out of order. The solution is to number the frames.

- When the receiver receives a data frame that is out of order, this means that frames were either lost or duplicated.
- The completed and lost frames need to be resent in this protocol.
- If the receiver does not respond when there is an error, how can the sender know which frame to resend?
- To remedy this problem, the sender keeps a copy of the sent frame.
- At the same time, it starts a timer.
- If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted.
- Since the protocol uses the **stop-and-wait mechanism**, there is only one specific frame that needs an ACK even though several copies of the same frame can be in the network.
- Since an ACK frame can also be corrupted and lost, it too needs redundancy bits and a sequence number.
- The ACK frame for this protocol has a sequence number field
- In this protocol, the sender simply discards a corrupted ACK frame or ignores an out-of-order one.

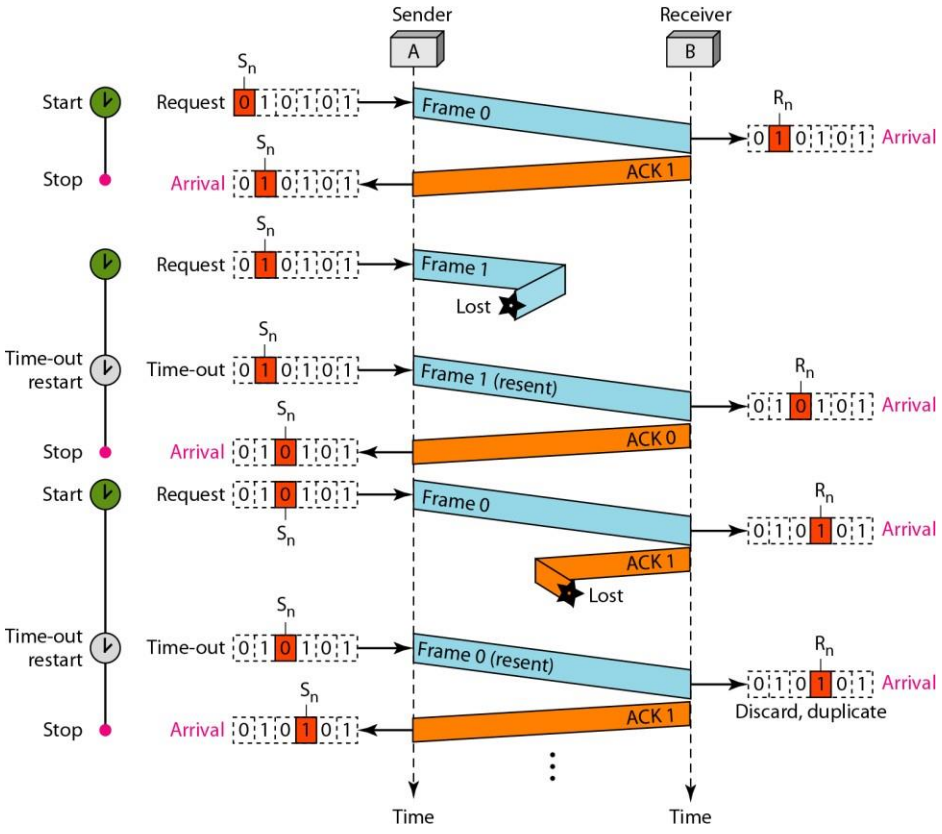
Sequence Numbers:

- The protocol specifies that frames need to be numbered. This is done by using **sequence numbers**.
- A field is added to the data frame to hold the sequence number of that frame.
- One important consideration is the range of the sequence numbers.
- Since we want to minimize the frame size, we look for the smallest range that provides unambiguous communication.
- The sequence numbers of course can wrap around.

Acknowledgment Numbers:

- The acknowledgment numbers always announce the sequence number of the next frame expected by the receiver.
- For example, if frame 0 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 1 (meaning frame 1 is expected next).
- If frame 1 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 0 (meaning frame 0 is expected).

Flow Diagram



The above figure shows an example of Stop-and-Wait ARQ. Frame A is sent and acknowledged. Frame 1 is lost and resent after the time-out. The resent frame 1 is acknowledged and the timer stops. Frame A is sent and acknowledged, but the acknowledgment is lost. The sender has no idea if the frame or the acknowledgment is lost, so after the time-out, it resends frame 0, which is acknowledged.

Go-Back-N Automatic Repeat Request (Go-Back-N ARQ)

In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive.

Sequence Numbers

Frames from a sending station are numbered sequentially. However, because we need to include the sequence number of each frame in the header, we need to set a limit. If the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to $2^m - 1$. For example, if m is 4, the only sequence numbers are 0 through 15 inclusive. However, we can repeat the sequence. So the sequence numbers are

0, 1,2,3,4,5,6, 7,8,9, 10, 11, 12, 13, 14, 15,0, 1,2,3,4,5,6,7,8,9,10, 11, ...

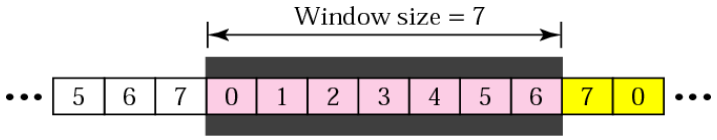
In other words, the sequence numbers are modulo-2^m.

Sliding Window

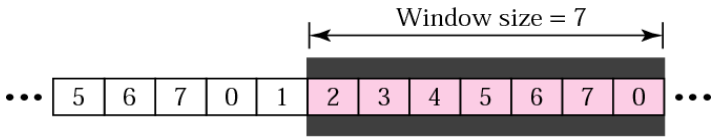
In this protocol, the sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver The range which is the concern of the sender is called the send sliding window; the range that is the concern of the receiver is called the receive sliding window.

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 here m is the number of bits for the sequence number.
- The window slides to include new unsent frames when the correct ACKs are received.



a. Before sliding



b. After sliding two frames

Receiver Sliding Window

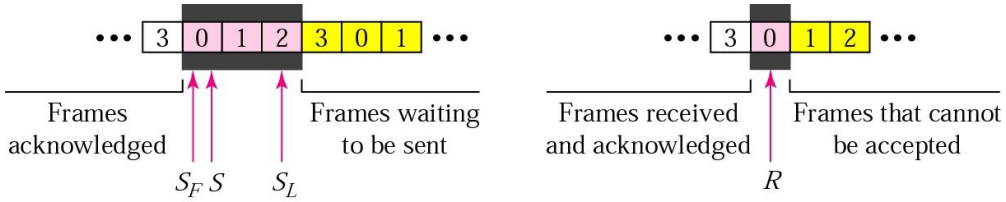
- Size of the window at the receiving site is always 1 in this protocol.
- Receiver is always looking for a specific frame to arrive in a specific order.
- Any frame arriving out of order is discarded and needs to be resent.
- Receiver window slides as shown in fig. Receiver is waiting for frame 0 in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

Control Variables

Sender has 3 variables: S, SF, and SL

- S holds the sequence number of recently sent 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.



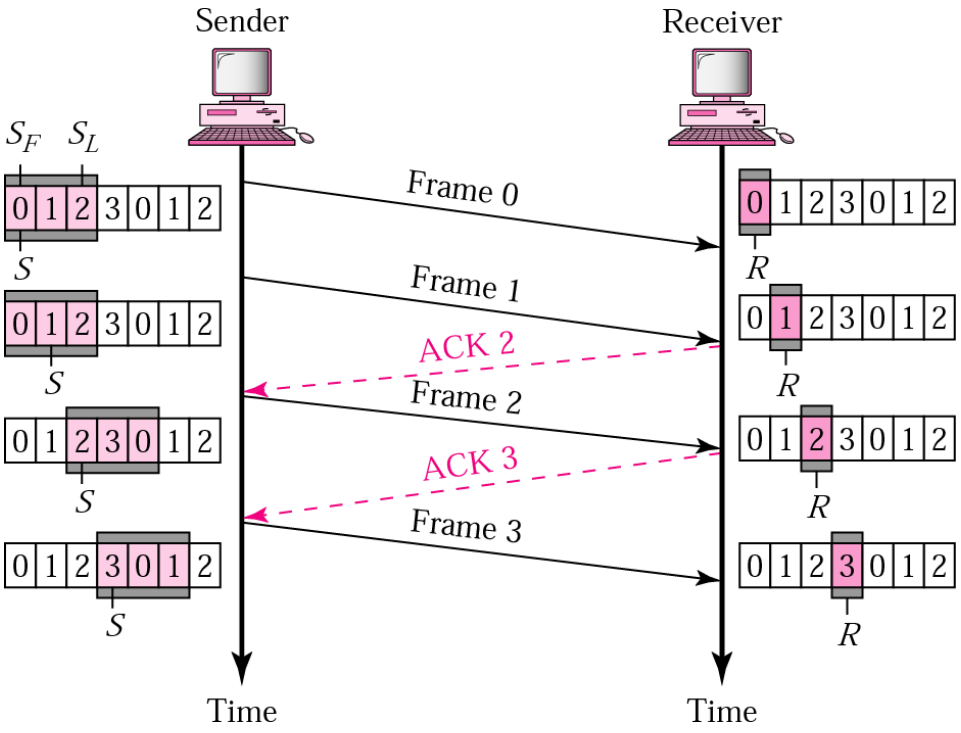
a. Sender window b. Receiver window

Acknowledgement

- Receiver sends positive ACK if a frame arrived safe and in order.
- If the frames are damaged/out of order, receiver is silent and discard all subsequent frames until it receives the one it is expecting.
- The silence of the receiver causes the timer of the unacknowledged frame to expire.
- Then the sender resends all frames, beginning with the one with the expired timer.
- For example, suppose the sender has sent frame 6, but the timer for frame 3 expires (i.e. frame 3 has not been acknowledged), then the sender goes back and sends frames 3, 4, 5, 6 again. Thus it is called Go-Back-N-ARQ
- The receiver does not have to acknowledge each frame received, it can send one cumulative ACK for several frames.

Go-Back-N ARQ, normal operation

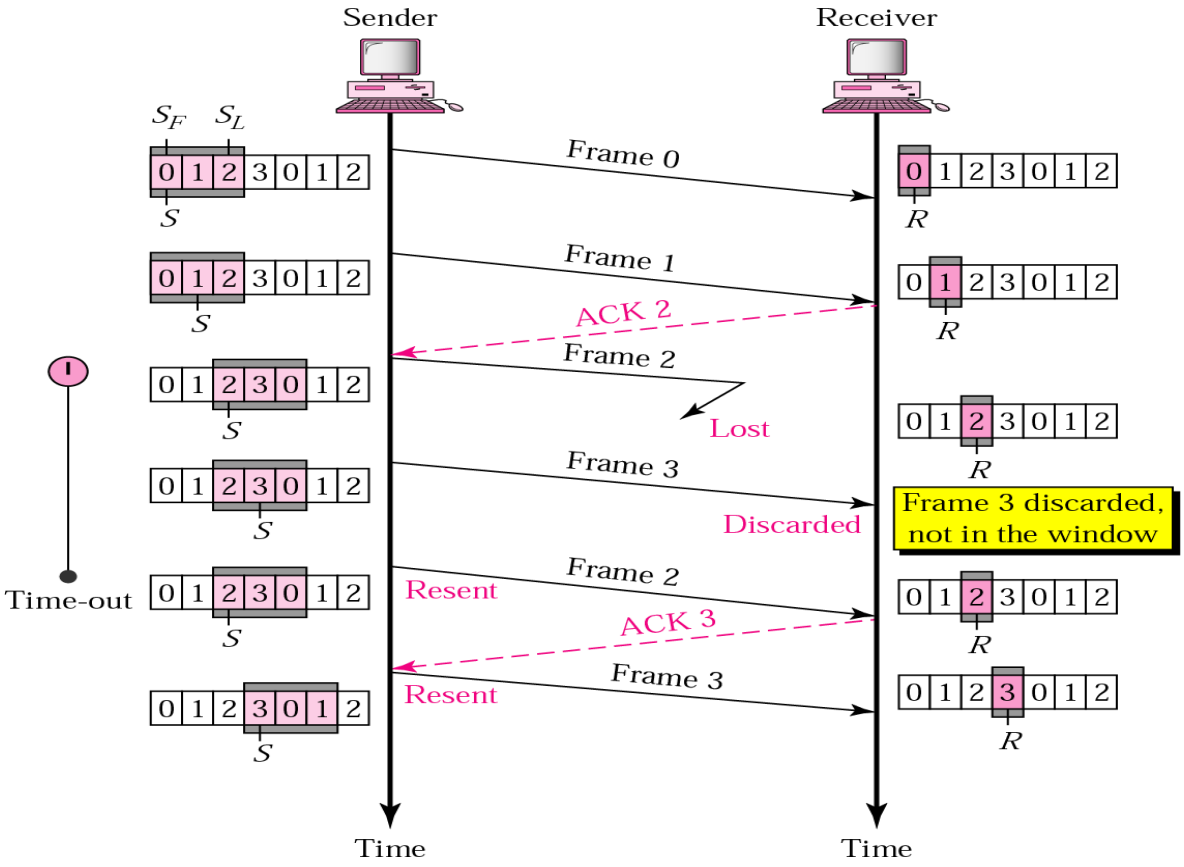
The sender keeps track of the outstanding frames and updates the variables and windows as the ACKs arrive.



Go-Back-N ARQ, lost frame

In the following figure :

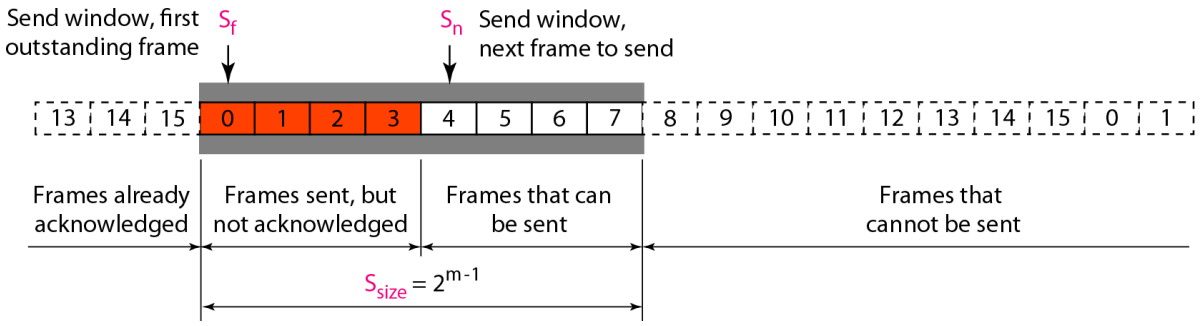
- Frame 2 is lost
- When the receiver receives frame 3, it discards frame 3 as it is expecting frame 2 (according to window).
- After the timer for frame 2 expires at the sender site, the sender sends frame 2 and 3. (go back to 2)



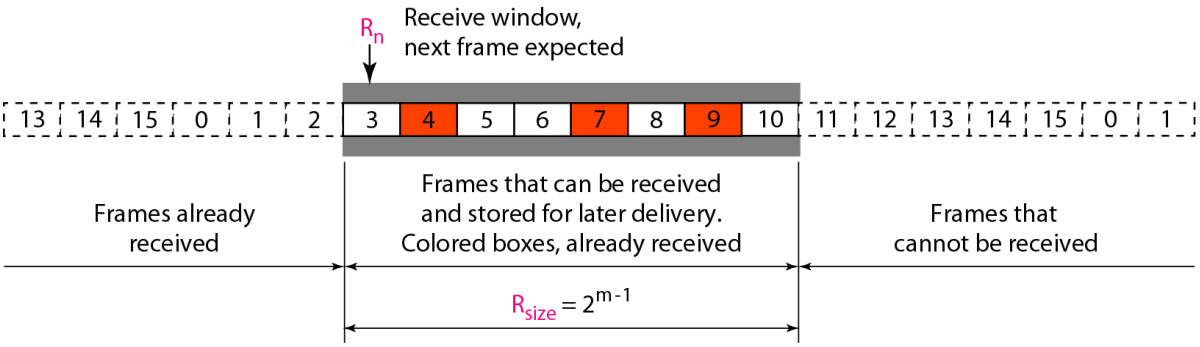
Selective Repeat Automatic Repeat Request (Selective Repeat ARQ)

Selective repeat protocol, also called Selective Repeat ARQ (Automatic Repeat reQuest), is a data link layer protocol that uses sliding window method for reliable delivery of data frames. Here, only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

The Selective Repeat Protocol also uses two windows of equal size: a send window and a receive window. Sending window stores the frames to be sent and receiving window stores the frames receive by the receiver. The size is half the maximum sequence number of the frame. For example, if the sequence number is from 0 – 15, the window size will be 8.



Send window for Selective Repeat ARQ



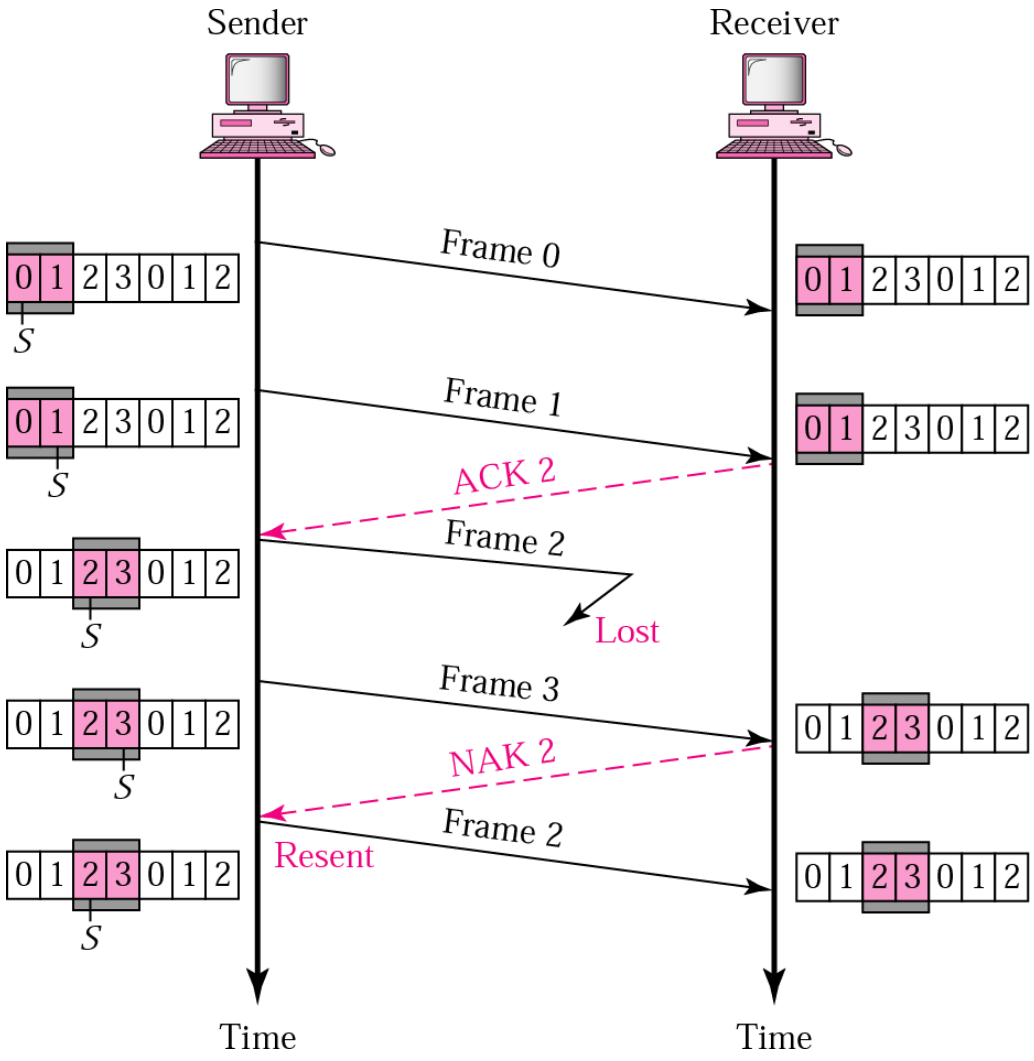
Receive window for Selective Repeat ARQ

Working Principle

Selective Repeat protocol provides for sending multiple frames depending upon the availability of frames in the sending window, even if it does not receive acknowledgement for any frame in the interim. The maximum number of frames that can be sent depends upon the size of the sending window.

The receiver records the sequence number of the earliest incorrect or un-received frame. It then fills the receiving window with the subsequent frames that it has received. It sends the sequence number of the missing frame along with every acknowledgement frame.

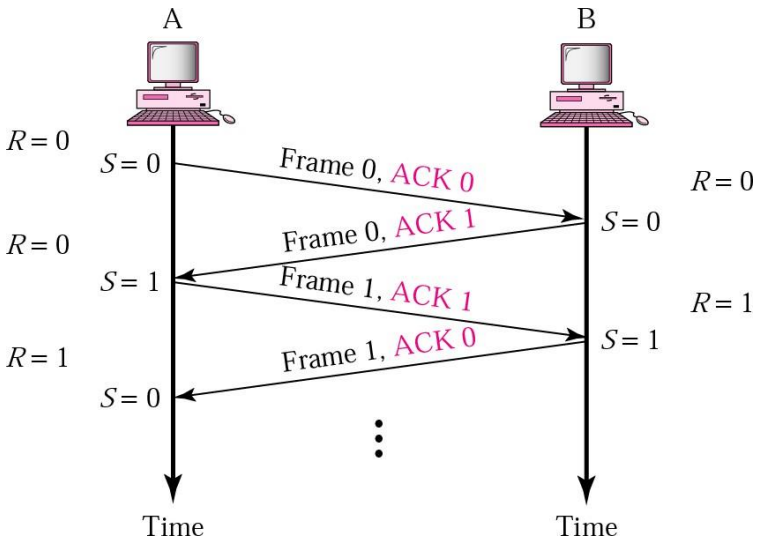
The sender continues to send frames that are in its sending window. Once, it has sent all the frames in the window, it retransmits the frame whose sequence number is given by the acknowledgements. It then continues sending the other frames.



Flow Diagram of Selective Repeat ARQ, lost frame

Piggybacking

The three protocols we discussed in this section are all unidirectional: data frames flow in only one direction although control information such as ACK and NAK frames can travel in the other direction. A technique called **piggybacking** is used to improve the efficiency of the bidirectional protocols. In this data frames are normally flowing in both directions: from node A to node B and from node B to node A. This means that the control information also needs to flow in both directions. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.



This technique has two windows: one send window and one receive window. Both also need to use a timer. Both also need to use a timer. Both are involved in three types of events: request, arrival, and time-out. However, the arrival event here is complicated; when a frame arrives, the site needs to handle control information as well as the frame itself. Both of these concerns must be taken care of in one event, the arrival event. The request event uses only the send window at each site; the arrival event needs to use both windows.

An important point about piggybacking is that both sites must use the same algorithm. This algorithm is complicated because it needs to combine two arrival events into one.

Network Layer

LOGICAL ADDRESSING

A global addressing system that identifies every host and router for delivery of a packet from network to network is called logical address or IP (Internet Protocol) address.

Usually, computers communicate through the Internet. The packet (data) transmitted by the sender computer may pass through several LANs or WANs before reaching the destination computer. For this level of communication, we need a global addressing scheme; what we call logical addressing.

An IP address is used globally to refer to the logical address in the network layer of the TCP/IP protocol.

The Internet addresses are 32 bits in length; this gives us a maximum of 2^{32} addresses. These addresses are referred to as **IPv4** (**IP version 4**) addresses or popularly as IP addresses.

IPv4 ADDRESSES

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

They are unique so that each address defines only one connection to the Internet. Two devices on the Internet can never have the same IPV4 address at the same time.

On the other hand, if a device operating at the network layer has m connections to the Internet, it needs to have m addresses, for example, a router.

The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

IPv4 addresses are unique and universal.

Address Space

A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses **N** bits to define an address, the address space is 2^N, because each bit can have two different values (0 or 1) and N bits can have 2^N values.

IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than 4 billion).

Notations

There are two notations to show an IPv4 address:

1. Binary notation
2. Dotted decimal notation.

1. Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation:

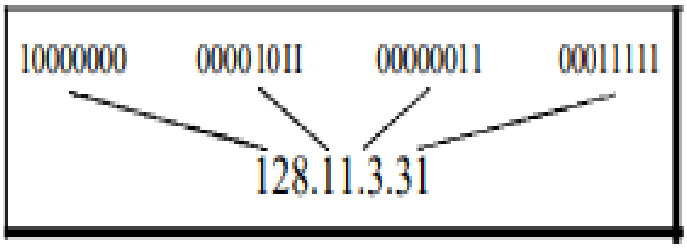
01110101 10010101 00011101 00000010

2. Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted decimal notation of the above address:

117.149.29.2

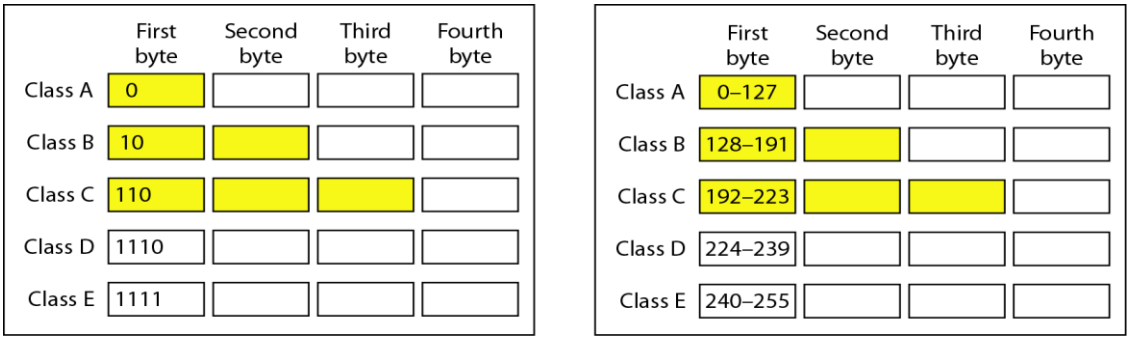
The following figure shows an IPv4 address in both binary and dotted-decimal notation. Note that because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255



Classful Addressing

IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing. In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.

We can find the class of an address when given the address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few bits can immediately tell us the class of the address. If the address is given in decimal-dotted notation, the first byte defines the class.



Finding the classes in binary and dotted-decimal notation

Example: Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first bit is 0. This is a class A address.

b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first byte is 14 (between 0 and 127); the class is A.

d. The first byte is 252 (between 240 and 255); the class is E.

Classless Addressing

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of

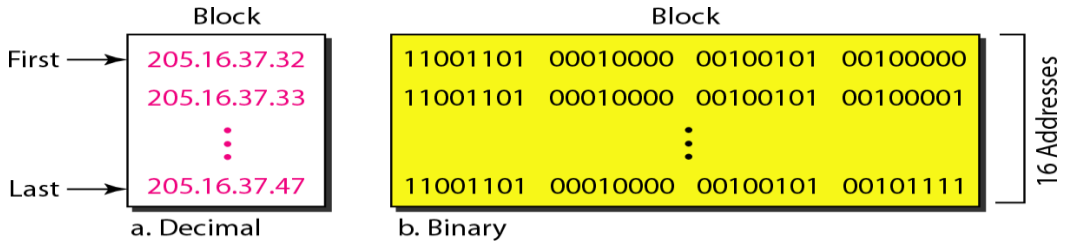
addresses) varies based on the nature and size of the entity. For example, a household may be given only two addresses; a large organization may be given thousands of addresses. An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve.

Restrictions to simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

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

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

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



A block of 16 addresses granted to a small organization

In the above figure, we can see that the restrictions are applied to this block. The addresses are contiguous. The number of addresses is a power of 2 (16 = 24), and the first address is divisible by 16. The first address, when converted to a decimal number, is 3,440,387,360, which when divided by 16 results in 215,024,210.

Network Address Translation (NAT)

The number of home users and small businesses that want to use the Internet is ever increasing. In the beginning, a user was connected to the Internet with a dial-up line, which means that she was connected for a specific period of time. An ISP with a block of addresses could dynamically assign an address to this user. An address was given to a user when it was needed. But the situation is different today. Home users and small businesses can be connected by an ADSL line or cable modem. In addition, many are not happy with one address; many have created small networks with several hosts and need an IP address for each host. With the shortage of addresses, this is a serious problem.

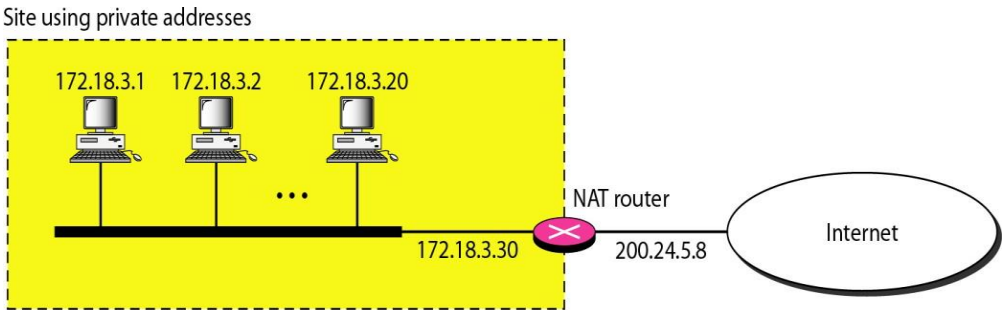
A quick solution to this problem is called network address translation (NAT). NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally.

To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved three sets of addresses as private addresses, shown in Table.

Addresses for private networks

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

NAT implementation



The site must have only one single connection to the global Internet through a router that runs the NAT software. As Figure shows, the private network uses private addresses. The router that connects the network to the global address uses one private address and one global address. The private network is transparent to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8.

Address Translation

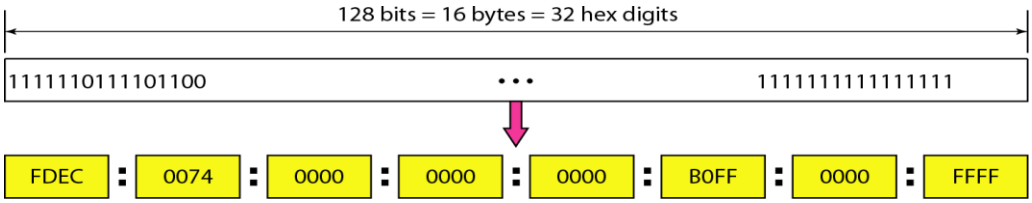
All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address. All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address.

IPv6 ADDRESSES

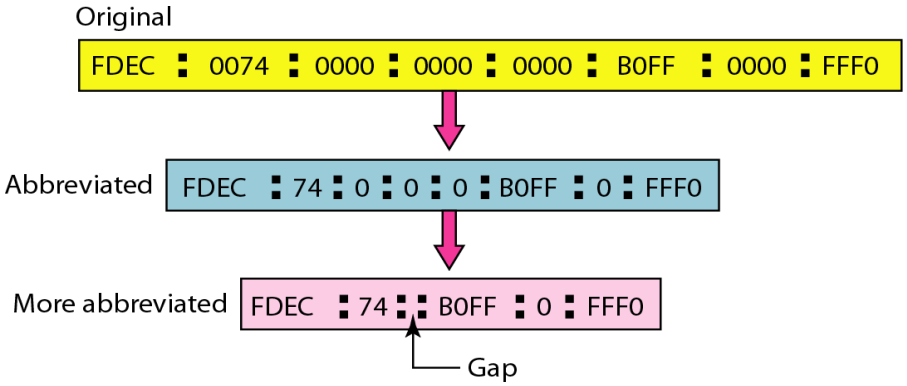
IPv6 (Internetworking Protocol, version 6), also known as IPng (Internetworking Protocol, next generation). An IPv6 address consists of 16 bytes (octets); it is 128 bits long.

Hexadecimal Colon Notation

To make addresses more readable, IPv6 specifies hexadecimal colon notation. In this notation, 128 bits is divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.



Abbreviation Although the IP address, even in hexadecimal format, is very long, many of the digits are zeros. In this case, we can abbreviate the address. The leading zeros of a section (four digits between two colons) can be omitted. Only the leading zeros can be dropped, not the trailing zeros.



Address Space

IPv6 has a much larger address space; 2^{128} addresses are available. The designers of IPv6 divided the address into several categories.

Unicast address - A unicast address defines a single computer. The packet sent to a unicast address must be delivered to that specific computer.

Multicast addresses - Multicast addresses are used to define a group of hosts instead of just one. A packet sent to a multicast address must be delivered to each member of the group.

Anycast addresses - IPv6 also defines anycast addresses. An anycast address, like a multicast address, also defines a group of nodes. However, a packet destined for an anycast address is delivered to only one of the members of the anycast group, the nearest one (the one with the shortest route).

Reserved address - Another category in the address space is the reserved address. These addresses start with eight Os (type prefix is 00000000).

Local Addresses - These addresses are used when an organization wants to use IPv6 protocol without being connected to the global Internet. In other words, they provide addressing for private networks. Nobody outside the organization can send a message to the nodes using these addresses.

Advantages of IPv6

I. **Larger address space**.IPv6 address is 128 bits long. Compared with the 32-bit address of IPv4, this is a huge (2^{96}) increase in the address space.

II. **Better header format**. IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process.

III. **New options**. IPv6 has new options to allow for additional functionalities.

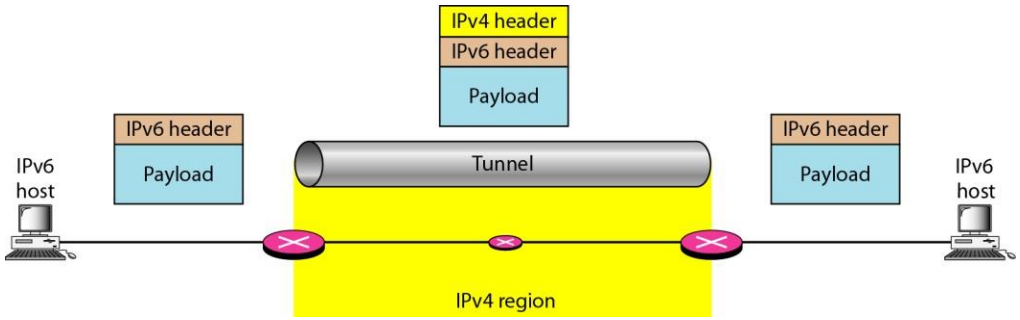
IV. **Allowance for extension**. IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

V. **Support for resource allocation**. A mechanism called flow label can be used to support traffic such as real-time audio and video.

VI. **Support for more security**. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Tunneling

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region. It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end.



ADDRESS MAPPING

The delivery of a packet to a host or a router requires two levels of addressing: **logical** and **physical**.

The **logical address** defines the sender and receiver at the **network** layer and is used to deliver messages across multiple **networks**. The hosts and routers are recognized at the network level by their logical (IP) addresses.

The **physical address** is the local **address** of a node; it is used by the data link layer to deliver data from one node to another within the same network. It must be unique locally, but is not necessarily unique universally.

We need to be able to map a logical address to its corresponding physical address and vice versa. This can be done by using either **static** or **dynamic mapping.**

Static mapping: Create a table that associates a logical address with a physical address. This table is stored in each machine on the network. The machine that know the IP address of another machine can look it up in table.

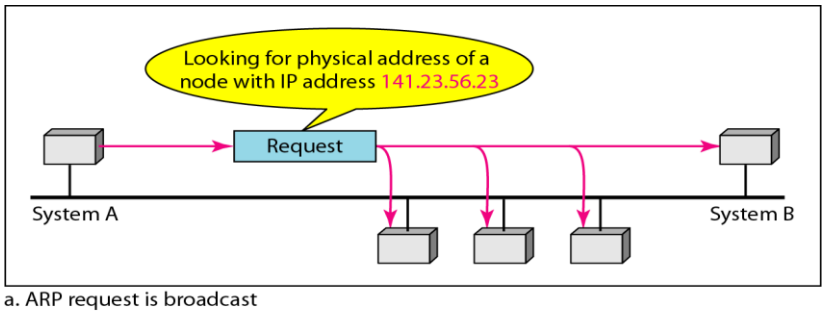
Dynamic mapping: The machine could know the logical address or physical address of another machine using following protocols

ARP (Address Resolution Protocol)

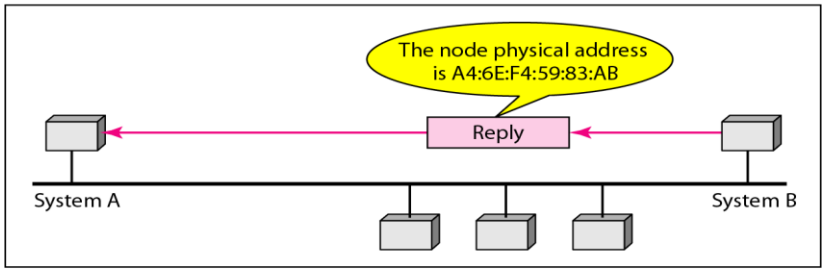
– Mapping a logical address to a physical address

Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver. The logical (IP) address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router. But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver. The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network.

Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses.



a. ARP request is broadcast



b. ARP reply is unicast

ARP operation

In the above figure, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of 141.23.56.23. This packet is received by every system on the physical network, but only system B will answer it. System B sends an ARP reply packet that includes its physical address. Now system A can send all the packets it has for this destination by using the physical address it received.

Mapping Physical to Logical Address: RARP, BOOTP, and DHCP

There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.

2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.

RARP

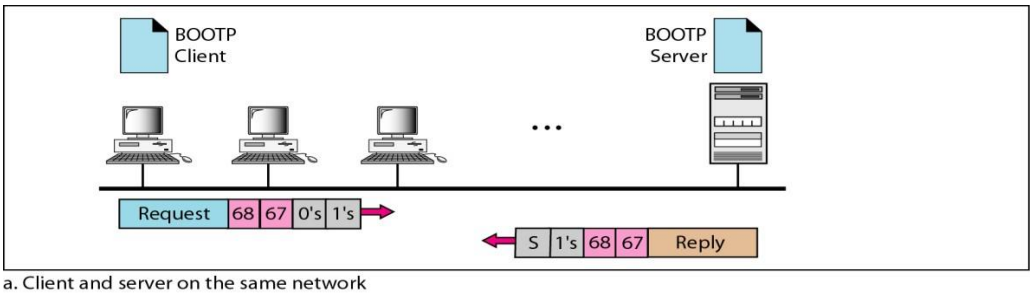
Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.

However, a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.

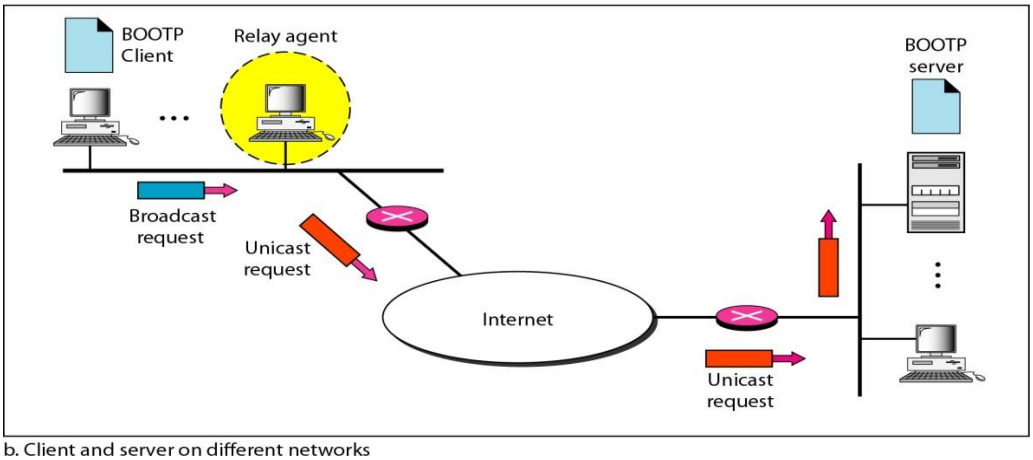
The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol. A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply. The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.

BOOTP

The Bootstrap Protocol (BOOTP) is a client/server protocol designed to provide physical address to logical address mapping. BOOTP is an application layer protocol. The administrator may put the client and the server on the same network or on different networks, as shown in figure, BOOTP messages are encapsulated in a UDP packet, and the UDP packet itself is encapsulated in an IP packet.



a. Client and server on the same network



b. Client and server on different networks

One of the advantages of BOOTP over RARP is that the client and server are application-layer processes. As in other application-layer processes, a client can be in one network and the server in another, separated by several other networks. However, there is one problem that must be solved. The BOOTP request is broadcast because the client does not know the IP address of the server. A broadcast IP datagram cannot pass through any router.

To solve the problem, there is a need for an intermediary. One of the hosts (or a router that can be configured to operate at the application layer) can be used as a relay. The host in this case is called a relay agent. The relay agent knows the unicast address of a BOOTP server. When it receives this type of packet, it encapsulates the message in a unicast datagram and sends the request to the BOOTP server. The packet, carrying a unicast destination address, is routed by any router and reaches the BOOTP server. The BOOTP server knows the message comes from a relay agent because one of the fields in the request message defines the IP address of the relay agent. The relay agent, after receiving the reply, sends it to the BOOTP client.

DHCP

The Dynamic Host Configuration Protocol (DHCP) has been devised to provide static and dynamic address allocation that can be manual or automatic.

Static Address Allocation In this capacity DHCP acts as BOOTP does. It is backward compatible with BOOTP, which means a host running the BOOTP client can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.

Dynamic Address Allocation DHCP has a second database with a pool of available IP addresses. This second database makes DHCP dynamic. When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.

When a DHCP client sends a request to a DHCP server, the server first checks its static database. If an entry with the requested physical address exists in the static database, the permanent IP address of the client is returned. On the other hand, if the entry does not exist in the static database, the server selects an IP address from the available pool, assigns the address to the client, and adds the entry to the dynamic database.

The dynamic aspect of DHCP is needed when a host moves from network to network or is connected and disconnected from a network (as is a subscriber to a service provider). DHCP provides temporary IP addresses for a limited time.

The addresses assigned from the pool are temporary addresses. The DHCP server issues a lease for a specific time. When the lease expires, the client must either stop using the IP address or renew the lease. The server has the option to agree or disagree with the renewal. If the server disagrees, the client stops using the address.

Unit - 4

Forwarding

Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination. However, this simple solution is impossible today in an internetwork such as the Internet because the number of entries needed in the routing table would make table lookups inefficient.

Forwarding Techniques

Several techniques can make the size of the routing table manageable and also handle issues such as security.

a. Next-Hop Method versus Route Method

One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method). The entries of a routing table must be consistent with one another.

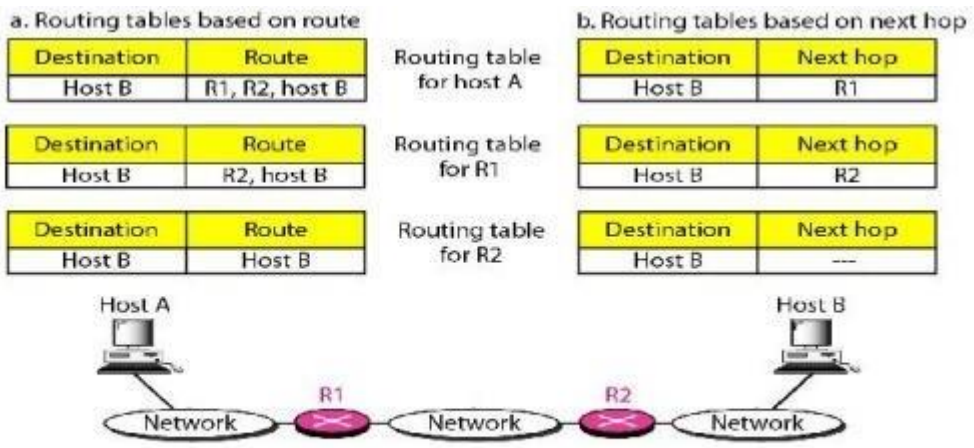


Figure 3.40 Route method versus next-hop method

b. Network-Specific Method versus Host-Specific Method

A second technique to reduce the routing table and simplify the searching process is called the network-specific method. Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself.

Host-specific routing is used for purposes such as checking the route or providing security measures

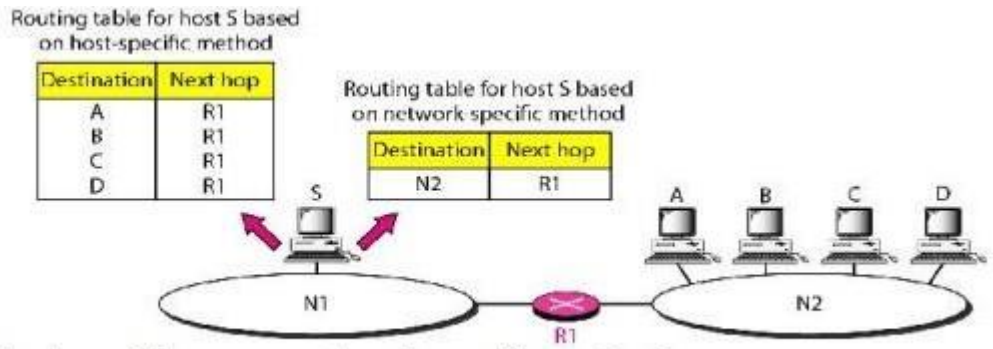


Figure 3.41 Host-specific versus network-specific method

c. Default Method

Another technique to simplify routing is called the default method. Host A is connected to a network with two routers. Router R1 routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in

the entire Internet, host A can just have one entry called the default (normally defined as network address 0.0.0.0).

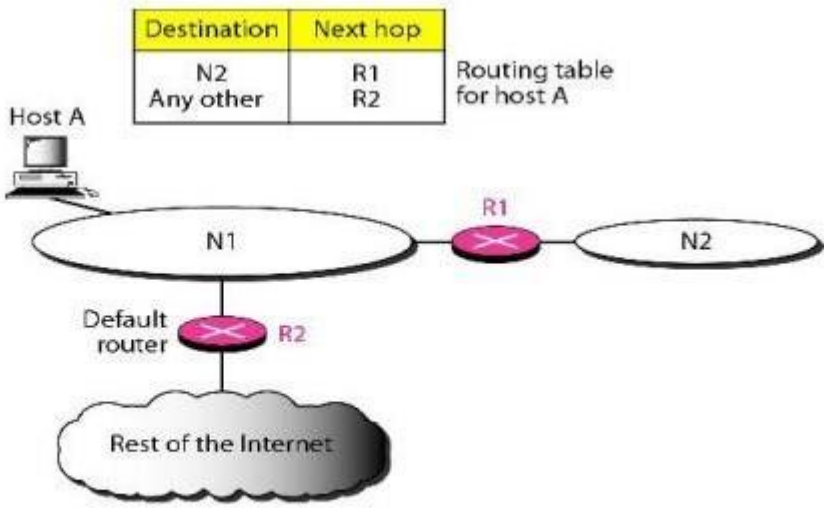


Figure 3.42 Default method

Routing Table

A routing table is a type of data file that acts as a map and is often installed on a router, networked computer or other hardware. The routing table contains information about various routes between devices in order to present the most efficient paths for data packets. The routing table can be either static or dynamic.

Static Routing Table

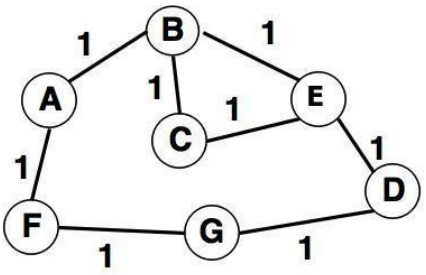
A static routing table contains information entered manually. The administrator enters the route for each destination into the table. When a table is created, it cannot update automatically when there is a change in the Internet. The table must be manually altered by the administrator. A static routing table can be used in a small internet that does not change very often.

Dynamic Routing Table

A dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP. Whenever there is a change in the Internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all the tables in the routers (and eventually in the host) automatically.

Distance Vector Routing

- Distance vector routing is the dynamic routing algorithm and also known as **Bellman-Ford** routing algorithm and **Ford- Fulkerson** algorithm.
- It was designed for small network topologies.
- In this algorithm, node router constructs a table containing the distance (total cost of path) to all other nodes and distributes that vector to its immediate neighbors.
- For distance vector routing, it is assumed that each node knows the cost of the link to each of its directly connected neighbours.
- A link, which is 'down' (which is not working) is assigned as an infinite cost.



Distance Vector Routing

The shortest path can be computed as:

Information at Node	Cost to Reach Node						
	A	B	C	D	E	F	G
A	0	1	2	3	2	1	2
B	1	0	1	2	1	2	3
C	2	1	0	2	1	3	3
D	3	2	2	0	1	2	2
E	2	1	1	1	0	3	2
F	1	2	3	2	3	0	1
G	2	3	3	1	2	1	0

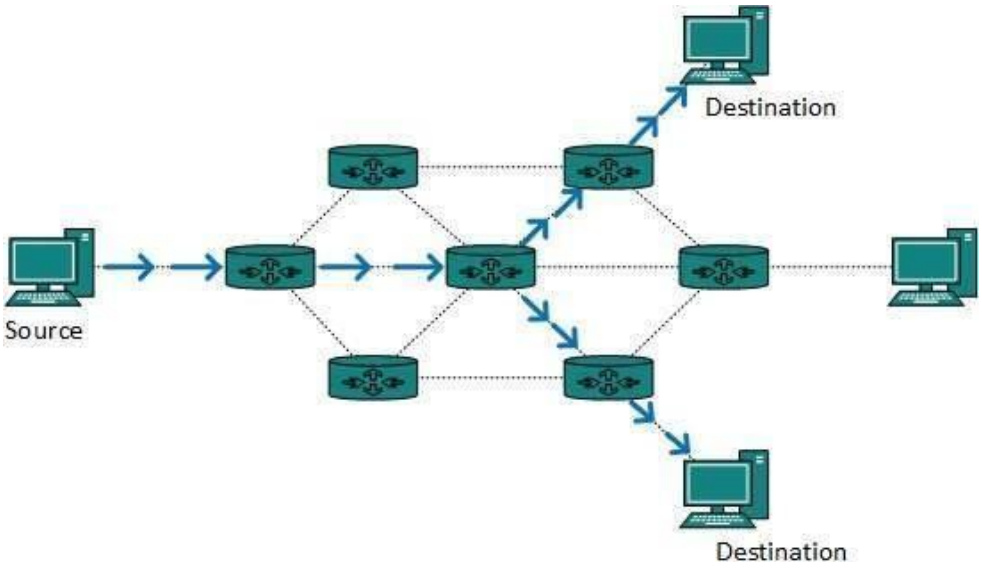
- Every node sends a message to its directly connected neighbours **For example:** A sends its information to B and F.
- After communicating to each directly connected node the shortest path can be easy to compute (as shown in above table).

Some issues with the Distance Vector Routing are:

1. Vulnerability to the 'Count-to-Infinity' problem is a serious issue with the distance vector.
2. It takes long time for convergence due to growth in the network.

Multicast Routing

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.



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.

Routing Protocols

Routing protocols have been created in response to the demand for dynamic routing tables. A routing protocol is a combination of rules and procedures that let routers in the internet inform each other of changes. It allows routers to share whatever they know about the internet or their neighbourhood.

Unicast Routing Protocols

There are two kinds of routing protocols available to route unicast packets:

- **Distance Vector Routing Protocol -** Distance Vector is simple routing protocol which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route.
- **Link State Routing Protocol** - Link State protocol is slightly complicated protocol than Distance Vector. It takes into account the states of links of all the routers in a network. This technique helps routes build a common graph of the entire network.

Multicast routing protocols

Unicast routing protocols use graphs while Multicast routing protocols use trees. Some of these protocols are

- **DVMRP** - Distance Vector Multicast Routing Protocol
- **MOSPF** - Multicast Open Shortest Path First
- **CBT** - Core Based Tree
- **PIM** - Protocol independent Multicast

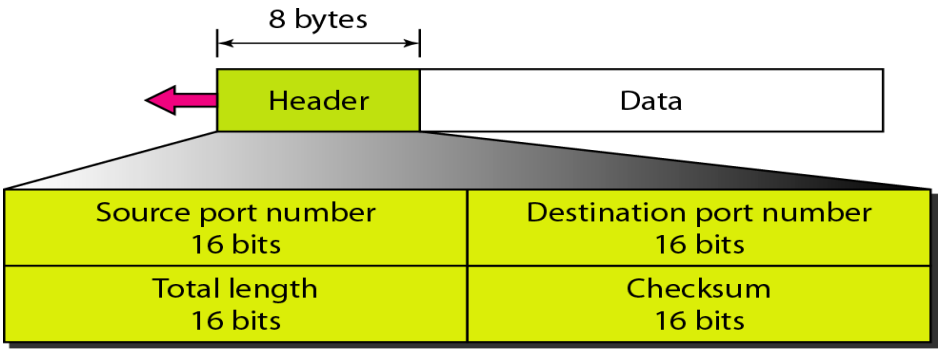
USER DATAGRAM PROTOCOL (UDP)

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

Datagrams

UDP packets, called user datagram, have a fixed-size header of 8 bytes. That is, the header details are stored in the very first eight bytes, but the rest is what holds the actual message.



The fields are as follows:

- **Source port number** - This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535.
- **Destination port number** - This is the port number used by the process running on the destination host. It is also 16 bits long.
- **Length** - This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes.

UDP length = IP length - IP header's length

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

Use of UDP

The following lists some uses of the UDP protocol:

- UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control.
- UDP is suitable for a process with internal flow and error control mechanisms.
- UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
- UDP is used for management processes such as SNMP.
- UDP is used for some route updating protocols such as Routing Information Protocol (RIP)

Transmission Control Protocol (TCP)

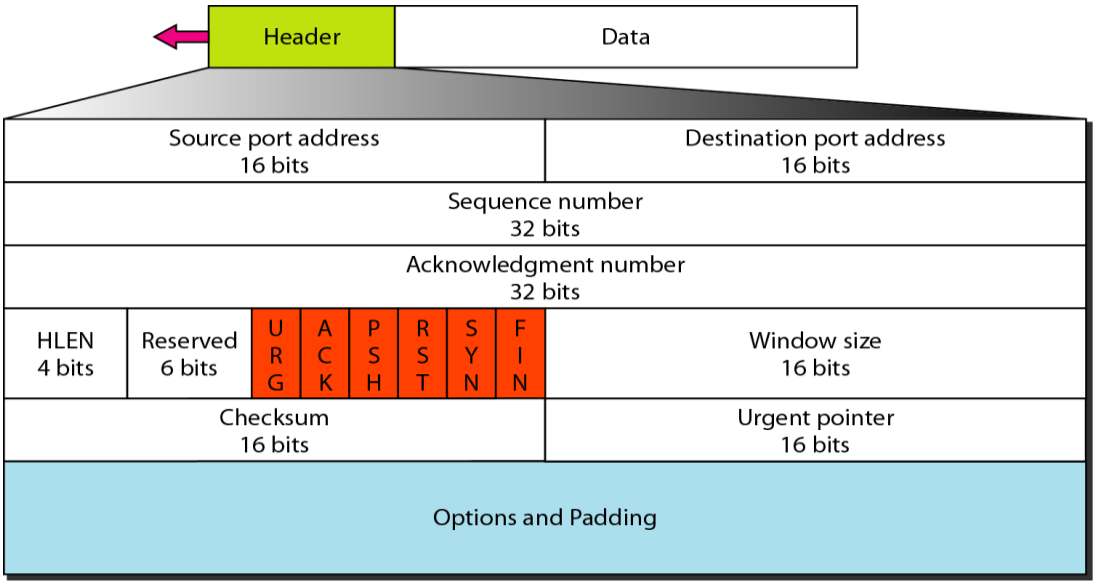
The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

TCP Segment

A packet in TCP is called a segment.

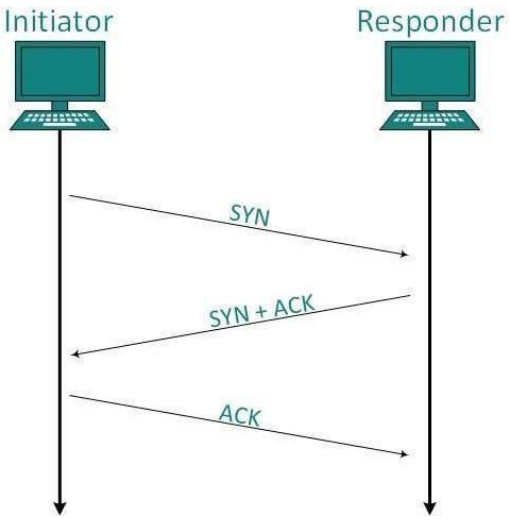


Description of flags in the control field

Flag	*Description*
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	Reset the connection.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

TCP- Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. **Three-way handshaking** is used for connection management.



Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by acknowledging FIN, that direction of TCP communication is closed and connection is released.

UNIT -5

Quality of Service

QoS is an overall performance measure of the computer network.

Important flow characteristics of the QoS are given below:

1. Reliability

If a packet gets lost or acknowledgement is not received (at sender), the re-transmission of data will be needed. This decreases the reliability.

The importance of the reliability can differ according to the application.

For example:

E- mail and file transfer need to have a reliable transmission as compared to that of an audio conferencing.

2. Delay

Delay of a message from source to destination is a very important characteristic. However, delay can be tolerated differently by the different applications.

For example:

The time delay cannot be tolerated in audio conferencing (needs a minimum time delay), while the time delay in the e-mail or file transfer has less importance.

3. Jitter

The jitter is the variation in the packet delay.

If the difference between delays is large, then it is called as **high jitter.** On the contrary, if the difference between delays is small, it is known as **low jitter.**

Example:

Case1: If 3 packets are sent at times 0, 1, 2 and received at 10, 11, 12. Here, the delay is same for all packets and it is acceptable for the telephonic conversation.

Case2: If 3 packets 0, 1, 2 are sent and received at 31, 34, 39, so the delay is different for all packets. In this case, the time delay is not acceptable for the telephonic conversation.

4. Bandwidth

Different applications need the different bandwidth.

For example:

Video conferencing needs more bandwidth in comparison to that of sending an e-mail.

Application Layer

Domain Names

Domain Name is a symbolic string associated with an IP address. There are several domain names available; some of them are generic such as **com, edu, gov, net** etc, while some country level domain names such as **au, in, za, us** etc.

The following table shows the **Generic** Top-Level Domain names:

Domain Name	Meaning

Com	Commercial business
Edu	Education
Gov	U.S. government agency
Int	International entity
Mil	U.S. military
Net	Networking organization
Org	Non profit organization

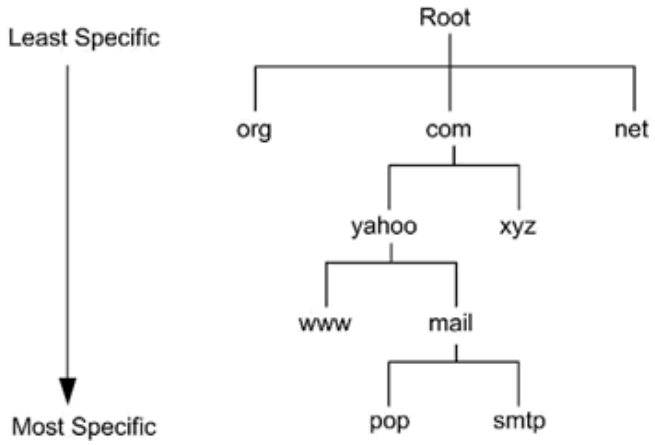
The following table shows the **Country top-level** domain names:

Domain Name	Meaning
au	Australia
in	India
cl	Chile
fr	France
us	United States
za	South Africa
uk	United Kingdom
jp	Japan

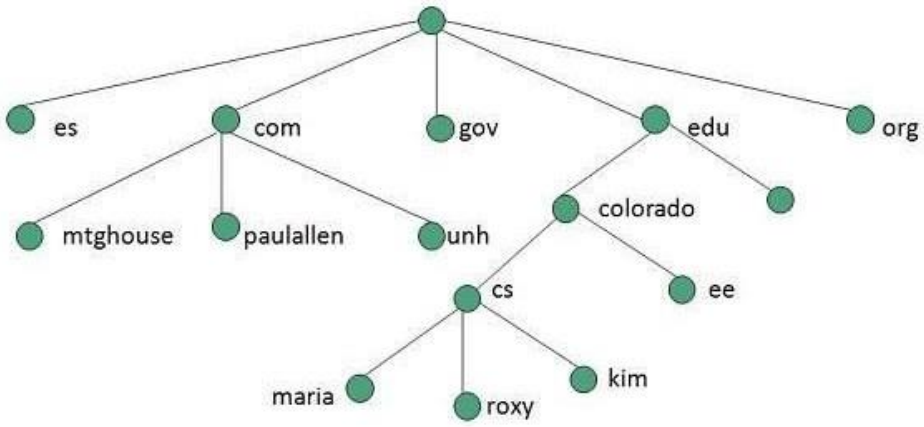
es	Spain
de	Germany
ca	Canada
ee	Estonia
hk	Hong Kong

Domain Name Space

Host names are divided into several pieces called domains. Domains are designed in a hierarchical structure. The top-level domains refer to the type of organization to which the network belongs, and subdomains further identify the specific network on which the host is situated.



The domain name space refers a hierarchy in the internet naming structure. This hierarchy has multiple levels (from 0 to 127), with a root at the top. The following diagram shows the domain name space hierarchy:



In the above diagram each subtree represents a domain. Each domain can be partitioned into sub domains and these can be further partitioned and so on.

Distribution of Name Space

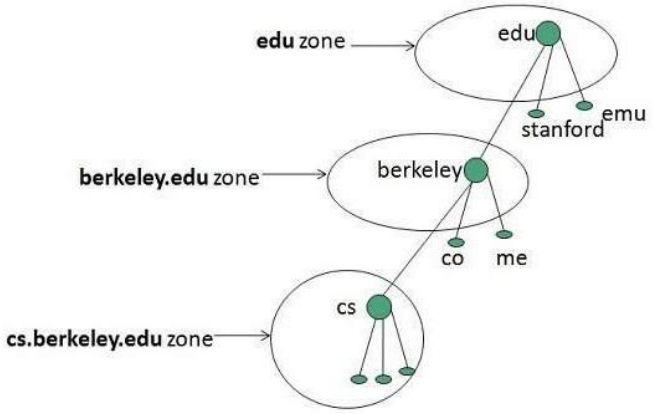
Name Server

Name server contains the DNS database. This database comprises of various names and their corresponding IP addresses. Since it is not possible for a single server to maintain entire DNS database, therefore, the information is distributed among many DNS servers.

- Hierarchy of server is same as hierarchy of names.
- The entire name space is divided into the zones

Zones

Zone is collection of nodes (sub domains) under the main domain. The server maintains a database called zone file for every zone.



If the domain is not further divided into sub domains then domain and zone refers to the same thing.

The information about the nodes in the sub domain is stored in the servers at the lower levels however; the original server keeps reference to these lower levels of servers.

Types of Name Servers

Following are the three categories of Name Servers that manages the entire Domain Name System:

- Root Server
- Primary Server
- Secondary Server

Root Server

Root Server is the top level server which consists of the entire DNS tree. It does not contain the information about domains but delegates the authority to the other server

Primary Servers

Primary Server stores a file about its zone. It has authority to create, maintain, and update the zone file.

Secondary Server

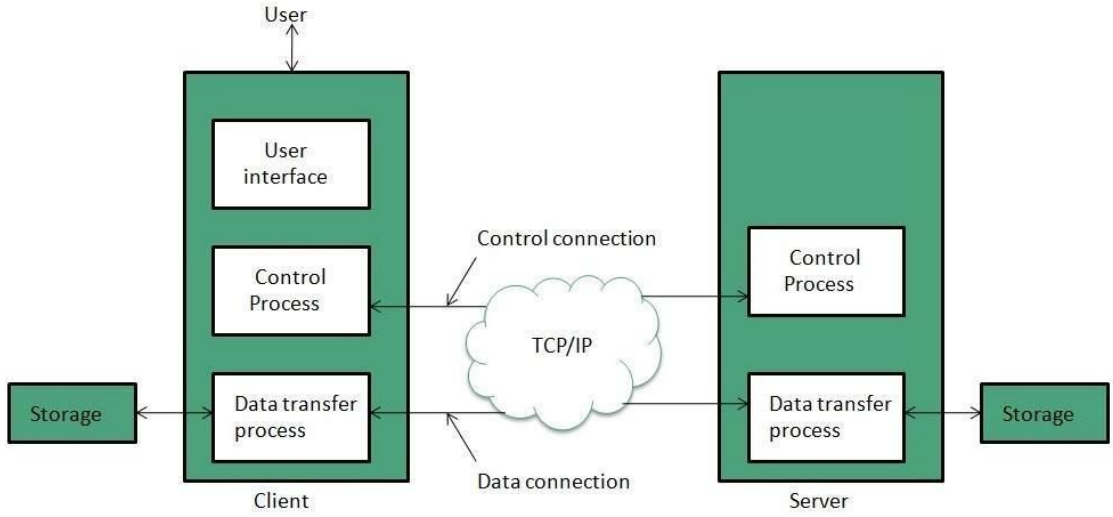
Secondary Server transfers complete information about a zone from another server which may be primary or secondary server. The secondary server does not have authority to create or update a zone file.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another.

FTP offers the mechanism for the same in following manner:

- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.
- FTP uses **port 21** for the control connection and **Port 20** for the data connection.



The above figure shows the basic model of FTP. The client has three components: userinterface, client control process, and the client data transfer process.

The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

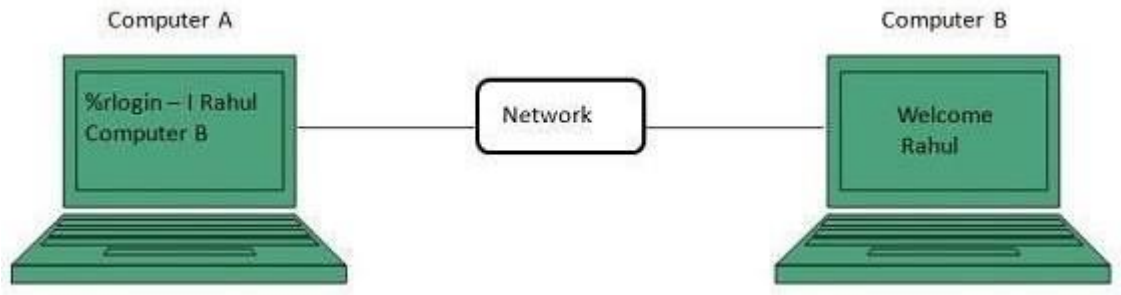
The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.

Telnet

TELNET is an abbreviation for **TErminaL NETwork**. Telnet is the standard TCP/IP protocol used to connect to a remote computer on the internet.

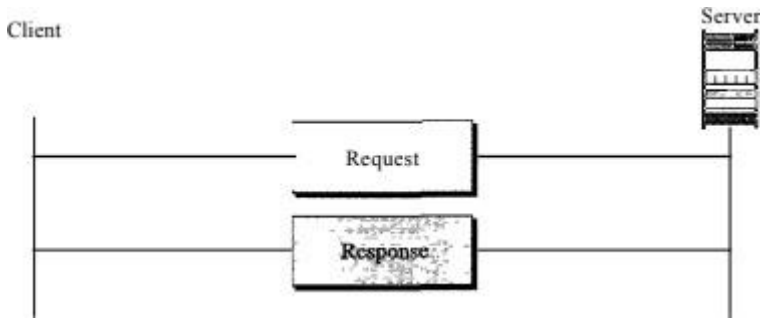
Using telnet client software on your computer, you can make a connection to a telnet server (that is, the remote host). Once your telnet client establishes a connection to the remote host, your client becomes a virtual terminal, allowing you to communicate with the remote host from your computer. In most cases, you'll need to log into the remote host, which requires that you have an account on that system.

The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.



Hyper Text Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is a communication protocol mainly used to access data on World Wide Web. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.



HTTP Request

HTTP request comprises of lines which contains:

- Request line
- Header Fields
- Message body

The first line in the request message is called a **request line,** which specifies the request method i.e. Get or Post. The header exchanges additional information between the client and the server**.**

HTTP Response

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

- Status line - the first line in the response message is called the status line.
- Headers
- Message body

SMTP

SMTP stands for **Simple Mail Transfer Protocol**. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.
- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

SMTP Commands

The following table describes some of the SMTP commands:

S.N.	Command Description
1	**HELLO** This command initiates the SMTP conversation.
2	**EHELLO** This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
3	**MAIL FROM** This indicates the sender's address.
4	**RCPT TO** It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
5	**SIZE** This command let the server know the size of attached message in bytes.
6	**DATA** The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message.
7	**QUIT** This commands is used to terminate the SMTP connection.
8	**VERFY** This command is used by the receiving server in order to verify whether the given username is valid or not.
9	**EXPN** It is same as VRFY, except it will list all the users name when it used with a distribution list.

URL

URL stands for **U**niform **R**esource **L**ocator, and is used to specify addresses on the World Wide Web. A URL is the fundamental network identification for any resource connected to the web (e.g., hypertext pages, images, and sound files).

A URL will have the following format −

protocol://hostname/other_information

The protocol specifies how information is transferred from a link. The protocol used for web resources is HyperText Transfer Protocol (HTTP). Other protocols compatible with most web browsers include FTP, telnet, newsgroups, and Gopher.

The protocol is followed by a colon, two slashes, and then the domain name. The domain name is the computer on which the resource is located.

Links to particular files or subdirectories may be further specified after the domain name. The directory names are separated by single forward slashes.

COOKIES

Cookies are files, generally from the visited webpages, which are stored on a user's computer. They hold a small amount of data, specific to a particular client and website, and can be accessed either by the web server or the client computer which can be usernames, password, session token, etc.

This allows the server to deliver a page personalized to a particular user, or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to that website.

Types of Cookies

There are three different types of cookies −

- **Session Cookies** − These are mainly used by online shops and allows you to keep items in your basket when shopping online. These cookies expire after a specific time or when the browser is closed.
- **Permanent Cookies** − These remain in operation, even when you have closed the browser. They remember your login details and password so you don’t have to type

them in every time you use the site. It is recommended that you delete these type of cookies after a specific time.

- **Third-Party Cookies** − These are installed by third parties for collecting certain information. For example: Google Maps.

Proxy server

It is an intermediary server between client and the internet. Proxy servers offer the following basic functionalities:

- Firewall and network data filtering.
- Network connection sharing
- Data caching

Proxy servers allow to hide, conceal and make your network id anonymous by hiding your IP address.

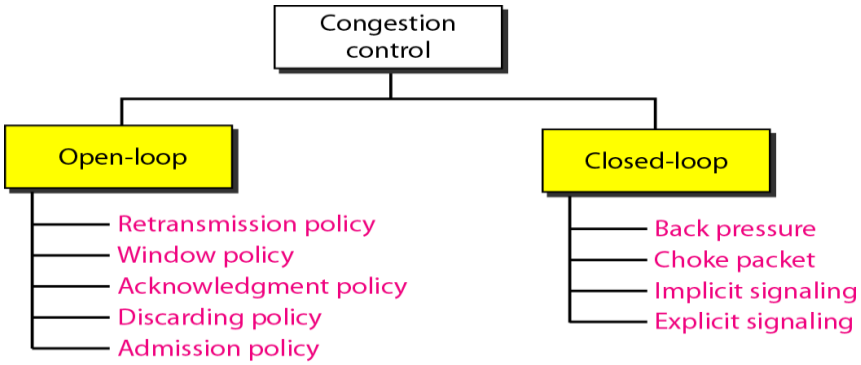
Purpose of Proxy Servers

Following are the reasons to use proxy servers:

- Monitoring and Filtering
- Improving performance
- Translation
- Accessing services anonymously
- Security

CONGESTION CONTROL

Congestion control refers to the techniques used to control or prevent congestion. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal).



Open-Loop Congestion Control

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

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.

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. The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet.

The receiver should send a acknowledgment only if it has to sent a packet or a timer expires.

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 case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

Admission Policy

In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of congestion or there is congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

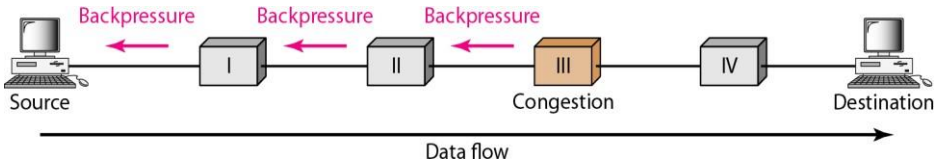
All the above policies are adopted to prevent congestion before it happens in the network.

Closed-Loop Congestion Control

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

Backpressure

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. Figure shows the idea of backpressure.

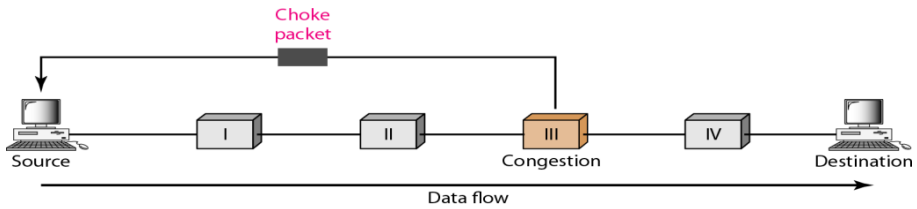


Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may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

Choke Packet

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly.

Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packet has travelled are not warned about congestion.



Implicit Signaling

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

receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

Explicit Signaling

In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. 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 signalling can occur in either the forward or the backward direction.

- **Backward Signaling** - In backward signalling, signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.
- **Forward Signaling** - In forward signalling, signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopts policies to prevent further congestion.