NAME: .....

PHONE: .....

COMPUTER NETWORK

BCA 5th (TU)
PERSPECTIVE

V 1.0

Er. Sital Pd Mandal
fb.com/rockingsital
info.sitalmandal@gmail.com

Push yourself, because no one else is going to do it for you.

Mechi Multiple Campus, Bhadrapur, Jhapa, Nepal

Course Title: Computer Networking
Course Code: CACS303
Year/Semester: 5th Sem/ III Year

1. Introduction

1.1	Network as an infrastructure for data communication	0.5	6 Hrs.
1.2	Applications of Computer network	0.5	
1.3	Network Architecture	1	
1.4	Types of computer Networks	0.5	
1.5	Protocols and Standards	0.5	
1.6	The OSI Reference Model	1	
1.7	The TCP/IP Protocol Suite	1	
1.8	Comparison between OSI and TCP/IP Reference model	0.5	
1.9	Critiques of OSI and TCP/IP Reference model	0.5	

2. The Physical Layer

2.1	Functions of Physical Layer	1	6 Hrs.
2.2	Data and Signals: Analog and Digital signals, Transmission Impairment, Data Rate Limits, Performance	1	
2.3	Data Transmission Media: Guided Media, Unguided Media and Satellites	1	
2.4	Bandwidth Utilization: Multiplexing and Spreading	1	
2.5	Switching: Circuit switching, Message switching & Packet switching	1	
2.6	Telephone, Mobile and Cable network for data Communication	1	

3:The Data Link Layer

3.1	Functions of Data Link Layer	1	8 Hrs.
3.2	Data Link Control: Framing, Flow and Error Control	1	
3.3	Error Detection and Correction	1	
3.4	High-Level Data Lin k Control(HDL C) & Point - to - Point protocol(PPP)	1	
3.5	Channel Allocation Problem	0.5	
3.6	Multiple Access: Radom Access(ALOH A, CSMA, CSMN CD, CSMA/CA), Controlled Access(Reservation, Polli ng, Token Passing), Channel i zation(FDMA, TDMA, CDMA)	1	
3.7	Wired LAN: Ethernet Standards and FDDI	1	
3.8	Wireless LAN : IEEE 802.11x and Bluetooth Standards	1	
3.9	Token Bus,Token Ring and Virtual LAN	0.5	

4. The Network Layer

4.1	Functions of Network Layer	1	
4.2	Virtual circu its and Datagram Subnets	1	

4.3	IPv4 Addresses: Address Space, Notations, Classful addressing, Classless addressing, Subnetting and Network Address Translation(NAT)	1	8 Hrs.
4.4	IPv4 Datagram format and fragmentation	1	
4.5	IPv6 Address Structure and advantages over IPv4	1	
4.6	Routing Algorithms: Distance Vector Routi ng, Lin k State Routing	1	
4.7	Internet Control Protocols: ARP, RARP, ICMP	1	
4.8	Routing protocols: OSPF, BGP, Unicusl, Multicast and Broadcast	1	

5.The Transport Layer

5.1	Functions of Transport Layer	1	7 Hrs.
5.2	Elements of Transport Protocols: Addressing, Establishi ng and Releasing Connection, Flow Control & Buffering, Error Control, Multiplexing & Demulti plexing, Crash Recovery	1	
5.3	User Datagram Protocol(UDP):User Datagram, U DP Operations, Uses of UDP, RPC	1	
5.4	Principles of Reliable Data Transfer:Bu ilding a Reliable Data Transfer Protocol, Pipelined Reliable Data Transfer Protocol, Go Back-N(GBN), Selective Repeat(SR)	2	
5.5	Transmission Control Protocol(TCP): TCP Services, TCP Features, TCP Segment Header	1	
5.6	Principle of Congestion Control	1	

6. The Application Layer

6.1	Functions of Application layer	1	5Hrs.
6.2	Application Layer Protocols: DNS, DHCP, WW W, HTTP, HTTPs, TELNET, FTP, SMTP, POP, IMAP	2	
6.3	Concept of traffic analyzer: MRTG, PRTG, SNMP. Packet tracer, Wireshark.	2	

7. Network Security

7.1	A Model for Network Security	1	5 Hrs.
7.2	Principles of cryptography: Symmetric Key and Public Key	1	
7.3	Public Key Algorithm - RSA	1	
7.4	Digital Signature Algorithm	1	
7.5	Communication Security: IPSec, VPN, Firewalls, Wireless Security.	1	

Lesson Plan

1. INTRODUCTION

S.No.	Contents	Check it (if Study)	Page	Spend Time in Hour
1.1	Network as an Infrastructure for Data Communication	✓	2	0.5
1.2	Applications of Computer Network		4	0.5
1.3	Network Architecture		5	1
1.4	Types of Computer Networks		7	0.5
1.5	Protocols and Standards		9	0.5
1.6	The OSI Reference Model		11	1
1.7	The TCP/IP Protocol Suite		14	1
1.8	Comparison between OSI and TCP/IP Reference model		16	0.5
1.9	Critiques of OSI and TCP/IP Reference model		18	0.5

2. PHYSICAL LAYER

S.No.	Contents	Check it (if Study)	Page	Spend Time in Hour
2.1	Functions of Physical Layer	✓	22	1
2.2	Data and Signals: Analog and Digital signals, Transmission Impairment, Data Rate Limits, Performance		23	1
2.3	Data Transmission Media: Guided Media, Unguided Media and Satellites		31	1
2.4	Bandwidth Utilization: Multiplexing and Spreading		35	1
2.5	Switching: Circuit switching, Message switching & Packet switching		40	1
2.6	Telephone, Mobile and Cable network for data Communication		46	1

7. NETWORK SECURITY

S.No.	Contents	Check it (if Study)	Page	Spend Time in Hour
7.1	A Model for Network Security	✓	55	1
7.2	Principles of cryptography: Symmetric Key and Public Key		57	1
7.3	Public Key Algorithm - RSA		59	1

7.4	Digital Signature Algorithm		61	1
7.5	Communication Security: IPSec, VPN, Firewalls, Wireless Security.		63	1

6. APPLICATION LAYER

S.No.	Contents	Check it (if Study)	Page	Spend Time in Hour
6.1	Functions of Application layer		71	1
6.2	Application Layer Protocols: DNS, DHCP, WWW, HTTP, HTTPs, TELNET, FTP, SMTP, POP, IMAP		71	2
6.3	Concept of traffic analyzer: MRTG, PRTG, SNMP. Packet tracer, Wireshark.		82	2

4. NETWORK LAYER

S.No.	Contents	Check it (if Study)	Page No.	Time to Spend (hrs)
4.1	Functions of Network Layer		91	1
4.2	Virtual circuits and Datagram Subnets		92	1
4.3	IPv4 Addresses: Address Space, Notations, Classful addressing, Classless addressing, Subnetting and Network Address Translation(NAT)		94	1
4.4	IPv4 Datagram format and fragmentation		96	1
4.5	IPv6 Address Structure and advantages over IPv4		99	1
4.6	Routing Algorithms: Distance Vector Routing, Link State Routing		103	1
4.7	Internet Control Protocols: ARP, RARP, ICMP		112	1
4.8	Routing protocols: OSPF, BGP, Unicast, Multicast and Broadcast		118	1

3. DATA LINK LAYER

S.No.	Contents	Check it (if Study)	Page	Spend Time in Hour
3.1	Functions of Data Link Layer	✓	126	1
3.2	Data Link Control: Framing, Flow and Error Control		126	1
3.3	Error Detection and Correction		156	1
3.4	High-Level Data Lin k Control(HDLC) & Point - to - Point protocol(PPP)		161	1

3.5	Channel Allocation Problem		167	0.5
3.6	Multiple Access: Radom Access(ALOH A, CSMA, CSMN CD, CSMA/CA), Controlled Access(Reservation, Polling, Token Passing), Channelization (FDMA, TDMA, CDMA)		168	1
3.7	Wired LAN: Ethernet Standards and FDDI		190	1
3.8	Wireless LAN : IEEE 802.11x and Bluetooth Standards		193	1
3.9	Token Bus, Token Ring and Virtual LAN		198	0.5

5. TRANSPORT LAYER

S.No.	Contents	Check it (if Study)	Page	Study in Hours
5.1	Functions of Transport Layer		203	1
5.2	Elements of Transport Protocols: Addressing, Establishing and Releasing Connection, Flow Control & Buffering, Error Control, Multiplexing & Demultiplexing, Crash Recovery		205	1
5.3	User Datagram Protocol(UDP):User Datagram, U DP Operations, Uses of UDP, RPC		217	1
5.4	Principles of Reliable Data Transfer: Building a Reliable Data Transfer Protocol, Pipelined Reliable Data Transfer Protocol, Go Back-N(GBN), Selective Repeat(SR)		222	2
5.5	Transmission Control Protocol(TCP): TCP Services, TCP Features, TCP Segment Header		236	1
5.6	Principle of Congestion Control		239	1

UNIT 1: INTRODUCTION

Answer own Innovation, Creativity & Tinkering.

Read Me First (3 times) Assumes Basic Key Terms while writing your unit1 answer.

analog	analog data	analog signal	attenuation	bandpass channel
bandwidth	baseband transmission	bit length	bit rate	bits per second (bps)
broadband transmission	composite signal	cycle	data	decibel (dB)
digital	digital data	digital signal	distortion	Fourier analysis
frequency	frequency-domain	fundamental frequency	harmonic	Hertz (Hz)
jitter	latency	low-pass channel	noise	nonperiodic signal
Nyquist bit rate	peak amplitude	period	periodic signal	phase
processing delay	propagation speed	propagation time	queuing time	Shannon capacity
signal	signal-to-noise ratio (SNR)	sine wave	throughput	time-domain
transmission time	wavelength	…….	……..	……..etc

1.1 NETWORK AS AN INFRASTRUCTURE FOR DATA COMMUNICATION:

- Network infrastructure *is the hardware and software resources of an entire network* that enable network connectivity, communication, operations and management of an enterprise network.
- It provides the *communication path and services between users, processes, applications, services and external networks/the internet.*
- Network infrastructure is typically part of the IT infrastructure found in most enterprise IT environments. The *entire network infrastructure is interconnected, and can be used for internal communications, external communications or both.*
- **A typical network infrastructure includes:**

Networking Hardware: • Routers • Switches • LAN cards • Wireless routers • Cables **Network Services:** • Satellite • Wireless protocols • IP addressing	**Networking Software:** • Network operations and management • Operating systems • Firewall • Network security applications

- *Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.*

- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

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

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

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

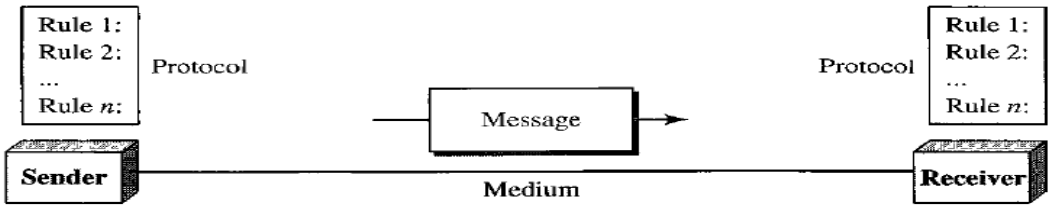
3. **Timeliness**: **The system must deliver data in a timely manner.**

4. **Jitter**: Jitter refers **to the variation in the packet arrival time**. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 millisecond. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

DATA COMMUNICATIONS COMPONENTS

- **A data communications system has five components:**
    1. *Message*
    2. *Sender*

3. *Receiver*
4. *Protocol*
5. *Medium*



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

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

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

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

5. ***Protocol***. A protocol is a set of rules that governs data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

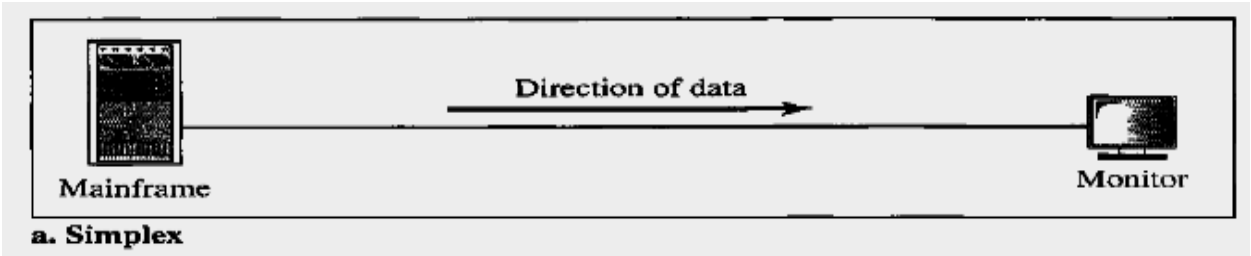
Direction of Data Flow

- **Communication between two devices i.e. sender & receiver can be of three types:**

1. **Simplex,**
2. **Half-duplex, or**
3. **Full-duplex**

Data Flow: Simplex

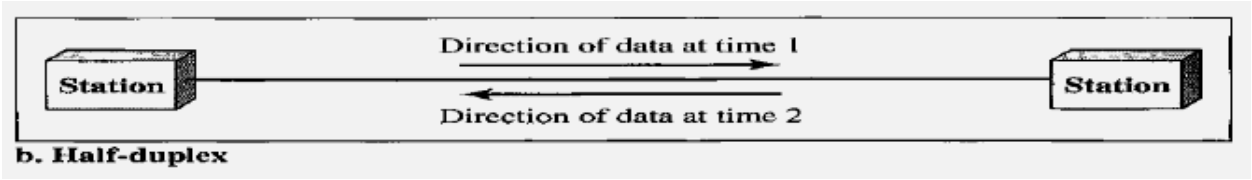
- In simplex mode, the communication is **unidirectional**, as on a one-way street.
- **Only one** of the two devices on a link can transmit; the other can only receive.
- **Keyboards** and traditional **monitors** are examples of simplex devices.
- The keyboard can only introduce input; the monitor can only accept output.
- The simplex mode can use the **entire capacity of the channel to send data in one direction**.



a. Simplex

Data Flow: Half-Duplex

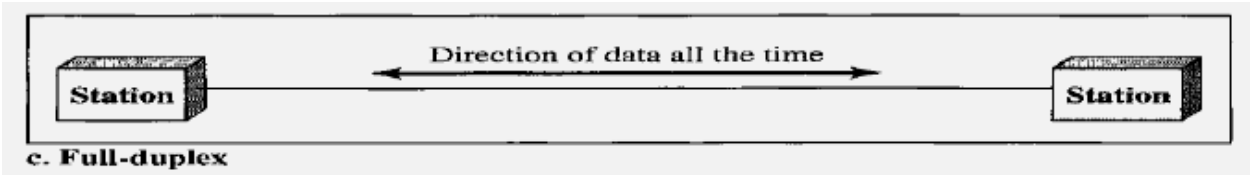
- In half-duplex mode, each station can **both transmit and receive**, but not at the same time.
- **When one device is sending, the other can only receive, and vice versa.**
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- **Walkie-talkies and CB** (citizens band) radios are both half-duplex systems.
- The half-duplex mode is used in cases where there is **no need for communication in both directions at the same** time; the entire capacity of the channel can be utilized for each direction.



b. Half-duplex

Data Flow: Full-Duplex

- In full-duplex made (also, called **duplex**), **both stations can transmit and receive** simultaneously.
- In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction.
- T**his sharing can occur in two ways**: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals travelling in both directions.
- One common example of full-duplex communication is the **telephone network.**



c. Full-duplex

1.2 Applications of Computer Network

- Major applications areas of computer networks are:

1. **Business Applications**
2. **Home Application**
3. **Mobile Computers, & etc.**

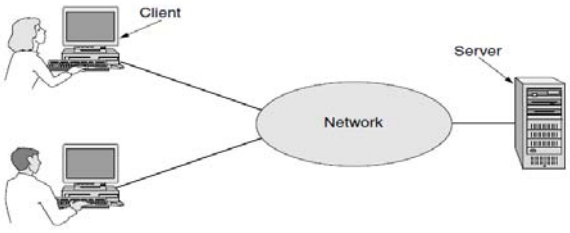


Figure 1-1. A network with two clients and one server.

1. Business Applications

- **R**esource Sharing
- VPNs (Virtual Private Networks)
- This whole arrangement is called the client-server model
- Web application,
- communication medium
- email (electronic mail),
- IP telephony
- Voice over IP (VoIP)
- Desktop sharing
- e-commerce (electronic commerce)

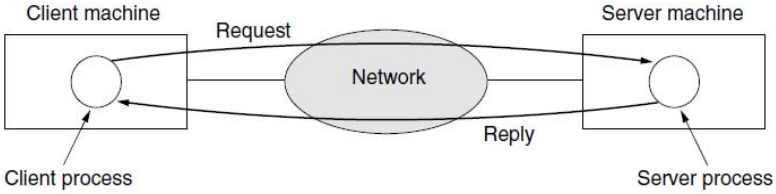


Figure 1-2. The client-server model involves requests and replies.

2. Home Applications

- Some of the most important uses of the Internet for home users are as follows:
- Access to remote information
- Person-to-person communication
- Interactive entertainment
- Electronic commerce

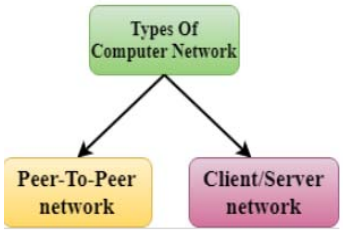
3. Mobile Users

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

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

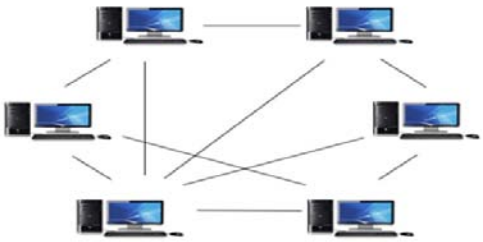
1.3 Network Architecture

- Computer Network Architecture is ***defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.***
- Simply we can say that how computers are organized and how tasks are allocated to the computer.
- *Architecture* also defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc.
- ***The two types of network architectures are used:***



Peer to Peer architecture

- In peer to peer architecture all the computers in a computer network are **connected with every computer** in the network.
- Every computer in the network uses the same resources as other computers.
- There is no central computer that acts as a server rather all computers acts as a server for the data that is stored in them.



Advantages of a Peer to Peer Architecture

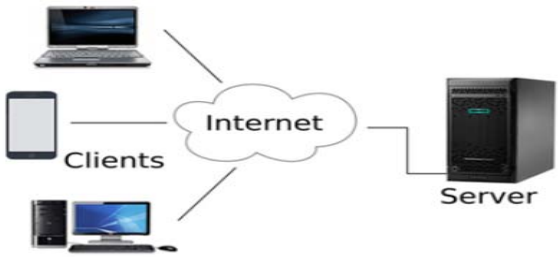
1. Less costly as there is no central server that has to take the backup.
2. In case of a computer failure all other computers in the network are not affected and they will continue to work as same as before the failure.
3. Installation of peer to peer architecture is quite easy as each computer manages itself.

Disadvantages of a Peer to Peer Architecture

1. Each computer has to take the backup rather than a central computer and the security measures are to be taken by all the computers separately.
2. Scalability is an issue in a peer to Peer Architecture as connecting each computer to every computer is a headache on a very large network.

Client/Server Network

- In Client Server architecture a central computer acts as a hub and serves all the requests from client computers.
- All the shared data is stored in the server computer which is shared with the client computer when a request is made by the client computer.
- All the communication takes place through the server computer, for example if a client computer wants to share the data with other client computer then it has to send the data to server first and then the server will send the data to other client.
- The central controller is known as a server while all other computers in the network are called clients.



Advantages of Client Server Architecture

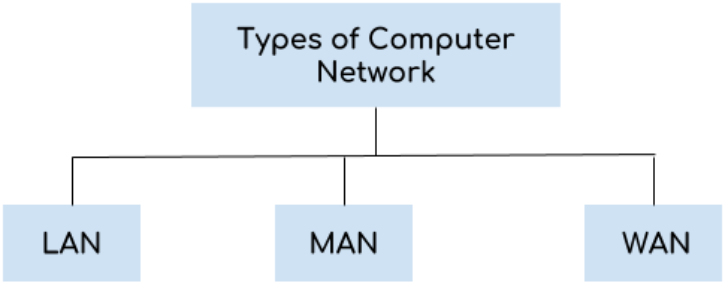
- Data backup is easy and cost effective as there is no need to manage the backup on each computer.
- Performance is better as the response time is greatly improves because the server is more powerful computer than the other computers in the network.
- Security is better as unauthorized access are denied by server computer and all the data goes through the server.
- Scalability is not an issue in this Architecture as large number of computers can be connected with server.

Disadvantages of Client Server Architecture

- In case of server failure entire network is down.
- Server maintenance cost is high as the server is the main component in this Architecture.
- Cost is high as the server needs more resources to handle that many client requests and to be able to hold large amount of data.

1.4 Types of Computer Networks (by their size / area/ geographical area)

- ***A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.***
- ***A computer network can be categorized by their size.***
- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- A computer network can be categorized by their size.
  1. Local Area Network (LAN)
  2. Metropolitan Area Network (MAN)
  3. Wide area network (WAN)

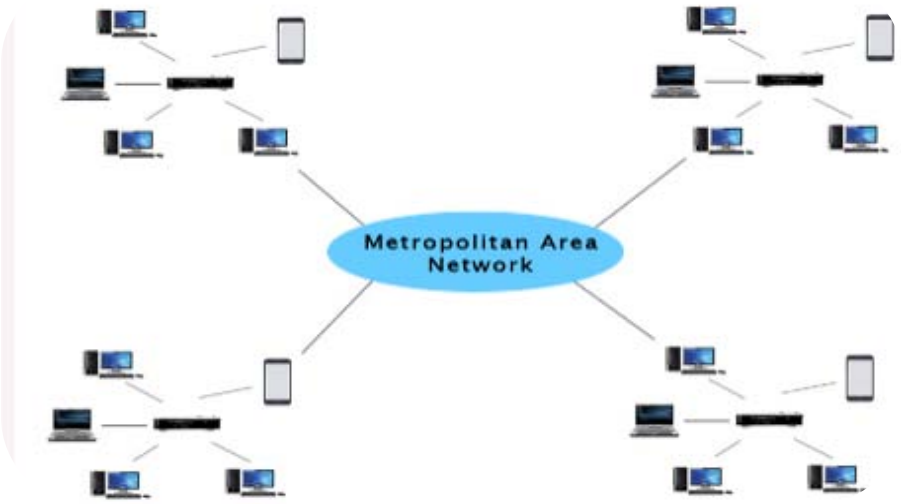


1. Local Area Network (LAN)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

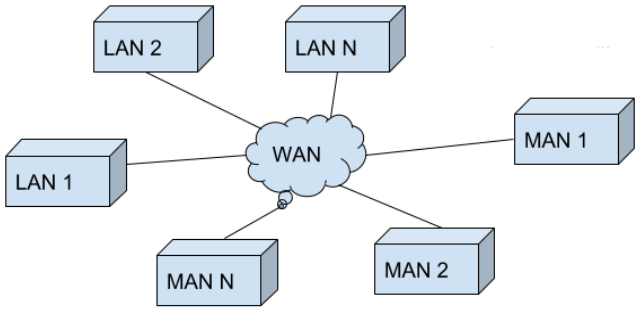
2. MAN (Metropolitan Area Network)

- MAN network covers larger area by connections LANs to a larger network of computers.
- In MAN various Local area networks are connected with each other through telephone lines.
- The size of the Metropolitan area network is larger than LANs and smaller than WANs (wide area networks), a MANs covers the larger area of a city or town.



3. Wide Area Network (WAN)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the MAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Advantages of Wide area network (WAN)

- **Geographical area:** A WAN provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype etc.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global Business:** We can do the business over the internet globally.
- **High bandwidth:** The high bandwidth increases the data transfer rate which in turn increases the productivity.

Disadvantages of Wide area network (WAN)

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

1.5 Protocols and Standards

1.5 PROTOCOLS AND STANDARDS

- A protocol is a **set of rules that governs(control)** data communications.
- A protocol defines **what** is communicated, **how** is communicated, and **when** it is communicated.
- The key elements of a protocol are :
    1. **Syntax,**
    2. **Semantics**
    3. **Timing.**

Elements of PROTOCOLS:

- **Syntax**
    - Structure or format of the data.
    - Indicates how to read the bits - field delineation (border or boundary).
    - Syntax should be same in sender and receiver for to communicate.

- **Semantics**
- Interprets the meaning of the bits
- Knows which fields define what action
- Interpretation of the syntax should be same
- **Timing**
- When data should be sent and what
- Speed at which data should be sent or speed at which it is being received

Standards

- Standards provide **guidelines** to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.
- Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing.
- ***Data communication standards fall into two categories:***
  1. **de facto (meaning "by fact" or "by convention")**
  2. **de jure (meaning "by law" or "by regulation").**

Two Categories of Standards

1. **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.
2. **De jure:** Those ***standards by law or by regulation.*** These are the standards recognized officially by an Organization.

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 fields of scientific, technological, and economic activity.
- **International Telecommunication Union-Telecommunication Standards Sector (ITU-T):** This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular.
- **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):** It 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, It is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and 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.

1.6 The OSI Reference Model

- ISO- International Organizations for Standard
- OSI- Opens System Interconnections
- Stats developing in late 1970s
- Approved by 1984
- The term "Open" in Open System Interconnections denotes "to communicate with any 2 systems"
- There are **7 layers in OSI Reference model**
- It is also **called OSI layered architecture /OSI Protocol architecture**
- ***The process of breaking up the functions or tasks of networking into layers reduces complexity.***
- Each layer **provides a service to the layer** above it in the **protocol** specification.
- Each layer communicates with the **same layer's software or hardware on other computers.**
- The **lower 4 layers are concerned with the flow of data from end to end** through the network
- The upper **Three layers of the OSI model are orientated more toward services** to the applications

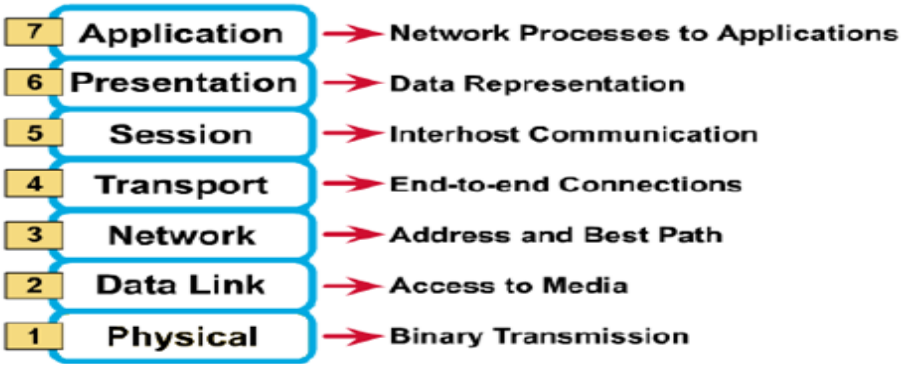


Figure: 7 *layers of the OSI model*

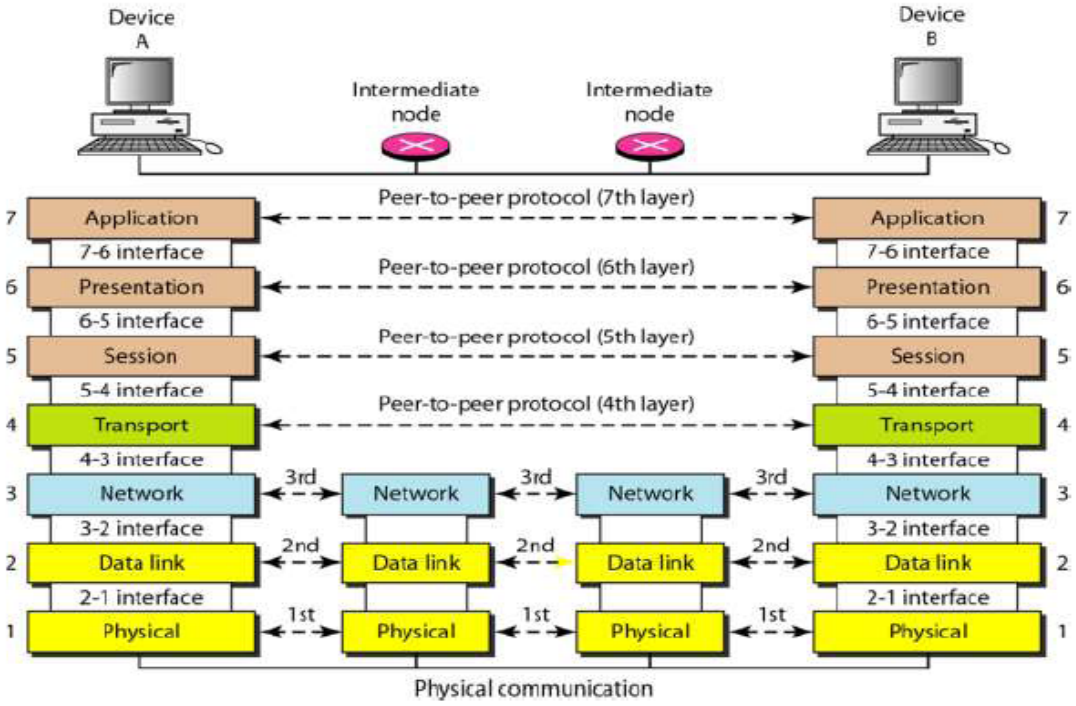


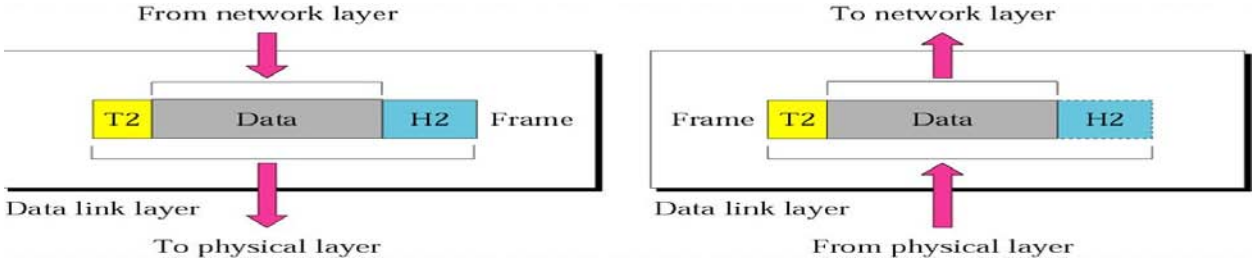
Figure: The interaction between layers in the OSI model

Physical Layer

- The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.
- It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
- The following figure shows the position of the physical layer with respect to the transmission medium and the data link layer.

Data Link Layer

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



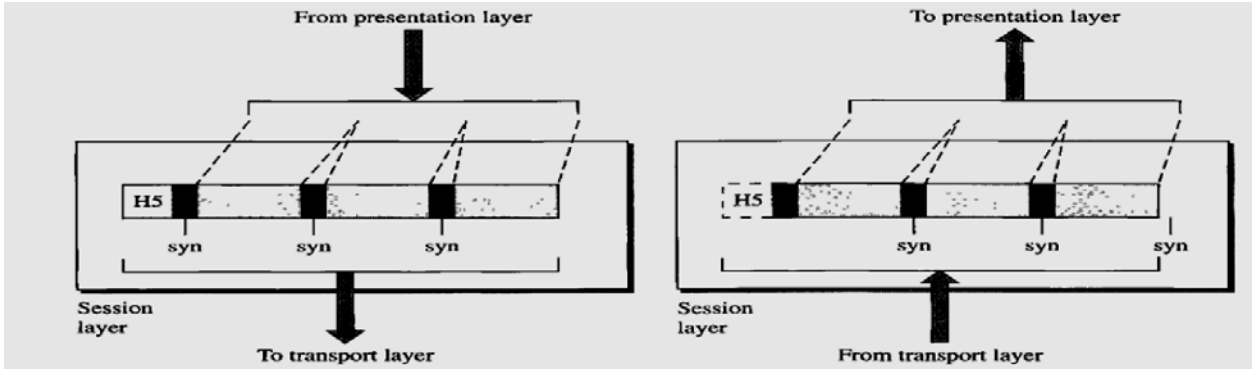
Network Layer

Other responsibilities of the network layer include the following:

- **Logical addressing.** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **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.

Session Layer

- The services provided by the first three layers (physical, data link, and network) *are not sufficient* for some processes.
- The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.



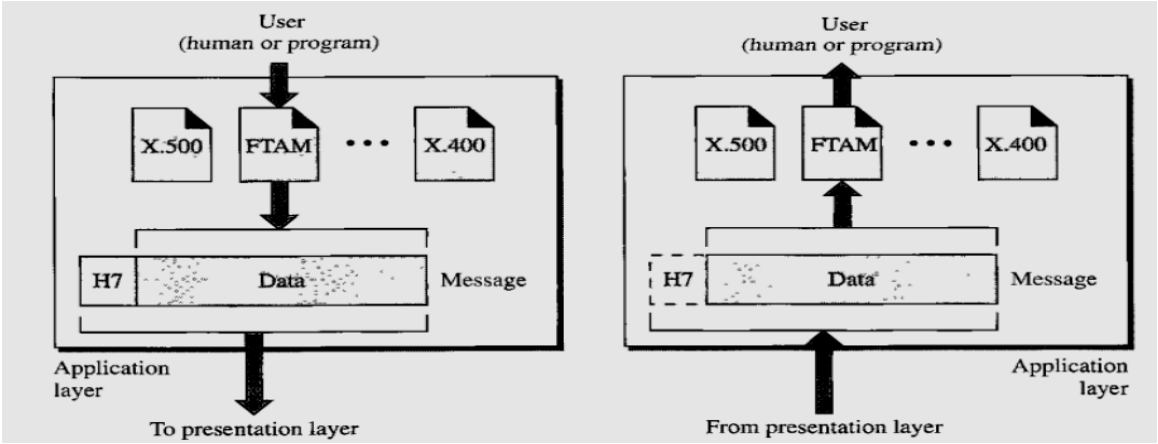
Presentation Layer

Specific responsibilities of the presentation layer include the following:

- **Translation**. The processes (running programs) in **two systems** are usually exchanging information in the ***form of character strings, numbers,*** and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- **Encryption**. To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression**. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer

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



Specific services provided by the application layer include the following:

- **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services.** This application provides the basis for e-mail forwarding and storage.
- **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

1.7 The TCP/IP Protocol Suite

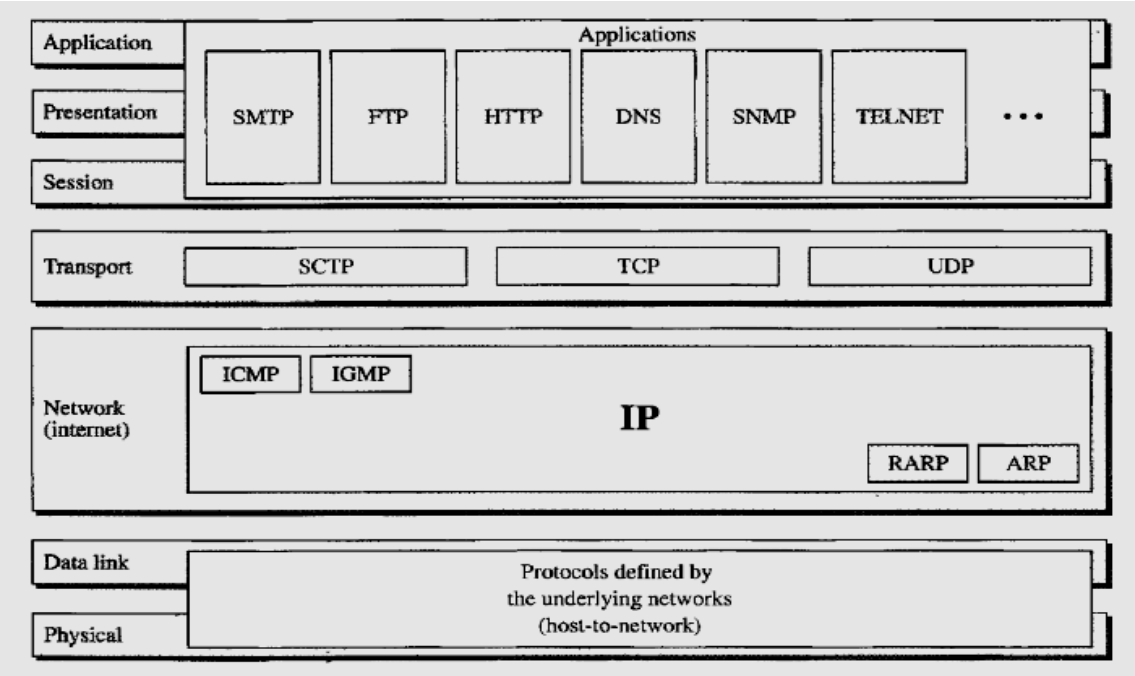
.

- The TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.
- The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.

PROTOCOL

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- virtual terminal (TELNET)
- file transfer(FTP), and electronic mail (SMTP)
- Domain Name System (DNS),
- HTTP (HyperText Transfer Protocol)
- Stream Control Transmission Protocol (SCTP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Internet Group Message Protocol (IGMP)
- ICMP (Internet Control Message Protocol)

Figure: TCP/IP PROTOCOL SUITE (*TCP/IP and OSI model)*



- TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.

- Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.
- The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.

- **At the transport layer, TCP/IP defines three protocols:** Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).
- At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

1. ***Physical and Data Link Layers:*** At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.
2. ***Network Layer:*** At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

- ***Internetworking Protocol (IP):*** The Internetworking Protocol (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 **datagrams**, each of which is transported separately. **Datagrams** 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 datagrams once they arrive at their destination.
- ***Address Resolution Protocol (ARP):*** *The 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):*** *Its 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:*** *The* ***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:*** *The* ***IGMP*** *is used to facilitate the simultaneous transmission of a message to a group of recipients.*

3. **Transport Layer:** Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP.

- IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another.
- 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:** The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. 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:** The TCP provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data. 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. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

- **Stream Control Transmission Protocol:** The 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.

4. **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.

1.8 Comparison between OSI and TCP/IP Reference model

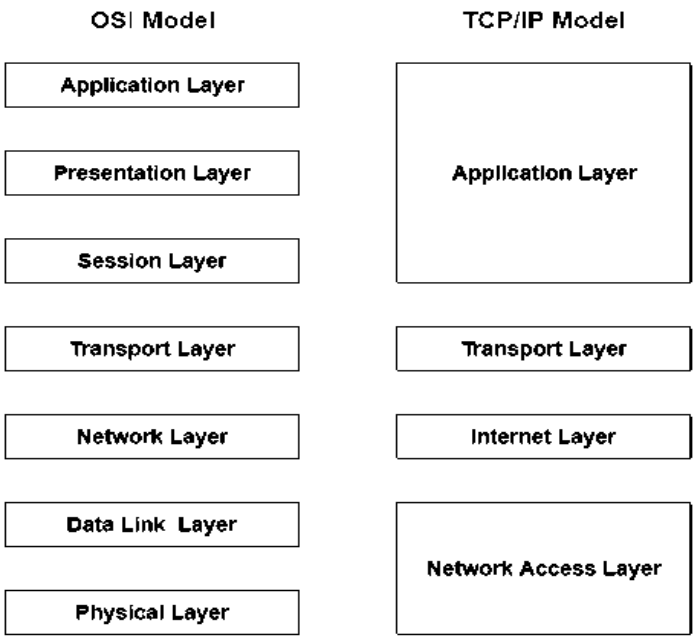
Following are ***some similarities between OSI Reference Model and TCP/IP Reference Model.***

- ***Both have layered architecture.***
- ***Layers provide similar functionalities.***
- ***Both are protocol stack.***
- ***Both are reference models.***

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a **generic**, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on **standard protocols around which the Internet has developed.** It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer **guarantees** the delivery of packets.	2. In TCP/IP model the transport layer does **not guarantees** delivery of packets. Still the TCP/IP model is more reliable.
3. Follows **vertical** approach.	3. Follows **horizontal** approach.

4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

Comparison of OSI and TCP/IP Reference Model



1.9 Critiques of OSI and TCP/IP Reference model

- A Critique of the OSI Model and Protocols
- A Critique of the TCP/IP Reference Model

A Critique of the OSI Model and Protocols

- Why OSI did not take over the world

- ✓ Bad timing
- ✓ Bad technology
- ✓ Bad implementations
- ✓ Bad politics
- ✓ Bad timing

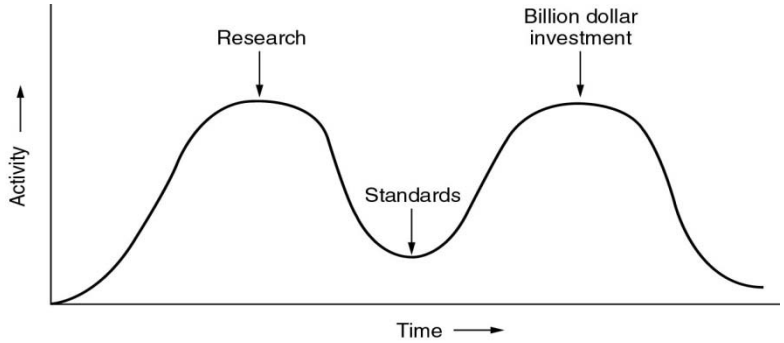


Fig. The apocalypse of the two elephants. (Standard came much later)

- Bad Implementation
- Initial version were huge, unwieldy and slow.
- Bad Politics
- TCP/IP part of Unix, OSI – government pushed

A Critique of the TCP/IP Reference Model

- **Problems:**

- Service, interface, and protocol not very successful
- Not a general model
- Host-to-network "layer" not really a layer
- No mention of physical and data link layers
- Minor protocols deeply establish, hard to replace

Hybrid Model

5	Application layer
4	Transport layer
3	Network layer
2	Data link layer
1	Physical layer

Fig: The hybrid reference model to be used.

POINT TO NOTE

INSPIRING LEARNING QUOTES

"NOTHING WILL WORK UNLESS YOU DO."

Don't be judgmental towards anyone, including yourself.

"YESTERDAY I WAS CLEVER, SO I CHANGED THE WORLD. TODAY I AM WISE, SO I AM CHANGING MYSELF."

"NEVER GIVE UP ON A DREAM JUST BECAUSE OF THE TIME IT WILL TAKE TO ACCOMPLISH IT. THE TIME WILL PASS ANYWAY."

"TELL ME AND I FORGET. TEACH ME AND I REMEMBER. INVOLVE ME AND I LEARN."

Ask yourself: how is this changing me?

Answer own Innovation, Creativity & Tinkering.

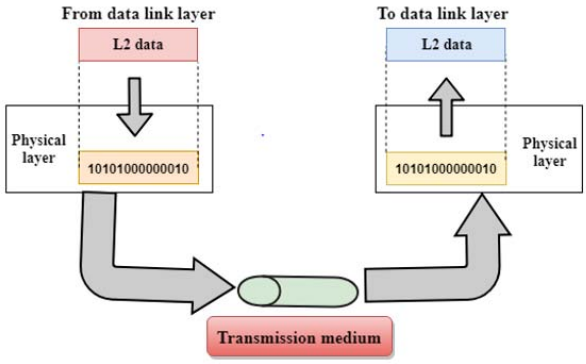
PHYSICAL LAYER

Read Me First (3 times) Assumes Basic Key Terms while writing your unit2 answer.

analog hierarchy	Barker sequence	channel	chip
demultiplexer (DEMUX)	dense WDM (DWDM)	digital signal (DS) service	direct sequence spread spectrum (DSSS)
E line	framing bit	frequency hopping spread spectrum (FHSS)	frequency-division multiplexing (FDM)
group	guard band	hopping period	interleaving
jumbo group	link	master group	multilevel multiplexing
multiple-slot allocation	multiplexer (MUX)	multiplexing	pseudorandom code generator
pseudorandom noise (PN)	pulse stuffing	spread spectrum (SS)	statistical TDM
supergroup	synchronous TDM	T line	time-division multiplexing (TDM)
wavelength-division multiplexing (WDM)			

2.1 Functions of Physical Layer

- Bit Representation
- Transmission Rate
- Physical Characteristics
- Synchronize
- Transmission mode
- Physical Topology



The **physical layer** consists of all the functions required to transmit a **bitstream** over a Physical medium. The electrical and mechanical specifications of the interface and transmission medium deals by this layer.

- However, it does not deal with the actual physical medium (like fiber, copper).
- **Physical Layer** devices are Hub, Repeater, Modem, Cables.

Main Function

Representation of bits: The **physical layer** data involves a stream of bits (sequence of 0's and 1's) without any interpretation. To be transmitted bits must be encoded into the signals - electrical or optical.

- The **physical layer** defines the type of encoding (how 0's and 1's are changed in signals).
- This layer is responsible for the bit by bit delivery of the data to its upper layer called the MAC layer. **Physical layer** obtains data in the form of signals or the radio signals or the optical signals.
- The physical layer is responsible for delivering those signals from a cable, a Wi-Fi router or an optical fiber.

Data Rate (Transmission Rate): The number of bits sends each second is also defined by the physical layer. In other words, the physical layer defines the duration of a bit also.
Synchronization of bits: It is necessary to have synchronization between sender and receiver at the bit level that is the clocks of the sender and the receiver must be synchronized.
Line c onfiguration: The physical layer is responsible for the connection of devices to the medium. Two devices are connected through a dedicated link in a point-to-point configuration.
Physical topology: The Physical topology determines how devices are connected to create a network. Devices can be using a mesh topology (every device can be connected to other devices), a star topology (all the devices are connected through a central device), a ring topology (devices are connected to the next forming a ring), or a bus topology (every device shared a common link).
Transmission mode: The mechanism of transferring data or information between two linked devices connected over a network is referred to as Transmission Modes. They are simplex, half-duplex, or full-duplex.

Design Issues with Physical Layer

- The **Physical Layer** is transmitted raw bits over a communication channel.
- Making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit and not as a 0 bit.
- The design issues here mostly deal with electrical, mechanical and timing interfaces.

2.2	Data and Signals: Analog and Digital signals, Transmission Impairment, Data Rate Limits, Performance		1

The term analog **data** refers to information that is continuous; digital data refers to information that has discrete states. To be transmitted, data must be transformed to electromagnetic **signals**.

Analog and Digital signals:

Analog Signals	Digital Signals
• Continuous signals	• Discrete signals
• Represented by sine waves	• Represented by square waves
• Human voice, natural sound, analog electronic devices are few examples	• Computers, optical drives, and other electronic devices
• Continuous range of values	• Discontinuous values
• Records sound waves as they are	• Converts into a binary waveform.
• Only be used in analog devices.	• Suited for digital electronics like computers, mobiles and more.

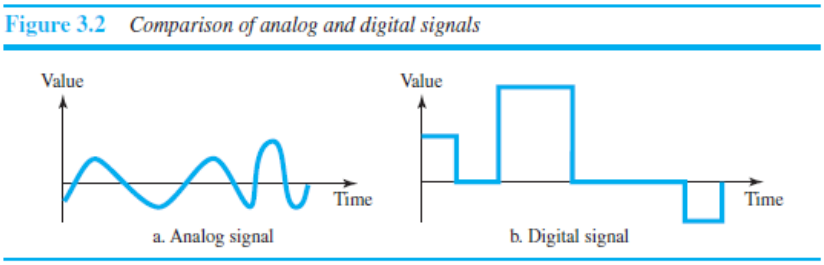


Figure 3.2 *Comparison of analog and digital signals*

Analog and digital signals can take one of two forms: periodic or non-periodic

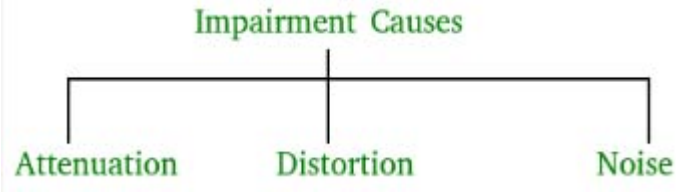
- ***Periodic Signal:*** A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.
- ***Non-periodic signal:*** A non-periodic signal changes without exhibiting a pattern or cycle that repeats over time.
- **Period** refers to the amount of time, in seconds, a signal needs to complete 1 cycle. **Frequency** refers to the number of periods in I s.

f= 1/T and t= 1/F

Transmission Impairment

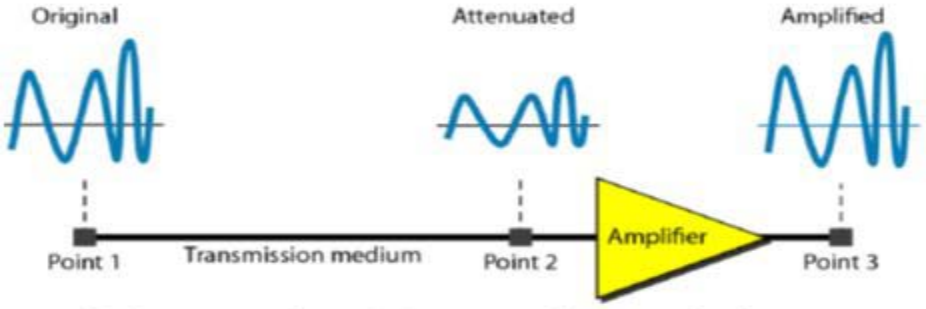
When a signal transmits from one transmission medium to other, the signal that is received may differ from the signal that is transmitted, due to various transmission impairments.

- *Consequences:*
  - For analog signals: degradation of signal quality
  - For digital signals: bit errors
- The most significant impairments include
  - ✓ **Attenuation**
  - ✓ **Distortion**
  - ✓ **Noise**



Attenuation

- **Attenuation** refers to lose of energy by a signal time.
- When a signal, simple or composite , travels through a medium ,it loses some of its energy in overcoming the resistance of the medium.
- It compensate for this lose, amplifier are used.



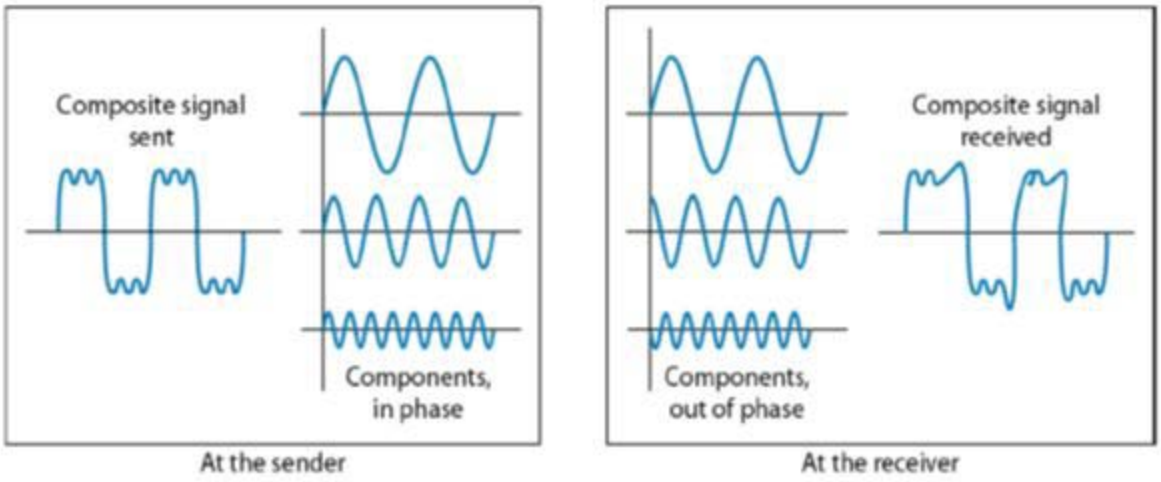
Decibel: Measure the relative power (attenuation)

$$dB = 10 \log_{10} P_2/P_1$$

- Attenuation is measured in **decibels(dB)**.
- It measures the relative strengths of two signals or one signal at two different point.
- **P1** is power at sending end and **P2** is power at receiving end.

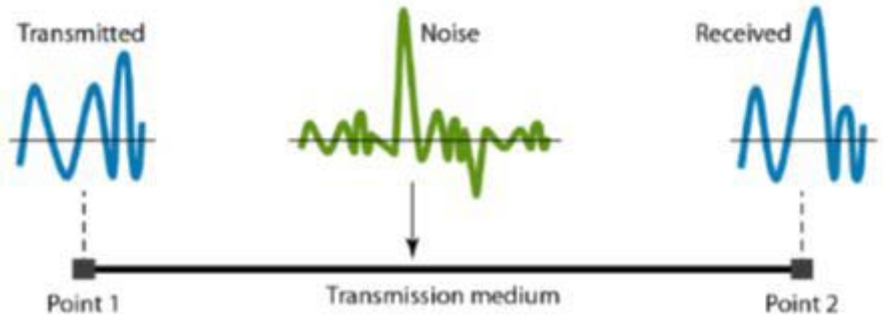
Distortion

- Distortion means signal changes its form or shape.
- Distortion can occur in a composite signal made of different frequency.
- Each signal component has its own propagation speed through a medium and therefore its own delay in arriving at the final signal.



Noise

- The random or unwanted signal that mixes up with the original signal is called noise.
- Several type of noise as thermal noise, induced noise , crosstalk noise, Impulse noise may corrupt the signal.



Induced *noise comes from sources such as motors and appliances. These devices act as sending antenna and transmission medium act as receiving antenna.*
Thermal *noise is movement of electrons in wire which creates an extra signal.*
Crosstalk *noise is when one wire affects the other wire.*
Impulse *noise is a signal with high energy that comes from lightning or power lines.*

SNR = AVG SIGNAL POWER / AVG NOISE POWER

Data rate Limits

- Data rate governs the speed of data transmission.
- A very important consideration in data communication is how fast we can send data, in bits per second, over a channel.

Data rate depends upon 3 factors:

1. The bandwidth available
2. Number of levels in digital signal
3. The quality of the channel – level of noise

Two theoretical formulas were developed to calculate the data rate:

1. **No**iseless Channel: **N**yquist Bit Rate
2. Noisy Channel: Shannon Capacity

1. Noiseless Channel: Nyquist Bit Rate

$$\textbf{BitRate} = 2 * \textbf{Bandwidth} * \log_2(L)$$

Where, **Bandwidth** is the bandwidth of the channel,
L is the number of signal levels used to represent data, and
BitRate is the bit rate in bits per second.

Bandwidth is a fixed quantity, so it cannot be changed. Hence, the data rate is directly proportional to the number of signal levels.

*Note –**Increasing the levels of a signal may reduce the reliability of the system.***

Problems: (page no. …. book)

Q1 : Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. What can be the maximum bit rate?

Output1 : BitRate = 2 * 3000 * $\log_2(2)$ = 6000bps

Q2 : We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?

Output2 : 265000 = 2 * 20000 * $\log_2(L)$
=> $\log_2(L)$ = 6.625
=> L = $2^{6.625}$ = 98.7 levels

2. Noisy Channel: Shannon Capacity

- In reality, we cannot have a noiseless channel; the channel is always noisy.
- Shannon capacity is used, to determine the theoretical highest data rate for a noisy channel:

$$\textbf{Capacity} = \textbf{Bandwidth} * \log_2(1 + \textbf{SNR})$$

Where, **Bandwidth** is the bandwidth of the channel,
SNR is the signal-to-noise ratio, and
Capacity is the capacity of the channel in bits per second.

Bandwidth is a fixed quantity, so it cannot be changed. Hence, the channel capacity is directly proportional to the power of the signal, as **SNR = (Power of signal) / (power of noise).**

The signal-to-noise ratio (S/N) is usually expressed in decibels (dB) given by the formula:

$$10 * \log10(S/N)$$

so for example a signal-to-noise ratio of 1000 is commonly expressed as:

⇨ **10 * log10(1000) = 30 dB.**

Note: The Shannon capacity gives us the upper limit; the Nyquist formula tells us how many signal levels we need.

Problems: (page no. …..book)

Q1 : A telephone line normally has a bandwidth of 3000 Hz (300 to 3300 Hz) assigned for data communication. The SNR is usually 3162. What will be the capacity for this channel?

Output1 : => C = 3000 * log2(1 + SNR) = 3000 * 11.62 = 34860 bps

Q2 : The SNR is often given in decibels. Assume that SNR(dB) is 36 and the channel bandwidth is 2 MHz. Calculate the theoretical channel capacity.

Output2 : => SNR(dB) = 10 * log10(SNR)

- ⇨ SNR = 10(SNR(dB)/10)
- ⇨ SNR = 103.6 = 3981
- ⇨ Hence, C = 2 * 106 * $\log_2$(3982) = 24 MHz

Q3. Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. For this channel the capacity C is calculated as

$$C = B \log_2 (1 + SNR)$$

- ⇨ B 1og $_2$ (l + 0)
- ⇨ B $\log_2$
- ⇨ 1 => B x 0
- ⇨ 0

This means that the capacity of this channel is zero regardless of the bandwidth. In other words, we cannot receive any data through this channel.

PERFORMANCE:

1. Bandwidth
2. Throughput
3. Latency (Delay)
4. Bandwidth Delay Product
5. Jitter

Bandwidth

- One characteristic that measures network-performance is bandwidth.
- Bandwidth of analog and digital signals is calculated in separate ways:

(2) Bandwidth of an Analog Signal (in hz)

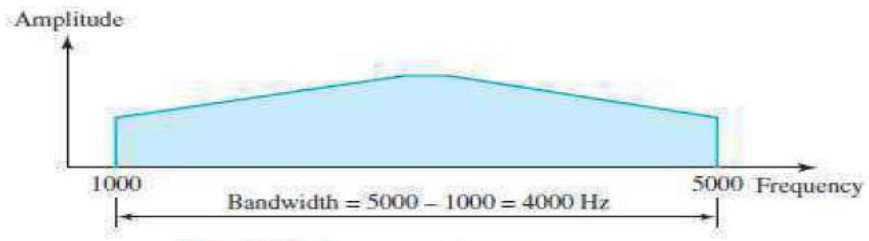


Figure 3.13 *The bandwidth of signals*

In figure 3.13, the signal has a minimum frequency of F1 = 1000Hz and maximum frequency of F2 = 5000Hz. Hence, the bandwidth is given by F2 - F1= 5000 - 1000 = 4000 Hz

(3) Bandwidth of a Digital Signal (in bps)

For example: The bandwidth of a Fast Ethernet is a maximum of 100 Mbps. (This means that this network can send 100 Mbps).

Throughput

• The throughput is a measure of **how fast we can actually send data through a network.**

In other words,

1) The bandwidth is a potential measurement of a link.

2) The throughput is an actual measurement of how fast we can send data.

Example 1.18

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution

We can calculate the throughput as

$$\text{Throughput} = (12{,}000 \times 10{,}000) / 60 = 2 \text{ Mbps}$$

Latency (Delay)

The latency defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

$$\text{Latency} = \text{propagation time} + \text{transmission time} + \text{queuing time} + \text{processing delay}$$

Propagation time is defined as the time required for a bit to travel from source to destination.

$$\text{Propagation time} = \text{Distance} / (\text{Propagation Speed})$$

Example 1.19

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4×10^8 m/s in cable.

Solution

We can calculate the propagation time as

$$\text{Propagation time} = (12{,}000 \times 10{,}000) / (2.4 \times 2^8) = 50 \text{ ms}$$

$$\text{Transmission time} = (\text{Message size}) / \text{Bandwidth}$$

Queuing-time is the time needed for each intermediate-device to hold the message before it can be processed.

(Intermediate device may be a router or a switch)

- ☐the queuing-time is not a fixed factor. This is because
  - i) Queuing-time changes with the load imposed on the network.
  - ii) When there is heavy traffic on the network, the queuing-time increases.
- ☐An intermediate-device
  - → queues they arrived messages and
  - → processes the messages one by one.
- ☐If there are many messages, each message will have to wait.

Processing Delay ☐ Processing delay is the time taken by the routers to process the packet header.

Bandwidth Delay Product

Two performance-metrics of a link are 1) Bandwidth and 2) Delay

- The bandwidth-delay product is very important in data-communications.
- Let us elaborate on this issue, using 2 hypothetical cases as examples.

Case 1: *The following figure shows case 1 (Figure 3.32).*

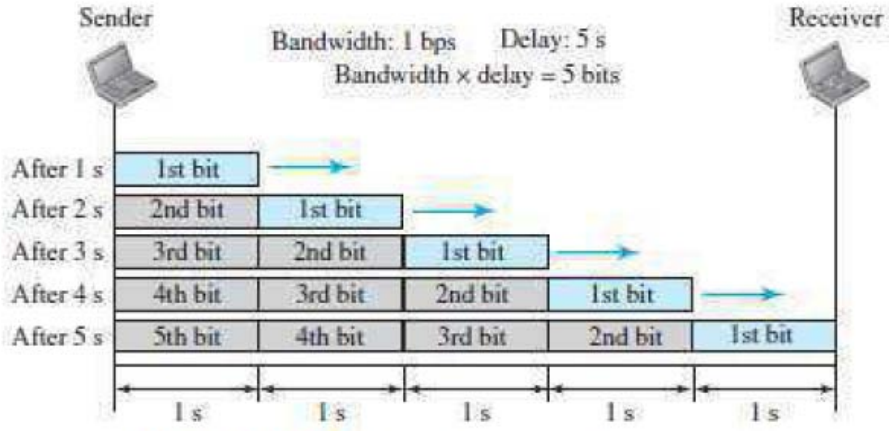


Figure 3.32 *Filling the link with bits for case 1*

☐Let us assume,
Bandwidth of the link = 1 bps Delay of the link = 5s.
☐From the figure 3.32, bandwidth-delay product is 1 x 5 = 5. Thus, there can be maximum 5 bits on the line.
☐ There can be no more than 5 bits at any time on the link.

Case2: *The following figure shows case 2 (Figure 3.33).*

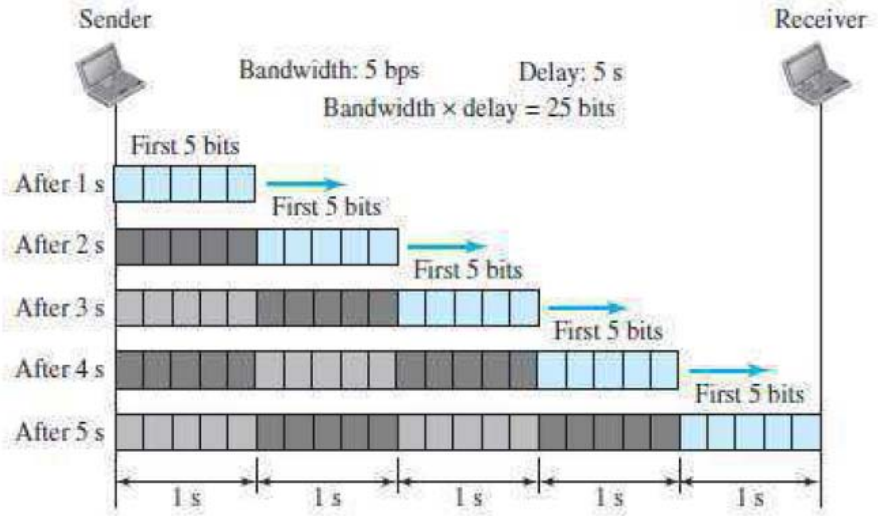


Figure 3.33 *Filling the link with bits in case 2*

From the figure 3.33, bandwidth-delay product is 5 x 5 = 25. Thus, there can be maximum 25 bits on the line.

To use the maximum capability of the link

→ We need to make the burst-size as (2 x bandwidth x delay).

→ We need to fill up the full-duplex channel (two directions).

• Amount (2x bandwidth x delay) is the number of bits that can be in transition at any time (Fig 3.34).

Figure 3.34 *Concept of bandwidth-delay product*

Jitter

• Another performance issue that is related to delay is jitter.

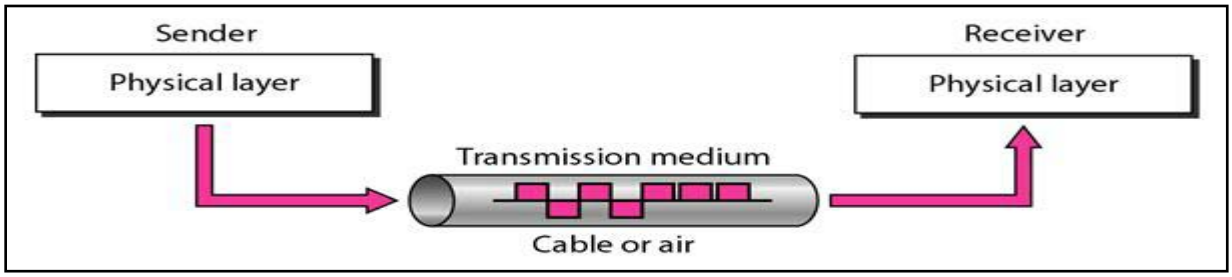
• We can say that jitter is a problem

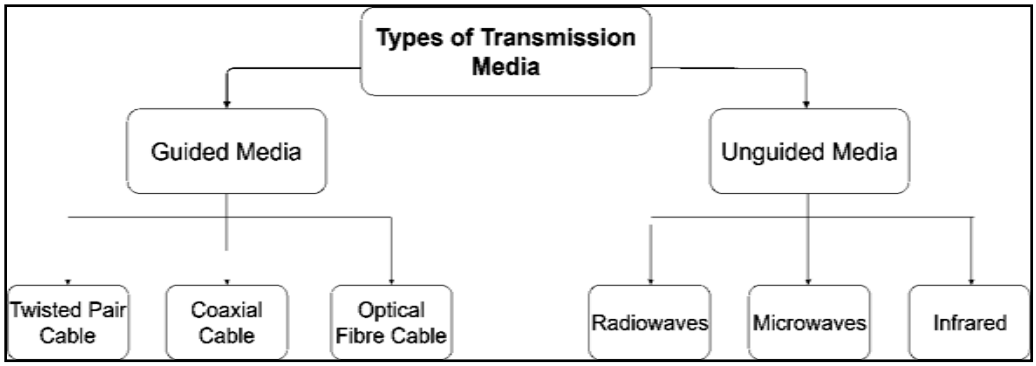
→ if different packets of data encounter different delays and

→ if the application using the data at the receiver site is time-sensitive (for ex: audio/video).

2.3	Data Transmission Media: Guided Media, Unguided Media and Satellites		1

Transmission media are actually located below the physical layer and are directly controlled by the physical layer. The following figure shows the position of transmission media in relation to the physical layer.





A transmission medium can be broadly defined as anything that can carry information from a source to a destination.

In telecommunications, transmission media can be divided into **two broad categories: guided and unguided.**

1. ***Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable.***
2. ***Unguided medium is free space***

1. Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

1. **Unshielded Twisted Pair (UTP):**
   This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

- Least expensive
- Easy to install
- High speed capacity

Disadvantages:

- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

2. **Shielded Twisted Pair (STP):**
   This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.
   Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparitively faster

Disadvantages:

- Comparitively difficult to install and manufacture
- More expensive
- Bulky

(ii) Coaxial Cable –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

(iii) Optical Fibre Cable –

It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.

Advantages:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile
- unidirectional, ie, will need another fiber, if we need bidirectional communication

2. Unguided Media:

It is also referred to as Wireless or Unbounded transmission media.No physical medium is required for the transmission of electromagnetic signals.

Features:

- Signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Unguided Media:

(i) Radiowaves –

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.

Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

(iii) Infrared –

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Satellites:

A satellite is an object that revolves around another object. For example, earth is a satellite of The Sun, and moon is a satellite of earth.

A **communication satellite** is a **microwave repeater station** in a space that is used for telecommunication, radio and television signals.

How a Satellite Works

Uplink frequency is the frequency at which ground station is communicating with satellite. The satellite transponder converts the signal and sends it down to the second earth station, and this is called **Downlink frequency**.

Satellite Communication Basics

The satellites **receive** and **retransmit** the signals back to earth where they are received by other earth stations in the coverage area of the satellite. **Satellite's footprint** is the area which receives a signal of useful strength from the satellite.

Satellite Frequency Bands

The satellite frequency bands which are commonly used for communication are the **Cband, Ku-band,** and **Ka-band**.

Earth Orbits

A satellite when launched into space, needs to be placed in certain orbit to provide a particular way for its revolution, so as to maintain accessibility and serve its purpose whether scientific, military or commercial. Such orbits which are assigned to satellites, with respect to earth are called as **Earth Orbits**.

The important kinds of Earth Orbits are −

- Geo-synchronous Earth Orbit
- Geo-stationary Earth Orbit
- Medium Earth Orbit
- Low Earth Orbit

In descriptions of satellite services, three abbreviations relate to the applications that are supported:

I. **FSS**—Fixed satellite services, the conventional fixed services, are offered in both the C-band and the Ku-band allocations.
II. **BSS**—Broadcast satellite services include standard television and direct broadcast. These largely operate in the Ku-band, at 18GHz. Because the general application of television so far has been one way, 18GHz shows just the downlink frequency allocation. As we begin to move toward interactive TV, we'll start to see the use of two different bands in BSS.
III. **MSS**—Mobile satellite services accommodate mobility (i.e., mobile users). They make use of either Ka-band or L-band satellites.

Satellite Network Segments

Satellite networks have three major segments:

i. **Space segment**—The space segment is the actual design of the satellite and the orbit in which it operates. Most satellites have one of two designs: a barrel-shaped satellite, normally used to accommodate standard communications, or a satellite with a very wide wingspan, generally used for television. Satellites are launched into specific orbits to cover the parts of the earth for which coverage is desired.
ii. **Control segment**—The control segment defines the frequency spectrum over which satellites operate and the types of signaling techniques used between the ground station and the satellite to control those communications.

iii. **Ground segment**—The ground segment is the earth station—the antenna designs and the access techniques used to enable multiple conversations to share the links up to the satellite. The ground segment of satellites continues to change as new technologies are introduced.

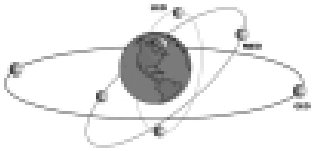


Fig: Satellite orbits

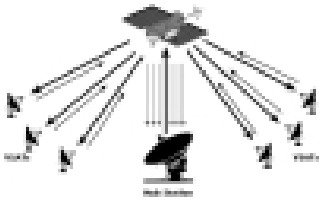


Fig: A VSAT system (private networking)

GEO Satellites

Advantages and Disadvantages of Satellite

The **advantages** of satellite include the following:

- Access to remote areas
- Coverage of large geographical areas
- Insensitivity to topology
- Distance-insensitive costs
- High bandwidth

The **disadvantages** of satellite include the following:

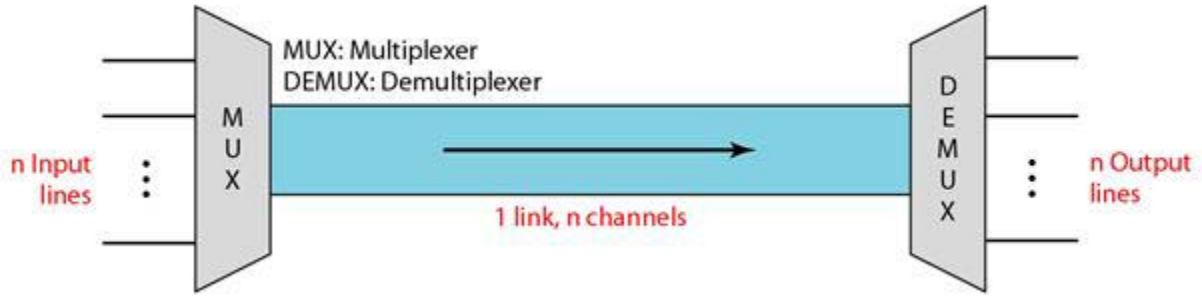
- High initial cost
- Propagation delay with GEO systems
- Environmental interference problems
- Licensing requirements
- Regulatory constraints in some regions
- Danger posed by space debris, solar flare activity, and meteor showers

2.4	Bandwidth Utilization: Multiplexing and Spreading		1

Multiplexing

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. In a multiplexed system, n lines share the bandwidth of one link.

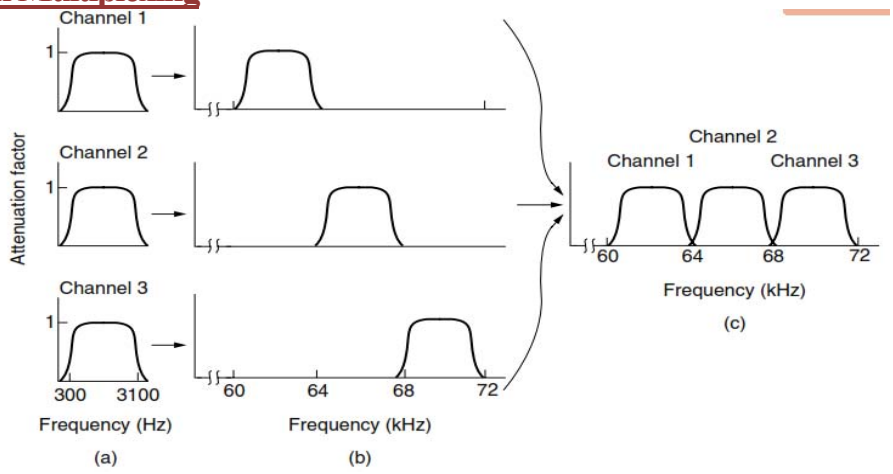
The following figure shows the basic format of a multiplexed system. The lines on the left direct their transmission streams to a multiplexer (MUX), which combines them into a single stream (many-toone). At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines.



The three basic multiplexing techniques are

1. ***Frequency-division multiplexing***
2. ***Time-division multiplexing.***
3. ***Wavelength-division multiplexing***

Frequency Division Multiplexing



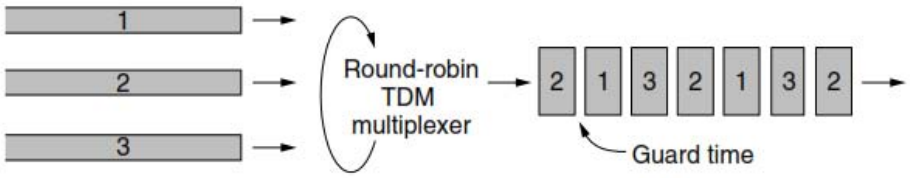
Frequency Division Multiplexing (FDM) is a networking technique in which multiple data signals are combined for simultaneous transmission via a shared communication medium. FDM uses a carrier signal at a discrete frequency for each data stream and then combines many modulated signals.

Detailed example is shown in above figure. There are three voice-grade telephone channels multiplexed using FDM. When many channels are multiplexed together, 4000Hz(4KHz) is allocated per channel. The excess is called a **guard band**. It keeps the channels well separated. First the voice channels are raised in frequency, each by a different amount. Then they can be combined because no two channels now occupy the same portion of the spectrum. Notice that even though there are gaps between the channels thanks to the guard bands which well separates two frequency even if there is some overlapping.

Time-Division Multiplexing.:

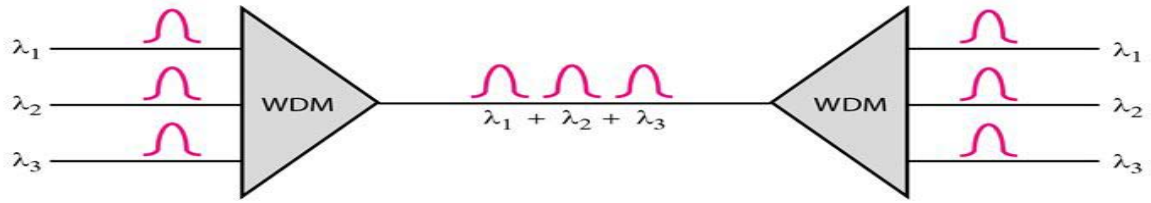
TDM was initially developed in 1870 for large system telegraphy implementation. Packet switching networks use TDM for telecommunication links, i.e., packets are divided into fixed lengths and assigned fixed time slots for transmission. Each divided signal and packet, which must be transmitted within assigned time slots, are reassembled into a complete signal at the destination.

TDM is comprised of two major categories: TDM and synchronous time division multiplexing (sync TDM). TDM is used for long-distance communication links and bears heavy data traffic loads from end users. Sync TDM is used for high-speed transmission.



Wavelength-Division Multiplexing

- Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber-optic cable.
- The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.
- WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels.
- The following figure gives a conceptual view of a WDM multiplexer and demultiplexer. Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer.

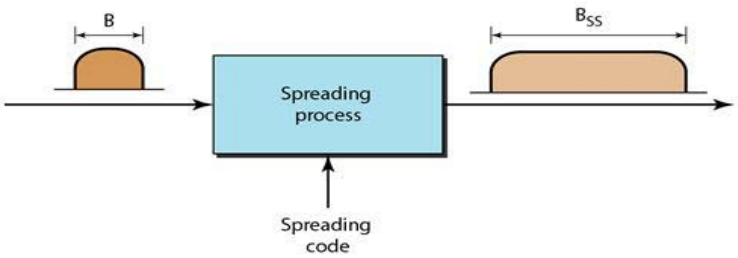


- In this method, we combine multiple light sources into one single light at the multiplexer and do the reverse at the demultiplexer.
- The combining and splitting of light sources are easily handled by a prism.
- Recall from basic physics that a prism bends a beam of light based on the angle of incidence and the frequency.
- Using this technique, a multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies.
- A demultiplexer can also be made to reverse the process.

Spread Spectrum Techniques

- Spread-Spectrum techniques are methods by which a signal (e.g. an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.

- These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density (e.g. in satellite downlinks).
- Spread spectrum is designed to be used in wireless applications (LANs and WANs). In wireless applications, all stations use air (or a vacuum) as the medium for communication. Stations must be able to share this medium without interception by an eavesdropper and without being subject to jamming from a malicious intruder.
- To achieve these goals, spread spectrum techniques add redundancy, they spread the original spectrum needed for each station. If the required bandwidth for each station is B, spread spectrum expands it to Bss such that Bss >> B. The expanded bandwidth allows the source to wrap its message in a protective envelope for a more secure transmission.



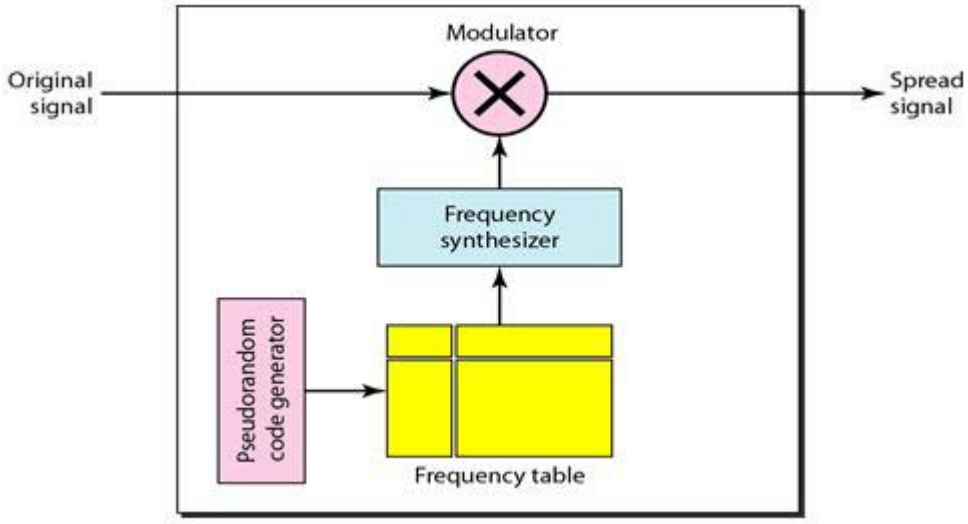
- **The f ollowing figure s hows t he i dea of s pread s pectrum. Spread s pectrum a chieves i ts g oals through two principles:**

  1. The bandwidth allocated to each station needs to be, by far, larger than what is needed. This allows redundancy.
  2. The expanding of the original bandwidth B to the bandwidth Bss must be done by a process that is independent of the original signal. In other words, the spreading process occurs after the signal is created by the source.

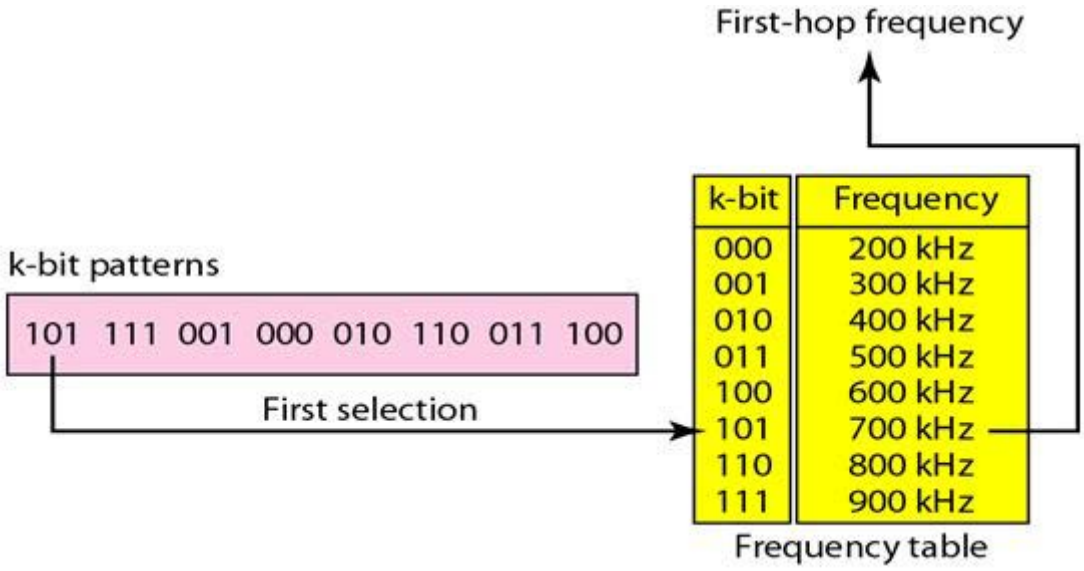
There are two techniques to spread the bandwidth:

Frequency Hopping Spread Spectrum (FHSS)

- The Frequency Hopping Spread Spectrum (FHSS) technique uses M different carrier frequencies that are modulated by the source signal.
- The bandwidth occupied by a source after spreading is BpHSS >> B.
- The following figure shows the general layout for FHSS. A pseudorandom code generator, called pseudorandom noise (PN), creates a k-bit pattern for every hopping period



For Example M is 8 and k is 3. The pseudorandom code generator will create eight different 3-bit patterns. These are mapped to eight different frequencies in the frequency table as shown in the following figure.



The pattern for this station is 101, 111, 001, 000, 010, all, 100. Note that the pattern is pseudorandom it is repeated after eight hoppings. This means that at hopping period 1, the pattern is 101. The frequency selected is 700 kHz, the source signal modulates this carrier frequency.

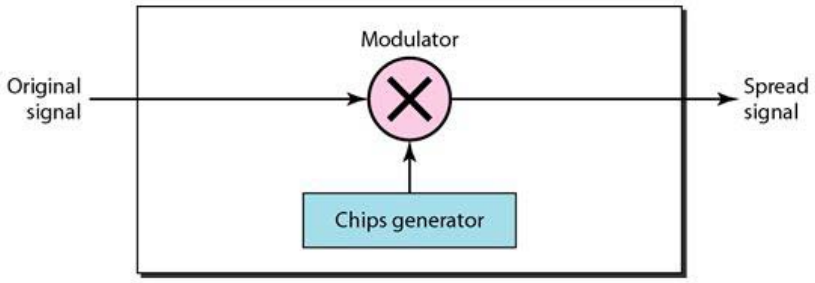
The second k-bit pattern selected is 111, which selects the 900-kHz carrier; the eighth pattern is 100, the frequency is 600 kHz. After eight hoppings, the pattern repeats, starting from 101 again.

Bandwidth Sharing

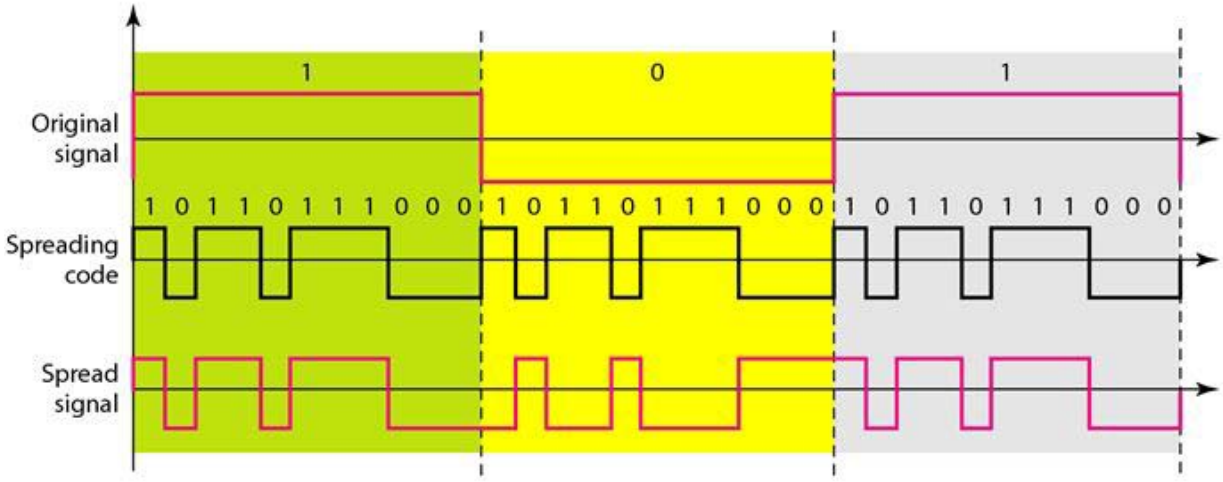
If the number of hopping frequencies is M, we can multiplex M channels into one by using the same Bss bandwidth.

Direct Sequence Spread Spectrum (DSSS).

The direct sequence spread spectrum (DSSS) technique also expands the bandwidth of the original signal, but the process is different. In DSSS, we replace each data bit with n bits using a spreading code. In other words, each bit is assigned a code of n bits, called chips, where the chip rate is n times that of the data bit.



In the figure, the spreading code is 11 chips having the pattern 10110111000 (in this case). If the original signal rate is N, the rate of the spread signal is 11N. This means that the required bandwidth for the spread signal is 11 times larger than the bandwidth of the original signal.



2.5	Switching: Circuit switching, Message switching & Packet switching		1

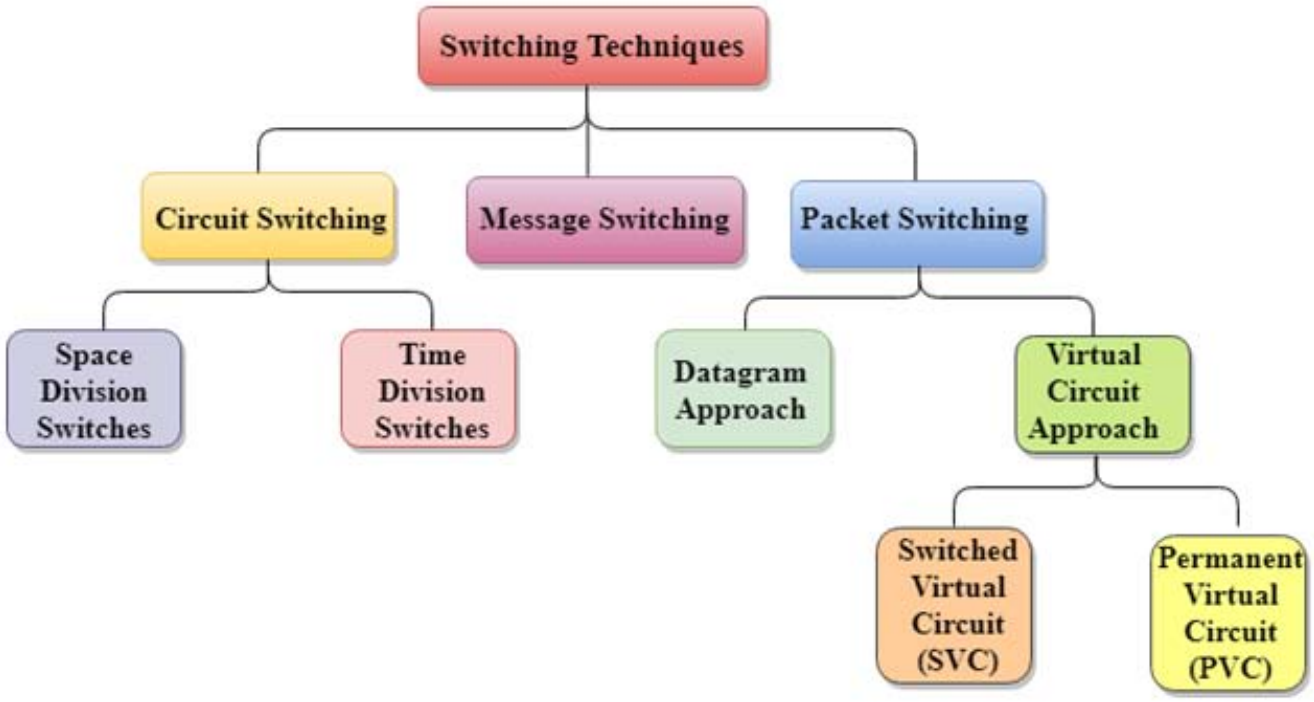
- **Switching** is process to forward packets coming in from one port to a port leading towards the destination.
- When data comes on a port it is called **ingress**, and when data leaves a port or goes out it is called **egress**.
- A communication system may include number of switches and nodes.

At broad level, switching can be divided into two major categories:

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

- In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques



Circuit Switching

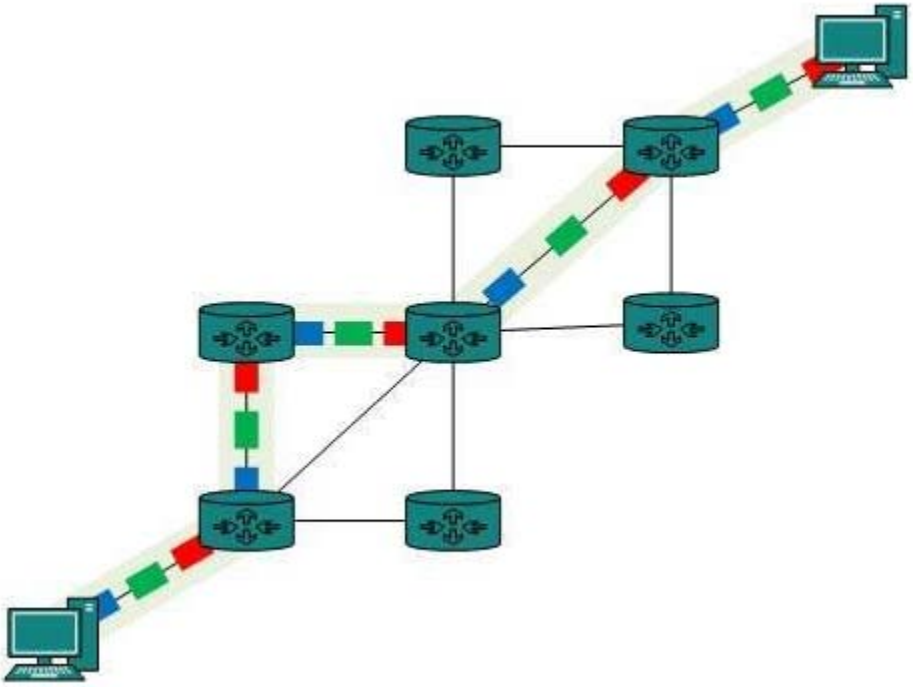
- When two nodes communicate with each other over a **dedicated communication path**, it is called circuit switching.
- There 'is a need of **pre-specified route** from which data will travels and no other data is permitted.
- In circuit switching, to transfer the data, circuit must be **established** so that the data transfer can take place.
- Circuits can be **permanent or temporary.**

- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.

- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public **telephone network. It is used for voice transmission.**
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and caller is established over the network.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.

- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

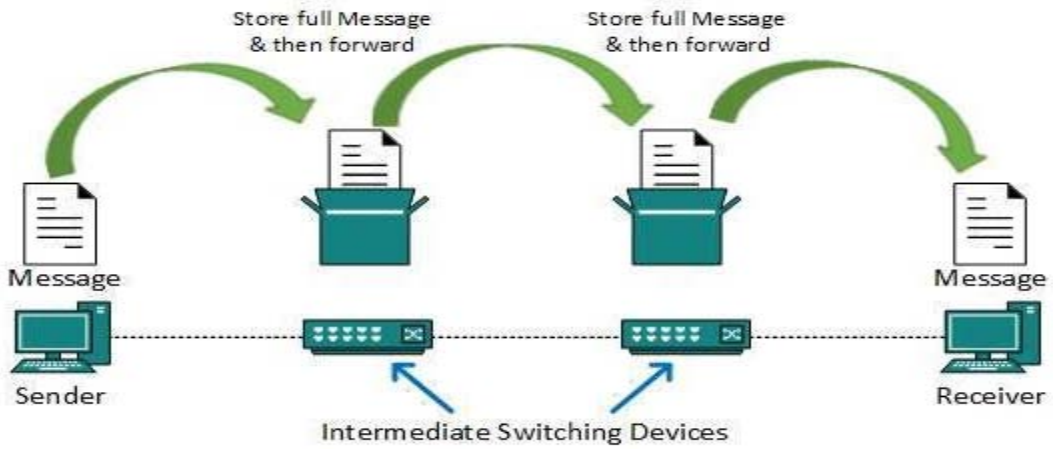
- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.

They provide 2 distinct and important characteristics:

Store and forward – The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity.

Message delivery – This implies wrapping the entire information in a single message and transferring it from the source to the destination node.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.



This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

Advantages Of Message Switching

- ☐ As message switching is able to store the message for which communication channel is not available, it helps in reducing the traffic congestion in network.
- ☐ In message switching, the data channels are shared by the network devices.
- ☐ It makes the traffic management efficient by assigning priorities to the messages.

Disadvantages Of Message Switching

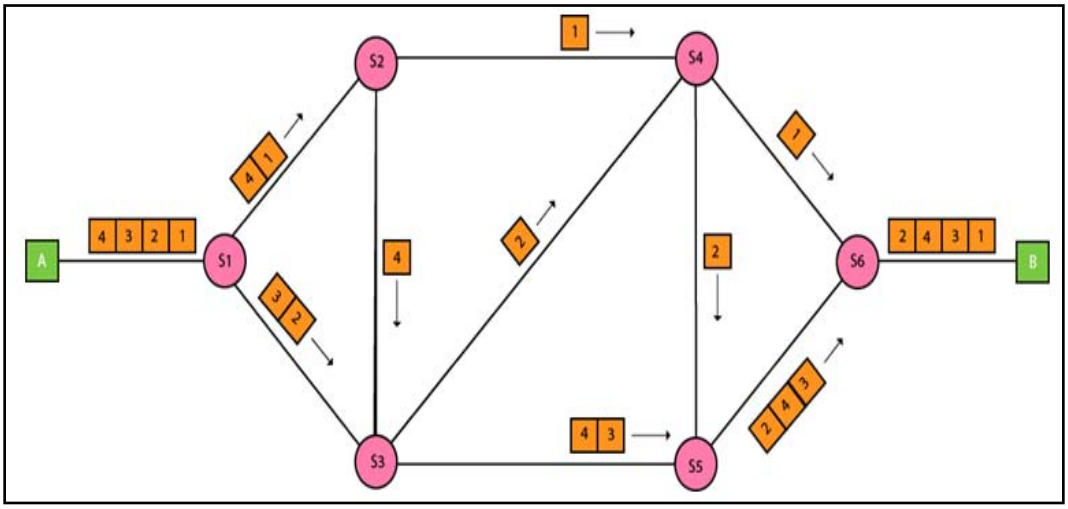
1. Message switching cannot be used for real time applications as storing of messages causes delay.
2. In message switching, message has to be stored for which every intermediate devices in the network requires a large storing capacity.

Applications –

The store-and-forward method was implemented in **telegraph** message switching centers.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

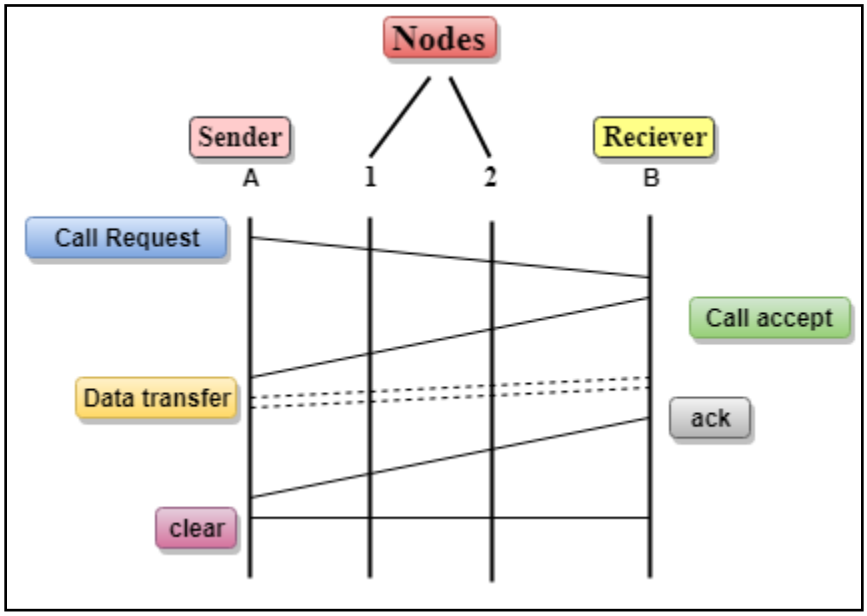
Datagram Packet switching:

- It is a packet switching technology in which packet is known as a **datagram**, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- It is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.

Let's understand the concept of virtual circuit switching through a diagram:



Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

- Cost-effective
- Reliable
- Efficient

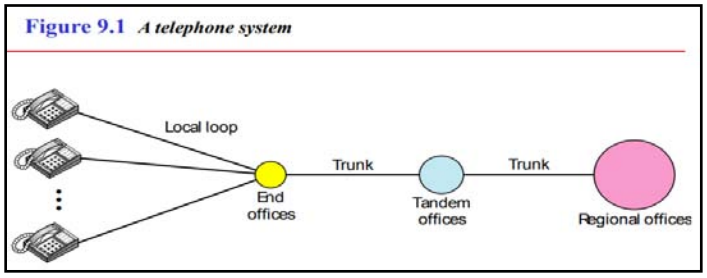
Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can not also lead to the loss of critical information if errors are nor recovered.

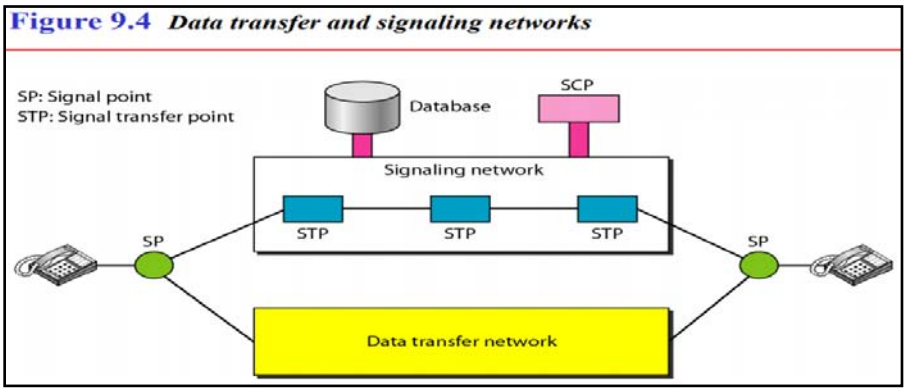
2.6	Telephone, Mobile and Cable network for data Communication		1

TELEPHONE NETWORK

Telephone networks use circuit switching. The telephone network had its beginnings in the late 1800s. The entire network, network, which is referred to as the **plain old telephone system** (POTS), was originally an analog system using analog signals to transmit voice.



The tasks of data transfer and signaling are separated in modern telephone network: data transfer is done by one network, signaling by another.



Modem stands for modulator/demodulator.

Figure 9.7 ***Modulation/demodulation***

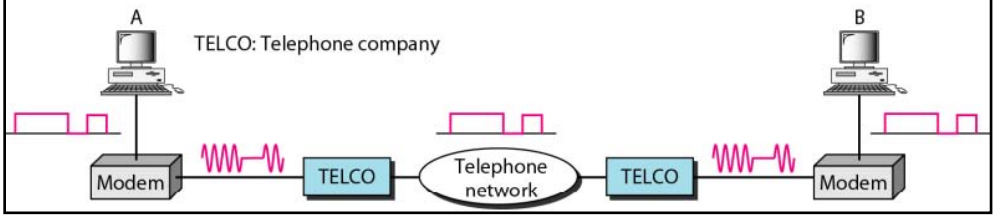
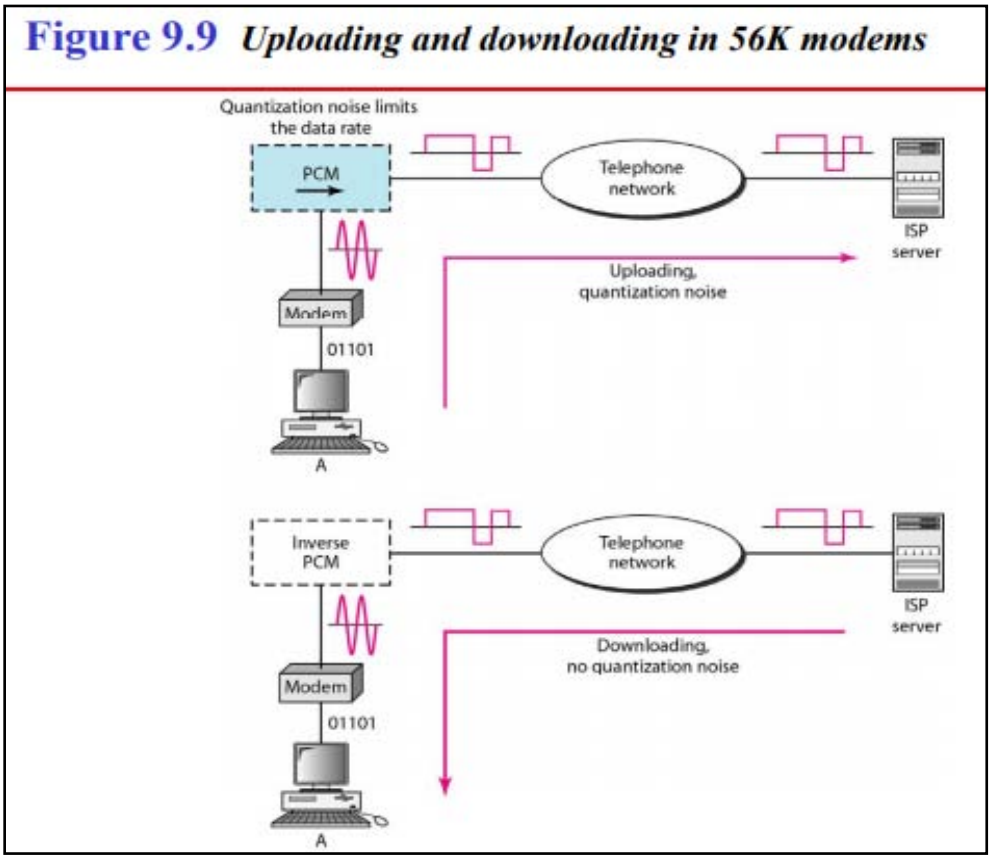


Figure 9.9 ***Uploading and downloading in 56K modems***



After traditional modems reached their peak data rate, telephone companies developed another technology, technology, DSL, to provide higher-speed access to the Internet. **Digital subscriber line** (DSL) technology is one of the most promising for supporting high-speed digital communication over the existing local loops.

Least Technology in this section:

- ADSL
- ADSL Lite
- VDSL, etc

ADSL is an asymmetric communication technology designed for residential users; it is not suitable for businesses

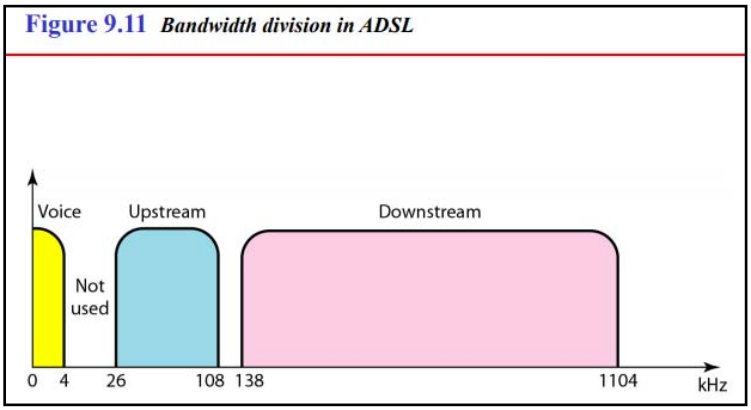


Figure 9.11 *Bandwidth division in ADSL*

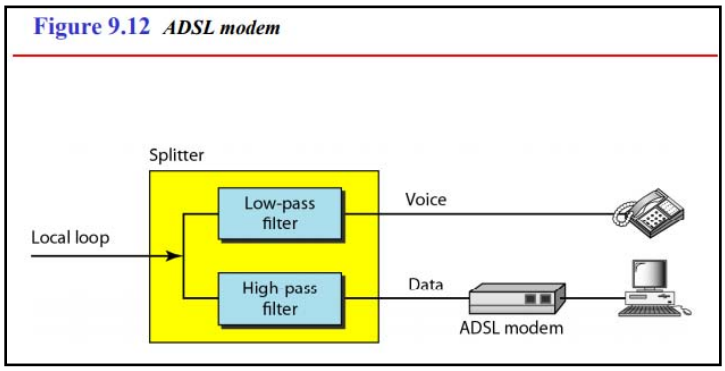


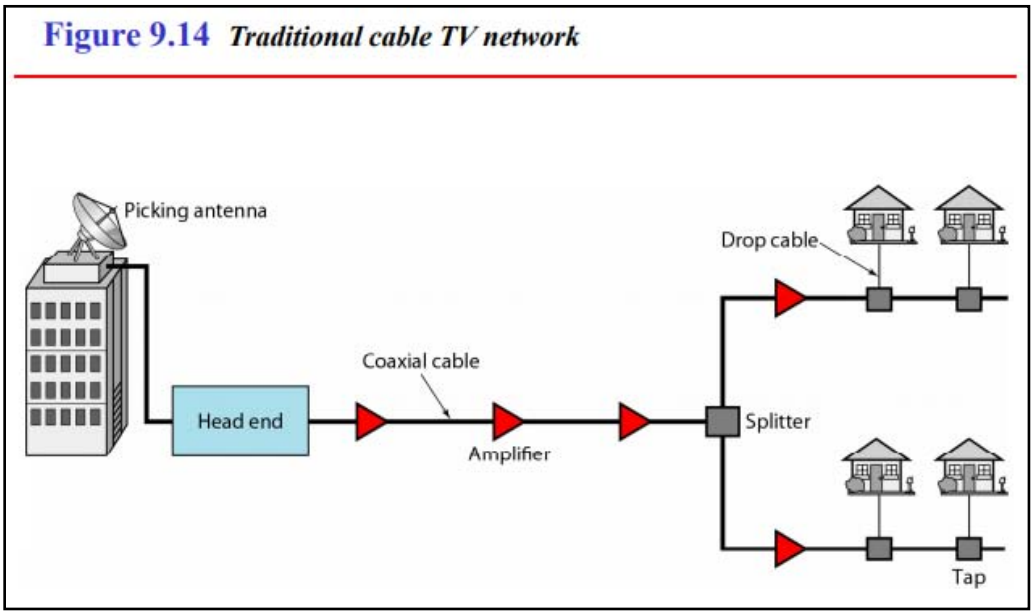
Figure 9.12 *ADSL modem*

CABLE NETWORKS

- The cable network started as a video service provider, but it has moved to the business of Internet access. This network can be used to provide high -speed access to the Internet.
- Cable television, generally, any system that distributes television signals by means of coaxial or fibre-optic cables. The term also includes systems that distribute signals solely via satellite.
- Cable-television systems originated in the United States in the late 1940s and were designed to improve reception of commercial network broadcasts in remote and hilly areas.
- During the 1960s they were introduced in many large metropolitan areas where local television reception is degraded by the reflection of signals from tall buildings.
- ***Commonly known as community antenna television*** (CATV), these cable systems use a "community antenna" to receive broadcast signals (often from communications satellites), which they then retransmit via cables to homes and establishments in the local area subscribing to the service.

1. Traditional Cable Networks

Communication in the traditional cable TV network is unidirectional.



2. Hybrid Fiber-Coaxial (HFC) Network

Communication in an HFC cable TV network can be bidirectional.

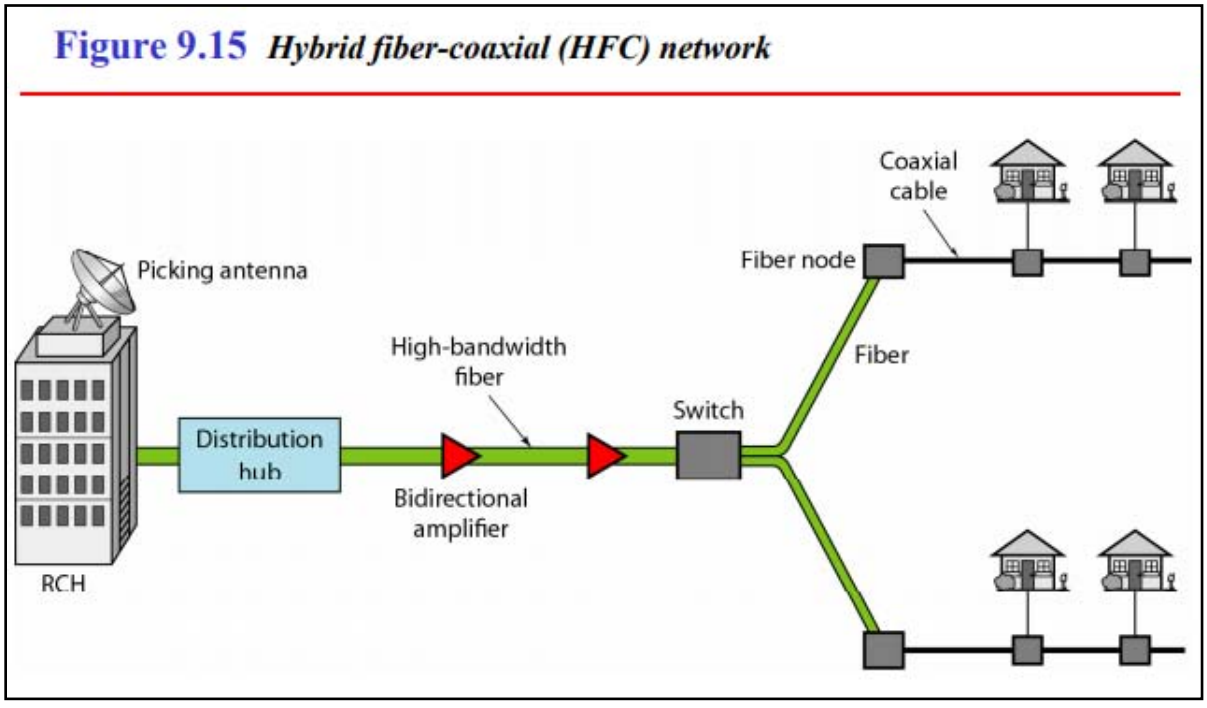
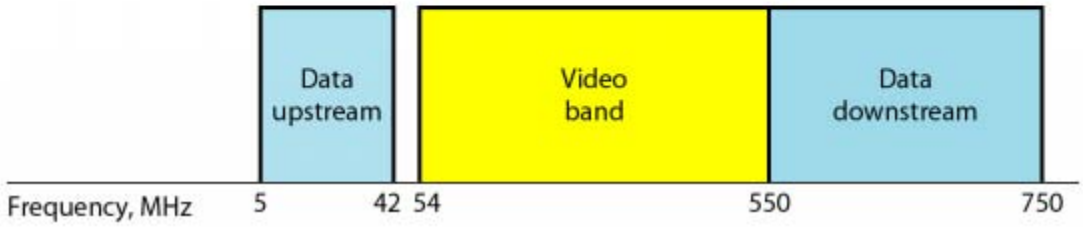
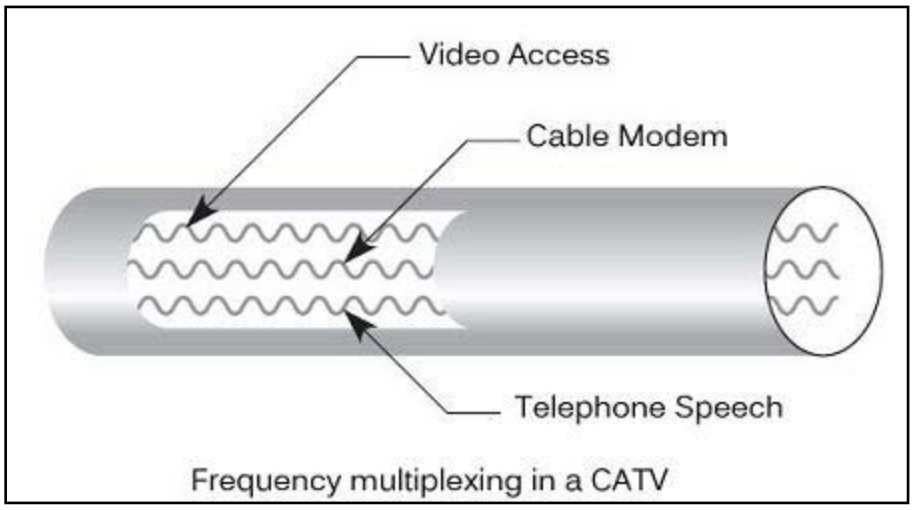


Figure 9.16 *Division of coaxial cable band by CATV*





Frequency multiplexing in a CATV

Figure 9.17 *Cable modem (CM)*

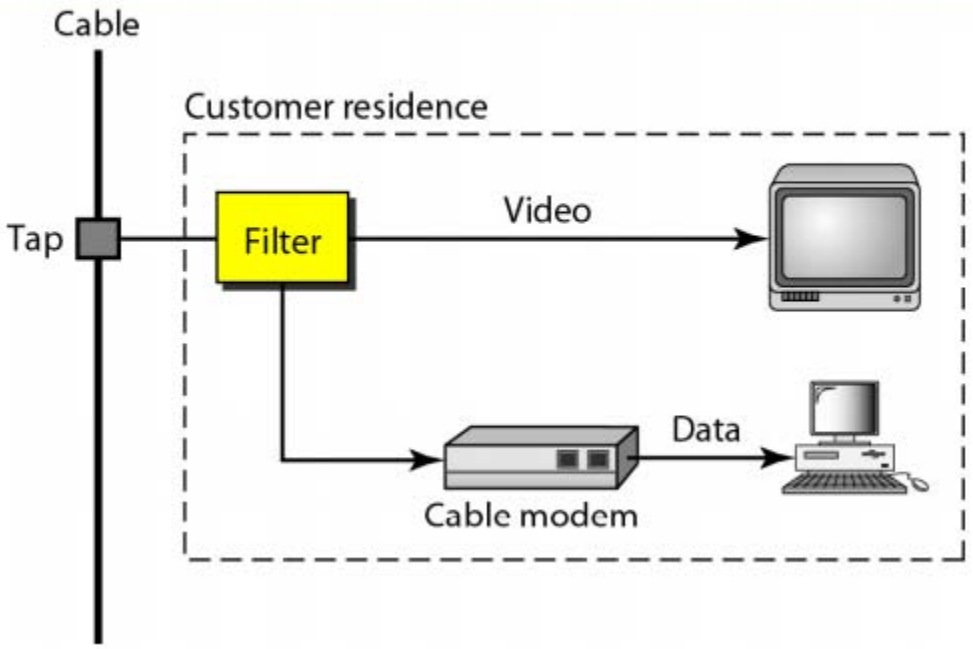
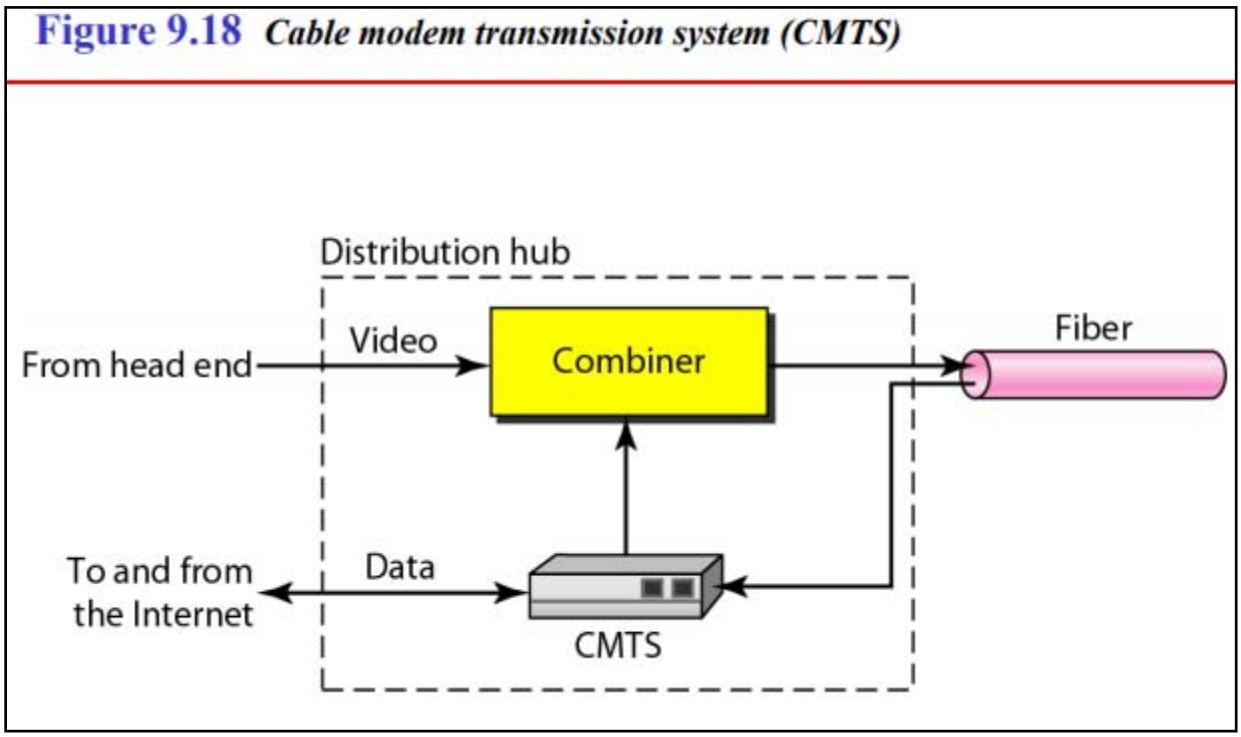


Figure 9.18 *Cable modem transmission system (CMTS)*



Mobile

Mobile Data is the term used by many to describe the use of wireless data communications using radio waves to send and receive information. This is part of the much broader mobile technology arena.

Benefits of using mobile data communications

Mobile Data technology lets your key staff operate more efficiently when they are out of the office. It can help you:

- Carry out tasks remotely, which would normally be done on a computer in the office,
- Communicate with people at remote locations,
- Work with data that is held in the office, even when you are in a different location,
- Communicate a message
- Create an electronic audit trail of messages sent/received
- Keep in touch with the office anytime and from anywhere.

Choosing the appropriate mobile data technology

The technology choices are many and varied and can be divided into two main categories

- The choice of wireless data network
- The type of device

Wireless data networks exist in such number and variety as to be difficult to categories and compare.

Some wireless data networks run over wireless voice networks, such as mobile telephone networks. **GPRS and 3G** are examples.

There are cost implications on the type of data network you use for you mobile data solution. The variables involved in calculating the data transmission costs include;

- The amount of data to be transmitted
- The frequency of the data transmissions
- The type of connection, e.g. permanent always on or occasional - as and when needed.

GSM

GSM stands for Global System for Mobile communications. GSM is one of the most widely used digital wireless telephony system.

GSM technology uses TDMA (Time Division Multiple Access) to support up to eight calls simultaneously. It also uses encryption to make the data more secure.

The frequencies used by the international standard is 900 MHz to 1800 MHz However, GSM phones used in the US use 1900 MHz frequency and hence are not compatible with the international system.

CDMA

CDMA stands for Code Division Multiple Access. It was first used by the British military during World War II. After the war its use spread to civilian areas due to high service quality.**WLL**

WLL stands for Wireless in Local Loop. It is a wireless local telephone service that can be provided in homes or offices.

GPRS

GPRS stands for General Packet Radio Services. It is a packet based wireless communication technology that charges users based on the volume of data they send rather than the time duration for which they are using the service.

GPRS is the mobile communication protocol used by second (2G) and third generation (3G) of mobile telephony. It pledges a speed of 56 kbps to 114 kbps, however the actual speed may vary depending on network load.

S.No.	Contents	Check it (if Difficult)	Page	Spend Time in Hour
2.1	Functions of Physical Layer		22	1
2.2	Data and Signals: Analog and Digital signals, Transmission Impairment, Data Rate Limits, Performance		23	1
2.3	Data Transmission Media: Guided Media, Unguided Media and Satellites		31	1
2.4	Bandwidth Utilization: Multiplexing and Spreading		35	1
2.5	Switching: Circuit switching, Message switching & Packet switching		39	1
2.6	Telephone, Mobile and Cable network for data Communication		45	1

Point to Note:

INSPIRING LEARNING QUOTES

"NOTHING WILL WORK UNLESS YOU DO."

Don't be judgmental towards anyone, including yourself.

"YESTERDAY I WAS CLEVER, SO I CHANGED THE WORLD. TODAY I AM WISE, SO I AM CHANGING MYSELF."

"NEVER GIVE UP ON A DREAM JUST BECAUSE OF THE TIME IT WILL TAKE TO ACCOMPLISH IT. THE TIME WILL PASS ANYWAY."

"TELL ME AND I FORGET. TEACH ME AND I REMEMBER. INVOLVE ME AND I LEARN."

Ask yourself: how is this changing me?

Answer own Innovation, Creativity & Tinkering.

Point to Note

Basic Concept Cryptography

Cryptography is a method of using advanced mathematical principles in storing and transmitting data in a particular form so that only those whom it is intended can read and process it.

Cryptography Terms

- **Encryption**: It is the process of locking up information using cryptography. Information that has been locked this way is encrypted.
- **Decryption**: The process of unlocking the encrypted information using cryptographic techniques.
- **Key**: A secret like a password used to encrypt and decrypt information. There are a few different types of keys used in cryptography.
- **Steganography**: It is actually the science of hiding information from people who would snoop on you. The difference between steganography and encryption is that the would-be snoopers may not be able to tell there's any hidden information in the first place.

7.1	A Model for Network Security			1

A MODEL FOR NETWORK SECURITY

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

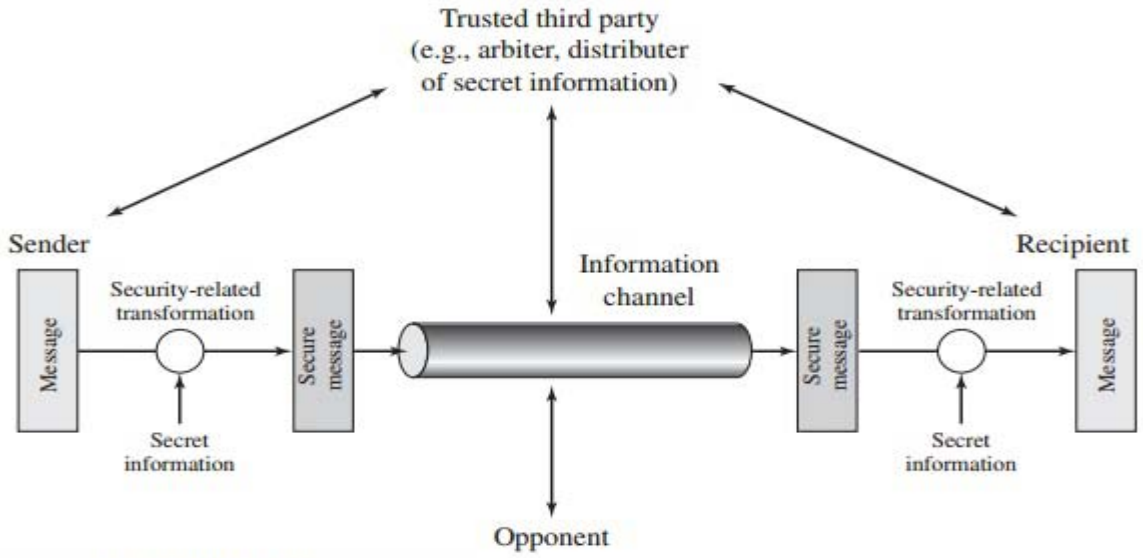


Figure 1.4 Model for Network Security

- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

- A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

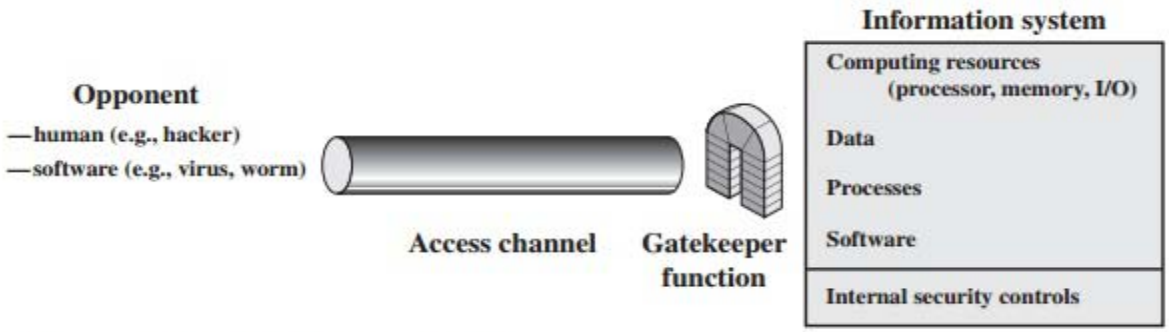


Figure 1.5 Network Access Security Model

A general model of these other situations is illustrated by Figure 1.5, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

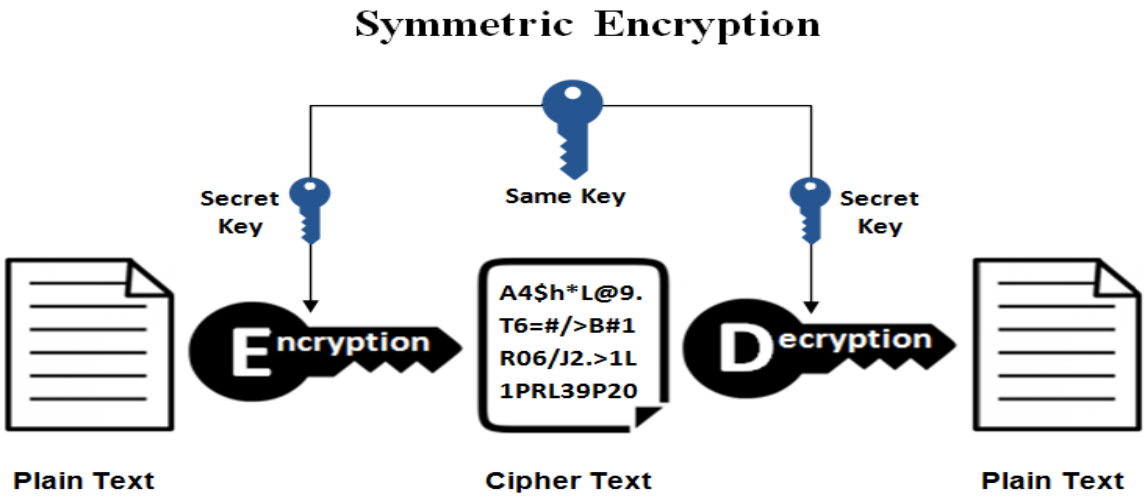
Programs can pre-sent two kinds of threats:-

- **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
- **Service threats:** Exploit service flaws in computers to inhibit use by legitimate users.

The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.5). The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

7.2	Principles of cryptography: Symmetric Key and Public Key		1

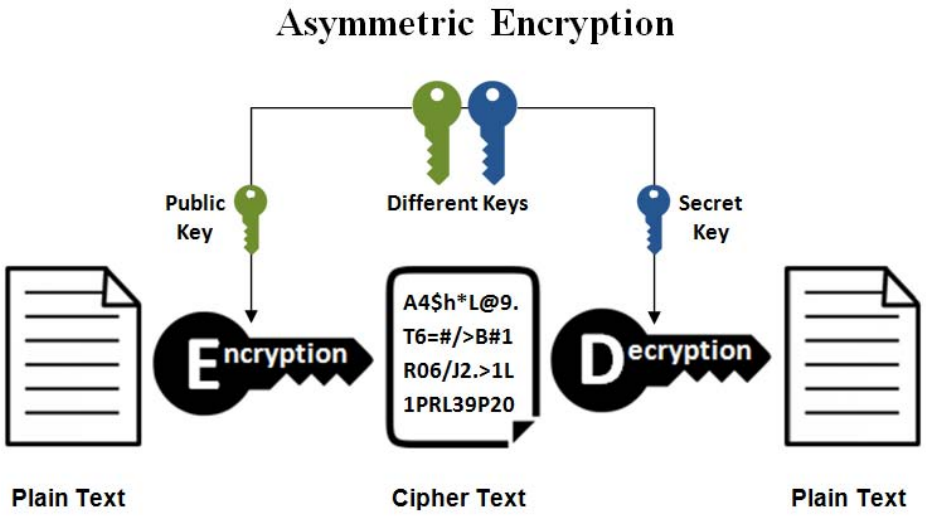
Symmetrical Encryption



- ✓ This is the simplest kind of encryption that involves only one secret key to cipher and decipher information.
- ✓ Symmetrical encryption is an old and best-known technique.
- ✓ It uses a secret key that can either be a number, a word or a string of random letters.
- ✓ It is a blended with the plain text of a message to change the content in a particular way.
- ✓ The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. AES, DES, RC5, and RC6 are examples of symmetric encryption.
- ✓ The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Asymmetrical Encryption



- ✓ Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption.
- ✓ Asymmetric encryption uses **two keys** to encrypt a plain text.
- ✓ Secret keys are exchanged over the Internet or a large network.
- ✓ It ensures that malicious persons do not misuse the keys.
- ✓ It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security.
- ✓ A public key is made freely available to anyone who might want to send you a message. The second **private key** is kept a secret so that you can only know.
- ✓ A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key.
- ✓ Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes RSA, DSA etc

Asymmetric Encryption in Digital Certificates

To use asymmetric encryption, there must be a way of discovering public keys. One typical technique is using digital certificates in a client-server model of communication. A certificate is a package of information that identifies a user and a server. It contains information such as an organization's name, the organization that issued the certificate, the users' email address and country, and users public key.

When a server and a client require a secure encrypted communication, they send a query over the network to the other party, which sends back a copy of the certificate. The other party's public key can be extracted from the certificate. A certificate can also be used to uniquely identify the holder.

DIFFERENCE BETWEEN SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHY

Characteristic	Symmetric key cryptography	Asymmetric key cryptography
Key used for encryption/decryption	Same key is used	One key is used for encryption and another ;different key is used for decryption
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original plain text size.	More than the original plain text size
Known keys	Both parties should know the key in symmetric key encryption	Only, either one of the keys is known by the two parties in public key encryption.
Usage	Confidentiality	Confidentiality, digital signature etc.

7.3	Public Key Algorithm - RSA		1

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

Algorithm

The RSA algorithm holds the following features −

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm −

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −

N=p*q

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

Step 3: Public key

The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.

Step 4: Private Key

Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −

ed = 1 mod (p-1) (q-1)

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is **(n,e).** To encrypt the plain text message in the given scenario, use the following syntax −

$C = P^e \bmod n$

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver **C** has the private key **d**, the result modulus will be calculated as −

$Plaintext = C^d \bmod n$

Let us learn the mechanism behind RSA algorithm (*Reference to Class Problem)*:

>> Generating Public Key :

- Select two prime no's. Suppose **P = 53 and Q = 59**.
- Now First part of the Public key : **n = P*Q = 3127**.

- We also need a small exponent say **e** :
- But e Must be
  - An integer.
  - Not be a factor of n.
  - **1 < e < Φ(n)** [Φ(n) is discussed below],
  - Let us now consider it to be equal to 3.
- Our Public Key is made of n and e

>> Generating Private Key :

- We need to calculate Φ(n) :
- Such that **Φ(n) = (P-1)(Q-1)**
- so, Φ(n) = 3016

- Now calculate Private Key, **d** :
- **d = (k*Φ(n) + 1) / e** for some integer k
- For k = 2, value of d is 2011.

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011)

Now we will encrypt **"HI"** :

- Convert letters to numbers : H = 8 and I = 9

- Thus **Encrypted Data c = 89^e mod n**.
- Thus our Encrypted Data comes out to be 1394

Now we will decrypt **1394** :

- **Decrypted Data = c^d mod n**.
- Thus our Encrypted Data comes out to be 89

8 = H and I = 9 i.e. "HI".

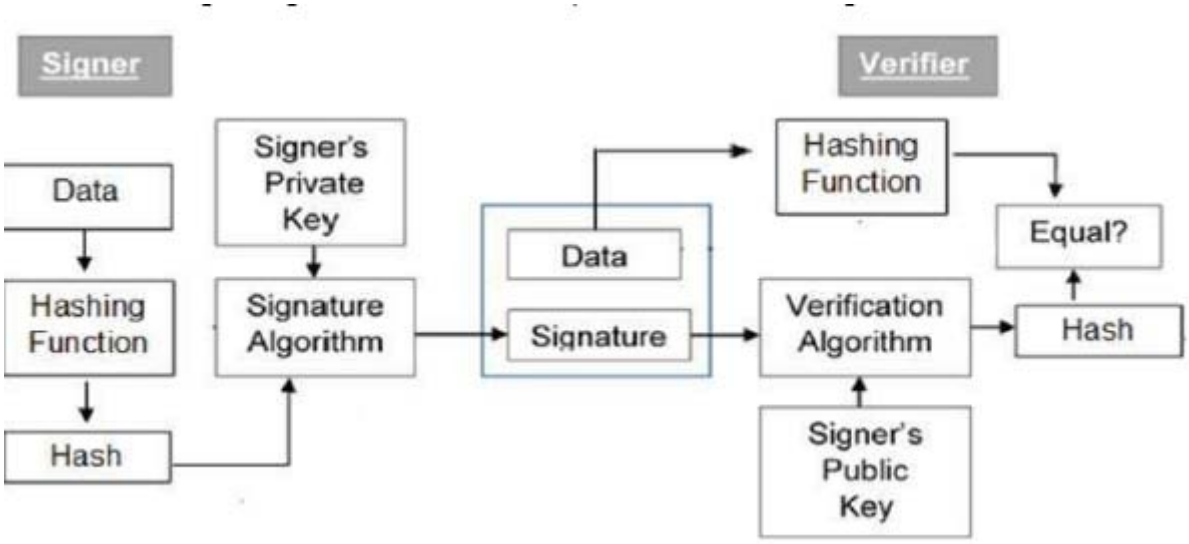
7.4	Digital Signature Algorithm		1

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, **a digital signature is a technique that binds a person/entity to the digital data**. **This binding can be independently verified by receiver as well as any third party**.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

Model of Digital Signature



Importance of Digital Signature

Let us briefly see how this is achieved by the digital signature −

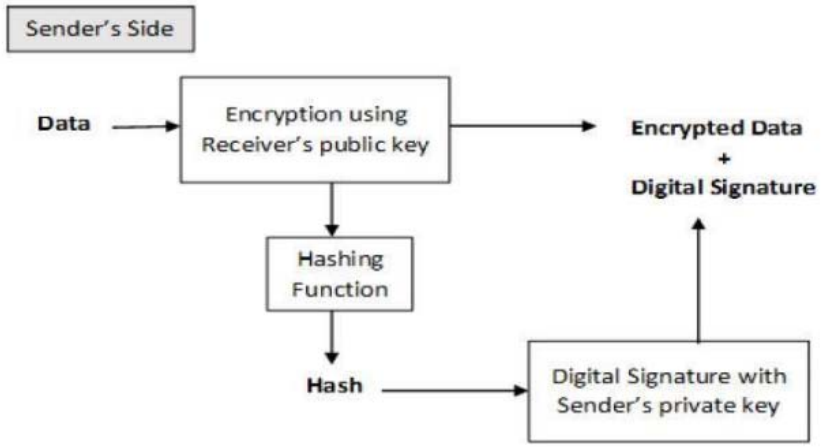
- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

Encryption with Digital Signature

There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −



The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

Advantages of Digital Signature Algorithm

- Along with having strong strength levels, the length of the signature is smaller as compared to other digital signature standards.
- The signature computation speed is less.
- DSA requires less storage to work as compared to other digital standards.
- DSA is patent free so it can be used free of cost.

Disadvantages of Digital Signature Algorithm

- It requires a lot of time to authenticate as the verification process includes complicated remainder operators. It requires a lot of time for computation.
- Data in DSA is not encrypted. We can only authenticate data in this.
- The digital signature algorithm firstly computes with SHA1 hash and signs it. Any drawbacks in cryptographic security of SHA1 are reflected in DSA because implicitly of DSA is dependent on it.
- With applications in both secret and non-secret communications, DSA is of the US National Standard.

7.5	Communication Security: IPSec, VPN, Firewalls, Wireless Security.		1

IP security (IPSec)

Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.Also known as IP Security.

IPsec involves two security services:

- **Authentication Header (AH)**: This authenticates the sender and it discovers any changes in data during transmission.
- **Encapsulating Security Payload (ESP):** This not only performs authentication for the sender but also encrypts the data being sent.

There are two modes of IPsec:

- **Tunnel Mode:** This will take the whole IP packet to form secure communication between two places, or gateways.
- **Transport Mode:** This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication.

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security –

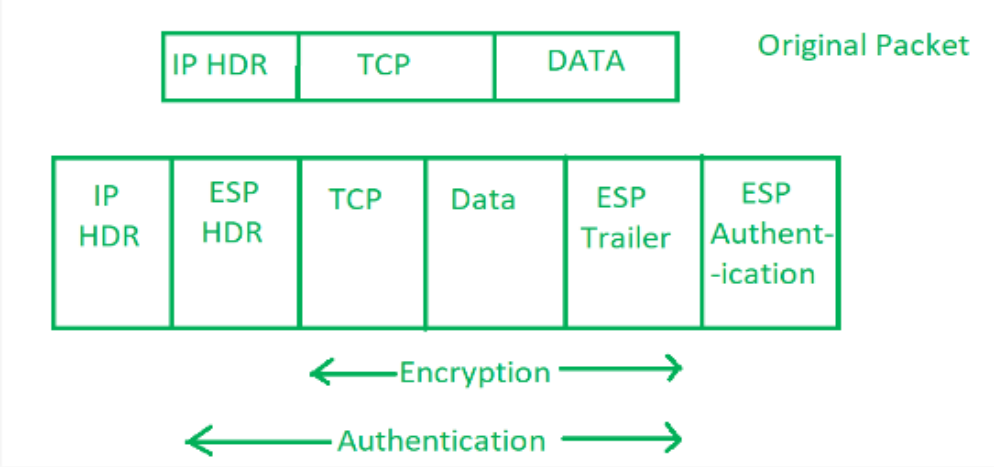
It has the following components:

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

Internet Key Exchange (IKE) –

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



IPsec provides the following security services for traffic at the IP layer:

- Data origin authentication—identifying who sent the data.
- Confidentiality (encryption)—ensuring that the data has not been read en route.
- Connectionless integrity—ensuring the data has not been changed en route.
- Replay protection—detecting packets received more than once to help protect against denial of service attacks.

Applications of IPSec

As we all know to help in the security of a network the Internet community has done lot of work and developed application-specific security mechanisms in numerous application areas, including electronic mail (*Privacy Enhanced Mail, P retty Good P rivacy* [PGP]), network management (*Simple N etwork M anagement P rotocol Version 3*[SNMPv3]), Web access (Secure HTTP, *Secure Sockets Layer* [SSL]), and others.

Benefits of IPSec

When IPSec is implemented in a firewall or router, it provides strong security whose application is to all traffic crossing this perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

IPSec is below the transport layer (TCP, UDP), and is thus transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router.

Even if IPSec is implemented in end systems, upper layer software, including applications is not affected. IPSec can be transparent to end users.

VPN (Virtual Private Network)

VPN stands for Virtual Private Network (VPN) that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection that is called VPN tunnel and all Internet traffic and communication is passed through this secure tunnel.

Virtual Private Network (VPN) is basically of 2 types:

1. **Remote Access VPN:**
   Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.
2. **Site to Site VPN:**
   A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

Types of Virtual Private Network (VPN) Protocols:

1. **Internet Protocol Security (IPSec):**
   Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection.
   IPSec runs in 2 modes:
   - (i) Transport mode
   - (ii) Tunneling mode

   The work of transport mode is to encrypt the message in the data packet and the tunneling mode encrypts the whole data packet. IPSec can also be used with other security protocols to improve the security system.
2. **Layer 2 Tunneling Protocol (L2TP):**
   L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.
3. **Point–to–Point Tunneling Protocol (PPTP):**
   PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

4. **SSL and TLS:**
   SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have "https" in the initial of the URL instead of "http".
5. **OpenVPN:**
   OpenVPN is an open source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol.
6. **Secure Shell (SSH):**
   Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

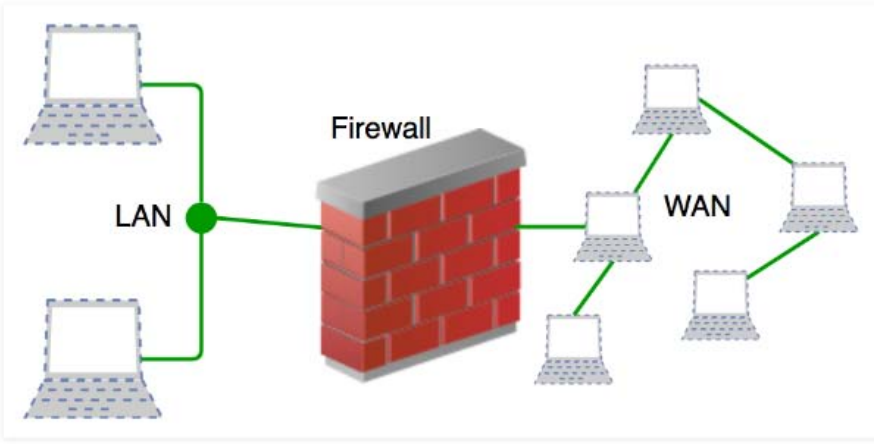
Firewall

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

A firewall is a **network security** device that monitors incoming and outgoing network traffic and permits or blocks data **packets** based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How does a firewall work?

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Generation of Firewall

Firewalls can be categorized based on its generation.

First Generation- Packet Filtering Firewall : Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

Second Generation- Stateful Inspection Firewall : Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient.

Third Generation- Application Layer Firewall : Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

Next Generation Firewalls (NGFW) : Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks.

Wireless-Security

Like the system's security and data security, keeping a sound knowledge about different wireless security measures is also essential to know for security professionals. It is because different wireless security mechanisms have a different level of strength and capabilities.

There are automated wireless hacking tools available that have made cybercriminals more powerful. List of some of these tools are:

- ✓ AirCrack.
- ✓ AirSnort.
- ✓ Cain & Able.
- ✓ Wireshark.
- ✓ NetStumbler etc.

Different various techniques of hacking include remote accessing, shoulder surfing, wireless router's dashboard accessing, and brute-forcing attack that are used to penetrate wireless security.

1. What is Wireless Security?
2. Wired Equivalent Privacy (WEP)
3. Wi-Fi Protected Access (WPA)
4. Wi-Fi Protected Access II (WPA2)
5. Wi-Fi Protected Access 3 (WPA3)

What is Wireless Security?

Wireless security revolves around the concept of securing the wireless network from malicious attempts and unauthorized access.
The wireless security can be delivered through different ways such as:

1. **Hardware-based:** where routers and switches are fabricated with encryption measures protects all wireless communication. So, in this case, even if the data gets compromised by the cybercriminal, they will not be able to decrypt the data or view the traffic's content.

2. **Wireless setup of IDS and IPS:** helps in detecting, alerting, and preventing wireless networks and sends an alarm to the network administrator in case of any security breach.
3. **Wireless security algorithms:** such as WEP, WPA, WPA2, and WPA3. These are discussed in the subsequent paragraphs.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the oldest security algorithm of 1999. It uses the initialization vector (IV) method. The very first versions of the WEP algorithm were not predominantly strong enough, even for that time when it got released. But the reason for this weak release was because of U.S. limits on the exporting of different cryptographic technologies, which led the manufacturing companies to restrict their devices to 64-bit encryption only. As the limitation was withdrawn, the 128 bit and 256 bit WEP encryption were developed and came into the wireless security market, though 128 became the standard one.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) was the next Wi-Fi Alliance's project that replaced the increasingly noticeable vulnerabilities of WEP standard. WPA was officially adopted in the year 2003, one year before the retirement of WEP. WPA's most common configuration is with WPA-PSK, which is abbreviated as Pre-Shared Key. WPA uses 256-bit, which was a considerable enhancement above the 64-bit as well as 128-bit keys.

Wi-Fi Protected Access II (WPA2)

Wi-Fi Protected Access II (WPA2) became official in the year 2006 after WPA got outdated. It uses the AES algorithms as a necessary encryption component as well as uses CCMP (Counter Cipher Mode - Block Chaining Message Authentication Protocol) by replacing TKIP.

Wi-Fi Protected Access 3 (WPA3)

Wi-Fi Protected Access 3 (WPA3) is the latest, and the third iteration of this family developed under Wi-Fi Alliance. It has personal as well as enterprise security-support feature and uses 384-bit Hashed Message Authentication Mode, 256-bit Galois / Counter Mode Protocol (GCMP-256), as well as Broadcast/Multicast Integrity Protocol of 256-bit. WPA3 also provides perfect forward secrecy mechanism support.

INSPIRING LEARNING QUOTES

"NOTHING WILL WORK UNLESS YOU DO."

Don't be judgmental towards anyone, including yourself.

"YESTERDAY I WAS CLEVER, SO I CHANGED THE WORLD. TODAY I AM WISE, SO I AM CHANGING MYSELF."

"NEVER GIVE UP ON A DREAM JUST BECAUSE OF THE TIME IT WILL TAKE TO ACCOMPLISH IT. THE TIME WILL PASS ANYWAY."

"TELL ME AND I FORGET. TEACH ME AND I REMEMBER. INVOLVE ME AND I LEARN."

Ask yourself: how is this changing me?

- ----- - ---------- ---------- ---------- ---------- ---------

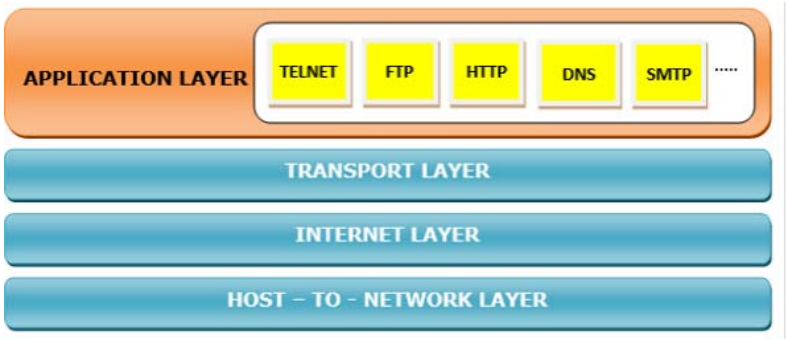
6.1 Functions of Application layer

The application layer is the highest abstraction layer of the TCP/IP model that provides the interfaces and protocols needed by the users. It combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model.

The functions of the application layer are −

- It facilitates the user to use the services of the network.
- It is used to develop network-based applications.
- It provides user services like user login, naming network devices, formatting messages, and e-mails, transfer of files etc.
- It is also concerned with error handling and recovery of the message as a whole.

The following diagram shows the transport layer in the TCP/IP protocol suite −



6.2 Application Layer Protocols: DNS, DHCP, WW W, HTTP, HTTPs, TELNET, FTP, SMTP, POP, IMAP

An application layer protocol defines how application processes (clients and servers), running on different end systems, pass messages to each other. In particular, an application layer protocol defines:

- The types of messages, e.g., request messages and response messages.
- The syntax of the various message types, i.e., the fields in the message and how the fields are delineated.
- The semantics of the fields, i.e., the meaning of the information that the field is supposed to contain;
- Rules for determining when and how a process sends messages and responds to messages.

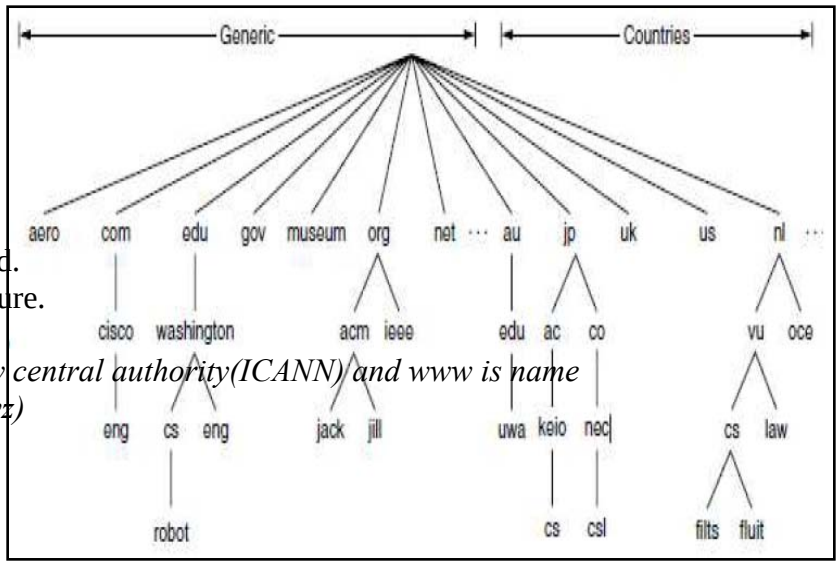
Application Type	Application-layer protocol	Transport Protocol
Electronic mail	Send: Simple Mail Transfer Protocol SMTP [RFC 821]	TCP 25
	Receive: Post Office Protocol v3 POP3 [RCF 1939]	TCP 110
Remote terminal access	Telnet [RFC 854]	TCP 23
World Wide Web (WWW)	HyperText Transfer Protocol 1.1 HTTP 1.1 [RFC 2068]	TCP 80
File Transfer	File Transfer Protocol FTP [RFC 959]	TCP 21
	Trivial File Transfer Protocol TFTP [RFC 1350]	UDP 69
Remote file server	NFS [McKusik 1996]	UDP or TCP
Streaming multimedia	Proprietary (e.g., Real Networks)	UDP or TCP
Internet telephony	Proprietary (e.g., Vocaltec)	Usually UDP

1. DNS:

Domain N ame S ystem (DNS) – It is a naming system for devices in networks. It provides services for translating domain names to IP addresses.

1. Name Server (DNS- Domain Name System)

- All system communicate using IP(Numbers)
- Numbers are difficult to remember for human beings than name
- Internet is very large there are millions of computer and servers
- Naming system is introduced(in 1983) for mapping of Host Name to IP address
- In DNS server, there is library procedure (program) called resolver that converts host name to IP.
- **ICANN (Internet Corporation for Assigned Names and Numbers)** is responsible for managing the DNS in internet.
- Domain names are unique



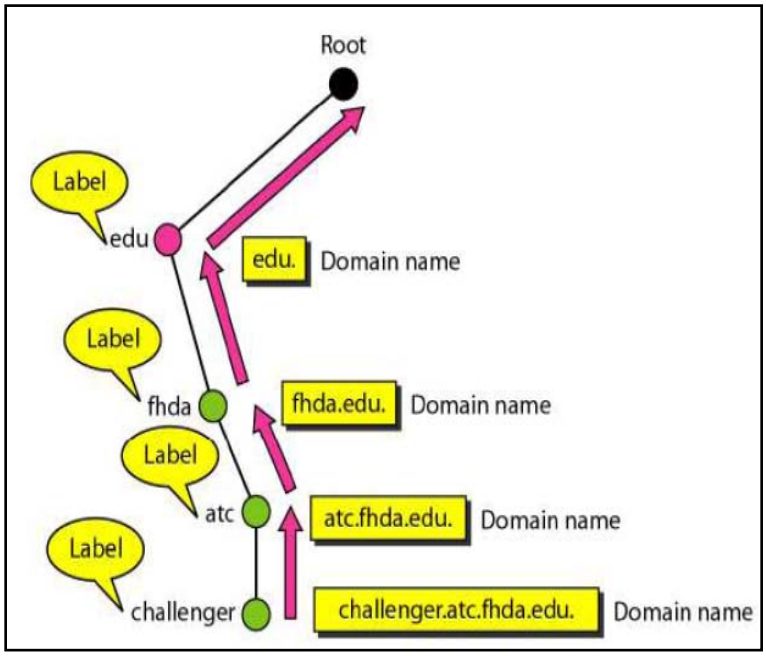
1.1. Name Spaces(Domain Name)

- ***Divided into 2 :***
  1. Flat Structure
  2. Hierarchical Structure
     - Hierarchical structure is used.
     - Name space have tree structure.
     - Example : www.xyz.com
     - *Here xyz.com is managed by central authority(ICANN) and www is name given by organization(here xyz)*

1.1.1. Domain Name Space

- Inverted Tree Structure, contains 0 to127 (128)levels
- 0 is root level
- Internet have nearly 250 **toplevel domains**, where each

domain covers many hosts
• Each domain is partitioned into **subdomains**, and these are further partitioned, and so on com, edu, gov are example of top level domain

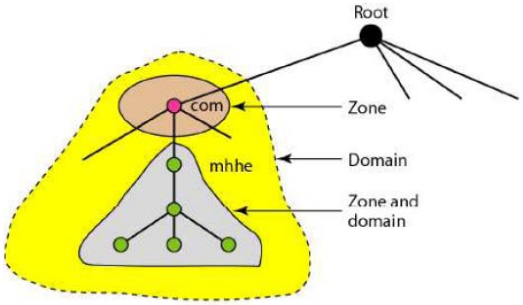


1.1.2. Domain Name

• All label is terminated by a null string(.), it is called a ***FQDN (Fully Qualified Domain Name)***
• **Example:** *challenger.ate.tbda.edu.*
• Label is not terminated by a null string, it is called a ***PQDN (Partially Qualified Domain Name)***
• A PQDN starts from a node, but it does not reach the root
• **Example :** *challenger.ate.tbda.edu*
• NB: **.(dot)** Is called root server

1.1.3. Zone

• Zone will keep track of all nodes in domain and all sub-domains under the domain.



1.2. Servers

• Root Server
• A root server is a server whose zone consists of the whole tree
• A root server usually does not store any information about domains but delegates its authority to other servers
• DNS defines two types of servers

1. Primary Server

• A primary server is a server
• That stores a file about the zone for which it is an authority
• It is responsible for **creating, maintaining, and updating the zone file**

2. Secondary Server

• A secondary server is a server that **transfers the complete information about a zone** from another server (primary or secondary) and stores the file on its local disk

1.3. Query

• ***DNS has two types of messages***

1. Query - sent by DNS client to server, **Query message consists** of a header and question records

2. Response – sent by DNS server to client, **Response message consists** of a header, question, records, answer records, authoritative records, and additional records

• **Query** is a question to the server, Client ask about the **IP address** of the mentioned **URL**

• **Response** is answer to the question provided by client from server, i.e. it sent information (IP address) of the mentioned URL.

2. DHCP:

DHCP(Dynamic Host Configuration Protocol)

• *Two possible way for configuring IP are:*

1. Manually

2. Dynamically (DHCP)

• DHCP is service that provide IP addresses.

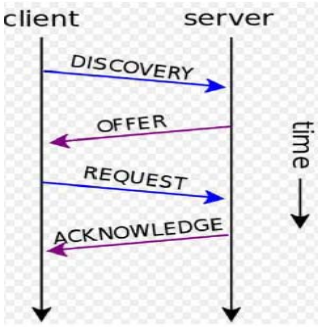
• Server that runs DHCP service is DHCP servers.

• Client that uses DHCP server for IP configuration is DHCP clients.

• DHCP server uses UDP port 67

• DHCP client uses UDP port 68

2.1. DHCP Operation



2.1.1. DHCP Discover Packet

• Sent by DHCP client to DHCP server (Broadcasting).

• DHCP client ***(****computer or device which wants IP****)*** broadcast broadcasts a request for an IP address on its network. It does this by using a DHCP DISCOVER packet.

• Packet must reach the DHCP server.

• A DHCP client may also request its last-known IP address with discover packet.

• DHCP discovers packet is for checking weather DHCP server is available in network and IP address lease request.

2.1.2. DHCP Offer Packet

• Sent by DHCP server to DHCP client (Unicasting)

• When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client

• This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer

2.1.3. DHCP Request Packet

• Sent by DHCP client to DHCP servers (Broadcasting)
• In response to the DHCP offer, the client replies with a DHCP request, broadcast to the server, requesting the offered address.
• A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer
• Based on required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted.
• When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

5.1.4. DHCP Acknowledgement Packet

• Sent by DHCP servers to DHCP client (Unicasting)
• When the DHCP server receives the DHCP REQUEST message from the client, the configuration process enters its final phase.
• The acknowledgement phase involves sending a DHCP ACK packet to the client.
• This packet includes the lease duration and any other configuration information that the client might have requested.
• At this point, the IP configuration process is completed

3. WWW:

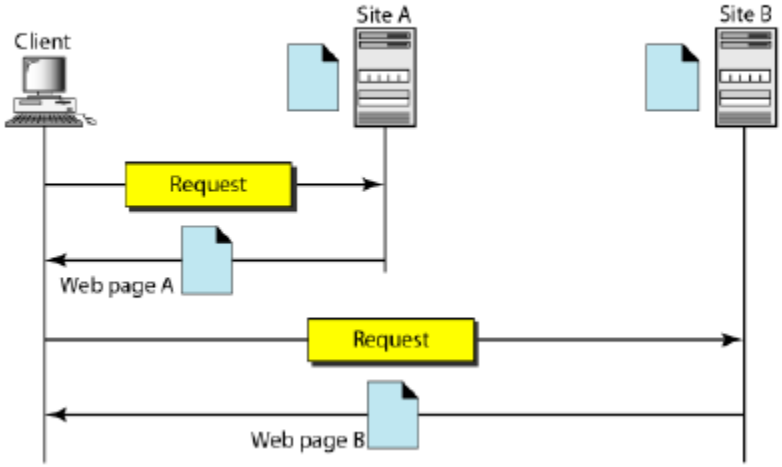
- ✓ This is a protocol used mainly to access data on the World Wide Web (www).
- ✓ The Hypertext Transfer Protocol (HTTP) the Web's main application-layer protocol although current browsers can access other types of servers
- ✓ A respository of information spread all over the world and linked together.
- ✓ The HTIP protocol transfer data in the form of plain text, hyper text, audio, video and so on.
- ✓ HTTP utilizes TCP connections to send client requests and server replies.
- ✓ it is a synchronous protocol which works by making both persistent and non persistent connections.

4. HTTP:

Hyper Text Transfer Protocol, HTTP − It is the underlying protocol for world wide web. It defines how hypermedia messages are formatted and transmitted.

• The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web(WWW)
• It is similar to FTP because it transfers files and uses the services of TCP.
• It uses only one TCP connection
• HTTP uses the services of TCP on well-known **port 80**
• Accessing of web page is based on URL

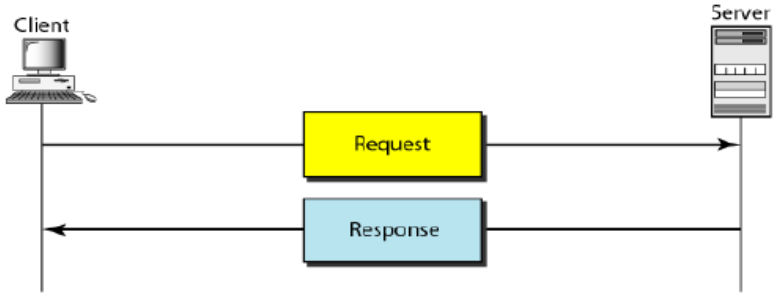
4.1. WWW Architecture



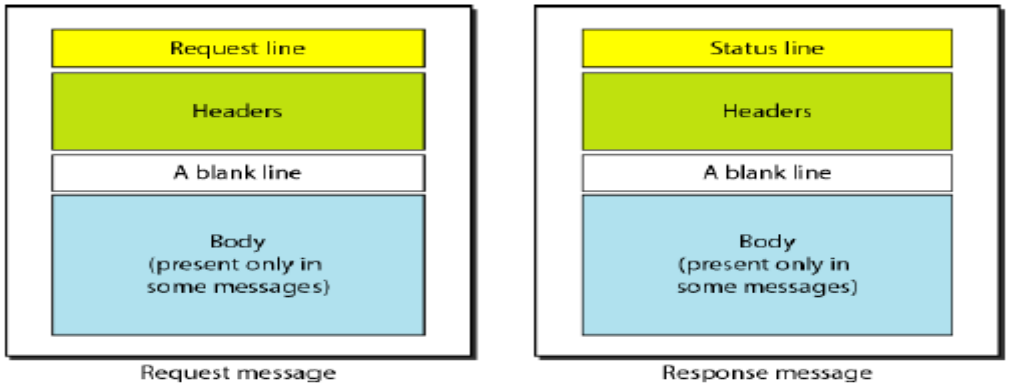
4.2. HTTP Transaction

- HTTP transaction between the client and server
- There are 2 transaction messages
- Request (sent from client to server for requesting a Page or other resource)
- Response (sent from server to client)

4.2. HTTP Transaction Figure



4.2.1 Message Format



5. HTTPs:

- ✓ Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, its predecessor, Secure Sockets Layer (SSL). The protocol is therefore also often referred to as HTTP over TLS, or HTTP over SSL.
- ✓ The principal motivations for HTTPS are authentication of the accessed website, protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks.
- ✓ HTTPS creates a secure channel over an insecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted.
- ✓ **Therefore, a user should trust an HTTPS connection to a website if and only if all of the following are true:**
  - The user trusts that the browser software correctly implements HTTPS with correctly pre-installed certificate authorities.
  - The user trusts the certificate authority to vouch only for legitimate websites.
  - The website provides a valid certificate, which means it was signed by a trusted authority.
  - The certificate correctly identifies the website (e.g., when the browser visits " https://www.tribhuvan-university.edu.np/", the received certificate is properly for " tribhuvan-university.edu.np " and not some other entity).
  - The user trusts that the protocol's encryption layer (SSL/TLS) is sufficiently secure against eavesdroppers.

6. TELNET:

TELNET − It provides bi-directional text-oriented services for remote login to the hosts over the network. **TELNET (Terminal Network):**

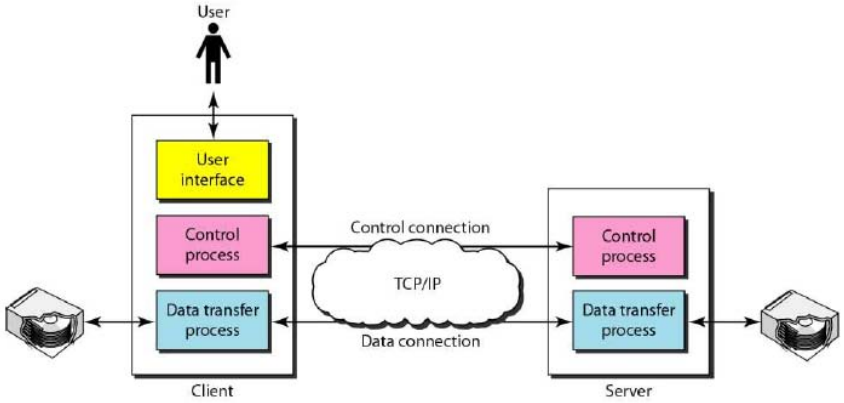
- TELNET is client-server application that allows a user to log onto remote machine and lets the user to access any application program on a remote computer.
- TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system.
- On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- TELNET is a protocol that provides a general, bi-directional, eight-bit byte oriented communications facility.
- Many application protocols are built upon the TELNET protocol
- Telnet services are used on PORT 23.

7. FTP:

File Transfer Protocol, FTP − It is a client-server based protocol for transfer of files between client and server over the network.

• File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for copying a file from one host to another.
• FTP establishes two connections between the hosts
• One connection is used for data transfer, the other for control information (commands and responses)
• Separation of commands and data transfer makes FTP more efficient
• FTP uses **two** well-known TCP ports: **Port 21** is used for the control connection, and **port 20** is used for the data connection.

7.1. FTP Architecture



7.2. FTP Working

- FTP uses Transmission Control Protocol (TCP) for reliable network communication by establishing a session before initiating data transfer
- FTP client send command/ request for connection to FTP server establishing connection(Port 21)
- FTP server Responds to the commands about the status wheatear connected/ not connected (Port 21)
- FTP Client connect to FTP server using control connection i.e. using port 21
- After establishing connection port 20 is used for data transfer

Q. E-mail

- Electronic mail, or more commonly **email**, used to communicate with different users in internet
- Email uses following protocols for storing & delivering messages, They are :
  1. **SMTP (Simple Mail Transfer Protocol)**
  2. **POP (Post Office Protocol)**
  3. **IMAP (Internet Message Access Protocol)**

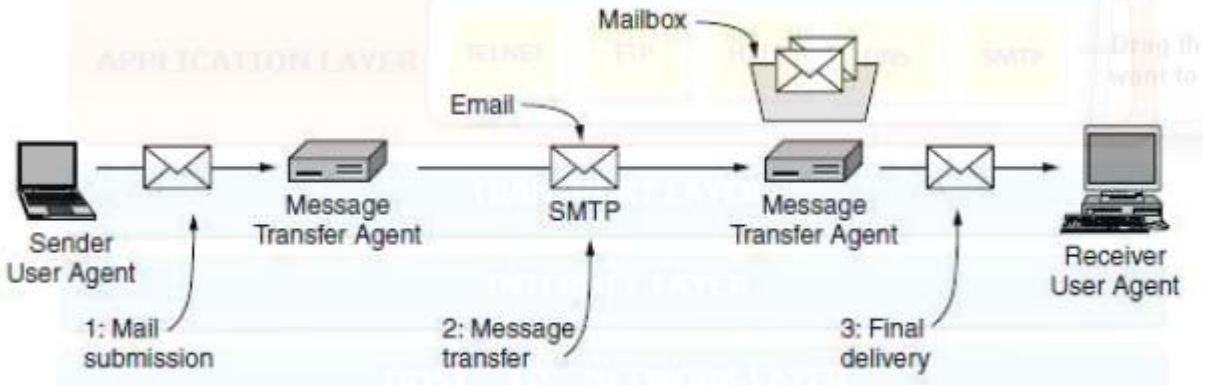


Figure Architecture of the email system.

• ***Email consists of two kinds of subsystems***

1. Mail User Agents (also called MUA/email client programs): which allow people to read and send email (Ex: Outlook)

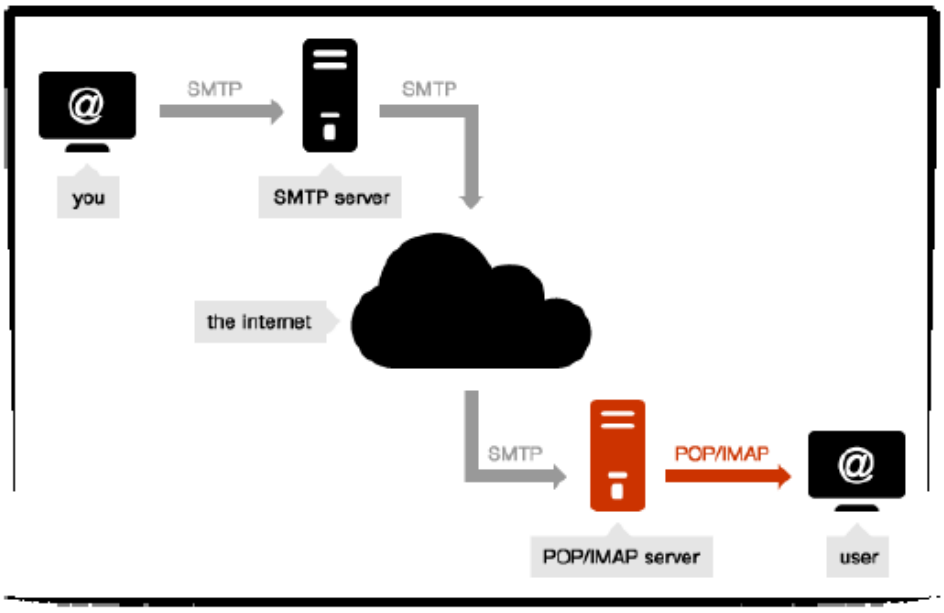
2. Message Transfer Agents(also called MTA/ Email Server) : which move the messages from the source to the destination (Ex: Gmail Server)

• Act of sending new messages into the mail system for delivery is called **Mail submission (Email Client to Email Sever)**

• The Process of transferring mail from one MTA to another (Ex : from gmail to yahoo server) is called **Message Transfer**

• **Mailboxes** store the email that is received for a user (Working all Protocols)

E-mail (Working all Protocols)



8. SMTP:

Simple Mail Transfer Protocol, SMTP − It lays down the rules and semantics for sending and receiving electronic mails (e-mails).

8.1. SMTP (Simple Mail Transfer Protocol)

• Message transfer form originator to the recipient mailbox is done with SMTP

• It uses TCP well known port 25

• SMTP server accepts incoming connections, subject to some security checks, and accepts messages for delivery

• If a message cannot be delivered, an error report containing the first part of the undeliverable message is returned to the sender

• Email is submitted by a mail client **(MUA, mail user agent)** to a mail server (**MSA, mail submission agent)** using SMTP on TCP port 587

• **MSA** delivers the mail to its mail transfer agent **MTA**

8.1.1. Features of SMTP

• SMTP supports sending of email only It cannot retrieve (deliver to user) messages from a remote server on demand

• SMTP provides system for sending message to same (or different) servers (gmail **to** gmail / gmail **to** yahoo)

• SMTP provide a mail exchange between users on same (or different) server

SMTP supports:

1. Sending a message to one or more recipients
2. Sending message that includes text, voice, video or graphics
3. Sending message to users on other network

9. POP:

9.1. POP (Post Office Protocol)

• Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection

• POP has been developed through several versions, with version 3 (POP3) being the last standard

• E-mails are downloaded from the server's mailbox to your computer

• No copy of Email will be kept in mailbox after downloading the email

• E-mails are available when you are not connected

9.1.1. POP Working

• Working of POP servers is as following steps:

1. Connect to server
2. Retrieve all mail
3. Store locally as new mail
4. Delete mail from server*
5. Disconnect

** Deletion of mail is default setting , However user can change the settings to keep the copy of email in mail box*

9.1.2.Features of POP

• POP is a much simpler protocol, making implementation easier

• POP mail moves the message from the email server onto your local computer, although there is usually an option to leave the messages on the email server as well

• POP treats the mailbox as one store, and has no concept of folders

• POP protocol requires the currently connected client to be the only client connected to the mailbox

• When POP retrieves a message, it receives all parts of it

9.1.3. Advantages of POP

• Advantages are:

1. Mail stored locally, i.e. always accessible, even without internet connection
2. Internet connection needed only for sending and receiving mail
3. Saves server storage space
4. Option to leave copy of mail on server

10. IMAP:

IMAP (Internet Message Access Protocol)

- Protocols that is used for final delivery is **IMAP**
- **IMAP** is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection
- IMAP provides mechanisms for storing messages received by SMTP in a mailbox
- IMAP server stores messages received by each user until the user connects to download and read them using an email clients

** Now a days IMAP replaced POP in all E-mail services*

10.1.1. IMAP Working

- Working of IMAP servers is as following steps:

1. Connect to server
2. Fetch user requested content and cache it locally, e.g. list of new mail, message summaries, or content of explicitly selected emails
3. Process user edits, *e.g. marking email as read, deleting email etc.*
4. Disconnect

10.1.2 Features of IMAP

- Connected and disconnected modes of operation (Faster Operation)
- Multiple clients simultaneously connected to the same mailbox
- Access to message parts and partial fetch of messages (No need for complete message to be displayed only **subject / user name** can be retrieved)
- Provides message state information (**Message states are :** read / unread / replied / forwarded)
- Provides multiple mailboxes on the server (create new mail boxes and copy form one to another)
- Provides mechanisms for server-side searches

10.1.3. IMAP Advantage

Advantages

1. Mail stored on remote server, i.e. accessible from multiple different locations
2. Internet connection needed to access mail
3. Faster overview as only headers are downloaded until content is explicitly requested
4. Mail is automatically backed up if server is managed properly
5. Saves local storage space
6. Option to store mail locally

6.3	Concept of traffic analyzer: MRTG, PRTG, SNMP. Packet tracer, Wireshark.			2

Simple Network Management Protocol, SNMP

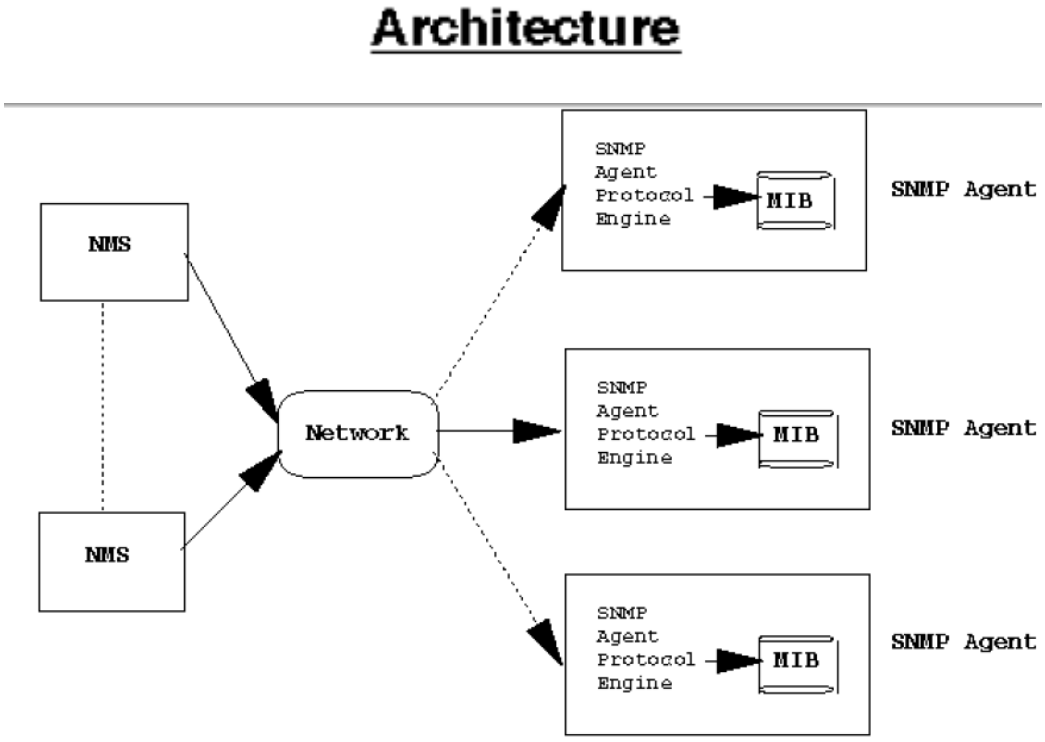
Simple N etwork M anagement P rotocol, S NMP – It is for managing, monitoring the network and for organizing information about the networked devices.

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

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

An SNMP-managed network consists of three key components:

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



To do management tasks, SNMP uses two other protocols:

1. Structure of Management Information (SMI)
2. Management Information Base (MIB).

A typical agent usually:

- Implements full SNMP protocol.
- Stores and retrieves management data as defined by the Management Information Base
- Can asynchronously signal an event to the manager
- Can be a proxy (The proxy agent then translates the protocol interactions it receives from the management station) for some non-SNMP manageable network node.

A typical manager usually:

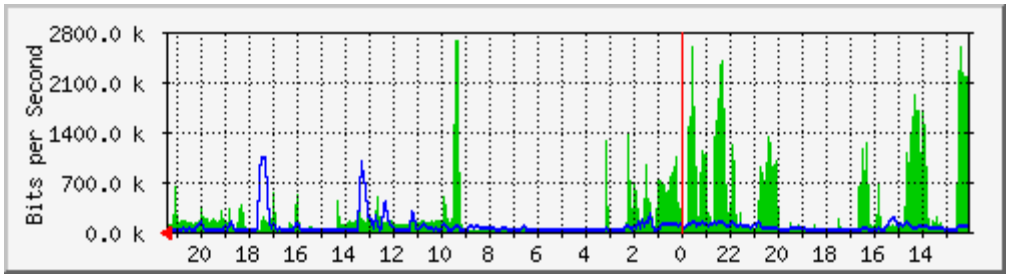
- Implemented as a Network Management Station (the NMS)
- Implements full SNMP Protocol
- Able to Query agents
- Get responses from agents

MRTG

- The **Multi Router Traffic Grapher** (MRTG) is free software for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form.

- It was originally developed by Tobias Oetiker and Dave Rand to monitor router traffic, but has developed into a tool that can create graphs and statistics for almost anything.

- MRTG is written in Perl and can run on Windows, Linux, Unix, Mac OS and NetWare.



How it works

- **SNMP**

✓ MRTG uses the **Simple N etwork Man agement P rotocol** (SNMP) to send requests with two object identifiers (OIDs) to a device.

✓ The device, which must be SNMP-enabled, will have a management information base (MIB) to look up the OIDs specified.

✓ After collecting the information it will send back the raw data encapsulated in an SNMP protocol. MRTG records this data in a log on the client along with previously recorded data for the device.

✓ The software then creates an HTML document from the logs, containing a list of graphs detailing traffic for the selected devices in the server.

- **Script output**

✓ Alternatively, MRTG can be configured to run a script or command, and parse its output for counter values.

✓ The MRTG website contains a large library of external scripts to enable monitoring of SQL database statistics, firewall rules, CPU fan RPMs, or virtually any integer-value data.

Features

- Measures two values (I for Input, O for Output) per target.
- Gets its data via an SNMP agent, or through the output of a command line.
- Typically collects data every five minutes (it can be configured to collect data less frequently).
- Creates an HTML page per target that features four graphs (GIF or PNG images).
- Results are plotted vs time into day, week, month and year graphs, with the I plotted as a full green area, and the O as a blue line.
- Automatically scales the Y axis of the graphs to show the most detail.
- Adds calculated Max, Average and Current values for both I and O to the target's HTML page.
- Can also send warning emails if targets have values above a certain threshold.

PRTG:

PRTG Network Monitor (Paessler Router Traffic Grapher until version 7) is an agentless network monitoring software from Paessler AG. It can monitor and classify system conditions like bandwidth usage or uptime and collect statistics from miscellaneous hosts as switches, routers, servers and other devices and applications.

1. **Specifications**
   - PRTG Network Monitor has an auto-discovery mode that scans predefined areas of an enterprise network and creates a device list from this data.
   - In the next step, further information on the detected devices can be retrieved using various communication protocols.
   - Typical protocols are Ping, SNMP, WMI, NetFlow, jFlow, sFlow, but also communication via DICOM or the RESTful API is possible.
   - The tool is only available for Windows systems. In addition, Paessler AG offers the cloud-based monitoring solution "PRTG hosted by Paessler"
   -

1.1 Sensors

The software is based on sensors that are configured for a specific purpose. For example, there are HTTP, SMTP/POP3 (e-mail) application sensors and hardware-specific sensors for switches, routers and servers. PRTG Network Monitor has over 200 different predefined sensors that retrieve statistics from the monitored instances, e.g. response times, processor, memory, database information, temperature or system status.

1.2 Web interface and desktop client

The software can be operated completely via a AJAX-based web interface. The web interface is suitable for both real-time troubleshooting and data exchange with non-technical staff via maps (dashboards) and user-defined reports. An additional administration interface in the form of a desktop application for Windows and macOS is available.

1.3 Notifications and reports

In addition to the usual communication channels such as Email and SMS, notification is also provided via push notification on smartphones using an app for iOS or Android. PRTG also offers customizable reports.

1.4 Pricing

PRTG Network Monitor's licensing is based on sensors. Most devices require between five and ten sensors to be fully monitored. A version with 100 integrated sensors is available free of charge.

Packet Analyzer:

- A packet analyzer (also known as a **packet s niffer)** is a computer program or piece of computer hardware (such as a packet capture appliance) that can intercept and log traffic that passes over a digital network or part of a network.
- Packet capture is the process of intercepting and logging traffic.
- A packet analyzer used for intercepting traffic on wireless networks is known as a wireless analyzer or WiFi analyzer.
- A packet analyzer can also be referred to as a network analyzer or protocol analyzer though these terms also have other meanings.

Capabilities

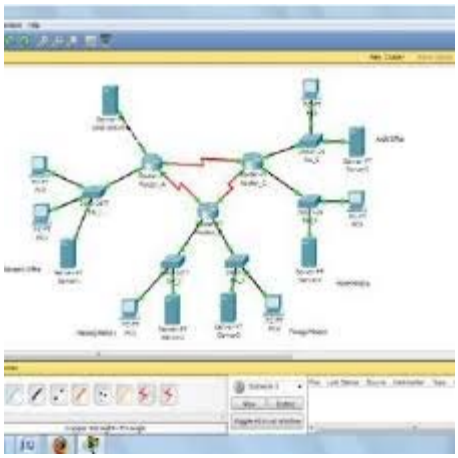
- On wired shared medias networks, such as Ethernet, Token Ring, and FDDI networks, depending on the network structure (hub or switch), it may be possible to capture all traffic on the network from a single machine on the network.
- On modern networks, traffic can be captured using a network switch with a so-called monitoring port that mirrors all packets that pass through designated ports of the switch.
- On wireless LANs, traffic can be captured on one channel at a time, or by using multiple adapters, on several channels simultaneously.

- When traffic is captured, either the entire contents of packets are recorded, or just the headers are recorded. Recording just headers reduces storage requirements, and avoids some legal issues, yet often provides sufficient information to diagnose problems.
- Captured information is decoded from raw digital form into a human-readable format that lets users easily review exchanged information. Protocol analyzers vary in their abilities to display and analyze data.
- Some protocol analyzers can also generate traffic and thus act as the reference device.
- Protocol analyzers can also be hardware-based, either in probe format or, as is increasingly common, combined with a disk array. These devices record packets (or a slice of the packet) to a disk array.

Uses:

Packet sniffers can:

- Analyze network problems
- Detect network misuse by internal and external users
- Monitor WAN bandwidth utilization
- Gather and report network statistics



Notable packet analyzers

- Wireshark formerly known as Ethereal)
- ngrep, Network Grep
- Fiddler

Wireshark

- Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format.
- Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.
- Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

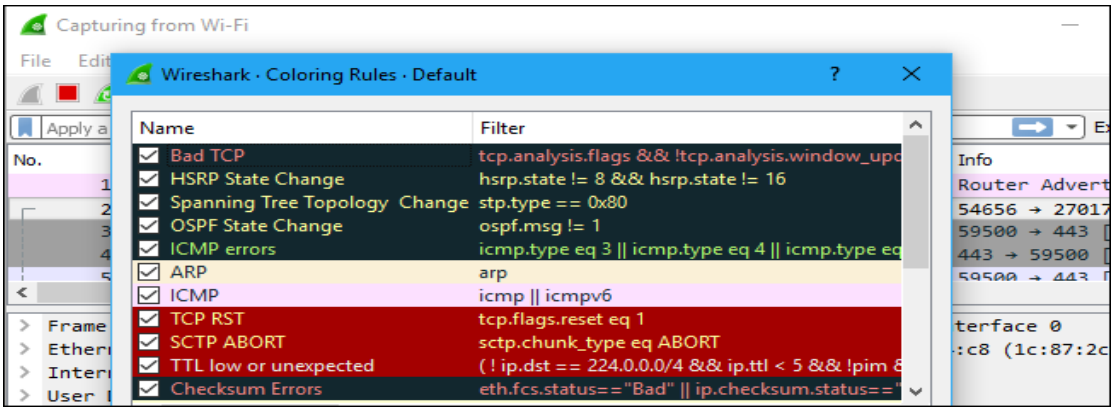
Features

Wireshark i s a d ata c apturing p rogram t hat " understands" t he s tructure (encapsulation) of d ifferent networking protocols.

- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Data display can be refined using a display filter.
- Wireless connections can also be filtered as long as they traverse the monitored Ethernet.
- Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic

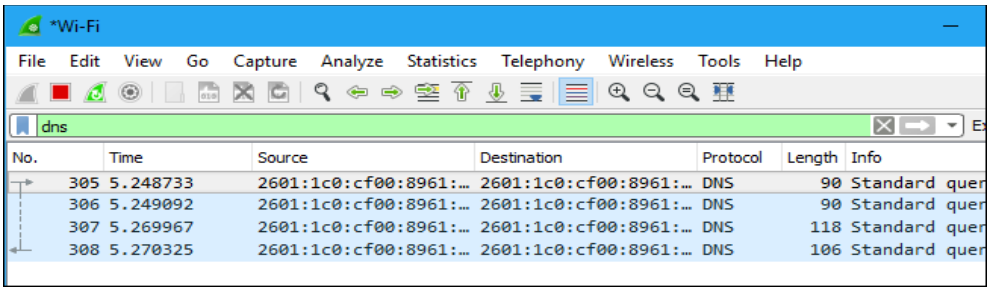
Color Coding

It probably can see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. ***By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.***

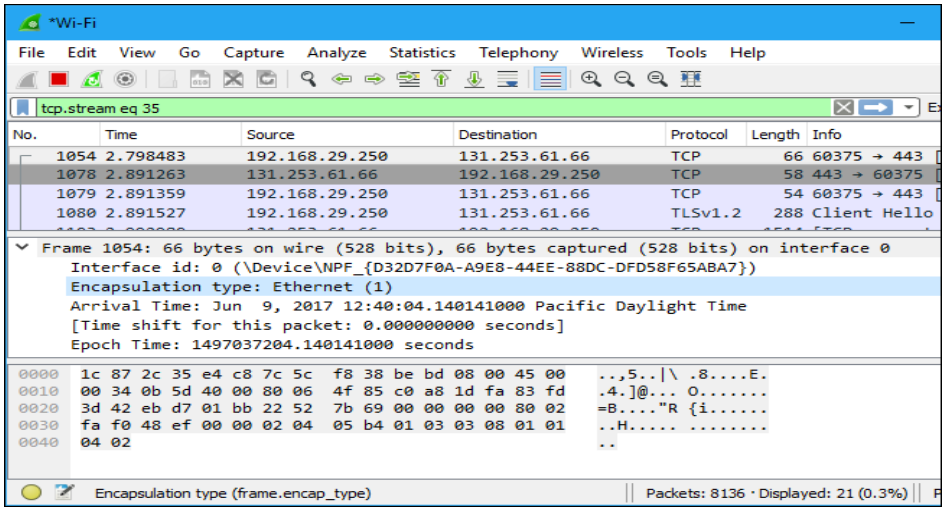


Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.



Inspecting Packets



S.No.	Contents	Check it (if Difficult)	Page	Spend Time in Hour
6.1	Functions of Application layer			1
6.2	Application Layer Protocols: DNS, DHCP, WWW, HTTP, HTTPs, TELNET, FTP, SMTP, POP, IMAP			2
6.3	Concept of traffic analyzer: MRTG, PRTG, SNMP. Packet tracer, Wireshark.			2

INSPIRING LEARNING QUOTES

"NOTHING WILL WORK UNLESS YOU DO."

Don't be judgmental towards anyone, including yourself.

"YESTERDAY I WAS CLEVER, SO I CHANGED THE WORLD. TODAY I AM WISE, SO I AM CHANGING MYSELF."

"NEVER GIVE UP ON A DREAM JUST BECAUSE OF THE TIME IT WILL TAKE TO ACCOMPLISH IT. THE TIME WILL PASS ANYWAY."

"TELL ME AND I FORGET. TEACH ME AND I REMEMBER. INVOLVE ME AND I LEARN."

Ask yourself: how is this changing me?

Answer own Innovation, Creativity & Tinkering.

address aggregation	address space	choke packet	classful addressing
classless addressing	classless interdomain routing (CIDR)	closed-loop congestion control	Dynamic Host Configuration Protocol (DHCP)
longest mask matching	magic cookie	network address	Network Address Translation (NAT)
open-loop congestion control	packetizing		
care-of address	collocated care-of address	double crossing	foreign agent
foreign network	fragmentation	home address	home agent
home network	Internet Control Message Protocol version 4	(ICMPv4)	mobile host
stationary host	triangle routing	…….	……..
autonomous system (AS)	Bellman-Ford	Border Gateway Protocol version 4 (BGP4)	Dijkstra's algorithm
distance vector	distance-vector (DV) routing	flooding	least-cost tree
link-state database (LSDB)	link-state (LS) routing	Open Shortest Path First (OSPF)	path-vector (PV) routing
poison reverse	Routing Information Protocol (RIP)	split horizon	Distance Vector Multicast Routing Protocol
(DVMRP)	group-shared tree	Internet Group Management Protocol	(IGMP)
Multicast Open Shortest Path First (MOSPF)	Protocol Independent Multicast (PIM)	Protocol Independent Multicast-dense Mode	(PIM-DM)
Protocol Independent Multicast-Sparse	Mode (PIM-SM)	prune message	reverse path broadcasting (RPB)
reverse path forwarding (RPF)	reverse path multicasting (RPM)	shortest path tree	source-based tree
tunneling	anycast address	authentication	autoconfiguration
colon hexadecimal notation	compatible address	destination option	dual stack
encrypted security payload (ESP)	extension header	fragmentation	header translation
Internet Protocol version 6 (IPv6)	IP new generation (IPng)	link local address	link local block
mapped address	next header	Path MTU Discovery technique	renumbering
tunneling	unique local unicast block	zero compression	……..etc

What is Network Layer?

The main aim of the **Network L ayer** the source-to- destination delivery of a packet across multiple networks (links). Whereas the data link layer oversees the delivery of a packet between two systems on the same network (links), the **network layer** ensures that each packet gets from its source to its final destination.

- It also breaks the messages that have to be sent into packets and to assemble incoming packets into messages for higher levels.
- If two systems are attached to the same network, there is usually no need for a **network layer**.
- However, if two systems are attached connecting devices on the different networks (links), so there is often needed for the **network layer** to complete the source-to-destination delivery of the message.

This figure shows the relationship of the **network layer** to the data link and transport layer,

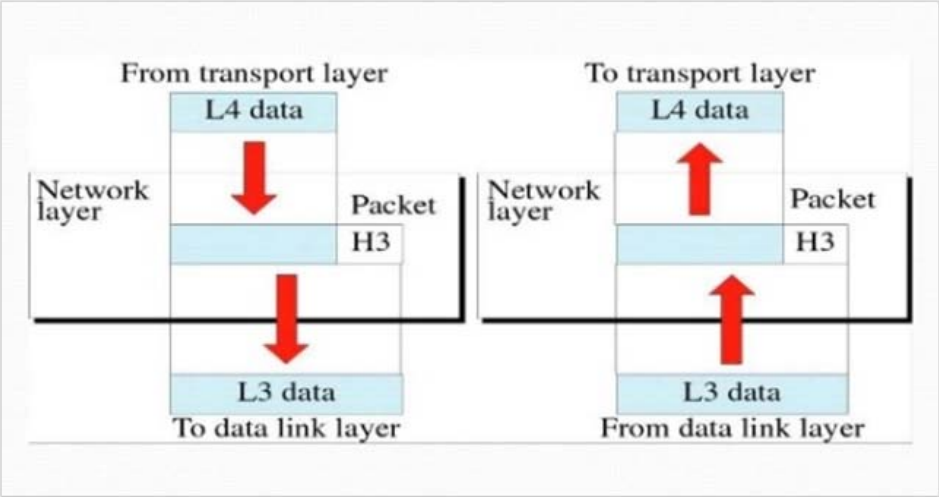


Fig: Network Layer

Design Issues with Network Layer

- A major design issue in the network layer is to determine the packet routing that is how each packet routed from source to destination.
- Routes can be based on static tables and also highly dynamic that is each packet has a predefined route or it can be changed for each packet.
- If there are too many packets are available in the subnet at the particular time, they will get into one another's way, forming bottlenecks.
- The network layer issue is the quality of service provided such as delay, transmit time, jitter, etc.
- When packet travel from one network to another to reach its destination, many problems can arise such as:
    - The addressing being used by two networks may be different from each other.
    - It is necessary to have different protocols.

4.1	Functions of Network Layer		1

The main functions performed by the network layer are:

- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical A ddressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Responsibilities of the Network layer

1. Logical Addressing

- In the internet world, there are two kinds of addressing implemented by the data link layer, it handles addressing problems locally.
- If the network passes through the network boundary, we need another system to distinguish source and destination systems.
- The logical addressing at the network layer while physical addressing at the data link layer is defined by the MAC address of a device, whereas the IP addressing is determined at the network layer of the OSI model. This addressing is also called as logical addressing.
- The network layer adds a header to the packet which is coming from the upper layer includes the logical addresses of the sender and receiver.

2. Routing

- When two independent networks or links are attached to create an internetwork that is the network of networks or a large network, the connecting devices route the packets to its destination.
- The forwarding of the data request to servers is known as routing.

3. Fragmentation and Reassembly

- The network layer must send data down to the data link layer for transmission. The data or information that the network layer receives is in the form of a packet and the data that data link layer forwards is called a frame.

- The network layer has the responsibility of Fragmentation and reassembly because some data link layer technologies have limits on the length of any message that can be sent.
- If the packet of data that the network layer has to send is too large, the network layer must break the packet up, send each packet to the data link layer, and then have pieces reassembled once they arrive at the network layer on the destination system.

Example:

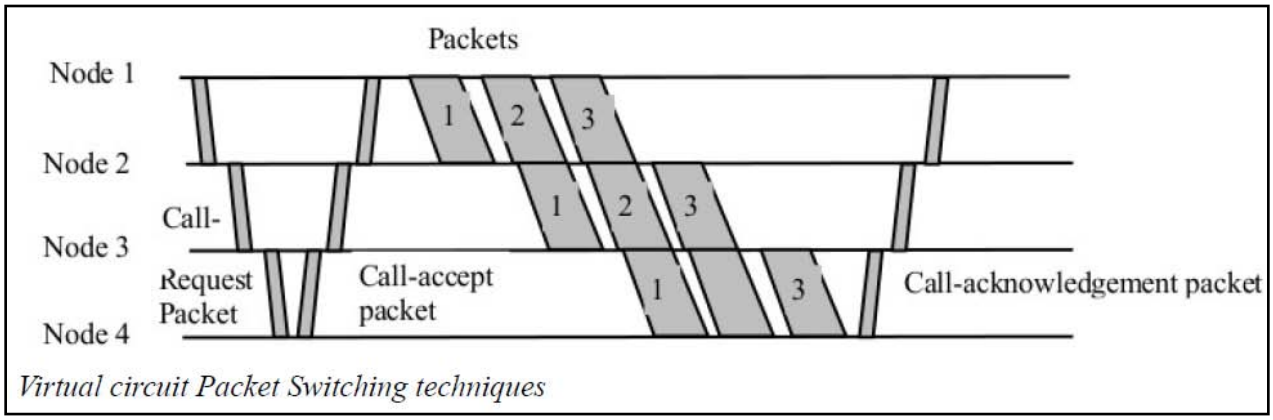
- If I want to access some data from Facebook then I will open my laptop, type URL of Facebook and send an HTTP request to facebook.com for some data.
- Since the server of Facebook is situated outside my local area network, my request is forwarded to Facebook through the default gateway or router of my institution.

4.2 Virtual circuits and Datagram Subnets | | 1

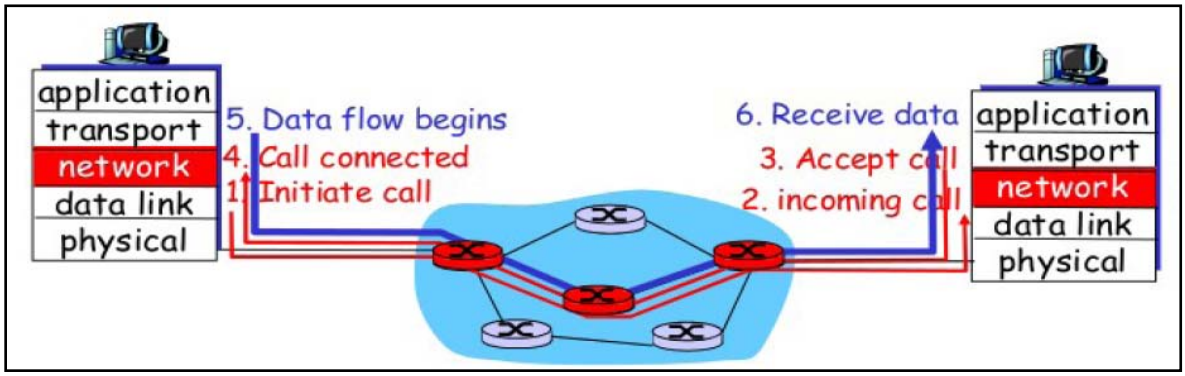
Sno	Datagram Packet Switching	Virtual-circuit Packet Switching
1	Two packets of the same user pair can travel along different routes.	All packets of the same virtual circuit travel along the same path.
2	The packets can arrive out of sequence.	Packet sequencing is guaranteed.
3	Packets contain full Src,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

Virtual Circuit:

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



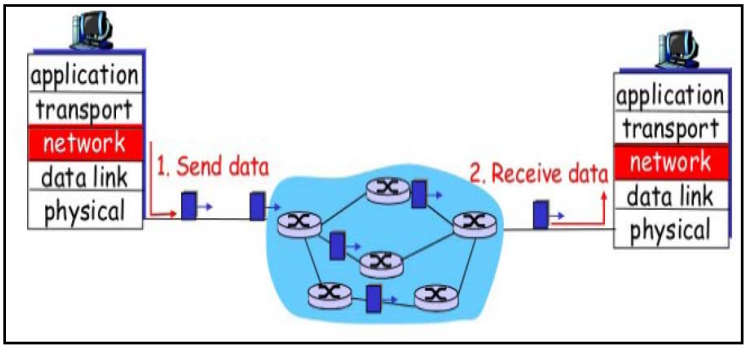
Virtual circuit Packet Switching techniques

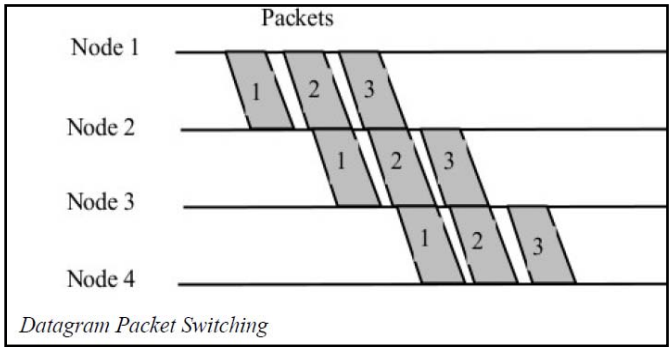


Virtual Circuit

Datagram:

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





Datagram Packet Switching

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

4.3	IPv4 Addresses: Address Space, Notations, Classful addressing, Classless addressing, Subnetting and Network Address Translation(NAT)		1

IPv4 Addresses

- An IPv4 address is 32 bits long
- The IPv4 addresses are unique and universal
- IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296(Maximum available theoretically)

1.1 Address Space is divided into three classes:

Class A—10.0.0.0/8 network block	10.0.0.0 – 010.255.255.255
Class B—172.16.0.0/12 network block	172.16.0.0 – 172.31.255.255
Class C—192.168.0.0/16 network block	192.168.0.0– 192.168.255.255

1.2 IPv4 have 2 types of notations:

1. Doted decimal notations

Denoted in decimal format each byte is separated by dot eg: 117.149.29.2

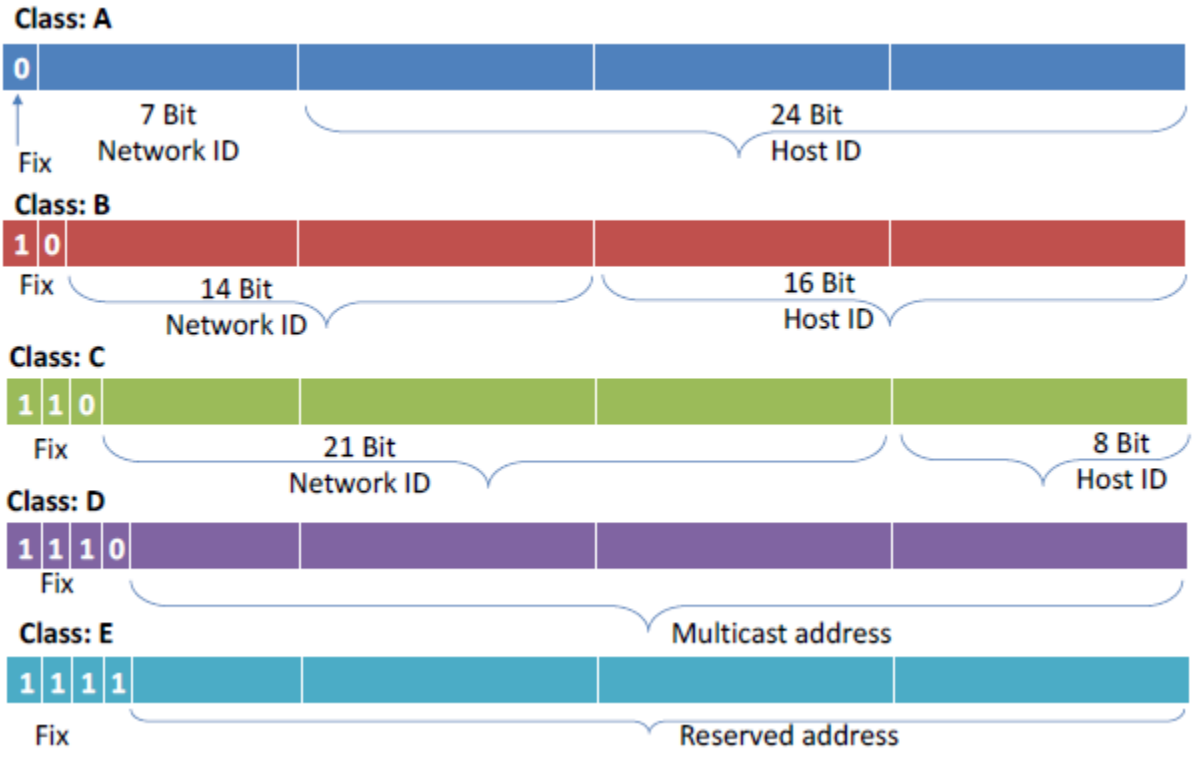
Mostly used by human configurations

2. Binary notation

In binary format eg: 01110101 10010101 00011101 00000010

- Mostly used by devices for processing.

1.3 Classful Addressing (Classification of IP Addresses)



1.4 Classless Addressing

• There is no classes hierarchy in the IP address but address is still granted in blocks.

Restriction

• 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.

1.4.1 Subnetting

• Subnetting means creating subnetwork
• Subnetting means increasing networks bits(i.e. 1s) in subnet mask
• If network bit is increased host bits will be decreased, so number of host will be decreased
• A Class A network have 8 bits for network (224 IP address available) if you wanted smaller block IP from class A increase the network bits /decreasing host bits

1.4.2. Supernetting

• Supernetting means creating bigger network from smaller one
• Supernetting means decreasing networks bits(i.e. 1s) in subnet mask
• If network bit is decreased host bits will be increased, so number of host will be decreased
• A Class C network have 24 bits for network (28 IP address available) if you wanted bigger block IP from class C decrease the network bits / increasing host bits
• Supernetting just opposite of subnetting

1.4.3. VLSM (Variable Length Subnet Mask)

• Subnetting and supernetting is achieved by varying default subnet mask
• Usually in classful IP address have 8,16,24 default CIDR values for Class A, B, C respectively, but in classless IP no default CIDR value / subnet mask is available CIDR value may be varying

1.4.4. Subnetting/supernetting Steps

• Identify needed block size (always in power of 2 i.e. 22 , 23 , 24 , … 231)
• If multiple block size is needed assign largest block first
• Find the host bits from block size (if block size $2n$ no of host bit is n)
• From host bits find the CIDR (CIDR=32-n)
• Find subnet mask convert CIDR into doted decimal format
(ex:255.255.240.0)
• Find wild card mask (255.255.255.255 - 255.255.240.0= 0.0.15.255)
• Add the first IP in the range to get last IP address

1.3 Network Address Translation(NAT)

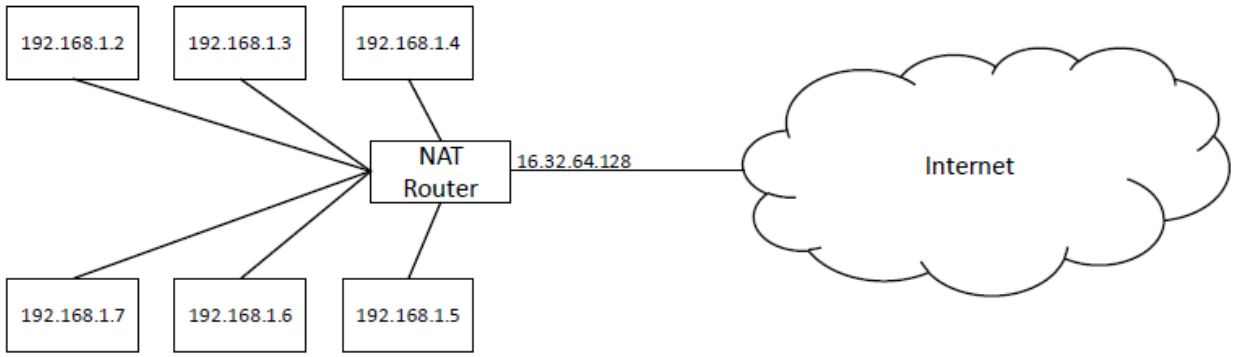
• IP address have public range and private range
• Public range is used for communication in internet and can used only with permission of internet authorities
• Private IP can be used for local communication without permission of Internet authorities

Answer own Innovation, Creativity & Tinkering.

Given below table shows private ranges of class A,B,C

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}

- Public IP should be unique globally
- Private IP should be unique inside a organization, not globally
- NAT router consist of public IP in exit interface and internal interface consist of Private IPs



Address Translation : Replace outgoing packets Source IP address as NAT router public IP and replaces incoming packet Destination IP with private (Private to public and public to private)

- Translation is done with help of translation table which consist of IP address of private range and public range and port address

Below table showing Translation table in NAT

Private Address	Private Port	External Address	External Port	Transport Protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
.. .	.. .	...	.. .	...

1.6. Limitations of IPv4

- Exponential growth of the Internet and the impending exhaustion of the IPv4 address space
- Need for simpler configuration
- Requirement for security at the IP level
- Need for better support for prioritized and real-time delivery of data

4.4	IPv4 Datagram format and fragmentation		1

IPv4 Datagram Header

IPv4 is a ***connectionless*** protocol for a packet- switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination.

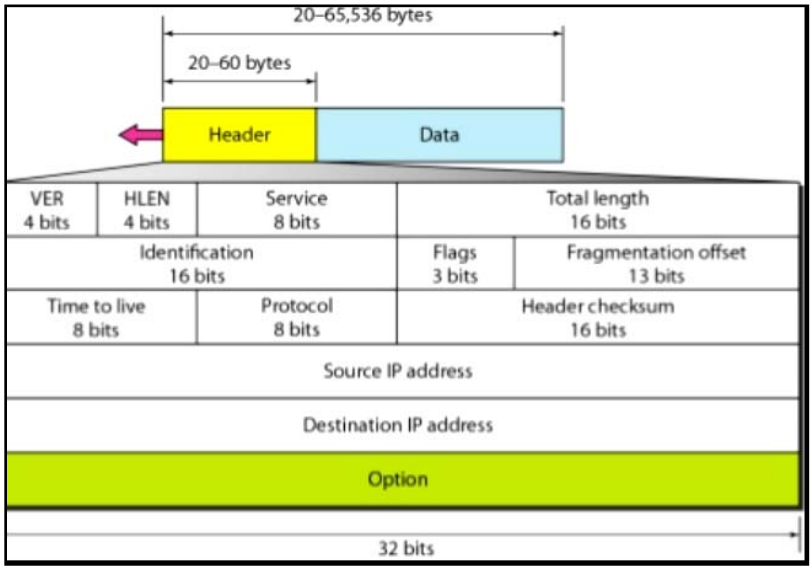


Figure: IPv4 Datagram Format

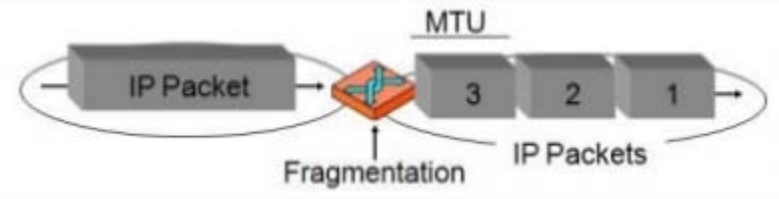
Packets in the IPv4 layer are called datagrams. A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing.

- **Version (VER):** This 4-bit field defines the version of the IPv4 protocol. Currently, the version is 4. However, version 6 (or IPng) may totally replace version 4 in the future.
- **Header l ength (HLEN):** This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
- **Services:** IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.
- **Type of service:** Low Delay, High Throughput, Reliability (8 bits)
- **Total L ength:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes
- **Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)
- **Flags:** 3 flags of 1 bit each: reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

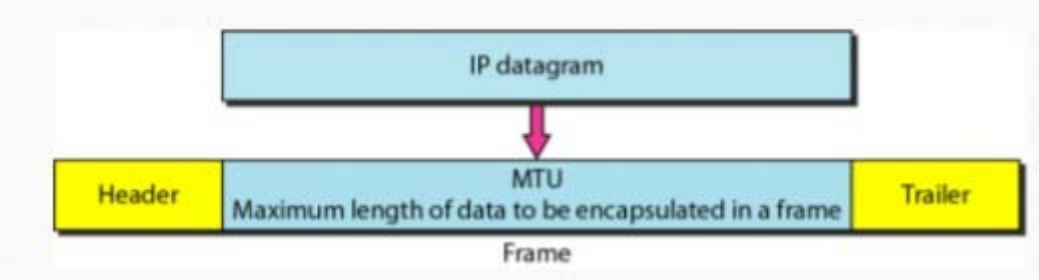
- **Fragment Offset:** Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes
- **Time to live:** Datagram's lifetime (8 bits), It prevents the datagram to loop in the network
- **Protocol:** Name of the protocol to which the data is to be passed (8 bits)
- **Header Checksum:** 16 bits header checksum for checking errors in the datagram header
- **Source IP address:** 32 bits IP address of the sender
- **Destination IP address:** 32 bits IP address of the receiver
- **Option:** Optional information such as source route. Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

Fragmentation

- ✓ Data field of a large IP packet is fragmented.
- ✓ The fragments are sent into a series of smaller IP packets fitting a network's MTU.
- ✓ Fragmentation is done by routers
- ✓ Fragmentation may be done multiple times along the route.
- ✓ If IP packet is longer than the MTU, the router breaks packet into smaller packets.
- ✓ Called IP fragments.
- ✓ Fragments are still IP packets.



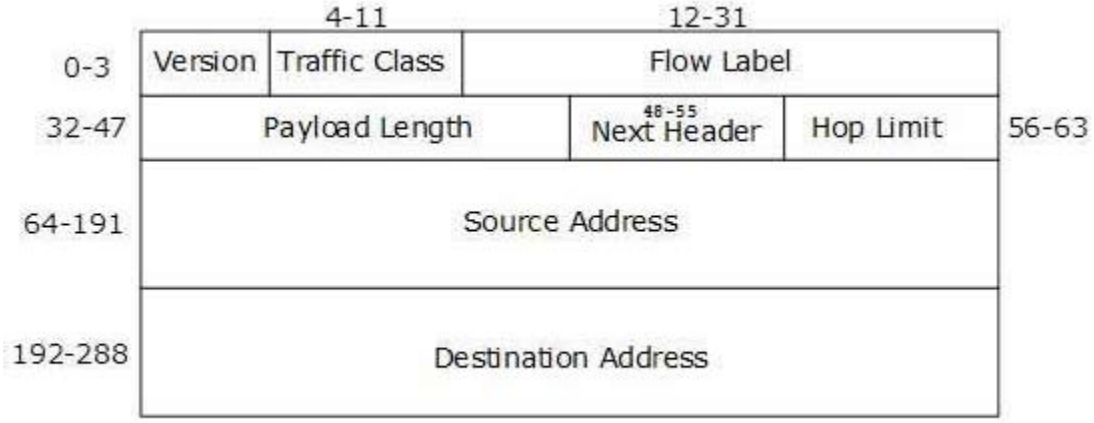
- ✓ Maximum Transfer Unit (MTU)
- ✓ Each data link layer protocol has its own frame format in most protocols.
- ✓ One of the fields defined in the format is the maximum size of the data field.
- ✓ In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size.
- ✓ A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet.
- ✓ In a case where a router receives a protocol data unit (PDU) larger than the next hop's MTU.
- ✓ It has two options if the transport is IPv4: drop the PDU and send an ICMP message which indicates the condition Packet too Big, or fragment the IP packet and send it over the link with a smaller MTU.



The value of the MTU depends on the physical network protocol.

4.5 IPv6 Address Structure and advantages over IPv4 | 1

- The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4.
- IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers.
- All the necessary information that is essential for a router is kept in the Fixed Header.
- The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.



[*Image: IPv6 Fixed Header*]

IPv6 fixed header is 40 bytes long and contains the following information.

S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow L abel** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.

4	**Payload L ength** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next H eader** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop L imit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination A ddress** (128-bits): This field provides the address of intended recipient of the packet.

Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.

For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ***':'*** symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:

Rule.1: Discard leading Zero(es):

In Block 5, 0063, ***the leading two 0s*** can be omitted, such as (5th block):

2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double ***colon sign ::,*** such as (6th and 7th block):

2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced ***only on ce by :*** so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

2001:0:3238:DFE1:63::FEFB

Advantages over IPv4

Feature	IPv4	IPv6
Address length	32 bits	128 bits
IPSec support	Optional	Required
QoS support	Some	Better
Fragmentation	Hosts and routers	Hosts only
Packet size	576 bytes	1280 bytes
Checksum in header	Yes	No
Options in header	Yes	No
Link-layer address resolution	ARP (broadcast)	ARP (Group)
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router Discovery	Optional	Required
Uses broadcasts	Yes	No
Configuration	Manual, DHCP	Automatic, DHCP
DNS name queries	Uses A records	Uses AAAA
recordsDNS reverse queries	Uses IN-ADDR.ARPA	Uses IP6.INT

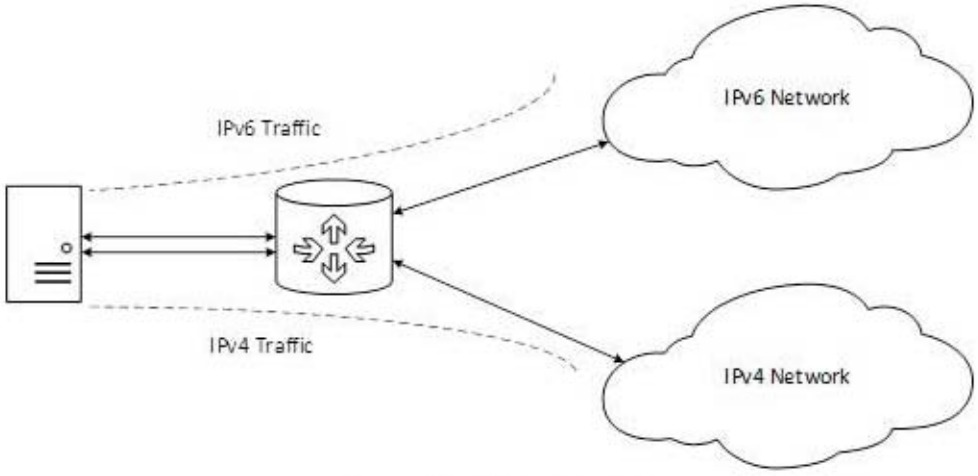
Transition From IPv4 to IPv6

Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible.

To overcome this short-coming, we have a few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6.

Dual Stack Routers

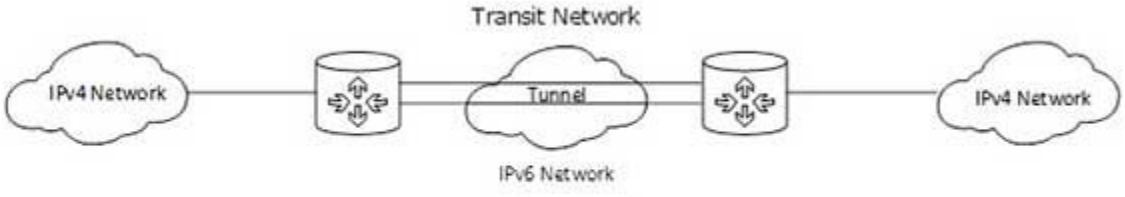
A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.



[Image: Dual Stack Router]

Tunneling

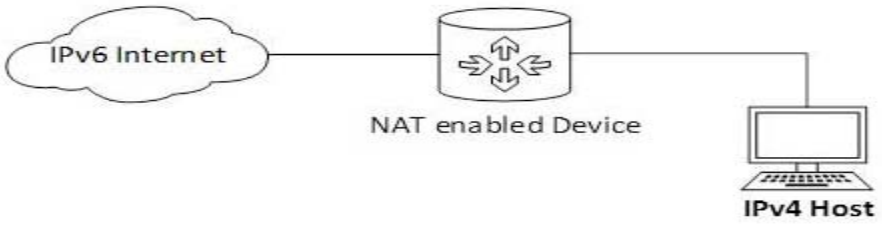
In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through a non-supported IP version.



[*Image: Tunneling*]

NAT Protocol Translation

This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa.



[*Image: NAT - Protocol Translation*]

Difference between IPv4 and IPv6

IPv4	IPv6
• IPv4 addresses are 32 bit length.	• IPv6 addresses are 128 bit length.
• Fragmentation is done by sender and forwarding routers.	• Fragmentation is done only by sender.
• No packet flow identification.	• Packet flow identification is available within the IPv6 header using the Flow Label field.
• Checksum field is available in header	• No checksum field in header.
• Options fields are available in header.	• No option fields, but Extension headers are available.
• Address Resolution Protocol (ARP)is available to map IPv4 addresses to MAC addresses.	• Address Resolution Protocol (ARP) is replaced with Neighbour Discovery Protocol.
• Broadcast messages are available.	• Broadcast messages are not available.
• Manual configuration (Static) of IP addresses or DHCP (Dynamic configuration) is required to configure IP addresses.	• Auto-configuration of addresses is available.

4.6	Routing Algorithms: Distance Vector Routing, Link State Routing		1

Routing algorithm

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm

1. Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
- **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

2. **Non-Adaptive Routing algorithm**

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

Random w alks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

Distance Vector Routing Algorithm

- **The Distance vector algorithm is iterative, asynchronous and distributed.**
  - **Distributed:** It is distributed in that each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
  - **Iterative:** It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
  - **Asynchronous:** It does not require that all of its nodes operate in the lock step with each other.
- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as **Vector**.

```
1  Initialization:
2     for all destinations y in N:
3        Dx(y) = c(x,y)    /* if y is not a neighbor then c(x,y) = ∞ */
4     for each neighbor w
5        Dw(y) = ? for all destinations y in N
6     for each neighbor w
7        send distance vector Dx = [Dx(y): y in N] to w
8
9  loop
10    wait (until I see a link cost change to some neighbor w or
11          until I receive a distance vector from some neighbor w)
12
13    for each y in N:
14       Dx(y) = minv{c(x,v) + Dv(y)}
15
16    if Dx(y) changed for any destination y
17       send distance vector Dx = [Dx(y): y in N] to all neighbors
18
19 forever
```

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   - It receives a distance vector from a neighbor containing different information than before.
   - It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y

C(x,v) = Node x knows cost to each neighbor v

Dx = [Dx(y): y ∈ N] = Node x maintains distance vector

Node x also maintains its neighbors' distance vectors

– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N]

Note –

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:

  $Dx(y) = \min \{ C(x,v) + Dv(y), Dx(y) \}$ for each node $y \in N$

Advantages of Distance Vector routing –

- It is simpler to configure and maintain than link state routing.

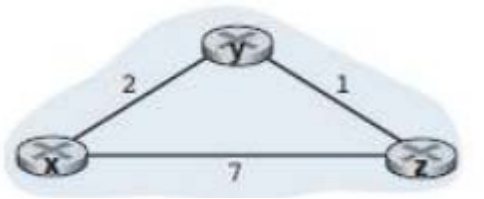
Disadvantages of Distance Vector routing –

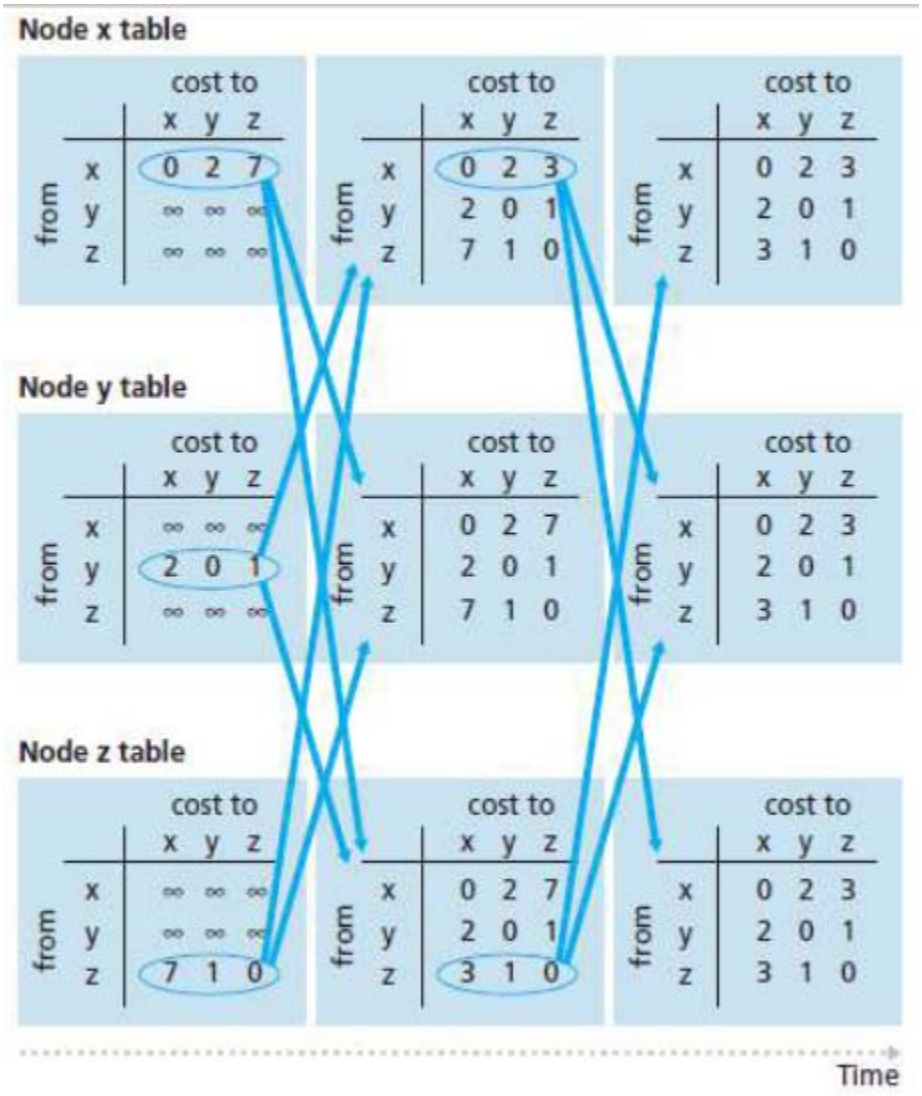
- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

Note – Distance Vector routing uses UDP(User datagram protocol) for transportation.

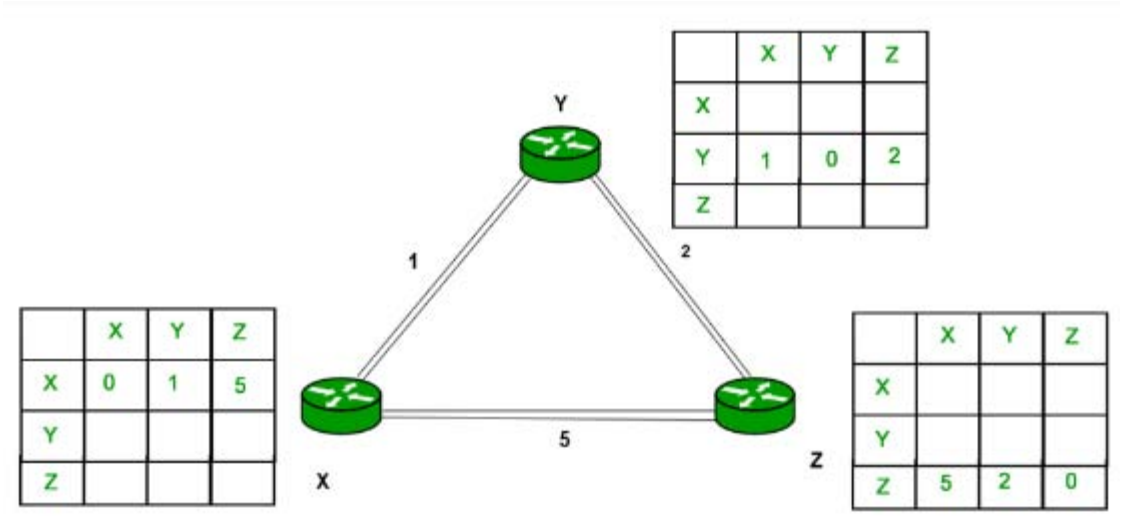
- For example, node x computes

$$D_x(x) = 0$$
$$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\} = \min\{2 + 0, 7 + 1\} = 2$$
$$D_x(z) = \min\{c(x,y) + D_y(z), c(x,z) + D_z(z)\} = \min\{2 + 1, 7 + 0\} = 3$$





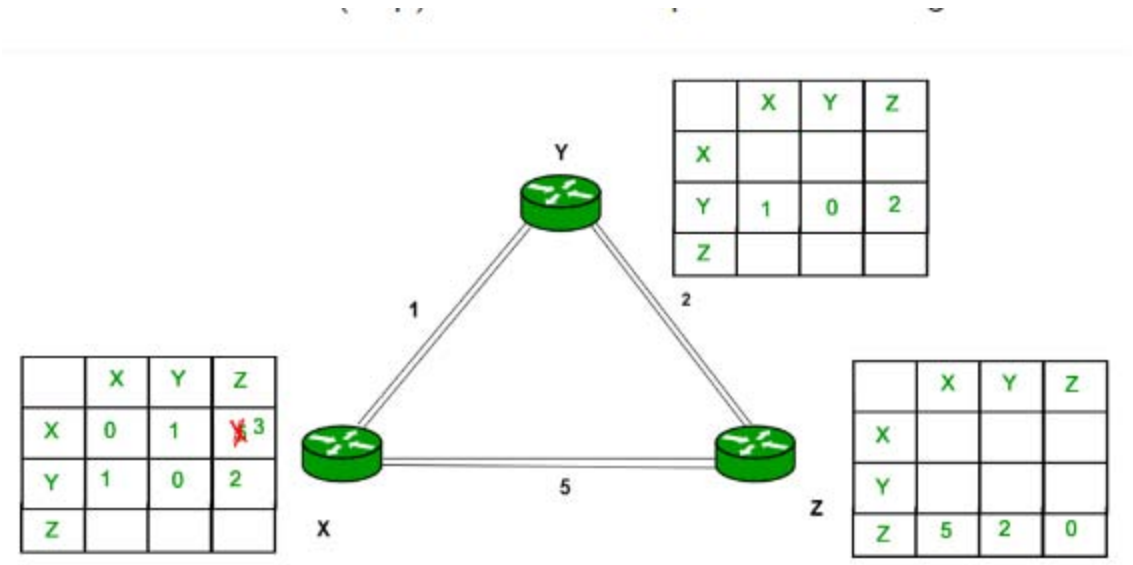
Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



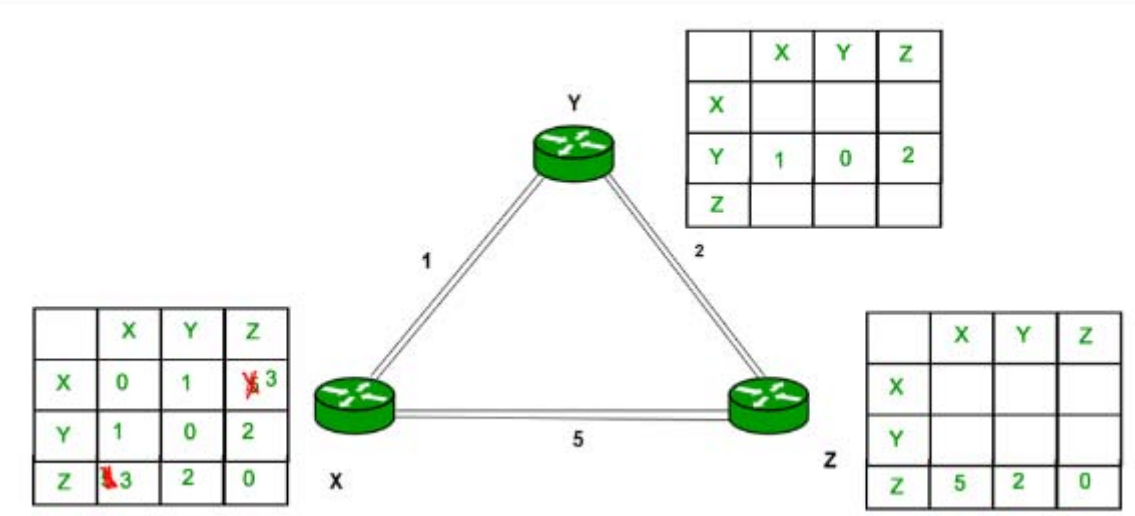
Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

$$Dx(y) = \min \{ C(x,v) + Dv(y)\} \text{ for each node } y \in N$$

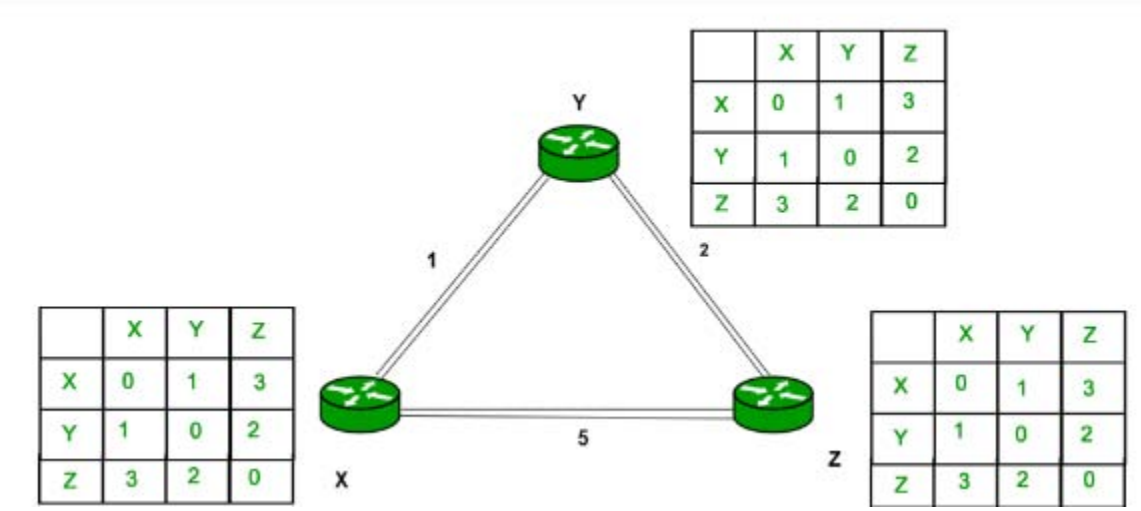
As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



Similarly for Z also –



Finally the routing table for all –



Link State Routing

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

- **Knowledge ab out t he ne ighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- **Information s haring:** A router sends the information to every other router only when the change occurs in the information.

Link State Routing –

Link state routing is the second family of routing protocols. While distance vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using a shortest path computation.

Features of link state routing protocols –

- **Link state packet –** A small packet that contains routing information.
- **Link state database –** A collection information gathered from link state packet.
- **Shortest path first algorithm (Dijkstra algorithm) –** A calculation performed on the database results into shortest path
- **Routing table –** A list of known paths and interfaces.

```
1  Initialization:
2     N' = {u}
3     for all nodes v
4       if v is a neighbor of u
5         then D(v) = c(u,v)
6       else D(v) = ∞
7
8  Loop
9     find w not in N' such that D(w) is a minimum
10    add w to N'
11    update D(v) for each neighbor v of w and not in N':
12          D(v) = min( D(v), D(w) + c(w,v) )
13    /* new cost to v is either old cost to v or known
14     least path cost to w plus cost from w to v */
15 until N'= N
```

Calculation of shortest path –

To find shortest path, each node need to run the famous **Dijkstra algorithm**. This famous algorithm uses the following steps:

- **Step-1:** The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database
- **Step-2:** Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree.The shape of the tree gets changed .
- **Step-3:** After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.
- **Step-4:** The node repeats the Step 2. and Step 3. until all the nodes are added in the tree

Disadvantage:

Heavy traffic is created in Line state routing due to Flooding. Flooding can cause an infinite looping, this problem can be solved by using Time-to-leave field

Distance Vector Protocol	Link state protocol
Entire routing table is sent as an update	Updates are incremental & entire routing table is not sent as update
Distance vector protocol send periodic update at every 30 or 90 second	Updates are triggered not periodic
Update are broadcasted	Updates are multicasted
Updates are sent to directly connected neighbour only	Update are sent to entire network & to just directly connected neighbour
Routers don't have end to end visibility of entire network.	Routers have visibility of entire network of that area only.
It is prone to routing loops	No routing loops

Link State Routing Problem:

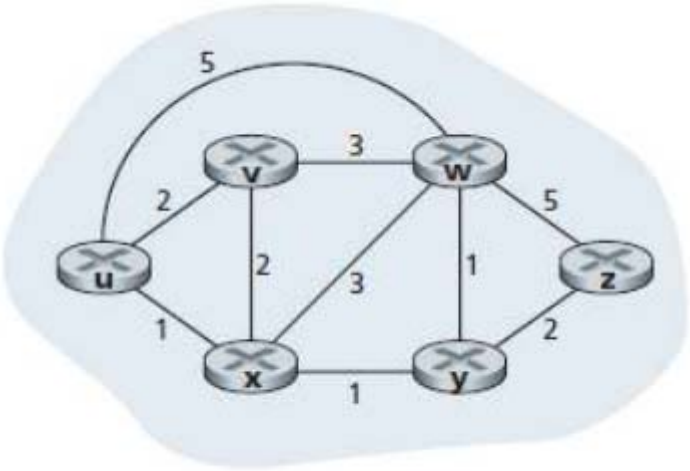


Fig. 13 Abstract graph model of a computer network

- Figure 14. Shows the resulting least-cost paths for u for the network in Figure 13.

step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

Table: Running the link-state algorithm on the network in Figure 13

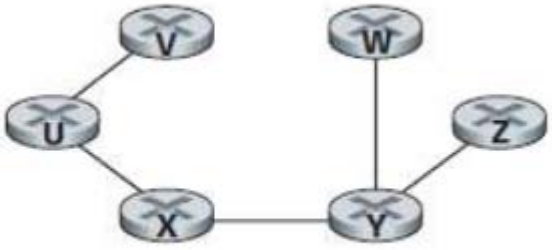


Fig. 14 Least cost path for nodule u

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

4.7	**Internet Control Protocols: ARP, RARP, ICMP**		**1**

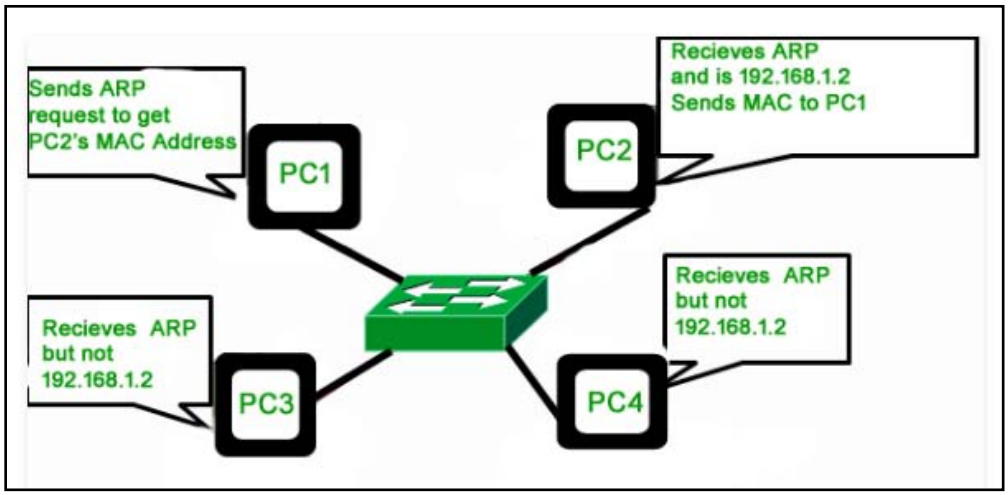
1. Address Resolution Protocol (ARP) –

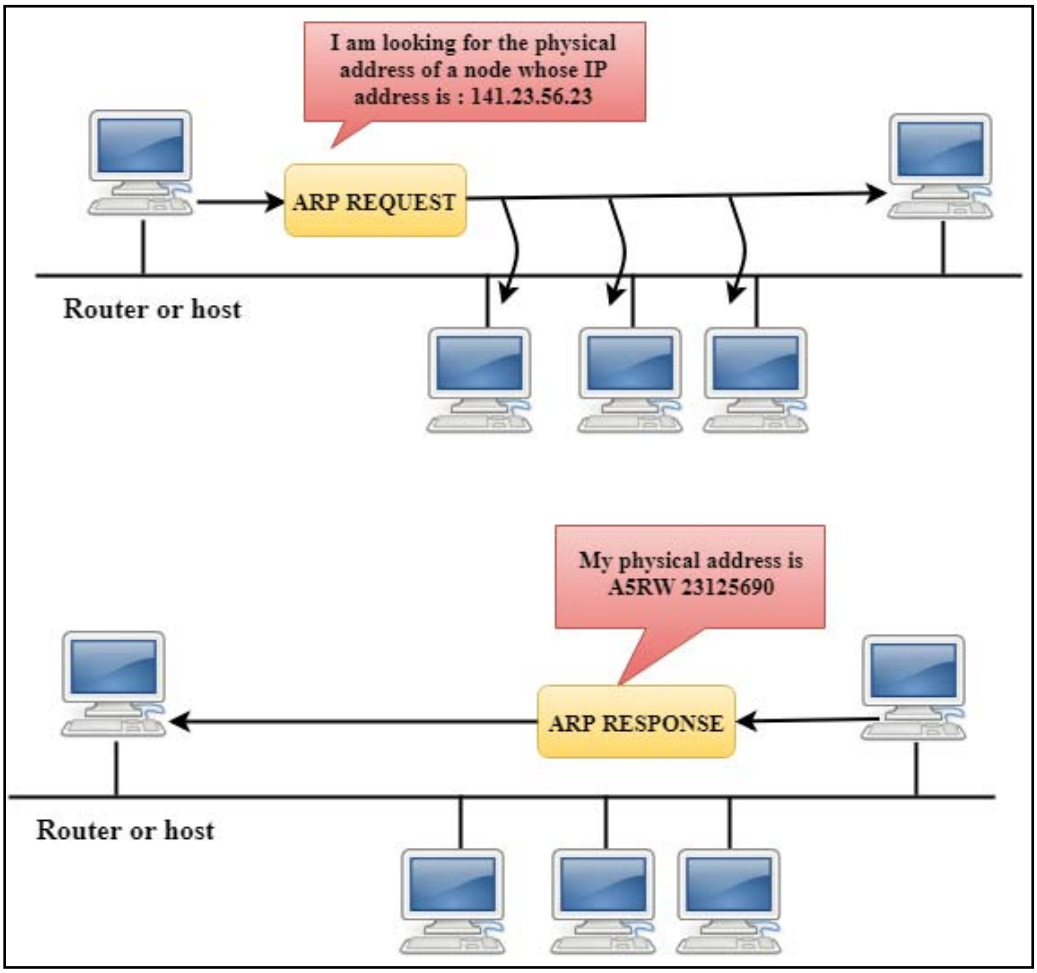
- Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address.
- Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.
- In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine.
- ARP is used to get the physical address (MAC address) of destination machine.

- It is used to associate an IP address with the MAC address.
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

How ARP works:

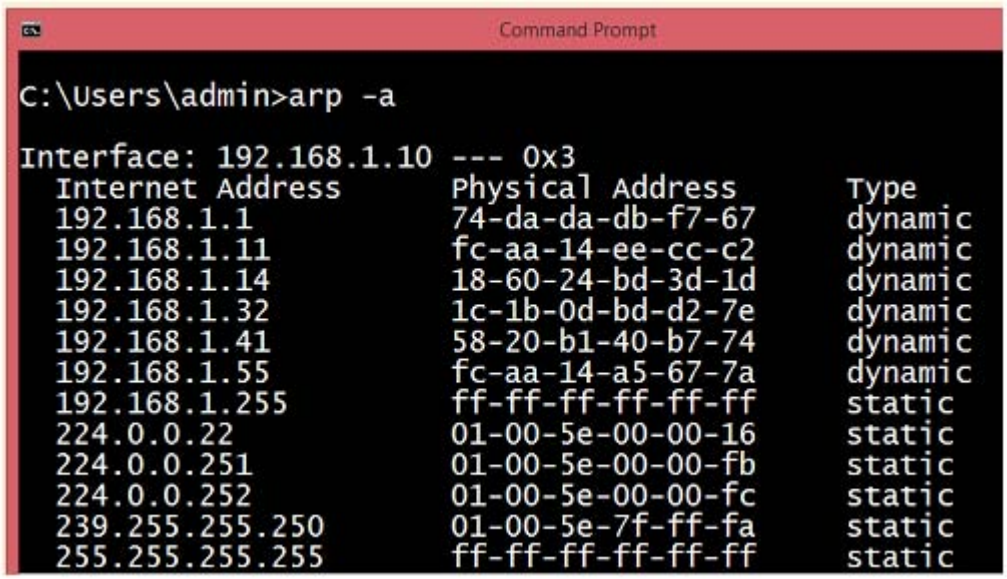
If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address. The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.





Steps taken by ARP protocol

It will check the ARP cache in **CMD** by using a command **arp-a**.



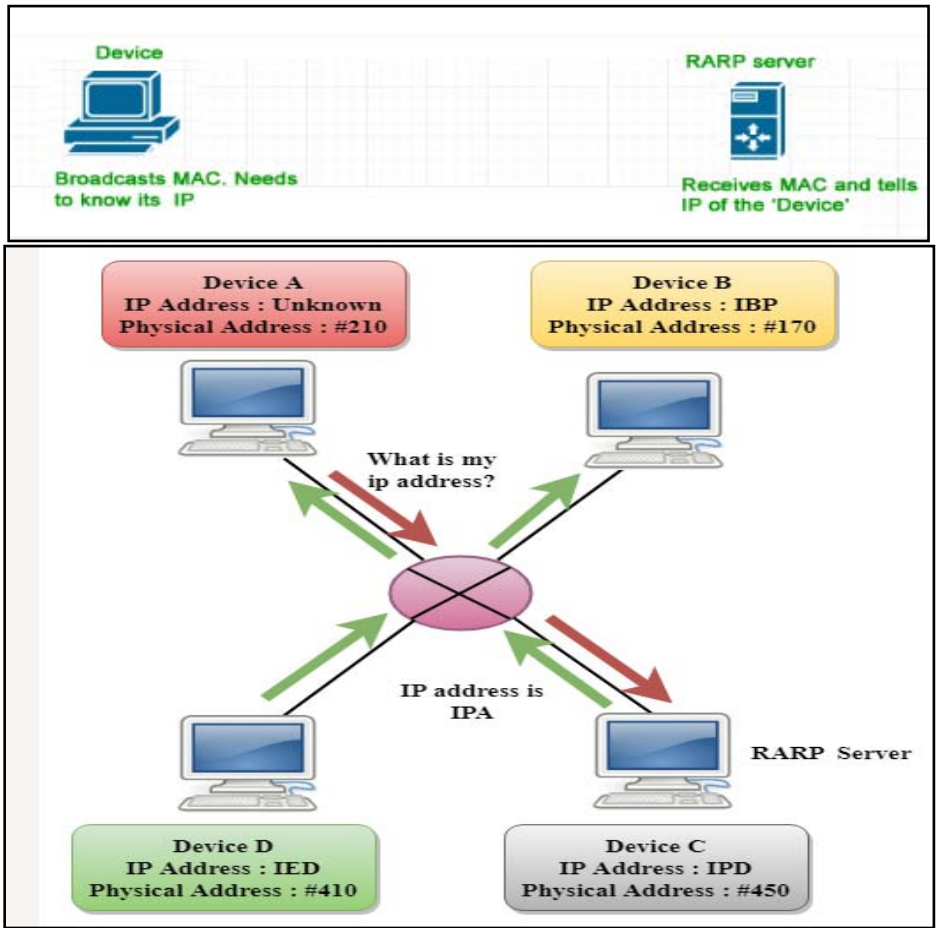
There are two types of ARP entries:

- **Dynamic entry:** It is an entry which is created automatically when the sender broadcast its message to the entire network. Dynamic entries are not permanent, and they are removed periodically.
- **Static entry:** It is an entry where someone manually enters the IP to MAC address association by using the ARP command utility.

2. Reverse Address Resolution Protocol (RARP) –

- Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table.
- The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.
- When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use.
- So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network.
- A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- The protocol which is used to obtain the IP address from a server is known as **Reverse A ddress Resolution Protocol**.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

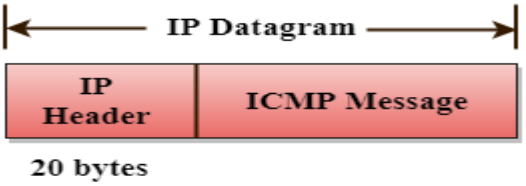


A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

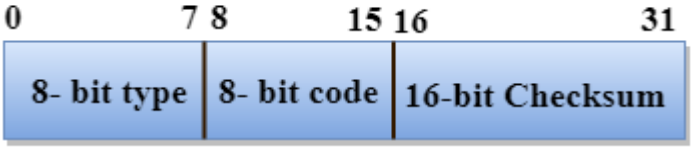
- ***LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.***
- ***RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP(Dynamic Host Configuration Protocol).***

ICMP stands for Internet Control Message Protocol.

- The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
- ICMP uses echo test/reply to check whether the destination is reachable and responding.
- ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
- An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
- ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
- ICMP messages are transmitted within IP datagram.



The Format of an ICMP message

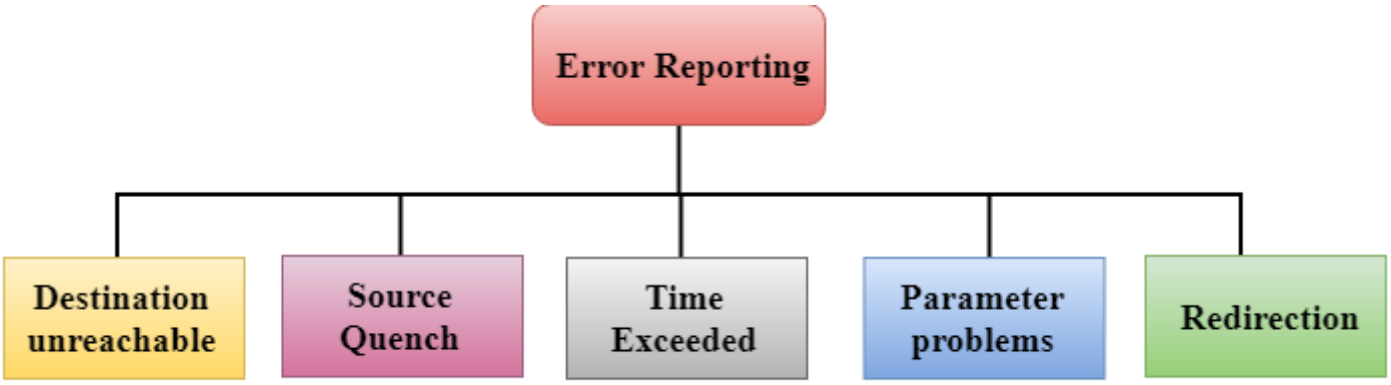


- The first field specifies the type of the message.
- The second field specifies the reason for a particular message type.
- The checksum field covers the entire ICMP message.

Error Reporting

ICMP protocol reports the error messages to the sender.

Five types of errors are handled by the ICMP protocol:



- **Destination u nreachable:** The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable.
- **Source Q uench:** The purpose of the source quench message is congestion control. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate so that the router will be free from congestion.
- **Time E xceeded:** Time Exceeded is also known as "Time-To-Live". It is a parameter that defines how long a packet should live before it would be discarded.

There are two ways when Time Exceeded message can be generated:

- **Parameter problems:** When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.
- **Redirection:** Redirection message is generated when host consists of a small routing table. When the host consists of a limited number of entries due to which it sends the datagram to a wrong router. The router that receives a datagram will forward a datagram to a correct router and also sends the "Redirection message" to the host to update its routing table.

4.8	Routing protocols: OSPF, BGP, Unicast, Multicast and Broadcast		1

Routing protocols:

- Purpose of Routing protocols:
  To determine the path taken by a datagram between source and destination.
- An **autonomous-system (AS)** is a collection of routers under the same administrative control.
- In AS, all routers run the same routing protocol among themselves.

Most common intra-AS routing protocols:

1) Routing-information Protocol (RIP) and

2) Open Shortest Path First (OSPF)

- **Intra-AS** routing protocols are also known as **interior gateway protocols.**

OSPF (Open Shortest Path First)

Open Shortest Path First (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First).

• OSPF is widely used for intra-AS routing in the Internet.
• OSPF is a ***link-state protocol*** that uses
→ flooding(means forward msg.) of link-state information and
→ Dijkstra least-cost path algorithm.
• ***Here is how it works:***
1) A router constructs a complete topological map (a graph) of the entire autonomous-system.
2) Then, the router runs Dijkstra's algorithm to determine a shortest-path tree to all subnets.
3) Finally, the router broadcasts link state info to all other routers in the **autonomous-system(**AS).
Specifically, the router broadcasts link state information
→ periodically at least once every 30 minutes and
→ whenever there is a change in a link's state. For ex: a change in up/down status.
• Individual link costs are configured by the network-administrator.
• OSPF advertisements are contained in OSPF messages that are carried directly by IP.
• HELLO message can be used to check whether the links are operational.
• The router can also obtain a neighboring router's database of network-wide link state.

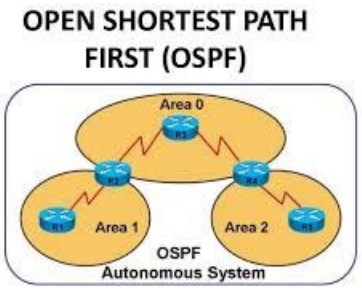
• Some of the advanced features include:

1) Security

➢ Exchanges between OSPF routers can be authenticated.
➢ With authentication, only trusted routers can participate within an AS.
➢ By default, OSPF packets between routers are not authenticated.
➢ Two types of authentication can be configured: 1) Simple and 2) MD5.

i) Simple Authentication

¤ The same password is configured on each router.
¤ Clearly, simple authentication is not very secure.



ii) MD5 Authentication

¤ This is based on shared secret keys that are configured in all the routers.

¤ Here is how it works:

1) The sending router

→ computes a MD5 hash on the content of packet

→ includes the resulting hash value in the packet and

→ sends the packet

2) The receiving router

→ computes an MD5 hash of the packet

→ compares computed-hash value with the hash value carried in packet and

→ verifies the packet's authenticity

2) Multiple Same Cost Paths

➢ When multiple paths to a destination have same cost, OSPF allows multiple paths to be used.

3) Integrated Support for Unicast & Multicast Routing

➢ Multicast OSPF (MOSPF) provides simple extensions to OSPF to provide for multicast-routing.

➢ MOSPF

→ uses the existing OSPF link database and

→ adds a new type of link-state advertisement to the existing broadcast mechanism.

4) Support for Hierarchy within a Single Routing Domain

➢ An autonomous-system can be configured hierarchically into areas.

➢ In area, an area-border-router is responsible for routing packets outside the area.

➢ Exactly one OSPF area in the AS is configured to be the backbone-area.

➢ The primary role of the backbone-area is to route traffic between the other areas in the AS.

Border Gateway Protocol (**BGP):**

Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes.

The protocol can connect together any internetwork of autonomous system using an arbitrary topology.

• BGP is widely used for inter-AS routing in the Internet.

• Using BGP, each AS can

1) Obtain subnet reachability-information from neighboring ASs.

2) Propagate the reachability-information to all routers internal to the AS.

3) Determine good routes to subnets based on i) reachability-information and ii) AS policy.

• Using BGP, each subnet can advertise its existence to the rest of the Internet.

Basics

• Pairs of routers exchange routing-information over semi-permanent TCP connections using port-179.

• One TCP connection is used to connect 2 routers in 2 different autonomous-systems.

Semi permanent TCP connection is used to connect among routers within an autonomous-system.

• Two routers at the end of each connection are called peers.

The messages sent over the connection is called a session.

• Two types of session:

1) External BGP (eBGP) session

- This refers to a session that spans 2 autonomous systems.

2) Internal BGP (iBGP) session

- This refers to a session between routers in the same AS.

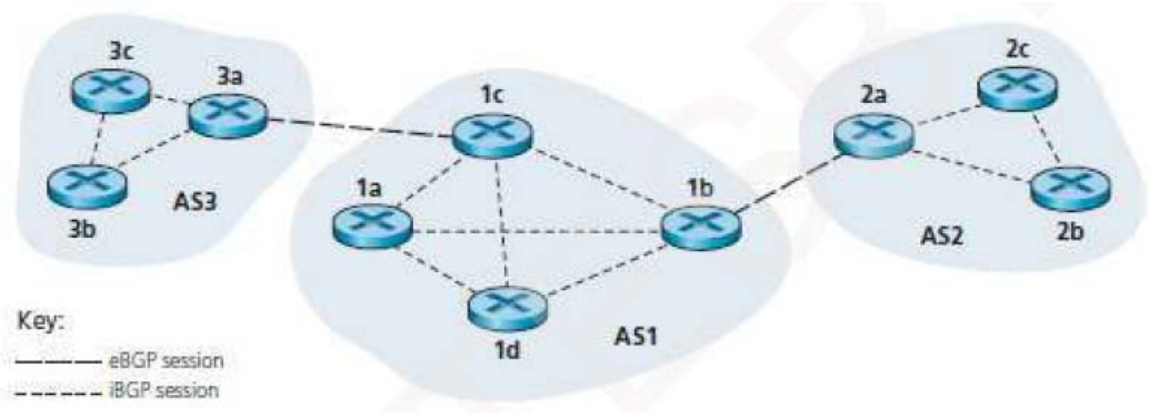


Figure: eBGP and iBGP sessions

- BGP operation is shown in above Figure
- The destinations are not hosts but instead are CIDR prefixes.
- Each prefix represents a subnet or a collection of subnets.

BGP Route Information Management Functions:

- **Route Storage:**
  Each BGP stores information about how to reach other networks.
- **Route Update:**
  In this task, Special techniques are used to determine when and how to use the information received from peers to properly update the routes.
- **Route Selection:**
  Each BGP uses the information in its route databases to select good routes to each network on the internet network.
- **Route advertisement:**
  Each BGP speaker regularly tells its peer what is knows about various networks and methods to reach them.

Path Attributes & Routes

- Two important attributes: 1) AS-PATH and 2) NEXT-HOP

1) AS-PATH

- This attribute contains the ASs through which the advertisement for the prefix has passed.
- When a prefix is passed into an AS, the AS adds its ASN to the ASPATH attribute.
- Routers use the AS-PATH attribute to detect and prevent looping advertisements.
- Routers also use the AS-PATH attribute in choosing among multiple paths to the same prefix.

2) NEXT-HOP

- This attribute provides the critical link between the inter-AS and intra-AS routing protocols.

☐ This attribute is the router-interface that begins the AS-PATH.

- BGP also includes
  - → attributes which allow routers to assign preference-metrics to the routes.
  - → attributes which indicate how the prefix was inserted into BGP at the origin AS.
- When a gateway-router receives a route-advertisement, the gateway-router decides
  - → whether to accept or filter the route and
  - → whether to set certain attributes such as the router preference metrics.

Route Selection

- For 2 or more routes to the same prefix, the following elimination-rules are invoked sequentially:
  1) Routes are assigned a local preference value as one of their attributes.
  2) The local preference of a route
     - → will be set by the router or
     - → will be learned by another router in the same AS.
  3) From the remaining routes, the route with the shortest AS-PATH is selected.
  4) From the remaining routes, the route with the closest NEXT-HOP router is selected.
  5) If more than one route still remains, the router uses BGP identifiers to select the route.

Routing Policy

- Routing policy is illustrated as shown in Figure 3.30.
- Let A, B, C, W, X & Y = six interconnected autonomous-systems.
  - W, X & Y = three stub-networks.
  - A, B & C = three backbone provider networks.
- All traffic entering a stub-network must be destined for that network.

All traffic leaving a stub-network must have originated in that network.

- Clearly, W and Y are stub-networks.
- X is a multihomed stub-network, since X is connected to the rest of the n/w via 2 different providers
- X itself must be the source/destination of all traffic leaving/entering X.
- X will function as a stub-network if X has no paths to other destinations except itself.
- There are currently no official standards that govern how backbone ISPs route among themselves.

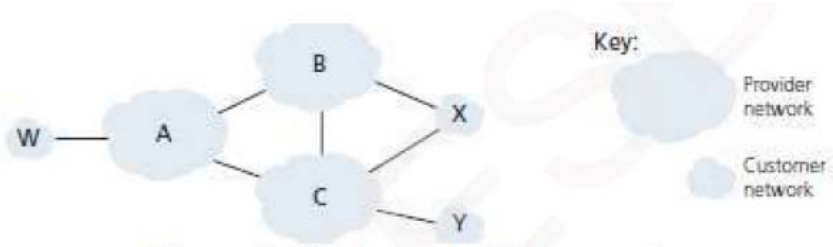
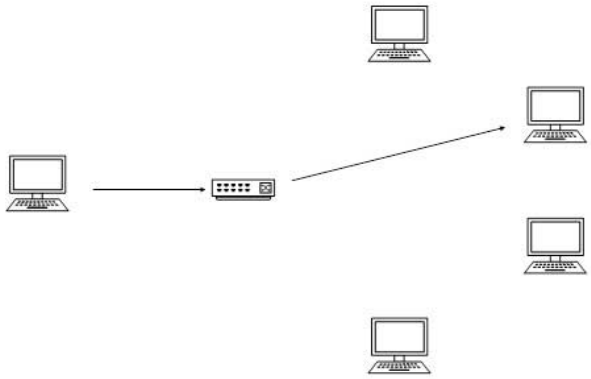


Figure 3.30: A simple BGP scenario

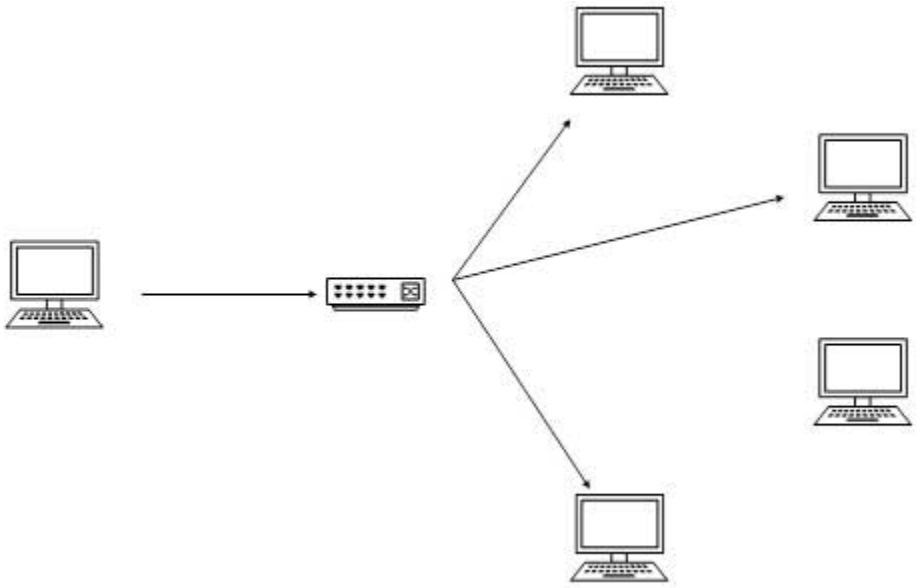
Unicast

In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment.When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host.



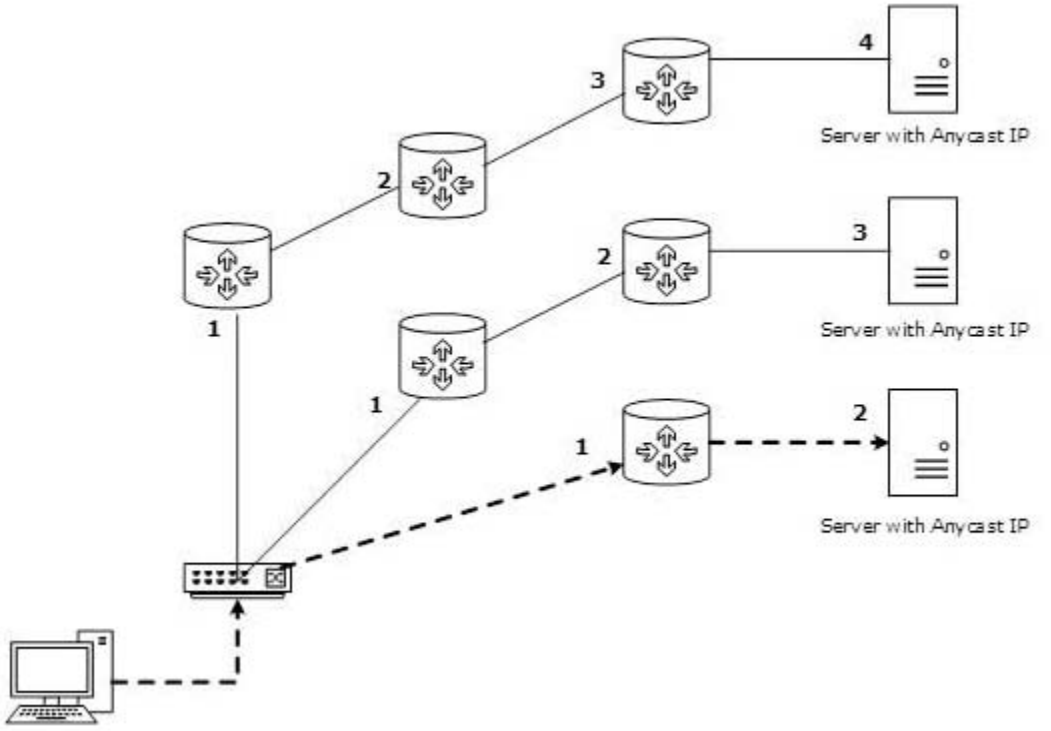
Multicast

The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All the hosts interested in that multicast information, need to join that multicast group first. All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information. ***Hence the router just has to look up the routing table and forward the packet to next hop.***



Anycast

IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.



Let's take an example of Tu.edu.np Web Servers, located in all continents. Assume that all the Web Servers are assigned a single IPv6 Anycast IP Address. Now when a user from Europe wants to reach Tu.edu.np the DNS points to the server that is physically located in Europe itself. If a user from Nepal tries to reach Tu.edu.np, the DNS will then point to the Web Server physically located in Asia. Nearest or Closest terms are used in terms of Routing Cost.

In the above picture, when a client computer tries to reach a server, the request is forwarded to the server with the lowest Routing Cost.

Broadcast Routing

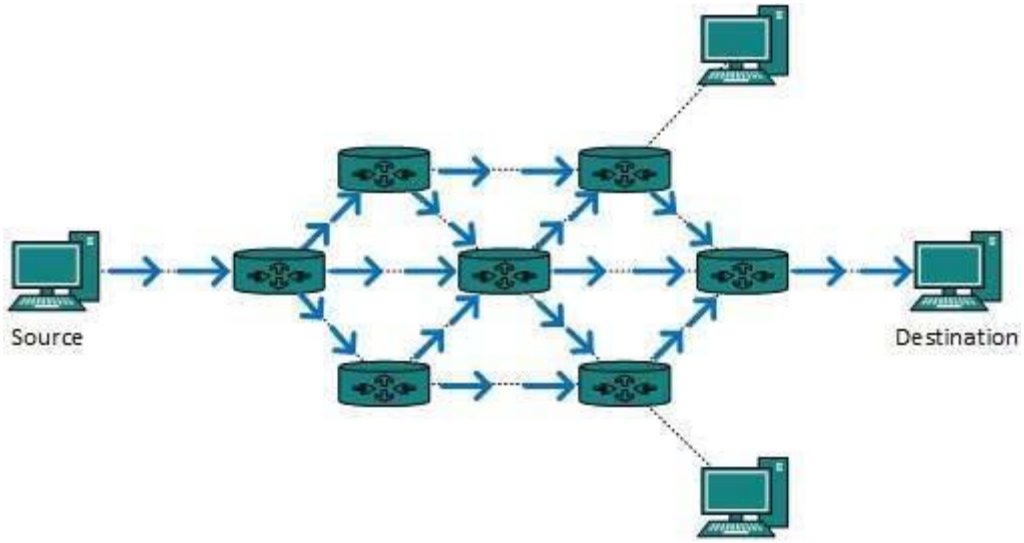
By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices. *Flooding is simplest method packet forwarding.*

Broadcast routing can be done in two ways (algorithm):

- A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.

  This method consumes lots of bandwidth and router must destination address of each node.

- Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.



This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.

Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

Read Me First (3 times) Assumes Basic Key Terms while writing your unit 3 answer.

Address Resolution Protocol (ARP)	data link control (DLC)	media access control (MAC)	block coding
burst error	check bit	checksum	codeword
cyclic code	cyclic redundancy check (CRC)	dataword	forward error correction (FEC)
generator polynomial	minimum Hamming distance	parity-check code	single-bit error
bit stuffing	byte stuffing	Challenge Handshake Authentication	Protocol (CHAP)
data link control (DLC)	finite state machine (FSM)	Internet Protocol Control Protocol (IPCP)	Link Control Protocol (LCP)
Password Authentication Protocol (PAP)	piggybacking	sequence number	1-persistent method
ALOHA	carrier sense multiple access with collision	avoidance (CSMA/CA)	carrier sense multiple access with collision
detection (CSMA/CD)	code-division multiple access (CDMA)	contention window	controlled access
DCF interframe space (DIFS)	frequency-division multiple access	(FDMA)	interface space (IFS)
jamming signal	media access control (MAC)	multiple access (MA)	nonpersistent method
p-persistent method	polling	primary station	propagation time
pure ALOHA	random access	secondary station	slotted ALOHA
time-division multiple access (TDMA)	token passing	vulnerable time	frame bursting
full-duplex switched Ethernet	logical link control (LLC)	media access control (MAC)	network interface card (NIC)
Standard Ethernet	direct sequence spread spectrum (DSSS)	distributed coordination function (DCF)	distributed interframe space (DIFS)
extended service set (ESS)	frequency-hopping spread spectrum (FHSS)	high-rate direct-sequence spread spectrum	(HR-DSSS)

3.1	**Functions of Data Link Layer**		1

Functions of the data link layer include:

- Providing a well-defined service interface to the network layer (framing)
- Dealing with transmission errors (error control)
- Regulating the flow of data so that slow receivers are not swamped by fast senders (flow control)

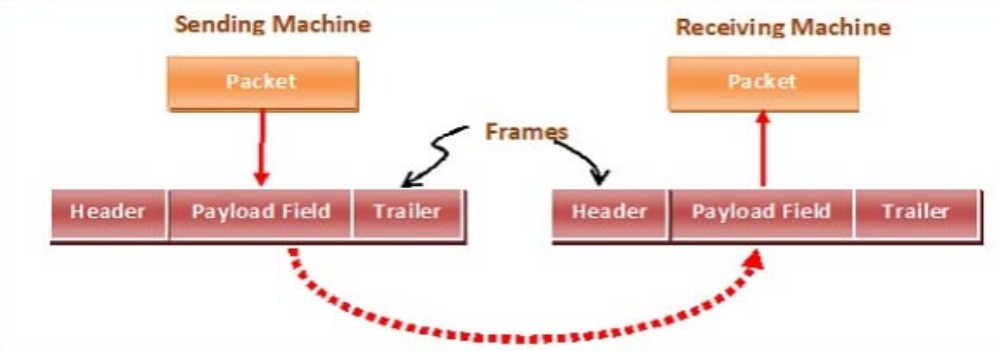
3.2	Data Link Control: Framing, Flow and Error Control		1

Framing

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

The Data Link layer frame includes:

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



Parts of a Frame

- **Frame Header** − It contains the source and the destination addresses of the frame.
- **Payload field** − It contains the message to be delivered.
- **Trailer** − It contains the error detection and error correction bits.
- **Flag** − It marks the beginning and end of the frame.

• Data link layer is divided into 2 sublayers

1. MAC (Media Access Control)
2. LLC (Logical Link Control)

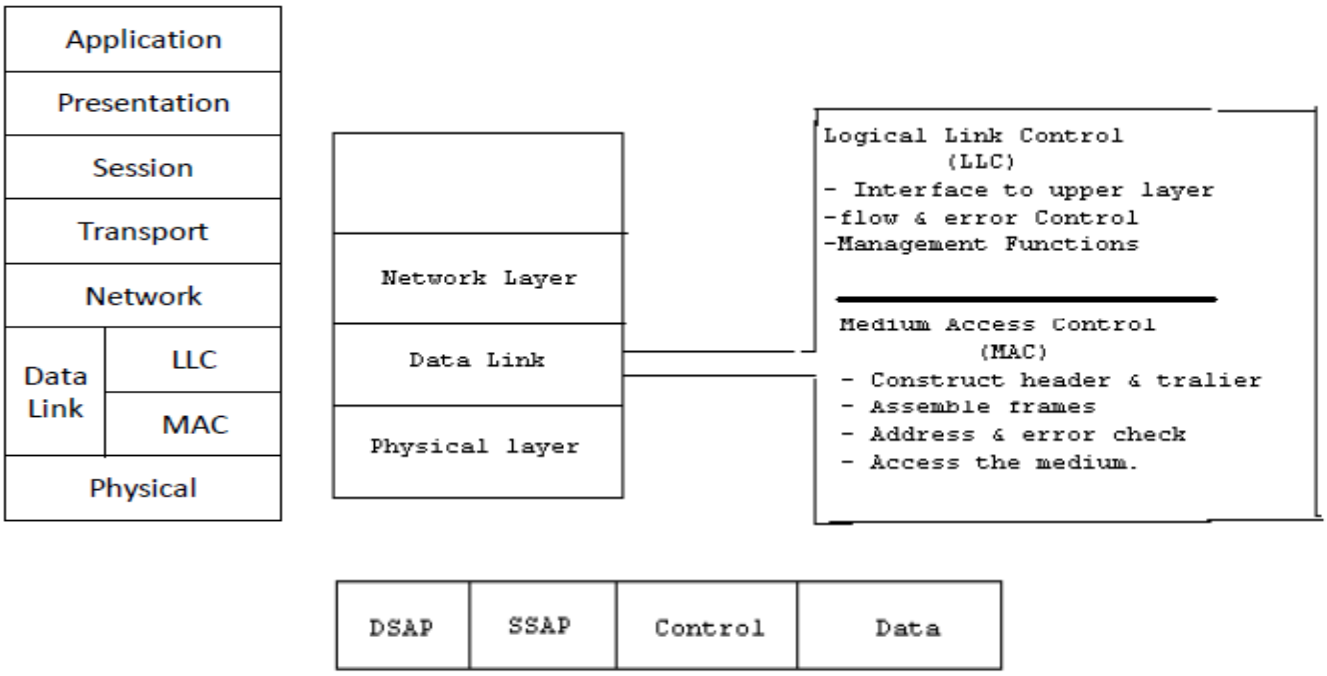


Fig :- LLC Frame Format

Destination Service Access Point (DSAP) -- IEEE 802.2 header begins with a 1 byte field, which identifies the receiving upper-layer process.
Source Service Access Point (SSAP) -- Following the DSAP address is the 1-byte address, which identifies the sending upper-layer process. **Control** -- The Control field employs three different formats, depending on the type of LLC frame used:

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

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

MAC Frame Format:

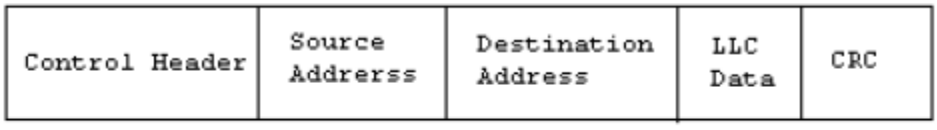


Fig : General MAC frame Format

Problems in Framing –

Detecting start of the frame: SFD (Starting Frame Delimeter).
How do station detect a frame: Station checks destination address to accept or reject frame.
Detecting end of frame: When to stop reading the frame.

Types of framing – There are two types of framing:

1. Fixed size – The frame is of fixed size and there is no need to provide boundaries to the frame, length of the frame itself acts as delimiter.

Drawback: It suffers from internal fragmentation if data size is less than frame size

Solution: Padding

2. Variable size – In this there is need to define end of frame as well as beginning of next frame to distinguish.

Header	Payload	Trailer	Header	Payload	Trailer
Frame 1			Frame 2		

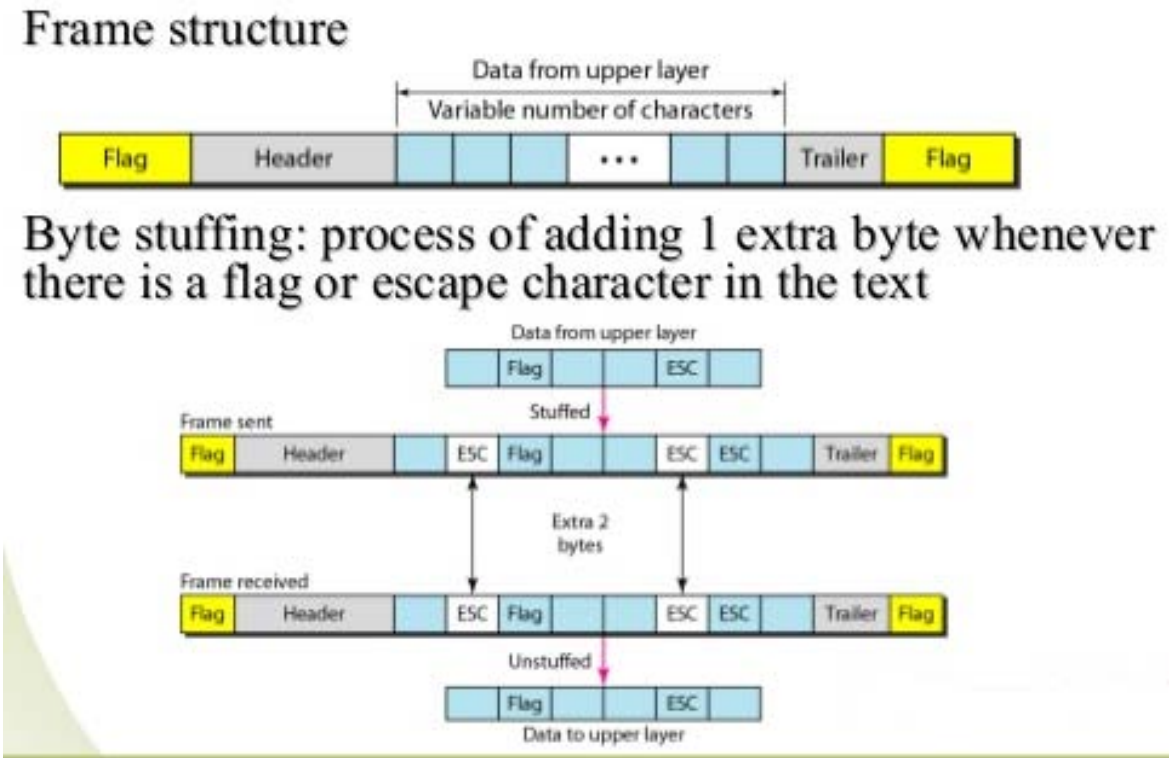
Figure : Frame Format in Variable Size frame

This can be done in two ways:

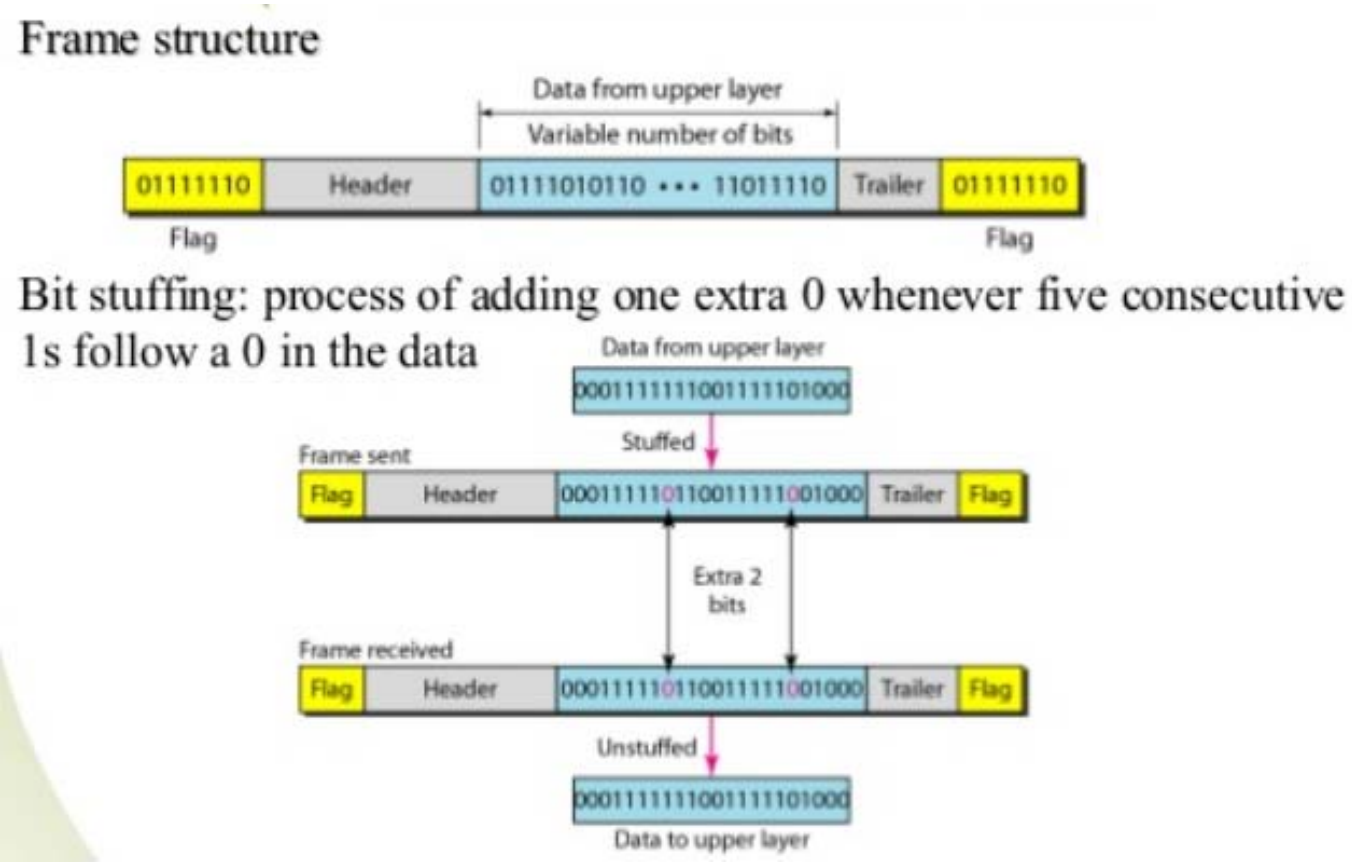
Length field – We can introduce a length field in the frame to indicate the length of the frame. Used in Ethernet(802.3). The problem with this is that sometimes the length field might get corrupted.

End Delimeter (ED) – We can introduce an ED(pattern) to indicate the end of the frame. Used in Token Ring. The problem with this is that ED can occur in the data. **This can be solved by:**

1. **Byte (character) – Stuffing** − A byte is stuffed in the message to differentiate from the delimiter. This is also called **character-oriented framing.**



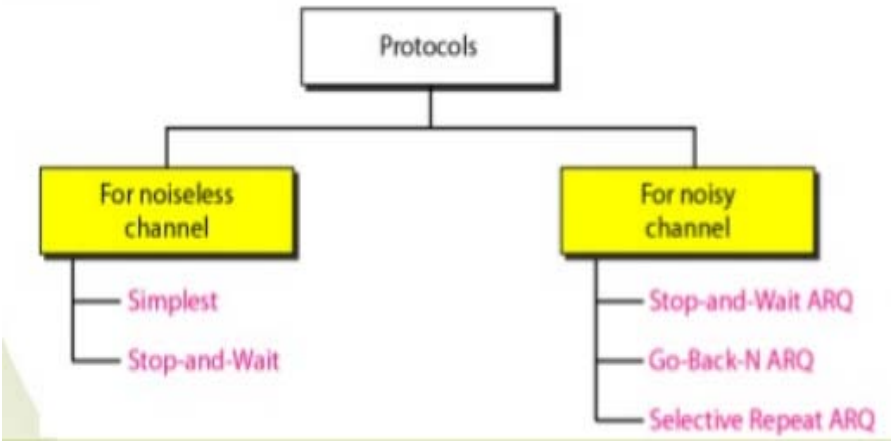
2. **Bit – Stuffing** − A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called **bit – oriented framing.**



Flow and Error Control

- **Data link control = flow control + error control**
- Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement
- Error control in the data link layer is based on automatic repeat request (ARQ), which is the retransmission of data
- ACK, NAK(Negative ACK), Piggybacking (ACKs and NAKs in data frames)

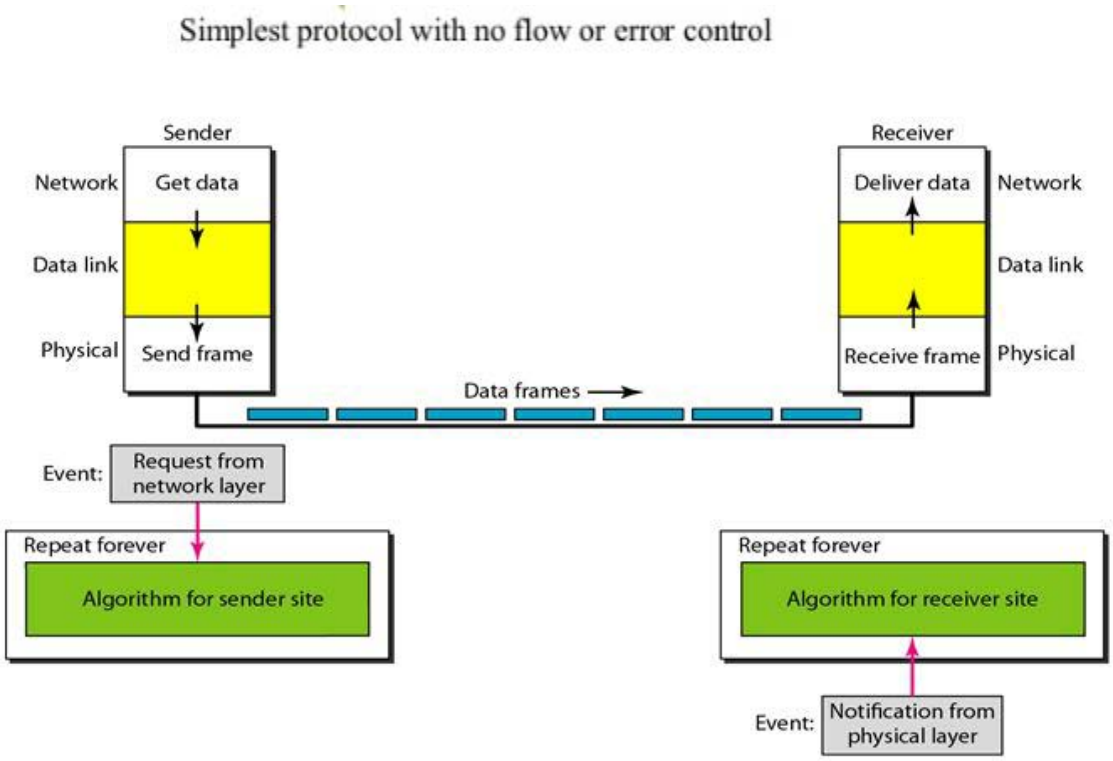
Flow Control-



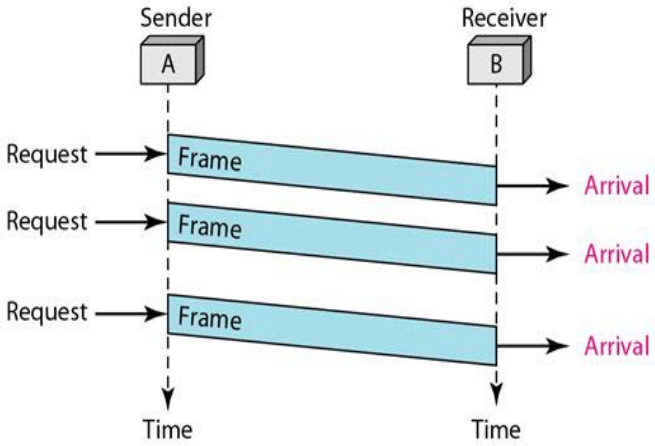
Simplest:

Simplest Protocol is one that has no flow or error control and it is a unidirectional protocol in which data frames are traveling in only one direction-from the sender to receiver. We assume that the receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately.

Design:



The following figure shows an example of communication using this protocol. It is very simple. The sender sends a sequence of frames without even thinking about the receiver. To send three frames, three events occur at the sender site and three events at the receiver site. Note that the data frames are shown by tilted boxes; the height of the box defines the transmission time difference between the first bit and the last bit in the frame.



Sender-site algorithm

```
1  while(true)                          // Repeat forever
2  {
3    WaitForEvent();                    // Sleep until an event occurs
4    if(Event(RequestToSend))           //There is a packet to send
5    {
6       GetData();
7       MakeFrame();
8       SendFrame();                    //Send the frame
9    }
10 }
```

Receiver-site algorithm

```
1  while(true)                          // Repeat forever
2  {
3    WaitForEvent();                    // Sleep until an event occurs
4    if(Event(ArrivalNotification))     //Data frame arrived
5    {
6       ReceiveFrame();
7       ExtractData();
8       DeliverData();                  //Deliver data to network layer
9    }
10 }
```

Stop & wait

Simple tokens of ACK and flow control added

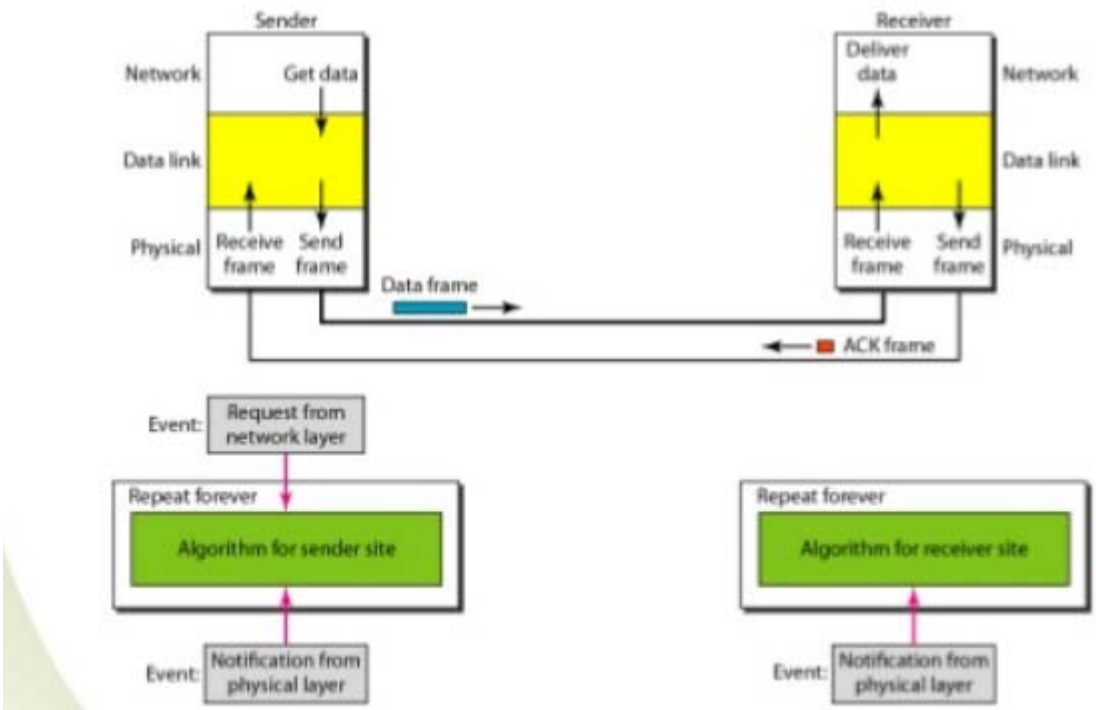
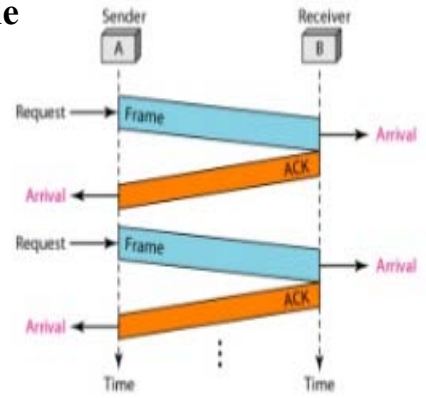
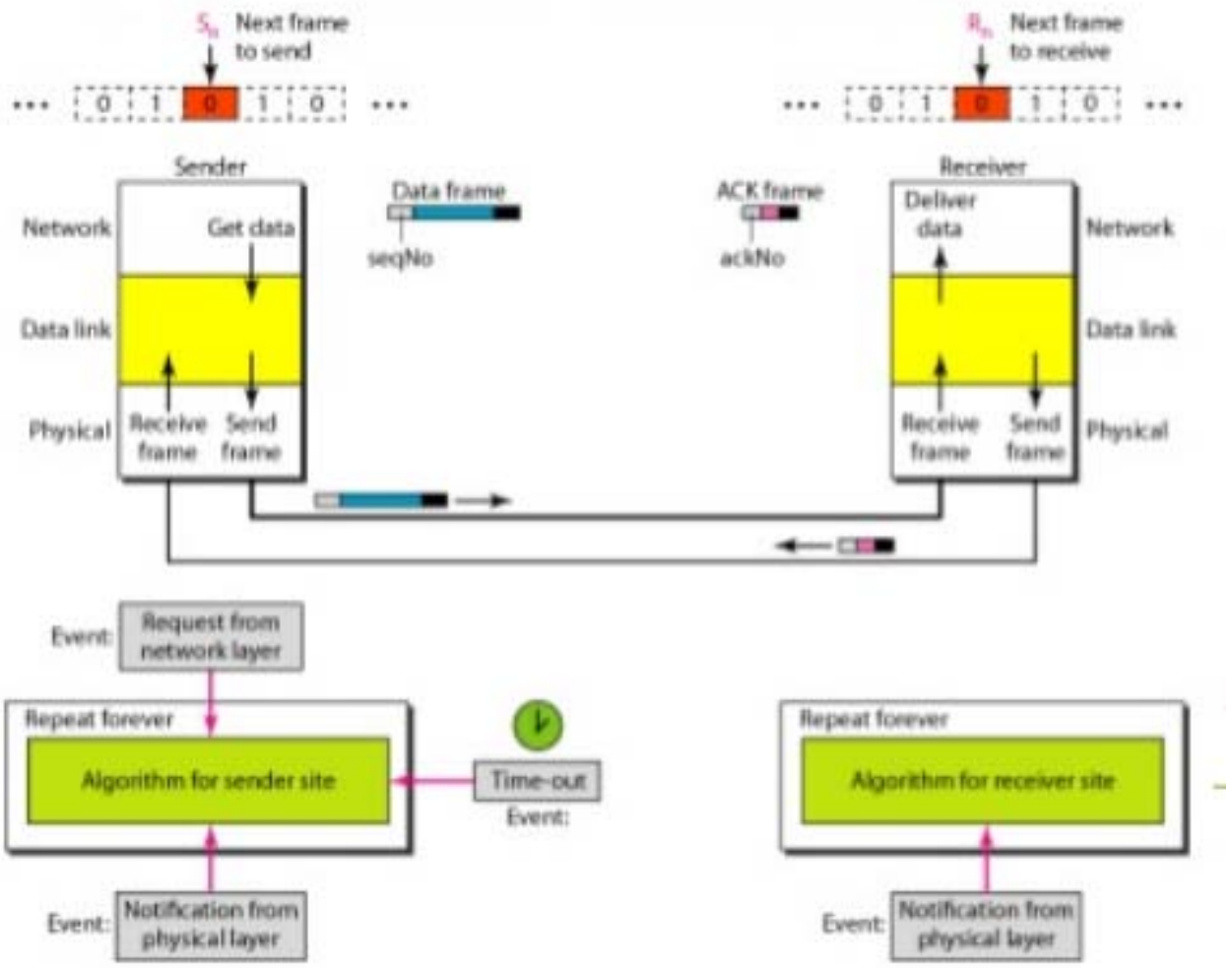


fig: Stop & wait example

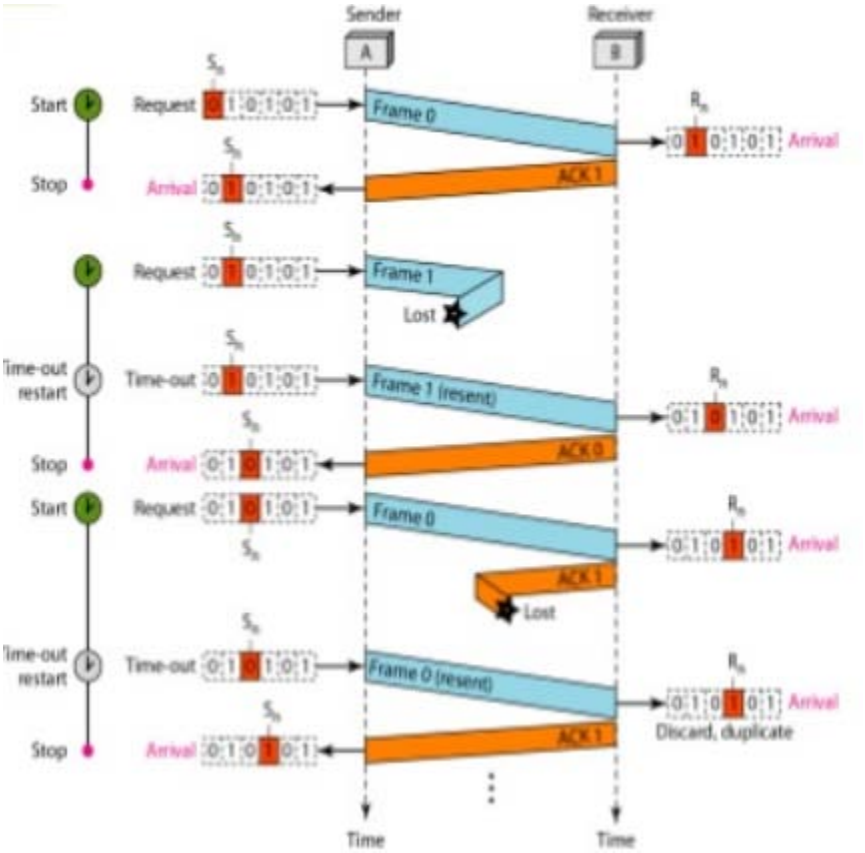


Stop-and-wait Automatic Repeat Request (ARQ)

- Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires
- In Stop-and-Wait ARQ, we use sequence numbers to number the frames. The sequence numbers are based on modulo-2 arithmetic
- Acknowledgment number always announces in modulo-2 arithmetic the sequence number of the next frame expected.

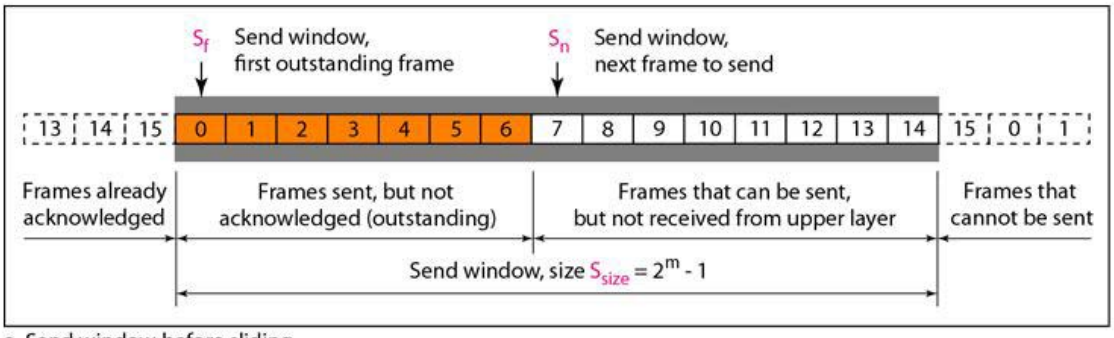


Example

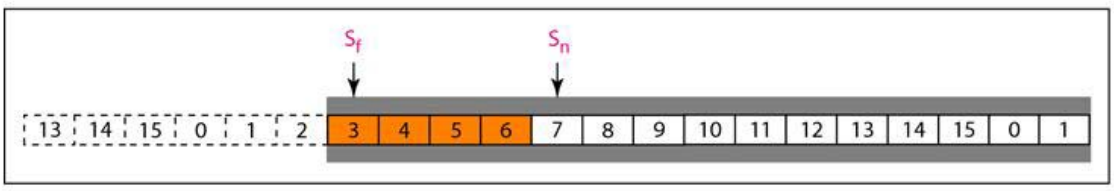


Go-Back-N ARQ

- Pipelining improves the efficiency of the transmission
- In the Go-Back-N Protocol, the sequence numbers are modulo 2m, where m is the size of the sequence number field in bits
- The send window is an abstract concept defining an imaginary box of size 2m − 1 with three variables: Sf, Sn, and S size
- The send window can slide one or more slots when a valid acknowledgment arrives

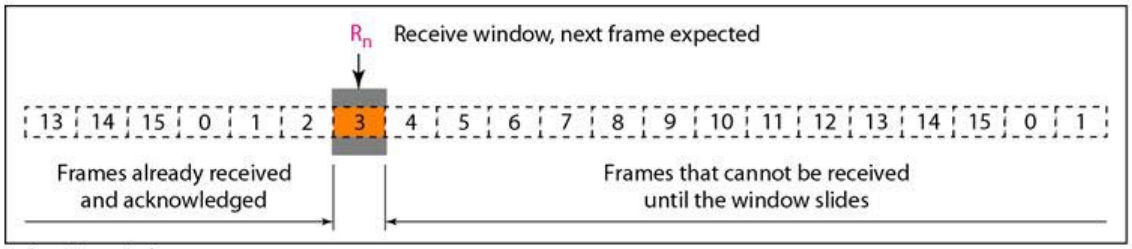


a. Send window before sliding

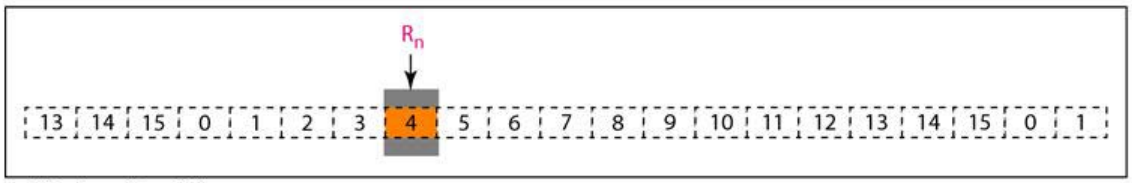


b. Send window after sliding

- Receive window for Go-Back-N ARQ
- The receive window is an abstract concept defining an imaginary box of size 1 with one single variable Rn. The window slides when a correct frame has arrived; sliding occurs one slot at a time.

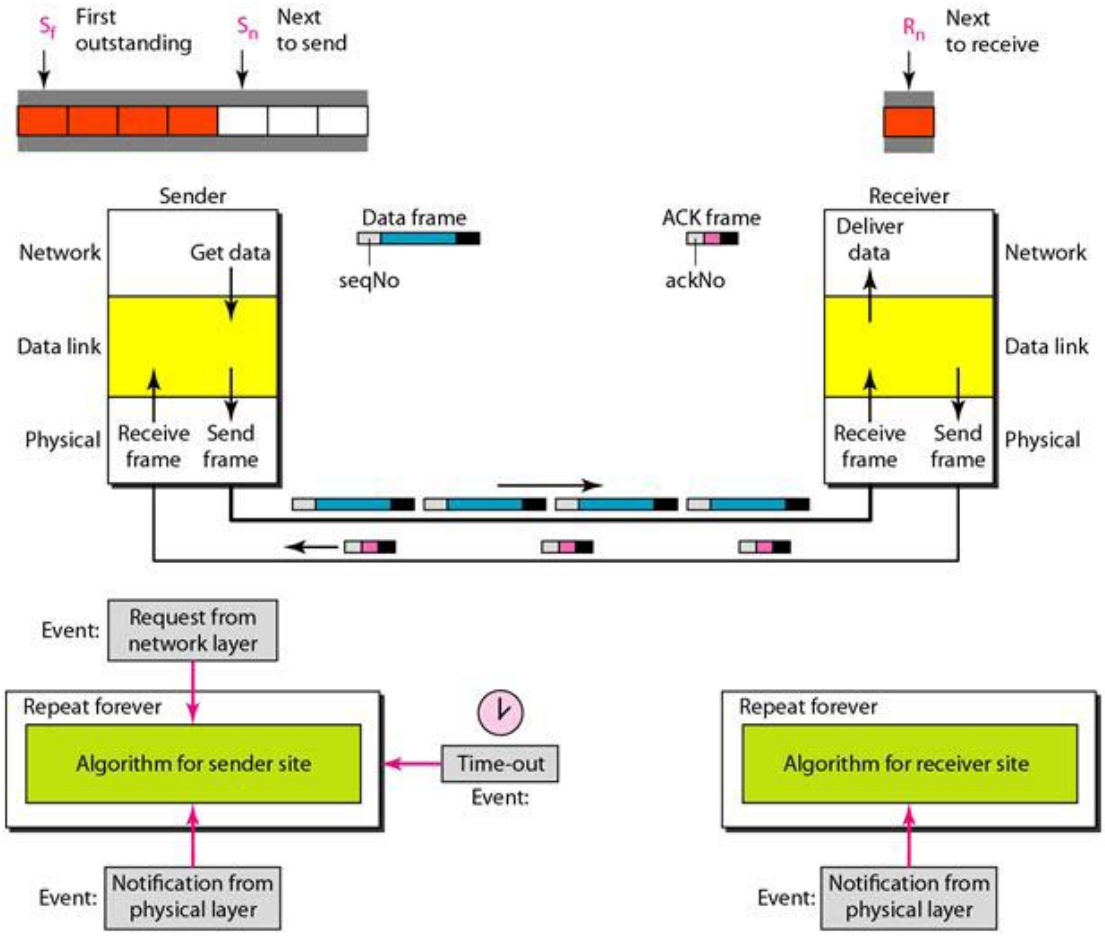


a. Receive window



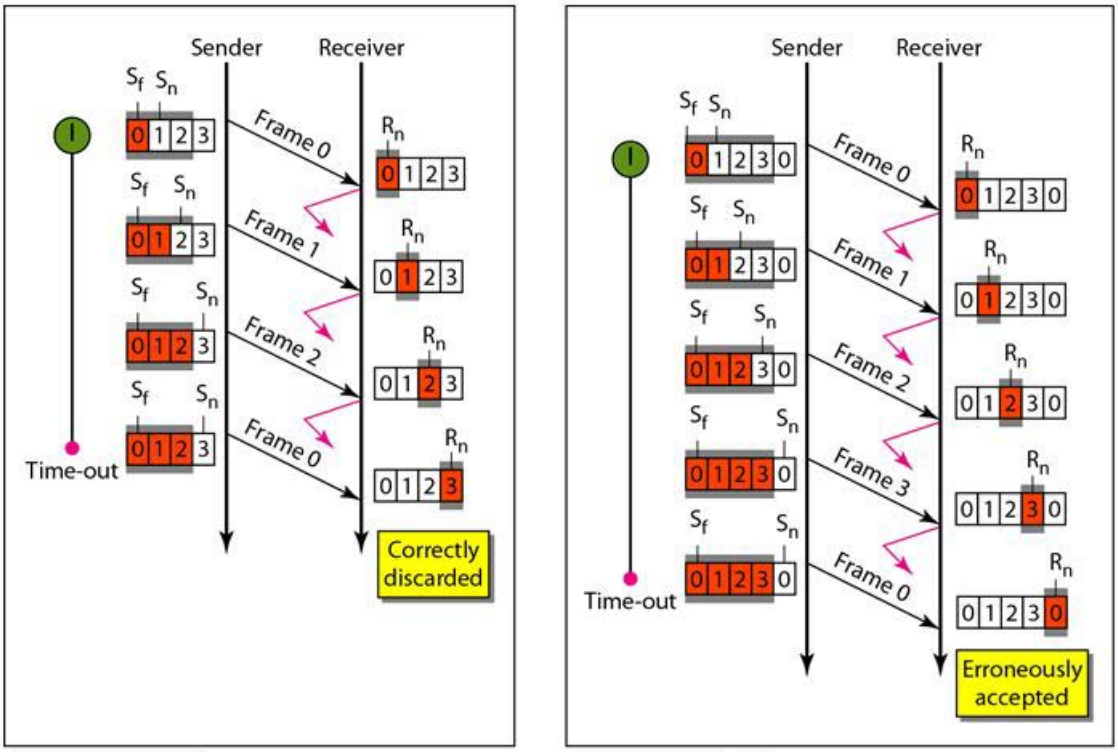
b. Window after sliding

Sliding windows, Timers, ACK, Resending a frame

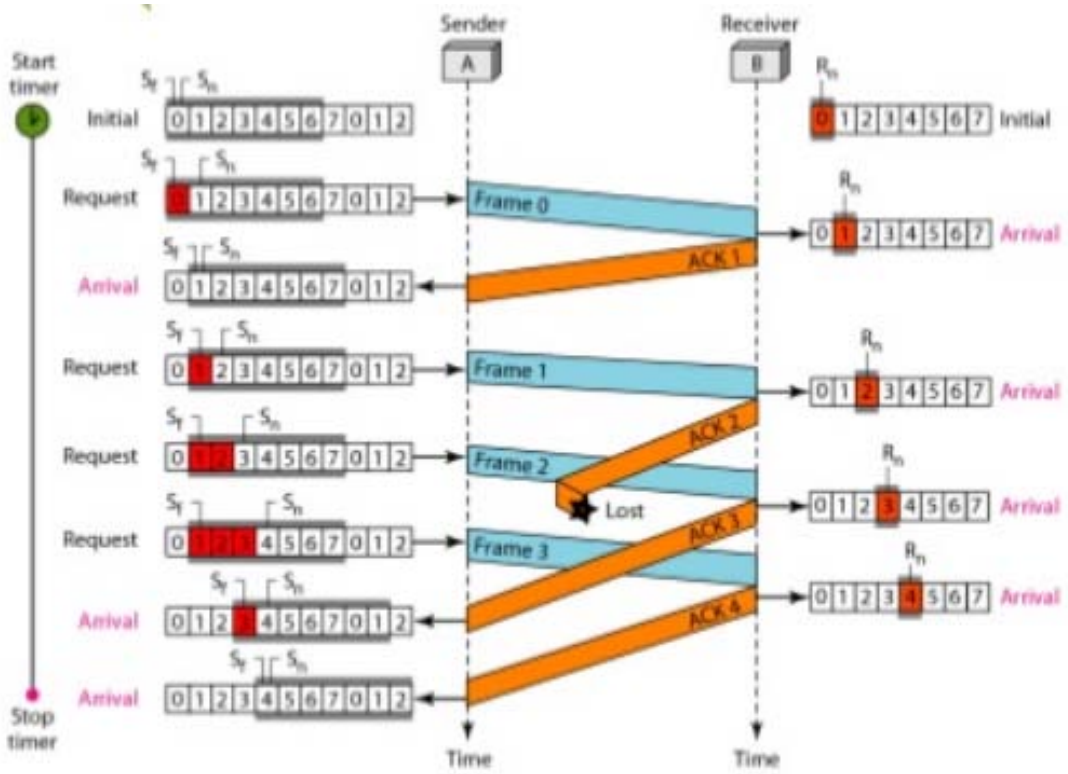


Send Window Size:

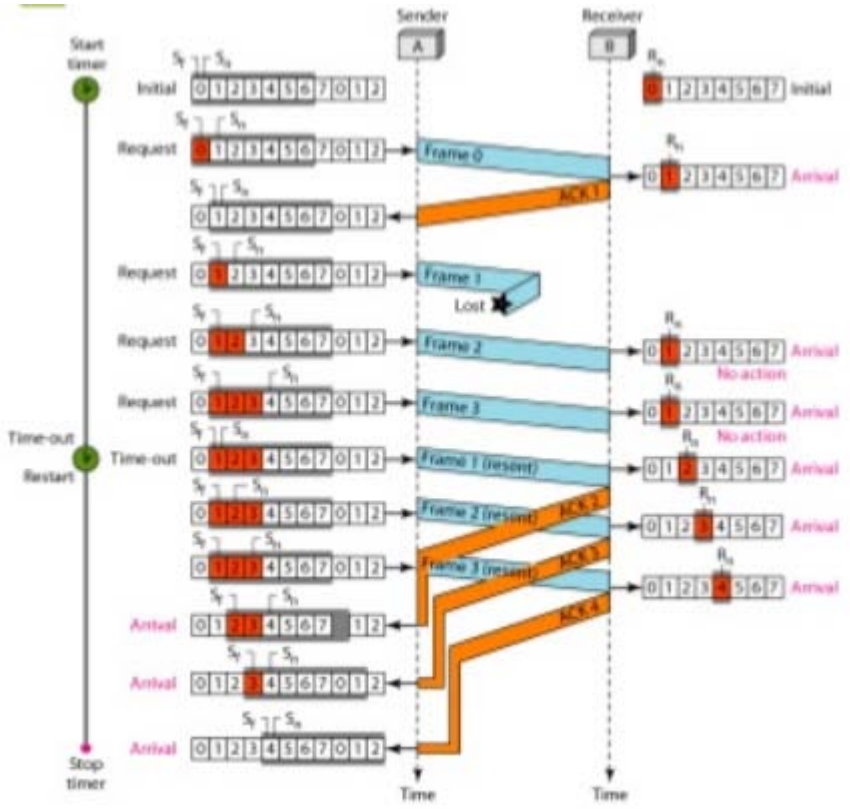
- Go-Back-N ARQ, the size of the send window must be less than 2m; the size of the receiver window is always 1
- Stop-and-Wait ARQ is a special case of Go-Back-N ARQ in which the size of the send window is 1



Example-1



Example-2



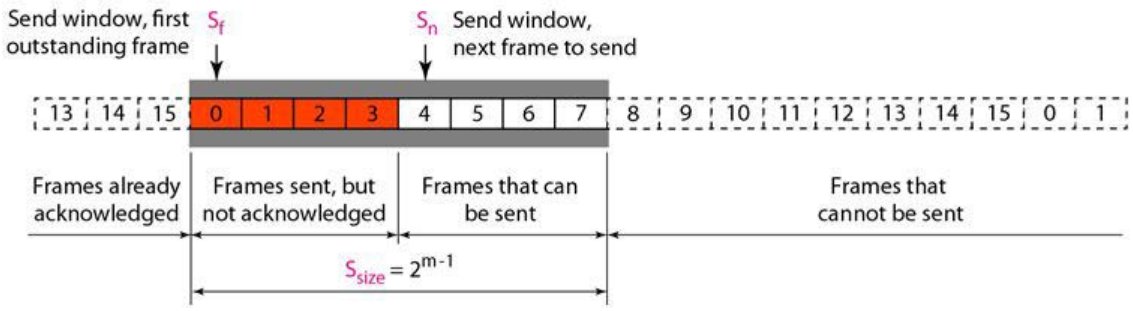
Selective Repeat ARQ (S R Automatic Repeat Request (ARQ)

Go-Back-N ARQ simplifies the process at the receiver site. The receiver keeps track of only one variable, and there is no need to buffer out-of-order frames; they are simply discarded. However, this protocol is very inefficient for a noisy link.

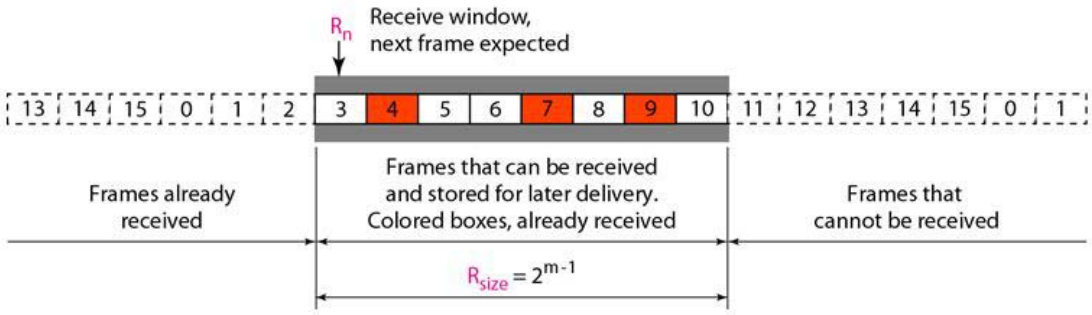
In a noisy link a frame has a higher probability of damage, which means the resending of multiple frames. This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent. This mechanism is called Selective Repeat ARQ. It is more efficient for noisy links, but the processing at the receiver is more complex.

The Selective Repeat Protocol also uses two windows: a send window and a receive window. However, there are differences between the windows in this protocol and the ones in Go-Back-N. First, the size of the send window is much smaller; it is $2^m - 1$.

- **Sender Window size**

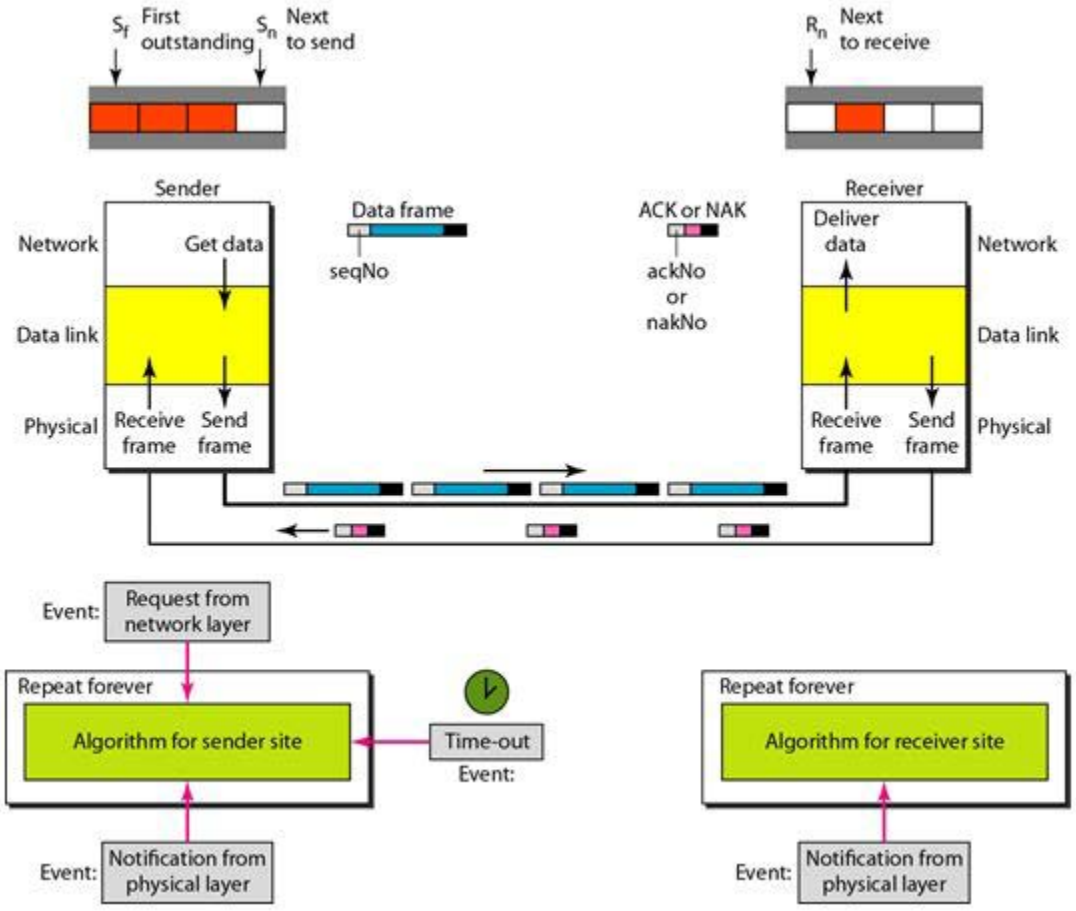


- **Receiver Window size**



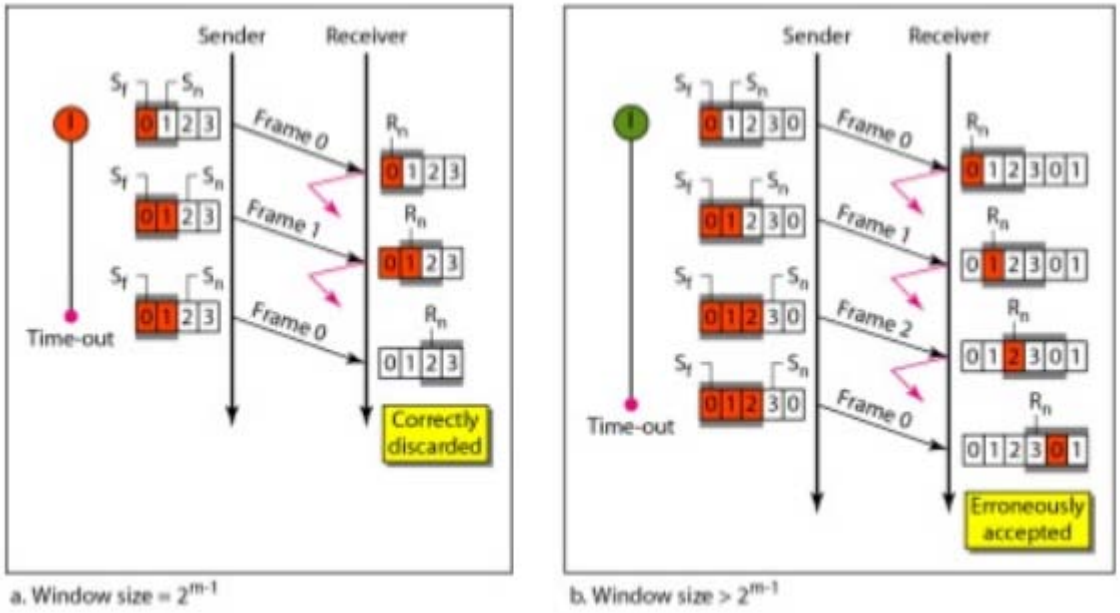
Design

We can now show why the size of the sender and receiver windows must be at most one half of 2m. For an example, we choose m = 2, which means the size of the window is 2m/2, or 2. The following figure compares a window size of 2 with a window size of 3.

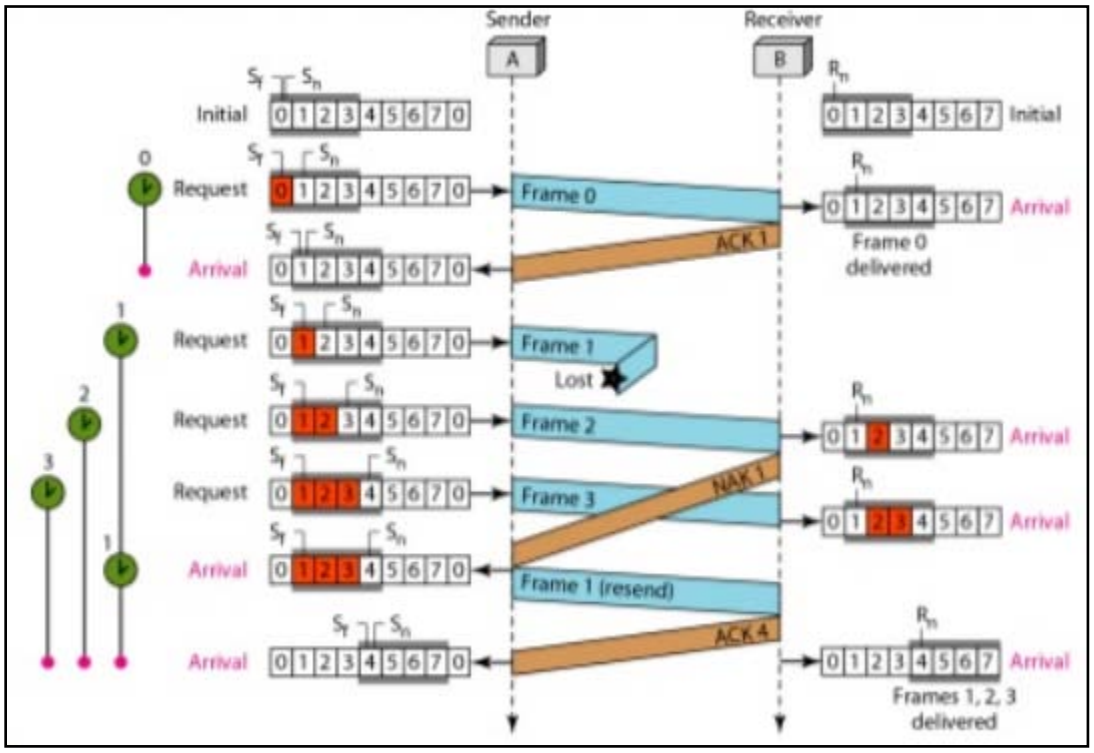


Window Size:

The size of the sender and receiver window must be at most one-half of 2^m

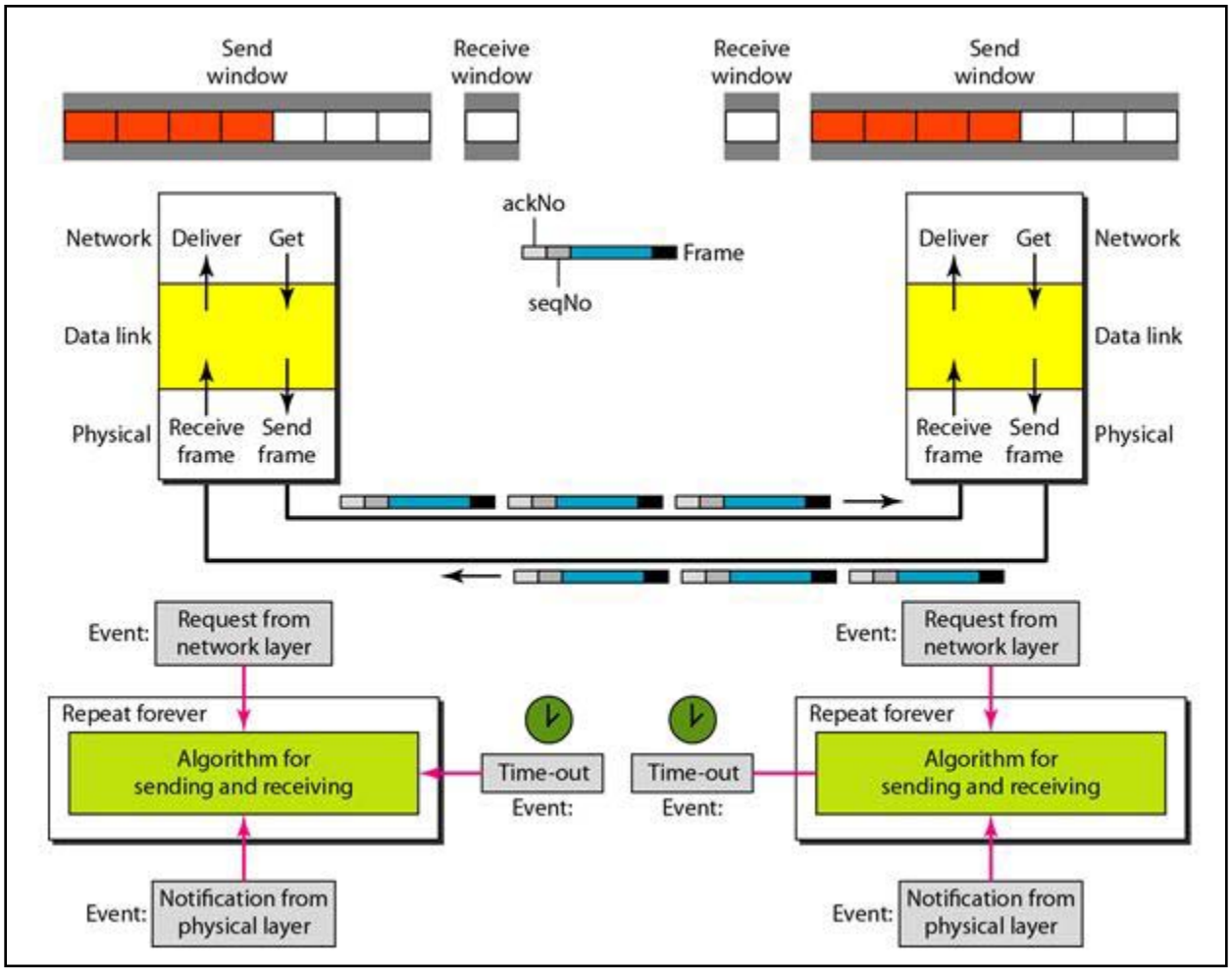


Example:



Piggybacking Protocol

- To improve the efficiency of the bidirectional protocols.
- Piggybacking in Go-Back-N ARQ

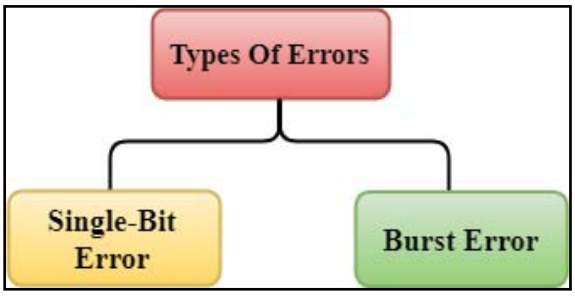


Error Control-

When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits leads to spurious data being received by the receiver and are **called errors.**

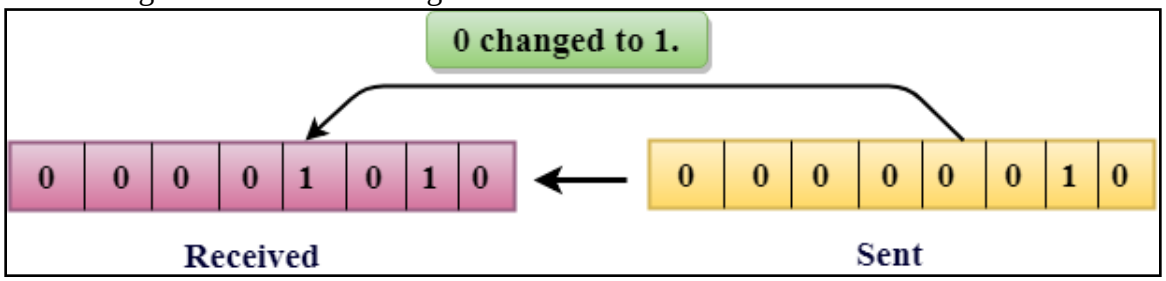
Error detection techniques are responsible for checking whether any error has occurred or not in the frame that has been transmitted via network. It does not take into account the number of error bits and the type of error.

When sender transmits data to the receiver, the data might get scrambled by noise or data might get corrupted during the transmission.



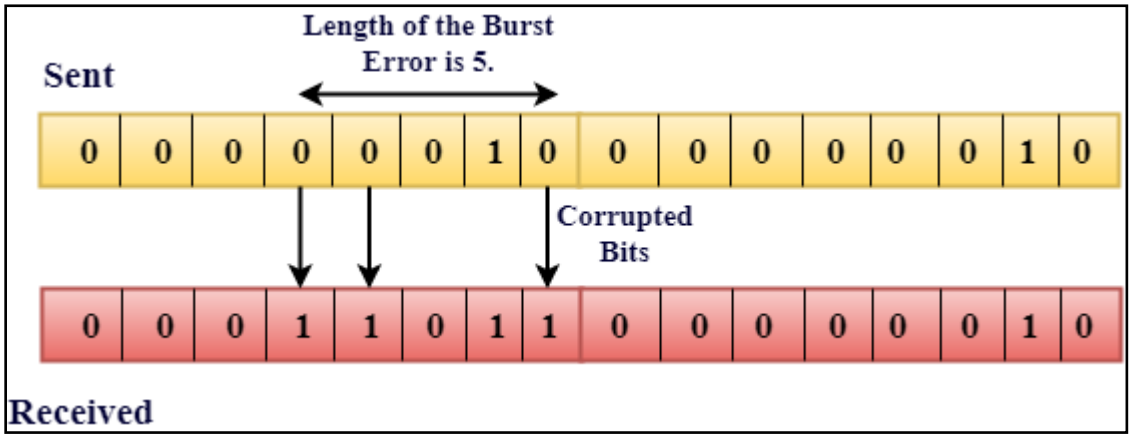
Single-Bit Error:

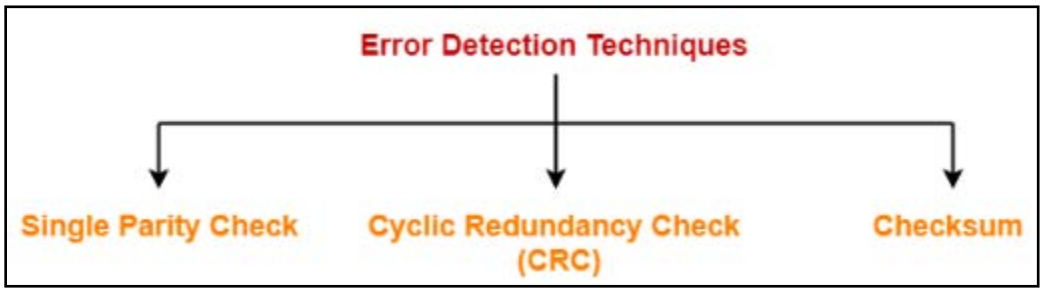
The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.
The Burst Error is determined from the first corrupted bit to the last corrupted bit.





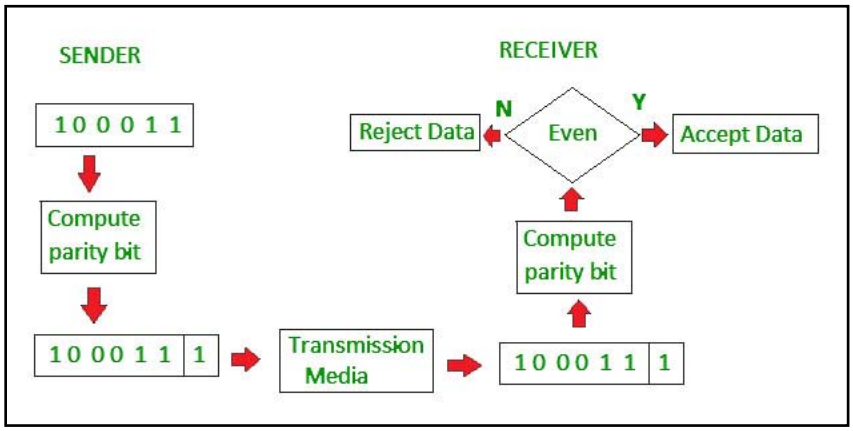
(Shortly Concept)

1. Simple Parity check

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

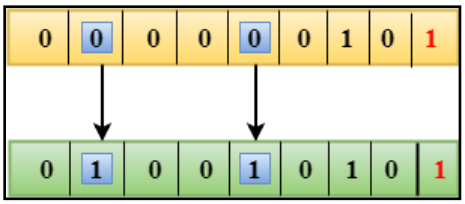
- 1 is added to the block if it contains odd number of 1's, and
- 0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.



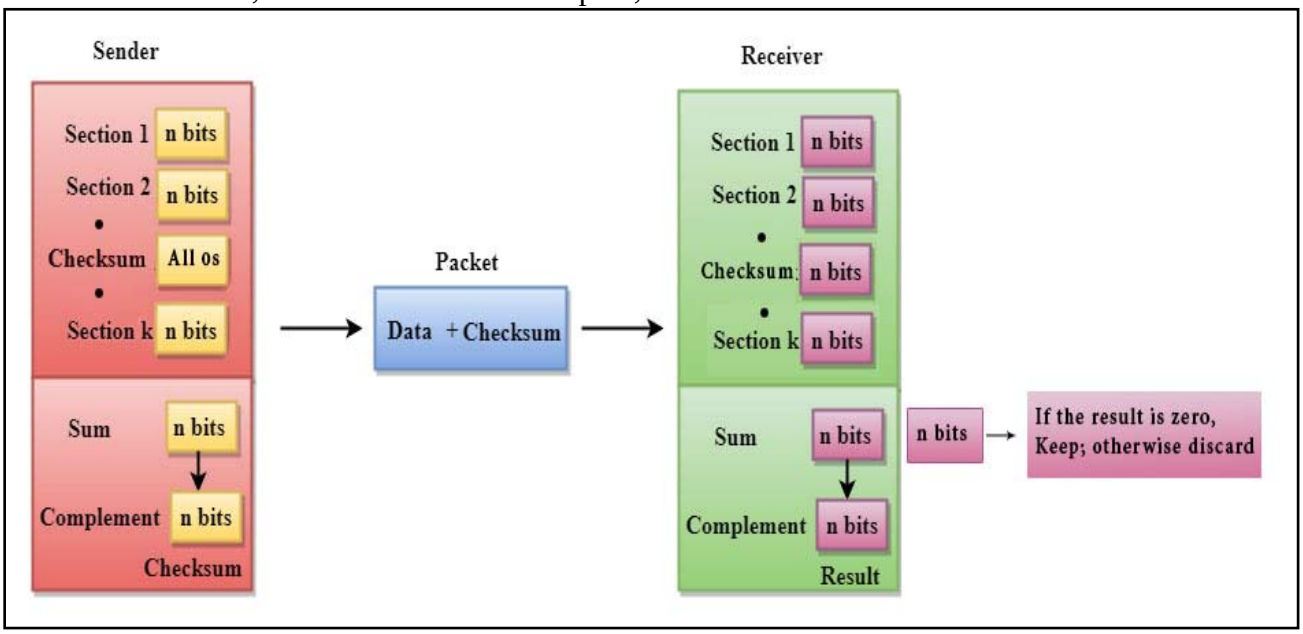
Drawbacks Of Single Parity Checking

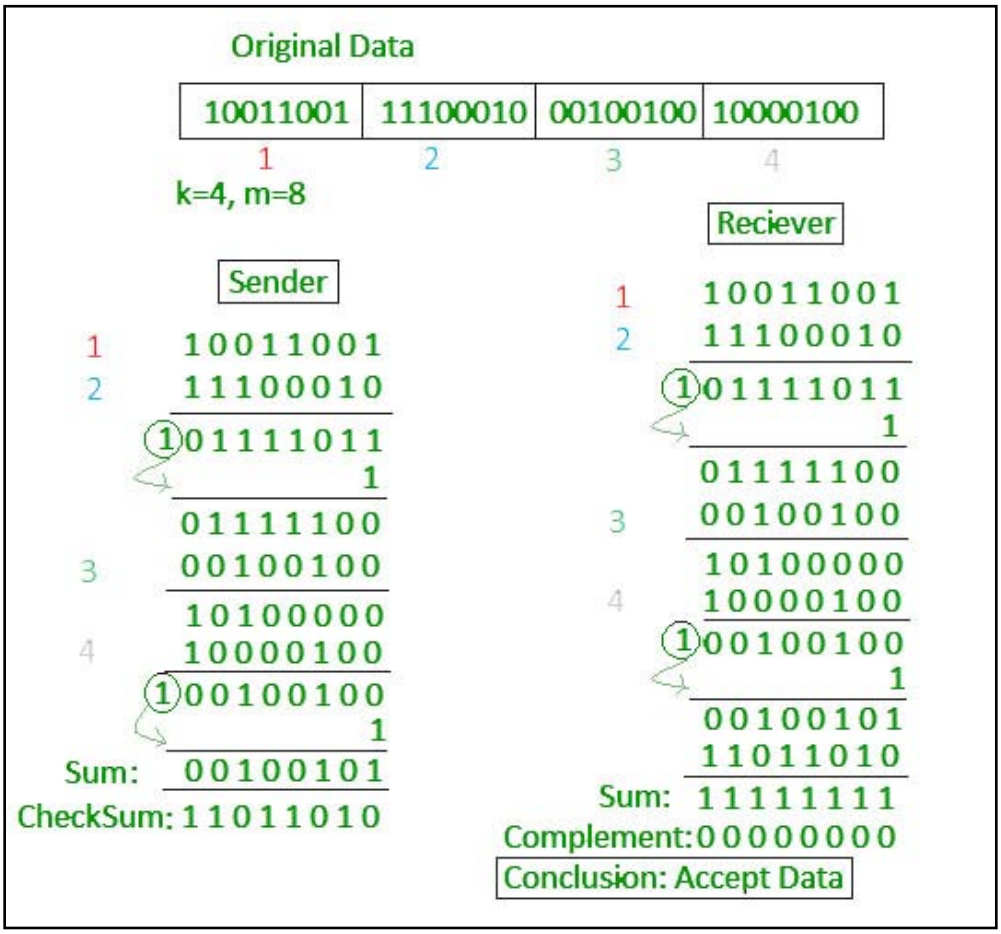
- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



2. Checksum

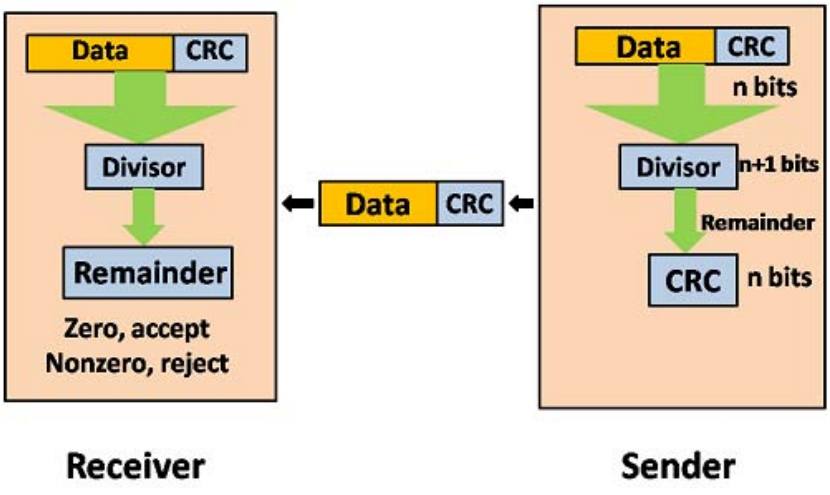
- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

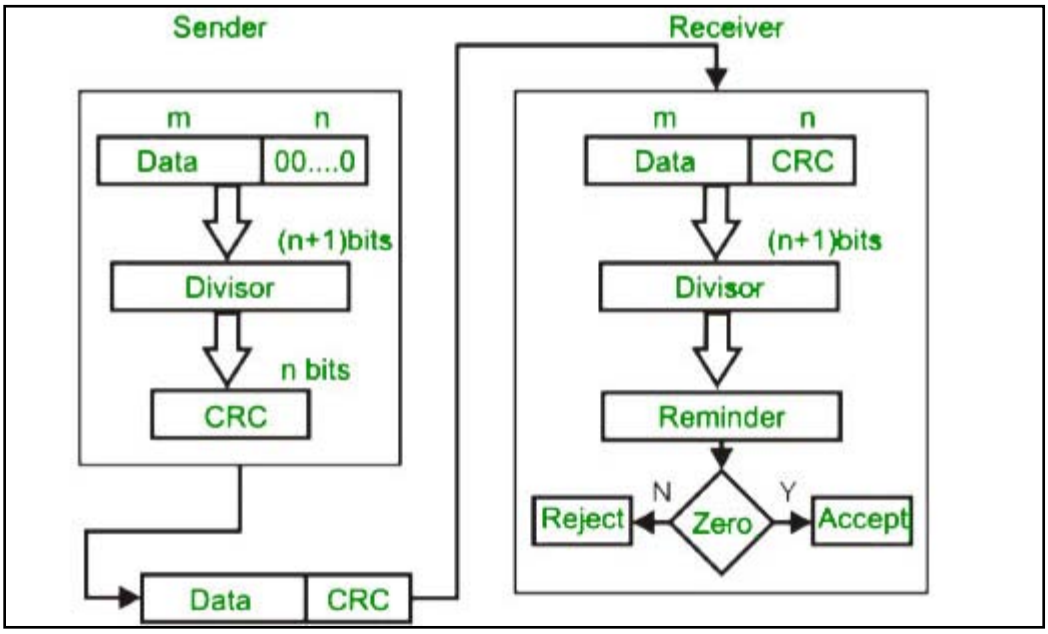


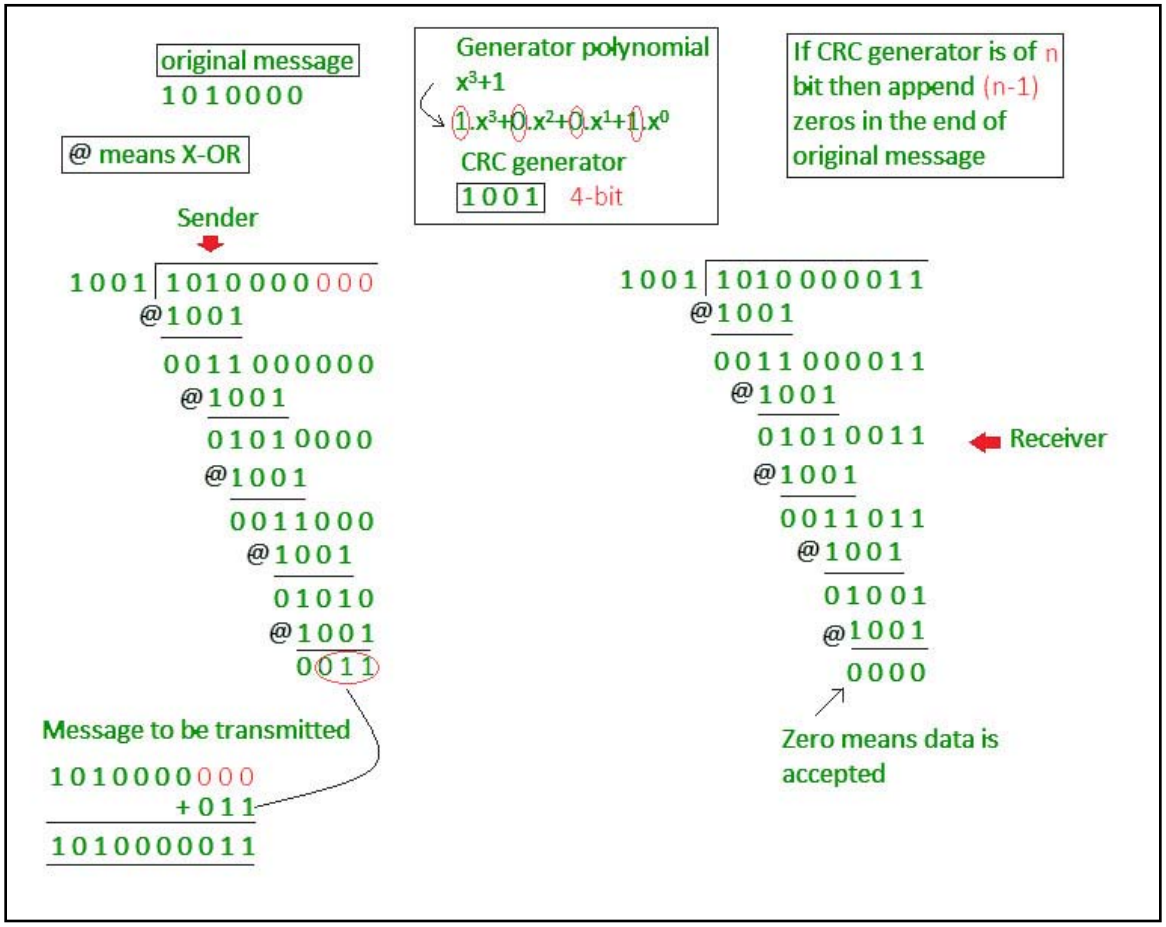


3. Cyclic redundancy check (CRC)

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




Sender
Receiver
m
n
Data
00....0
(n+1)bits
Divisor
n bits
CRC
Data
CRC
m
n
Data
CRC
(n+1)bits
Divisor
Reminder
N
Y
Reject
Zero
Accept


original message
1010000
@ means X-OR
Generator polynomial
x^3+1
$1.x^3+0.x^2+0.x^1+1.x^0$
CRC generator
1001 4-bit
If CRC generator is of n bit then append (n-1) zeros in the end of original message
Sender
1001 | 1010000000
@1001
0011000000
@1001
01010000
@1001
0011000
@1001
01010
@1001
0011
Message to be transmitted
1010000000
+011
1010000011
1001 | 1010000011
@1001
0011000011
@1001
01010011
@1001
0011011
@1001
01001
@1001
0000
Receiver
Zero means data is accepted

Single Parity Check-

In this technique,

- One extra bit called as parity bit is sent along with the original data bits.
- Parity bit helps to check if any error occurred in the data during the transmission.

Steps Involved-

Error detection using single parity check involves the following steps-

Step-01:

At sender side,

- Total number of 1's in the data unit to be transmitted is counted.
- The total number of 1's in the data unit is made even in case of even parity.
- The total number of 1's in the data unit is made odd in case of odd parity.
- This is done by adding an extra bit called as parity bit.

Step-02:

- The newly formed code word (Original data + parity bit) is transmitted to the receiver.

Step-03:

At receiver side,

- Receiver receives the transmitted code word.
- The total number of 1's in the received code word is counted.

Then, following cases are possible-

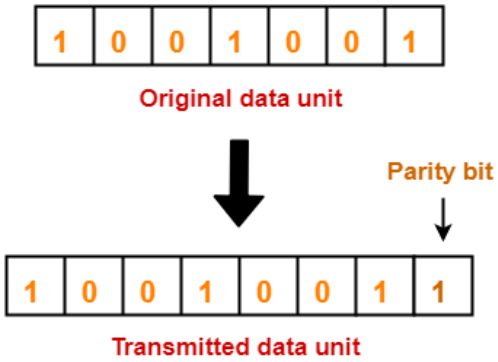
- If total number of 1's is even and even parity is used, then receiver assumes that no error occurred.
- If total number of 1's is even and odd parity is used, then receiver assumes that error occurred.
- If total number of 1's is odd and odd parity is used, then receiver assumes that no error occurred.
- If total number of 1's is odd and even parity is used, then receiver assumes that error occurred.

Parity Check Example-

Consider the data unit to be transmitted is 1001001 and even parity is used.

At Sender Side-

- Total number of 1's in the data unit is counted.
- Total number of 1's in the data unit = 3.
- Clearly, even parity is used and total number of 1's is odd.
- So, parity bit = 1 is added to the data unit to make total number of 1's even.
- Then, the code word 10010011 is transmitted to the receiver.



At Receiver Side-

- After receiving the code word, total number of 1's in the code word is counted.
- Consider receiver receives the correct code word = 10010011.
- Even parity is used and total number of 1's is even.
- So, receiver assumes that no error occurred in the data during the transmission.

Advantage-

- This technique is guaranteed to detect an odd number of bit errors (one, three, five and so on).
- If odd number of bits flip during transmission, then receiver can detect by counting the number of 1's.

Limitation-

- This technique can not detect an even number of bit errors (two, four, six and so on).
- If even number of bits flip during transmission, then receiver can not catch the error.

Cyclic Redundancy Check-

- Cyclic Redundancy Check (CRC) is an error detection method.
- It is based on binary division.

CRC Generator-

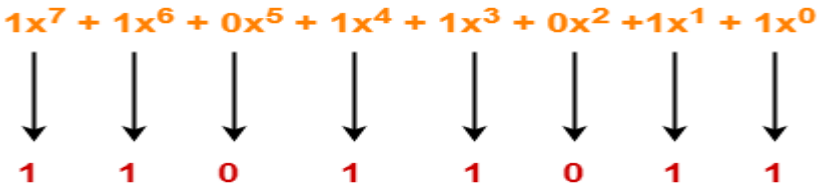
- CRC generator is an algebraic polynomial represented as a bit pattern.
- Bit pattern is obtained from the CRC generator using the following rule-

The power of each term gives the position of the bit and the coefficient gives the value of the bit.

Example-

Consider the CRC generator is $x^7 + x^6 + x^4 + x^3 + x + 1$.

The corresponding binary pattern is obtained as-



Thus, for the given CRC generator, the corresponding binary pattern is 11011011.

Properties Of CRC Generator-

The algebraic polynomial chosen as a CRC generator should have at least the following properties-

Rule-01:

- It should not be divisible by x.
- This condition guarantees that all the burst errors of length equal to the length of polynomial are detected.

Rule-02:

- It should be divisible by x+1.
- This condition guarantees that all the burst errors affecting an odd number of bits are detected.

Important Notes-

If the CRC generator is chosen according to the above rules, then-

- CRC can detect all single-bit errors

- CRC can detect all double-bit errors provided the divisor contains at least three logic 1's.
- CRC can detect any odd number of errors provided the divisor is a factor of x+1.
- CRC can detect all burst error of length less than the degree of the polynomial.
- CRC can detect most of the larger burst errors with a high probability.

Steps Involved-

Error detection using CRC technique involves the following steps-

Step-01: *Calculation Of CRC At Sender Side-*

At sender side,

- A string of n 0's is appended to the data unit to be transmitted.
- Here, n is one less than the number of bits in CRC generator.
- Binary division is performed of the resultant string with the CRC generator.
- After division, the remainder so obtained is called as CRC.
- It may be noted that CRC also consists of n bits.

Step-02: Appending CRC To Data Unit-

At sender side,

- The CRC is obtained after the binary division.
- The string of n 0's appended to the data unit earlier is replaced by the CRC remainder.

Step-03: *Transmission To Receiver-*

- The newly formed code word (Original data + CRC) is transmitted to the receiver.

Step-04: Checking at Receiver Side-

At receiver side,

- The transmitted code word is received.
- The received code word is divided with the same CRC generator.
- On division, the remainder so obtained is checked.

The following two cases are possible-

Case-01: Remainder = 0

If the remainder is zero,

- Receiver assumes that no error occurred in the data during the transmission.
- Receiver accepts the data.

Case-02: Remainder ≠ 0

If the remainder is non-zero,

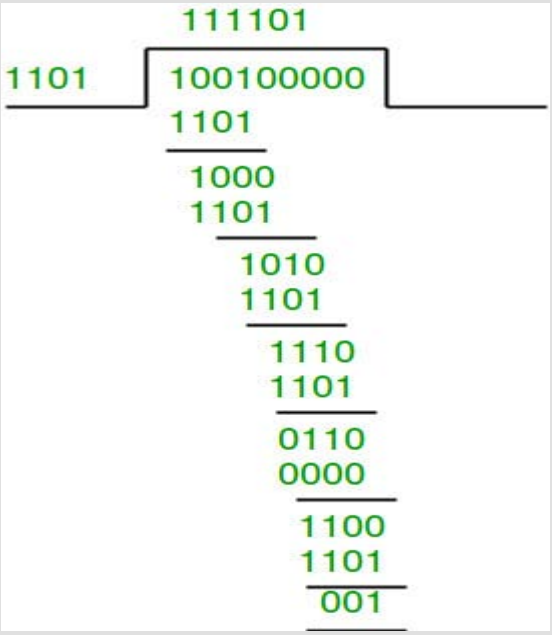
- Receiver assumes that some error occurred in the data during the transmission.
- Receiver rejects the data and asks the sender for retransmission.

Illustration:

Example 1 (No error in transmission):

Data word to be sent - 100100
Key - 1101 [Or generator polynomial $x^3 + x^2 + 1$]

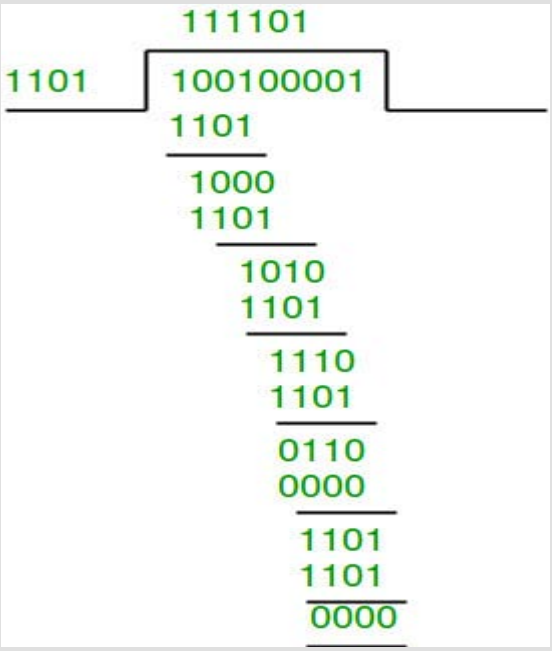
Sender Side:



Therefore, the remainder is 001 and hence the encoded data sent is 100100001.

Receiver Side:

Code word received at the receiver side 100100001

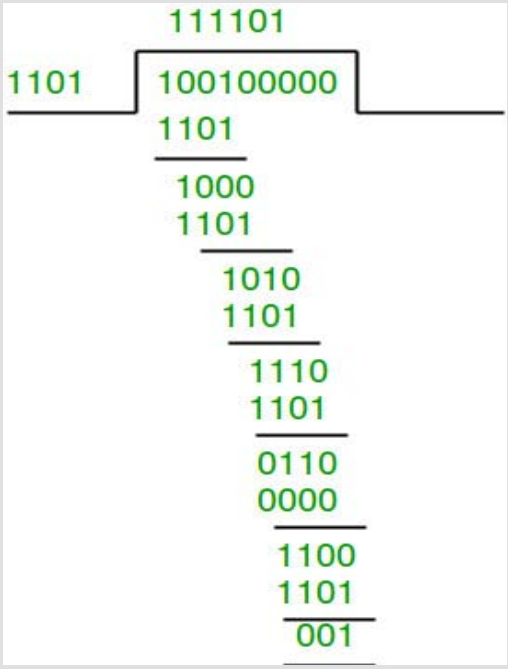


Therefore, the remainder is all zeros. Hence, the data received has no error.

Example 2: (Error in transmission)

Data word to be sent - 100100
Key - 1101

Sender Side:

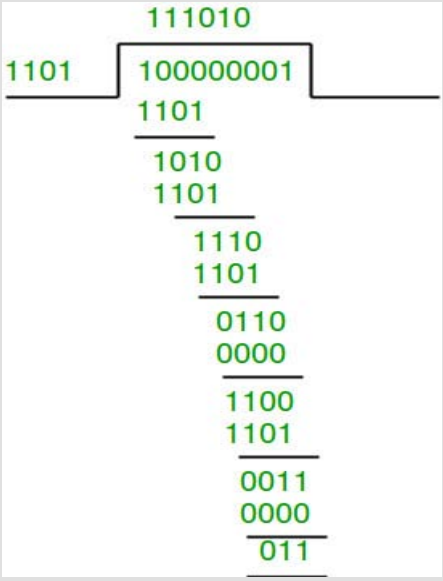


Therefore, the remainder is 001 and hence the code word sent is 100100001.

Receiver Side:

Let there be error in transmission media

Code word received at the receiver side - 100000001



Since the remainder is not all zeroes, the error is detected at the receiver side.

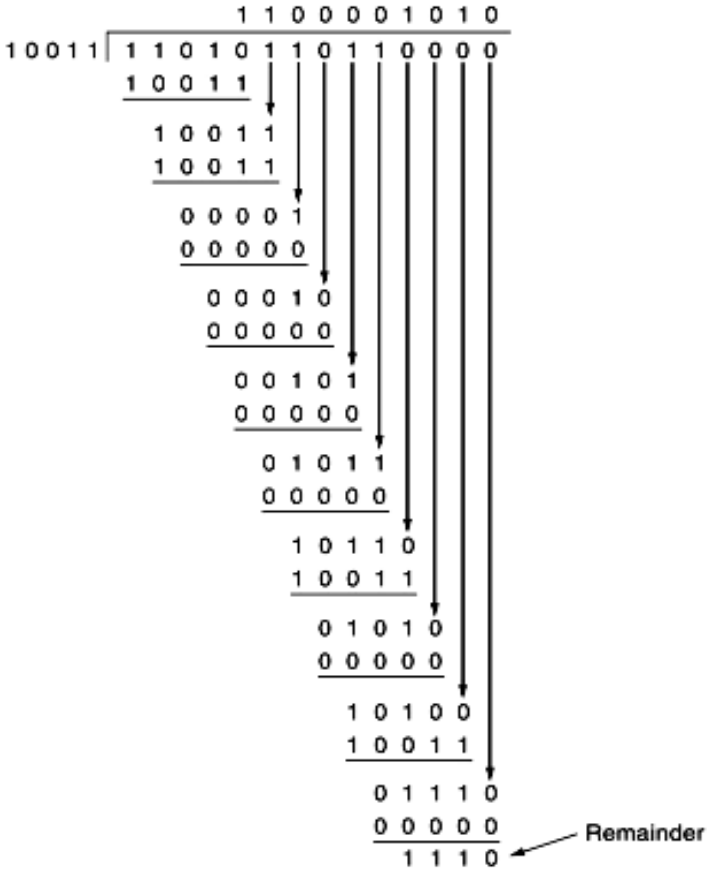
Problem-01:

A bit stream 1101011011 is transmitted using the standard CRC method. The generator polynomial is x^4+x+1. What is the actual bit string transmitted?

Solution-

- The generator polynomial $G(x) = x^4 + x + 1$ is encoded as 10011. (i.e.$x^4x^3\ x^2\ x^1x^0$)
- Clearly, the generator polynomial consists of 5 bits.
- So, a string of 4 zeroes is appended to the bit stream to be transmitted.
- The resulting bit stream is 1101011011**0000**.

Now, the binary division is performed as-



From here, CRC = 1110.

Now,

- The code word to be transmitted is obtained by replacing the last 4 zeroes of 1101011011**0000** with the CRC.
- Thus, the code word transmitted to the receiver = 1101011011**1110**.

Problem-02:

A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is x^3+1.

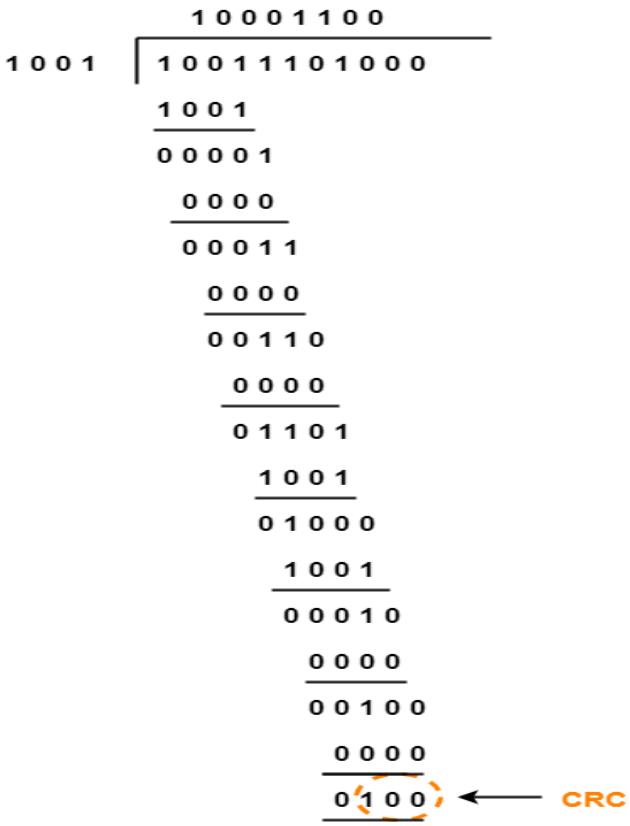
1. What is the actual bit string transmitted?
2. Suppose the third bit from the left is inverted during transmission. How will receiver detect this error?

Solution-

Part-01:

- The generator polynomial $G(x) = x^3 + 1$ is encoded as 1001.
- Clearly, the generator polynomial consists of 4 bits.
- So, a string of 3 zeroes is appended to the bit stream to be transmitted.
- The resulting bit stream is 10011101**000**.

Now, the binary division is performed as-



From here, CRC = 100.

Now,

- The code word to be transmitted is obtained by replacing the last 3 zeroes of 10011101**000** with the CRC.
- Thus, the code word transmitted to the receiver = 10011101**100**.

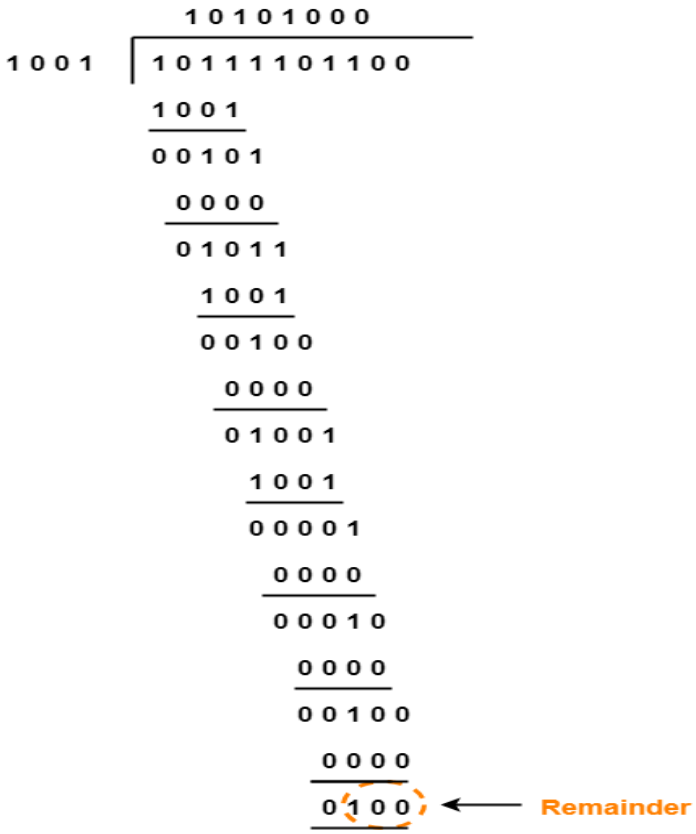
Part-02:

According to the question,

- Third bit from the left gets inverted during transmission.
- So, the bit stream received by the receiver = 10111101100.

Now,

- Receiver receives the bit stream = 10111101100.
- Receiver performs the binary division with the same generator polynomial as-



From here,

- The remainder obtained on division is a non-zero value.
- This indicates to the receiver that an error occurred in the data during the transmission.
- Therefore, receiver rejects the data and asks the sender for **retransmission**.

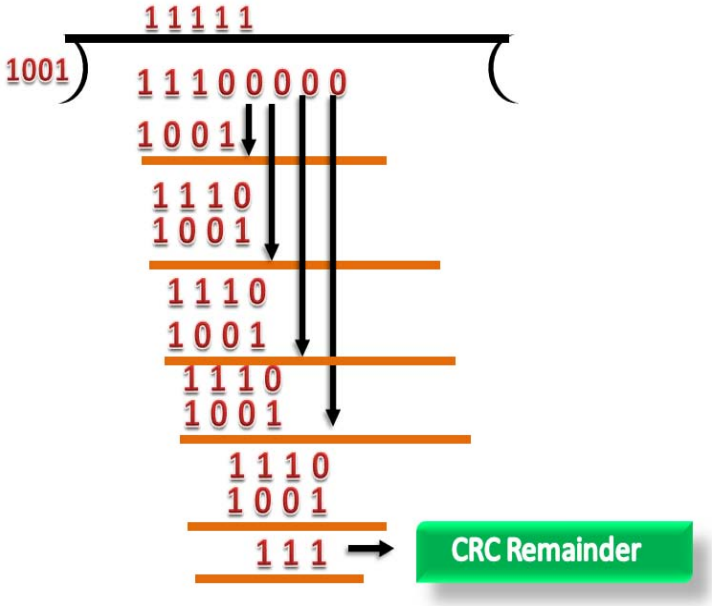
Example: **Suppose the original data is 11100 and divisor is 1001 CRC.**

Solution

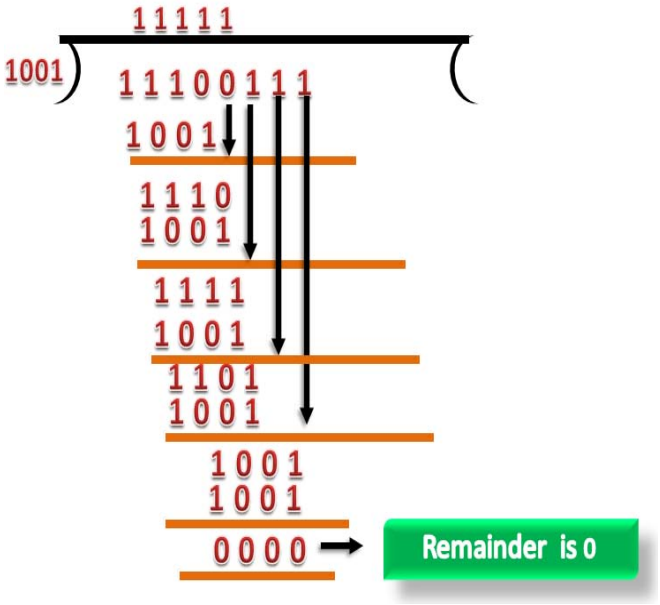
- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.

- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.

Sender



Receiver



Checksum

A Checksum is an error detection technique based on the concept of redundancy.

Error detection using checksum method involves the following steps-

Step-01:

At sender side,

- If m bit checksum is used, the data unit to be transmitted is divided into segments of m bits.
- All the m bit segments are added.
- The result of the sum is then complemented using 1's complement arithmetic.
- The value so obtained is called as **checksum**.

Step-02:

- The data along with the checksum value is transmitted to the receiver.

Step-03:

At receiver side,

- If m bit checksum is being used, the received data unit is divided into segments of m bits.
- All the m bit segments are added along with the checksum value.
- The value so obtained is complemented and the result is checked.

Then, following two cases are possible-

Case-01: Result = 0

If the result is zero,

- Receiver assumes that no error occurred in the data during the transmission.
- Receiver accepts the data.

Case-02: Result ≠ 0

If the result is non-zero,

- Receiver assumes that error occurred in the data during the transmission.
- Receiver discards the data and asks the sender for retransmission.

Checksum Example-

Consider the data unit to be transmitted is-

10011001111000100010010010000100

Consider 8 bit checksum is used.

Step-01:

At sender side,

The given data unit is divided into segments of 8 bits as-

10011001	11100010	00100100	10000100

Now, all the segments are added and the result is obtained as-

- 10011001 + 11100010 + 00100100 + 10000100 = 1000100011
- Since the result consists of 10 bits, so extra 2 bits are wrapped around.
- 00100011 + 10 = 00100101 (8 bits)
- Now, 1's complement is taken which is 11011010.
- Thus, checksum value = 11011010

Step-02:

- The data along with the checksum value is transmitted to the receiver.

Step-03:

At receiver side,

- The received data unit is divided into segments of 8 bits.
- All the segments along with the checksum value are added.
- Sum of all segments + Checksum value = 00100101 + 11011010 = 11111111
- Complemented value = 00000000
- Since the result is 0, receiver assumes no error occurred in the data and therefore accepts it.

Example 2:

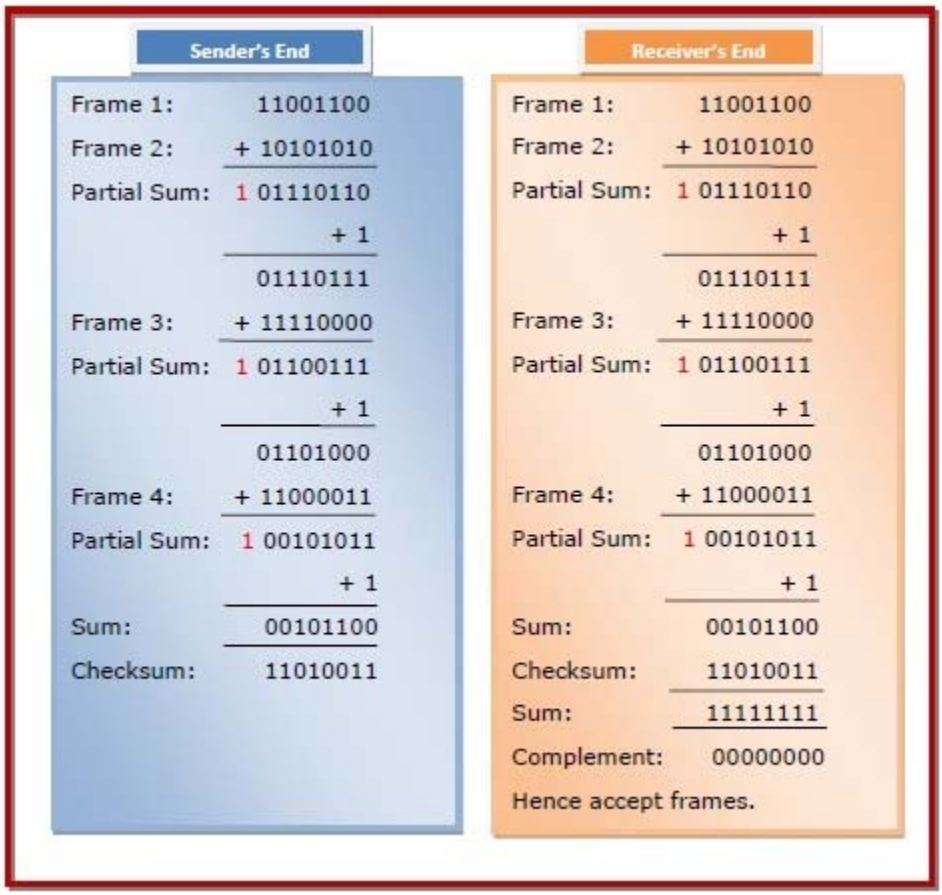
Suppose that the sender wants to send 4 frames each of 8 bits, where the frames are 11001100, 10101010, 11110000 and 11000011.

Solution:

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.

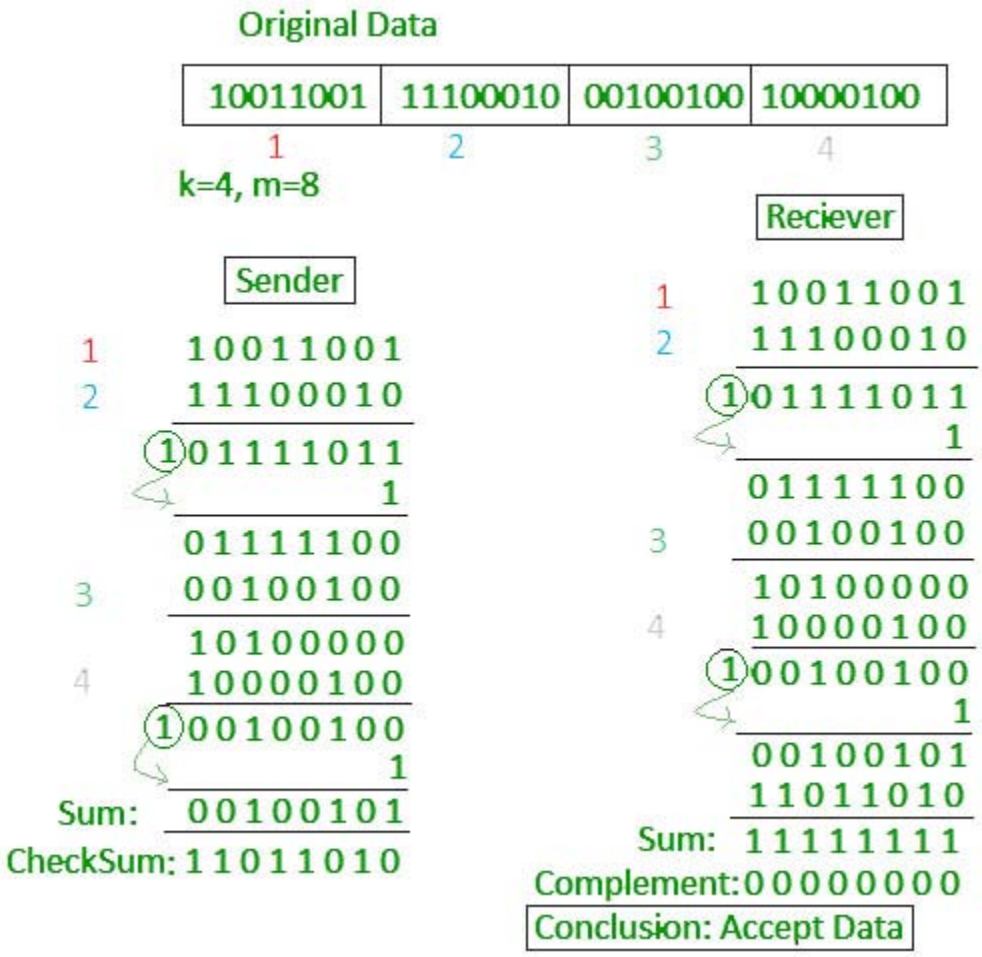
The receiver performs 1s complement arithmetic sum of all the frames including the checksum. The result is complemented and found to be 0. Hence, the receiver assumes that no error has occurred.



Sender's End		Receiver's End	
Frame 1:	11001100	Frame 1:	11001100
Frame 2:	+ 10101010	Frame 2:	+ 10101010
Partial Sum:	1 01110110	Partial Sum:	1 01110110
	+ 1		+ 1
	01110111		01110111
Frame 3:	+ 11110000	Frame 3:	+ 11110000
Partial Sum:	1 01100111	Partial Sum:	1 01100111
	+ 1		+ 1
	01101000		01101000
Frame 4:	+ 11000011	Frame 4:	+ 11000011
Partial Sum:	1 00101011	Partial Sum:	1 00101011
	+ 1		+ 1
Sum:	00101100	Sum:	00101100
Checksum:	11010011	Checksum:	11010011
		Sum:	11111111
		Complement:	00000000
		Hence accept frames.	

(Please see short details of Checksum example in above)

Example 3:



3.3	**Error Detection and Correction**		1

Error-Detecting codes

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. A simple example of error-detecting code is **parity check**.

Error-Correcting codes

Along with error-detecting code, we can also pass some data to figure out the original message from the corrupt message that we received. This type of code is called an error-correcting code. Error-correcting codes also deploy the same strategy as error-detecting codes but additionally, such codes also detect the exact location of the corrupt bit.

In error-correcting codes, parity check has a simple way to detect errors along with a sophisticated mechanism to determine the corrupt bit location. Once the corrupt bit is located, its value is reverted (from 0 to 1 or 1 to 0) to get the original message.

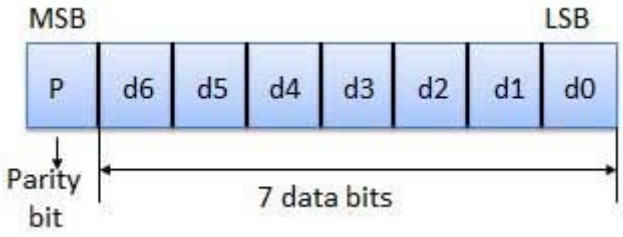
How to Detect and Correct Errors?

To detect and correct the errors, additional bits are added to the data bits at the time of transmission.

- The additional bits are called **parity bits**. They allow detection or correction of the errors.
- The data bits along with the parity bits form a **code word**.

Parity Checking of Error Detection

It is the simplest technique for detecting and correcting errors. The MSB of an 8-bits word is used as the parity bit and the remaining 7 bits are used as data or message bits. The parity of 8-bits transmitted word can be either even parity or odd parity.



Even parity -- Even parity means the number of 1's in the given word including the parity bit should be even (2,4,6,....).

Odd parity -- Odd parity means the number of 1's in the given word including the parity bit should be odd (1,3,5,....).

Use of Parity Bit

The parity bit can be set to 0 and 1 depending on the type of the parity required.

- For even parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is even. Shown in fig. (a).
- For odd parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is odd. Shown in fig. (b).

Fig. (a)

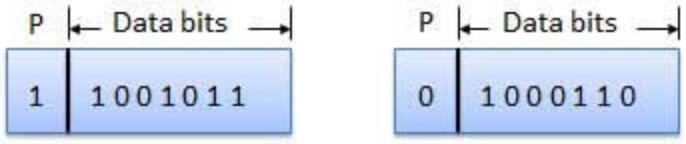
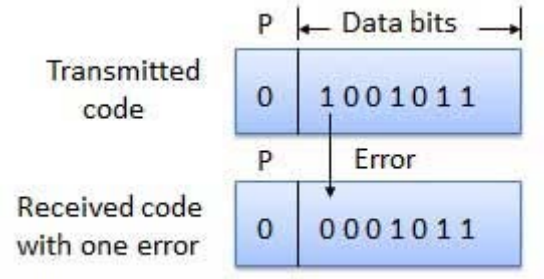


Fig. (b)

How Does Error Detection Take Place?

Parity checking at the receiver can detect the presence of an error if the parity of the receiver signal is different from the expected parity. That means, if it is known that the parity of the transmitted signal is always going to

be "even" and if the received signal has an odd parity, then the receiver can conclude that the received signal is not correct. If an error is detected, then the receiver will ignore the received byte and request for retransmission of the same byte to the transmitter.



More research

https://computernetwork-mmc.blogspot.com/2020/04/error-correction-hamming-code-in_15.html

Hamming Code

Parity bits: The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity bit is 1.

Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

General Algorithm of Hamming code –

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

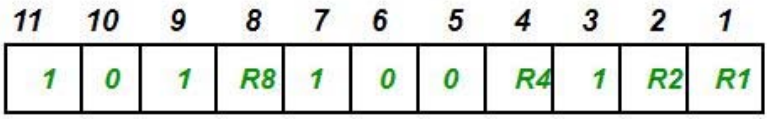
1. Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
2. All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
3. All the other bit positions are marked as data bits.
4. Each data bit is included in a unique set of parity bits, as determined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

Determining the position of redundant bits – **(problem in Class notes)**

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

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

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

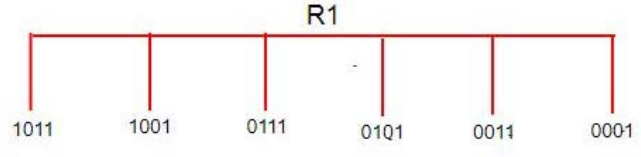


Determining the Parity bits –

Even=0 & Odd =1

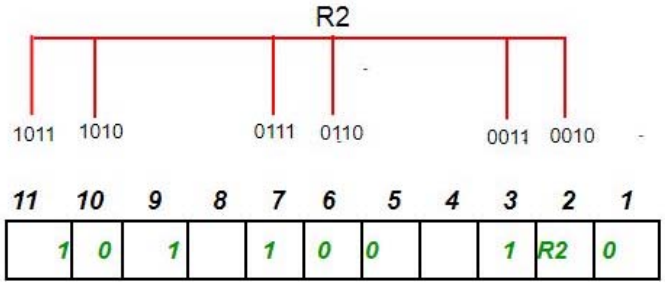
R1: bits 1, 3, 5, 7, 9, 11

1's even number the value of R1 (parity bit's value) = 0



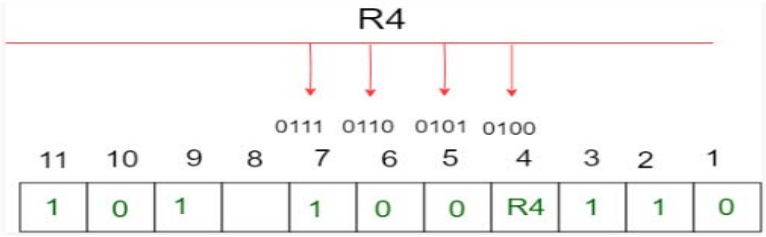
R2: bits 2,3,6,7,10,11

1's odd the value of R2(parity bit's value)=1



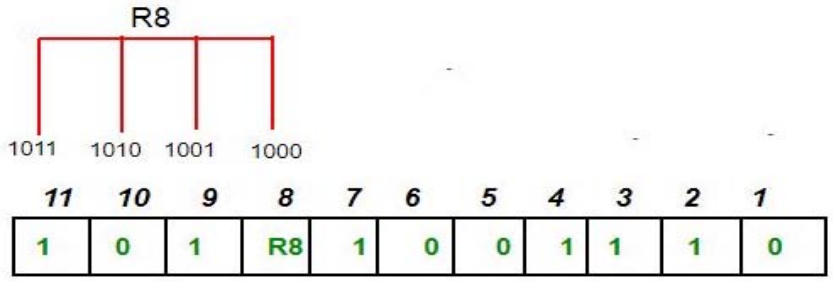
R4: bits 4, 5, 6, 7

1's is odd the value of R4(parity bit's value) = 1

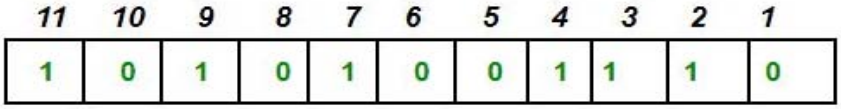


R8: bit 8,9,10,11

1's is an even number the value of R8(parity bit's value)=0.

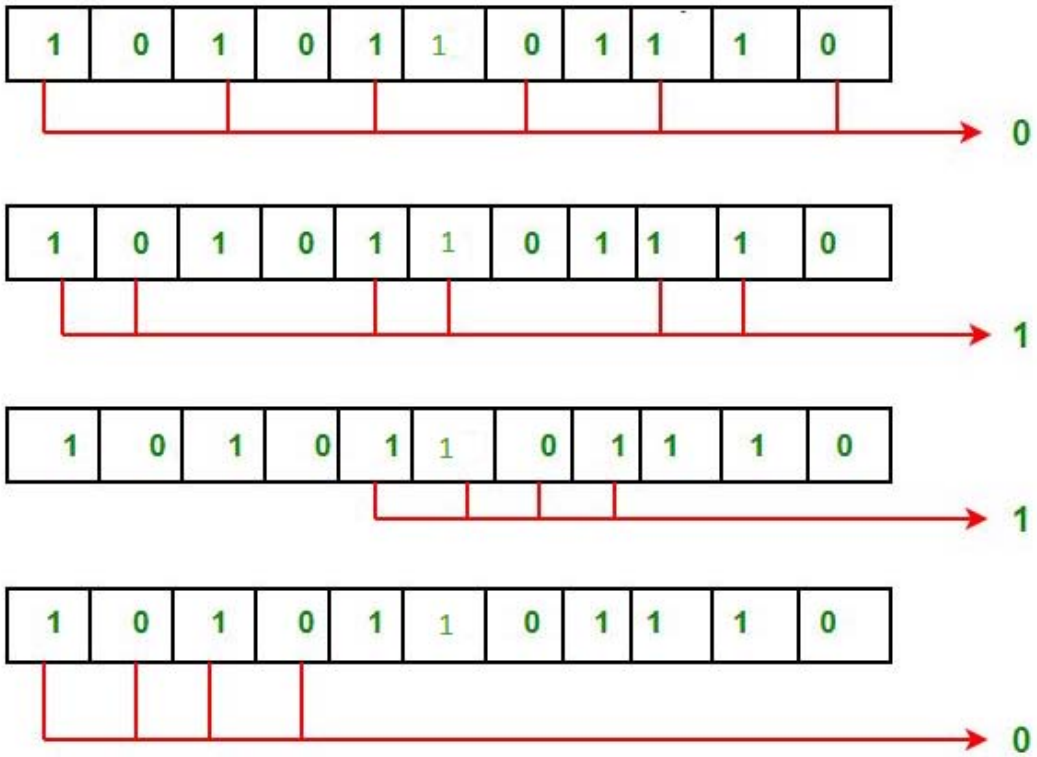


Thus, the data transferred is:



Error detection and correction –

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



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

3.4	**High-Level Data Lin k Control(HDLC) & Point - to - Point protocol(PPP)**		**1**

High-Level Data Lin k Control(HDLC)

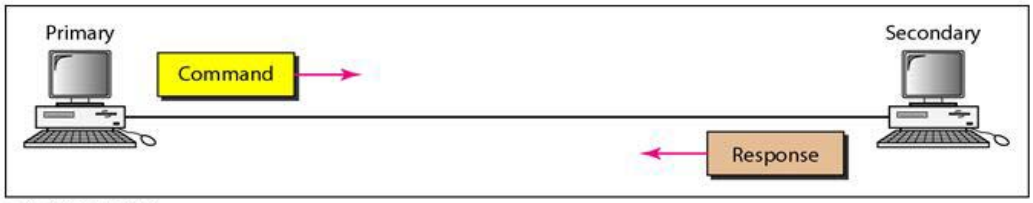
- High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival.
- High-level Data Link Control (HDLC) is a **bit-oriented protocol for communication** over point-to-point and multipoint links. It implements the ARQ mechanisms.

Configurations and Transfer Modes:

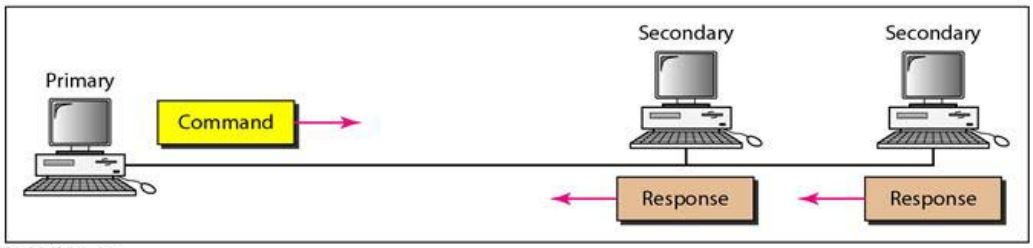
HDLC provides two common transfer modes that can be used in different configurations: normal response mode (NRM) and asynchronous balanced mode (ABM).

Normal Response Mode:

Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



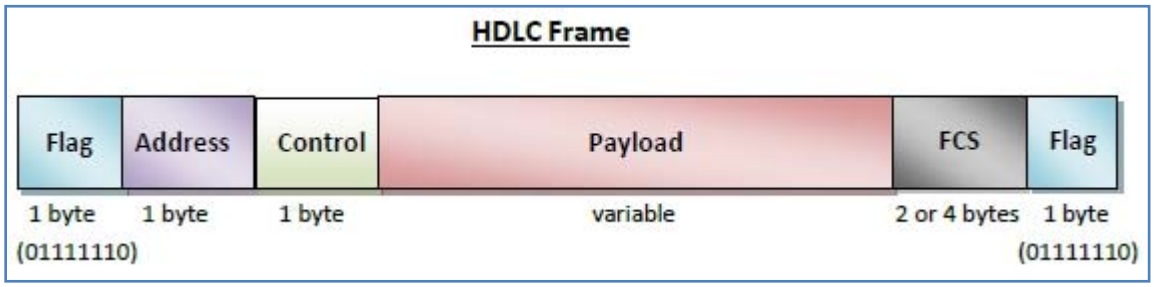
a. Point-to-point



b. Multipoint

Asynchronous Balanced Mode:

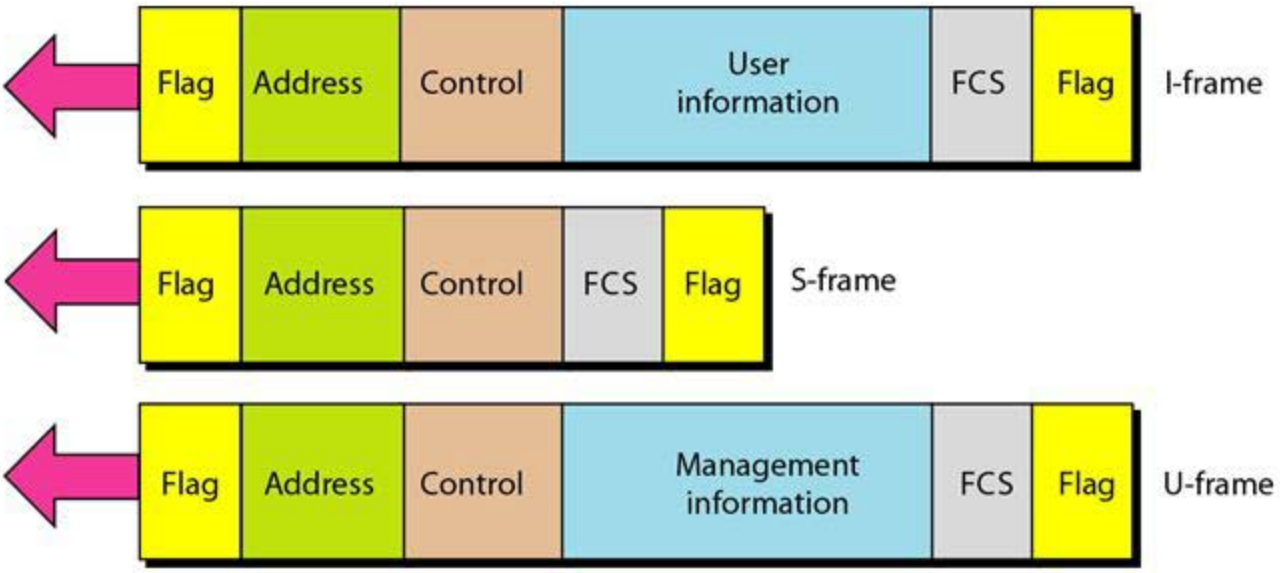
Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



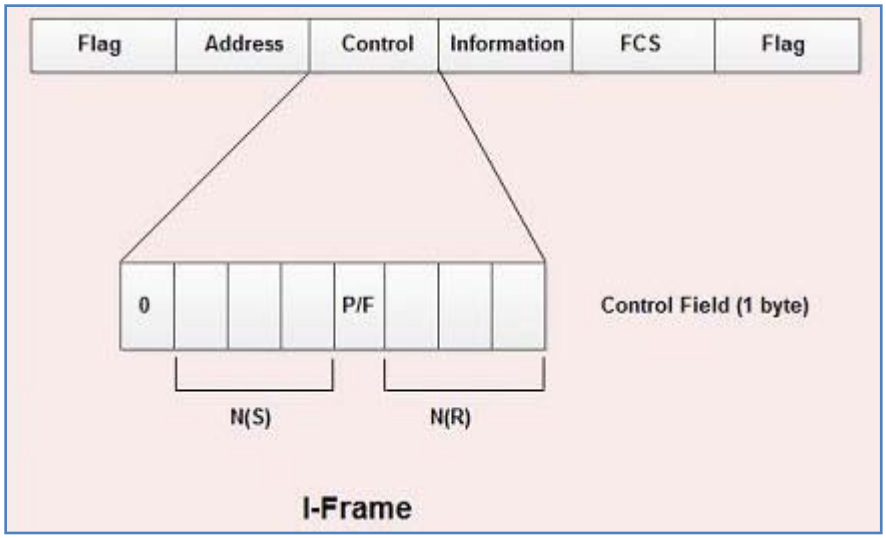
The fields of a HDLC frame are −

- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

- ## Types of HDLC Frames



1. **I-frame –** I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.



N(S) = sequence number of the frame

N(R) = sequence number of the frame expected in return in two-way communication

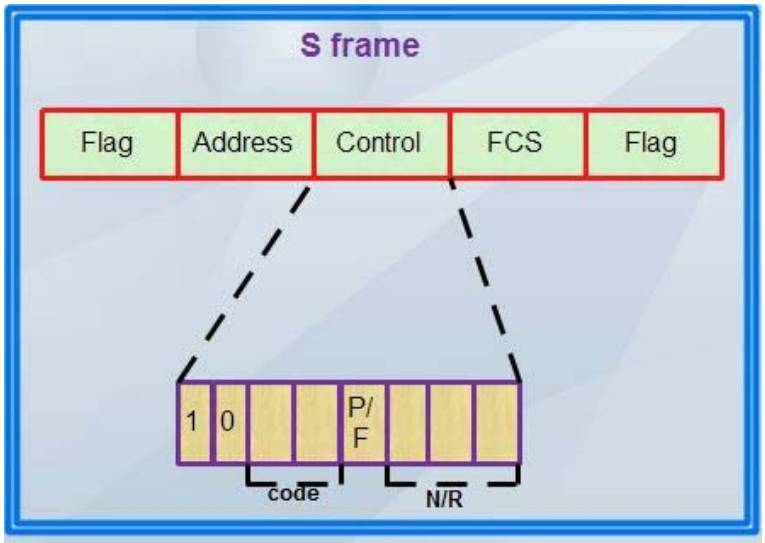
P/F= Poll/Final

When P/F =1 , it follow two case:

Poll when Frame is sent by a primary station to secondary (address of receiver)

Final when frame is send by secondary to primary (address of sender)

2. **S-frame** – S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.



3. **U-frame** – U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.

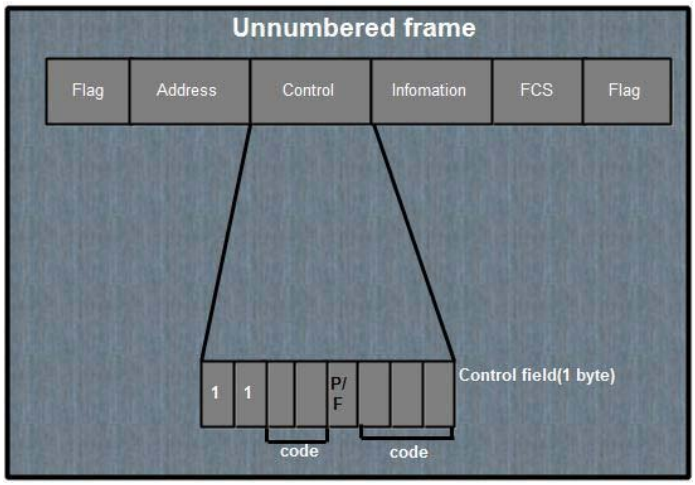


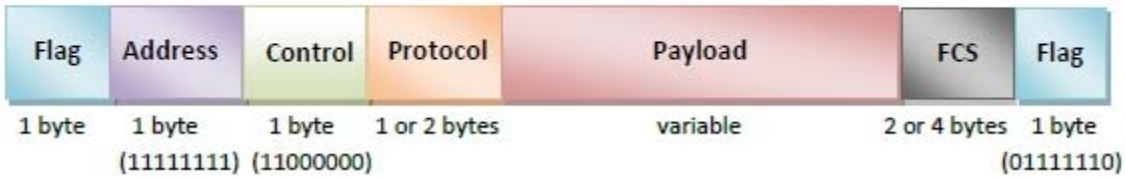
Table: Types of S-frame

Code	Command
00	RR Receive Ready
01	REJ Reject
10	RNR Receive Not Ready
11	SREJ Selective Reject

Point - to - Point Protocol (PPP)

- Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers.
- It is a **byte - oriented protocol** that is widely used in broadband communications having heavy loads and high speeds.
- Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.
- One of the most common protocols for point-to-point access
- Many Internet users who need to connect their home computer to the server of an Internet service provider use PPP
- A point-to-point link protocol is required to control and manage the transfer of data
- **PPP defines/provides**
    - ✓ the format of the frame to be exchanged between devices
    - ✓ how two devices negotiate the establishment of the link and the exchange of data
    - ✓ how network layer data are encapsulated in the data link frame
    - ✓ how two devices can authenticate each other
    - ✓ multiple network layer services
    - ✓ connection over multiple links
    - ✓ Network address configuration
- But, several services are missing for simplicity
    - ✓ no flow control, simple error control (detection and discard), no sophisticate addressing for multipoint configuration

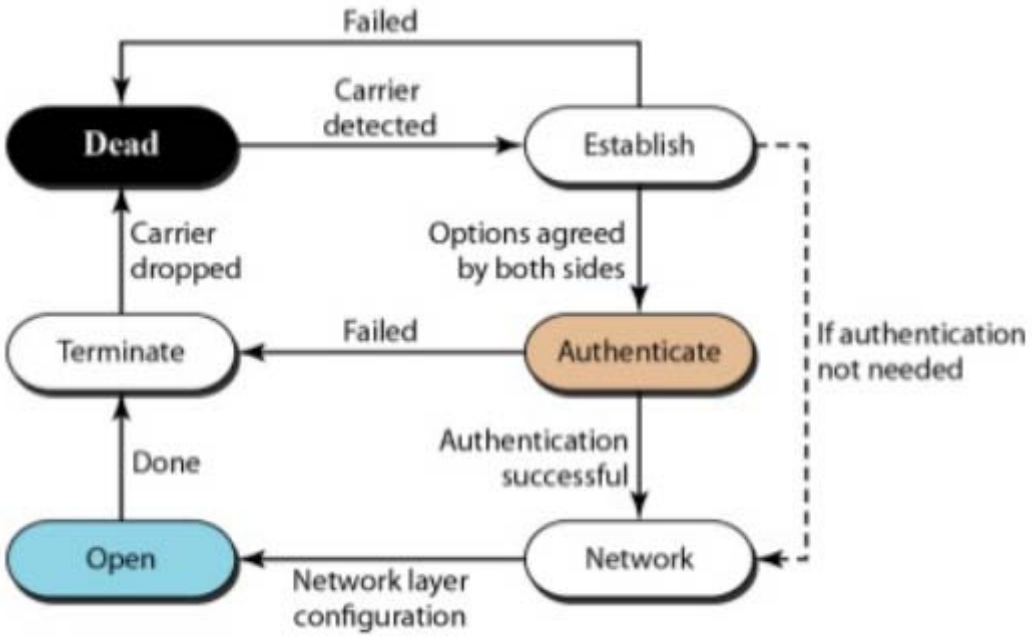
PPP Frame



- **Flag** − marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** – it is set to 11111111 in case of broadcast.
- **Control** − set to a constant value of 11000000.(No need because PPP has no flow control and limited error control)
- **Protocol** − 1 or 2 bytes that define the type of data contained in the payload field.
- **Payload** − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

❖ *PPP is a byte-oriented protocol using byte stuffing with the escape byte 01111101*

PPP: Transition States

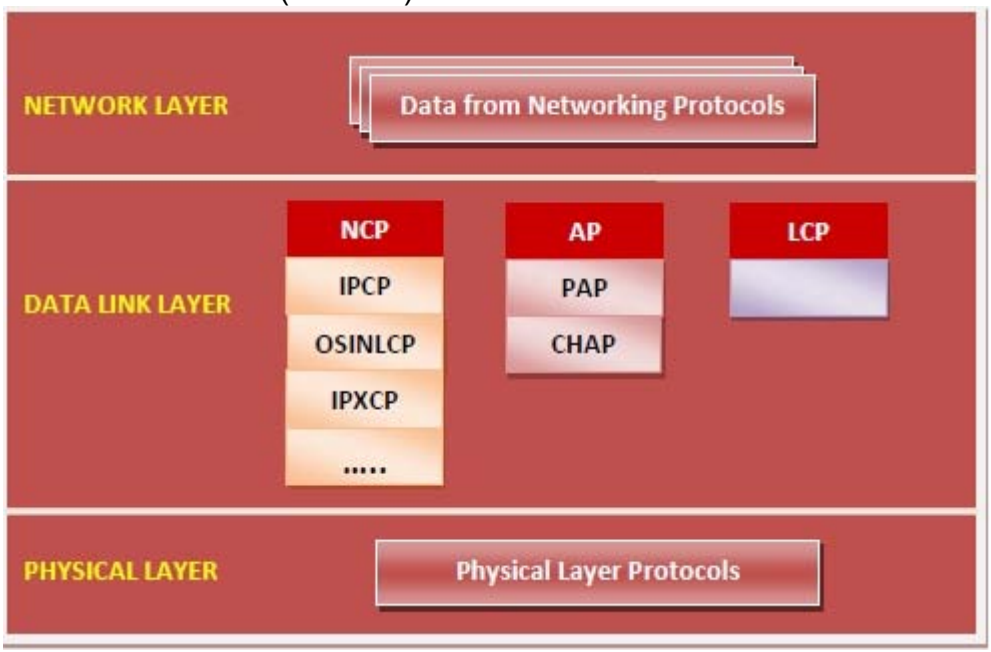


Components of PPP

Point - to - Point Protocol is a layered protocol having three components −

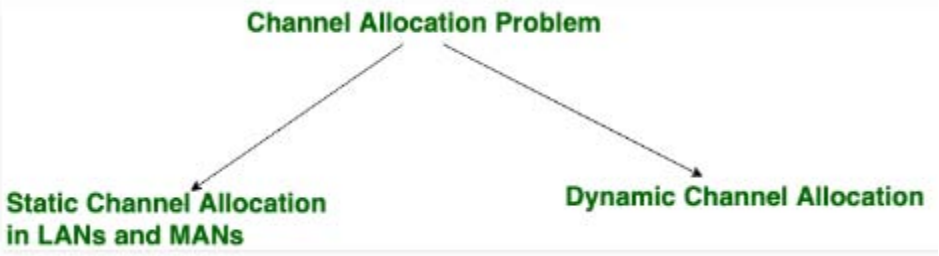
Encapsulation Component − It encapsulates the datagram so that it can be transmitted over the specified physical layer.

- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Authentication Protocols (AP)** − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are:
    - Password Authentication Protocol (PAP)
    - Challenge Handshake Authentication Protocol (CHAP)
- **Network Control Protocols (NCPs)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are:
    - Internet Protocol Control Protocol (IPCP)
    - OSI Network Layer Control Protocol (OSINLCP)
    - Internetwork Packet Exchange Control Protocol (IPXCP)
    - DECnet Phase IV Control Protocol (DNCP)
    - NetBIOS Frames Control Protocol (NBFCP)
    - IPv6 Control Protocol (IPV6CP)



3.5	Channel Allocation Problem		0.5

- When there are more than one user who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users.
- The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.
- Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.
- Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place.
- If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, than Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.
- Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.



Static Channel Allocation

- In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user. For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.
- This scheme is also referred as fixed channel allocation or fixed channel assignment.
- It is not efficient to divide into fixed number of chunks.

```
T = 1/(U*C-L)

T(FDM) = N*T(1/U(C/N)-L/N)
```

Where,

```
T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time
```

- In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel. However, it is not suitable in case of a large number of users with variable bandwidth requirements.

Dynamic Channel Allocation

- In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.
- This allocation scheme optimizes bandwidth usage and results is faster transmissions.
- Dynamic channel allocation is further divided into centralized and distributed allocation.

Possible assumptions include:

1. **Station Model:**
   Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.

2. **Single Channel Assumption:**
   In this allocation all stations are equivalent and can send and receive on that channel.

3. **Collision Assumption:**
   If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must re transmitted. Collisions are only possible error.

4. **Time** can be divided into Slotted or Continuous.

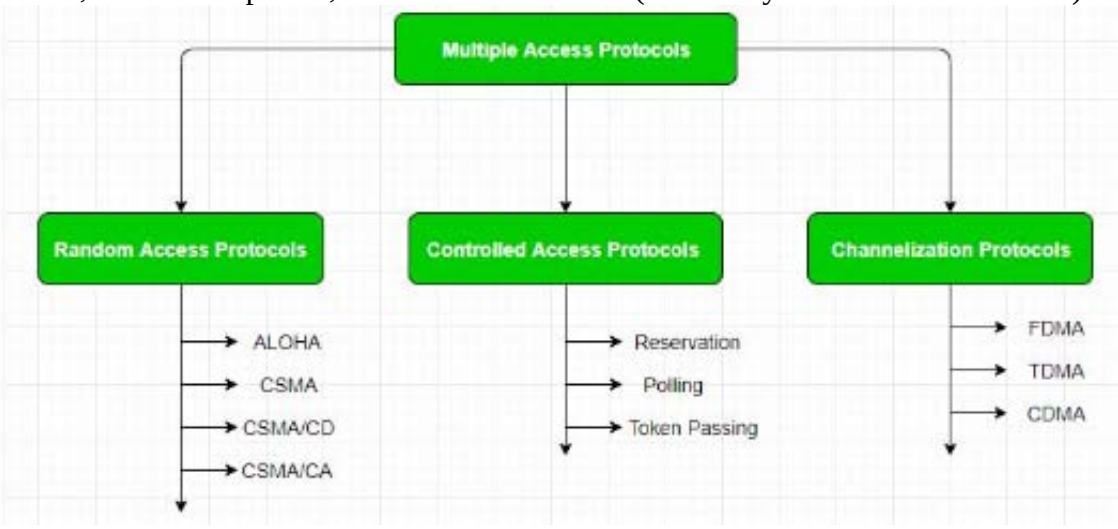
5. **Stations** can sense a channel is busy before they try it.

3.6	**Multiple Access:** **1. Radom Access(ALOHA, CSMA, CSMN CD, CSMA/CA),** **2. Controlled Access(Reservation, Polling, Token Passing),** **3. Channelization(FDMA, TOMA, CDMA)**		**1**

Media Access(Multiple Access)

• In random access or contention methods, no station is superior to another station and none is assigned the control over another

• No station permits, or does not permit, another station to send(Randomly send if medium is free)



ALOHA

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

There are two different versions of ALOHA:

1. Pure Aloha

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

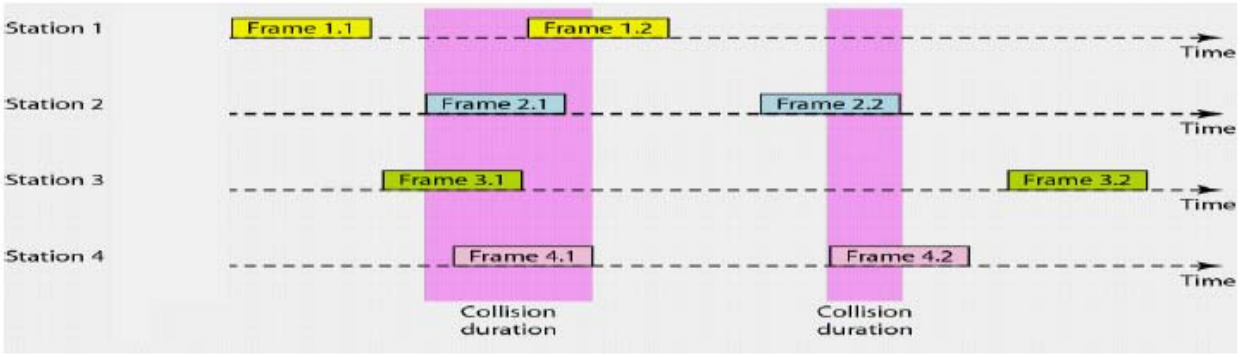
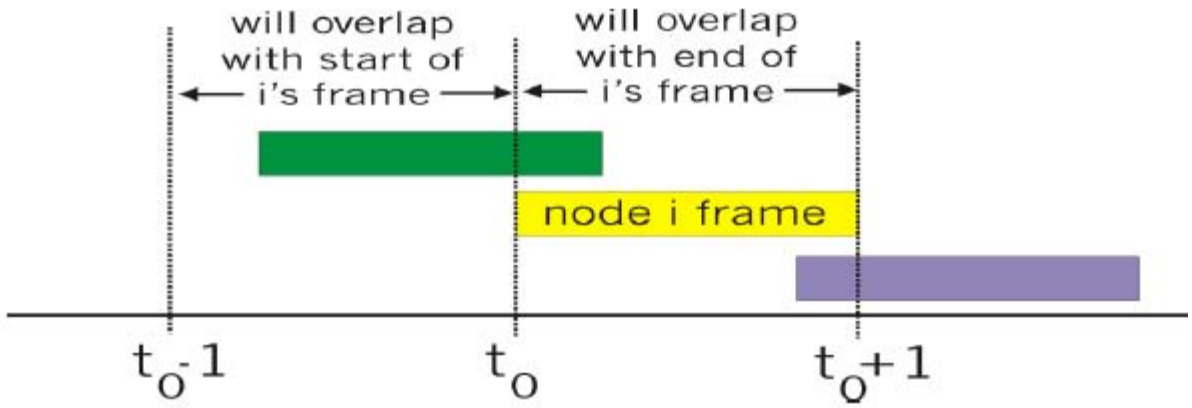


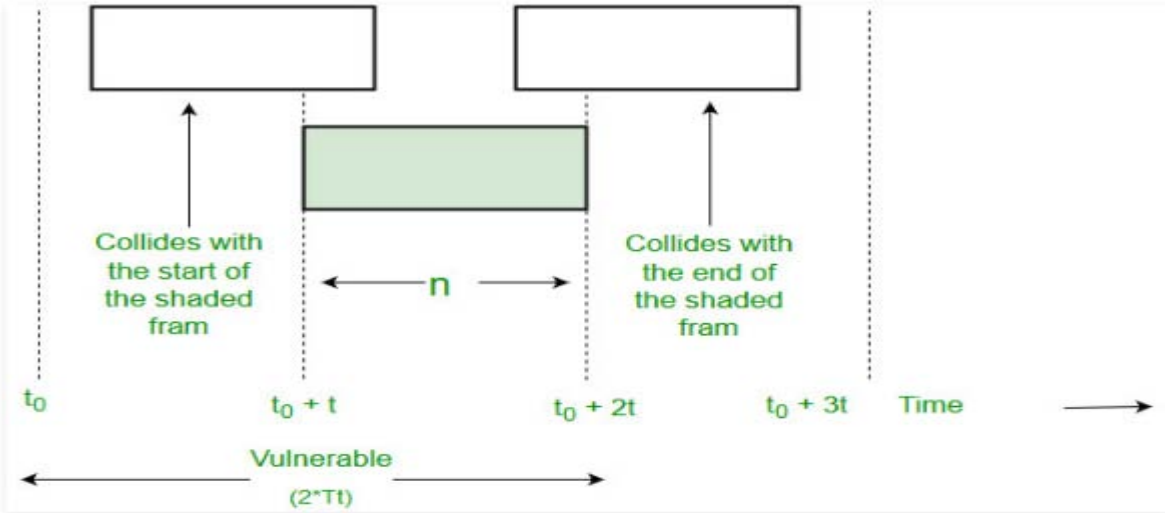
Figure 4-1. In pure ALOHA, frames are transmitted at completely arbitrary times.

- For that to make some assumption:

  i) All the frames should be the same length.
  ii) Stations can not generate frame while transmitting or trying to transmit frame.
  iii)The population of stations attempts to transmit (both new frames and old frames that collided) according to a Poisson distribution.



Overlapping frames in the pure ALOHA protocol. Frame-time is equal to 1 for all frames.



Vulnerable Time = 2 * Tt

Efficiency of Pure ALOHA:

Spure= G * e^-2G
where G is number of stations wants to transmit in Tt slot.

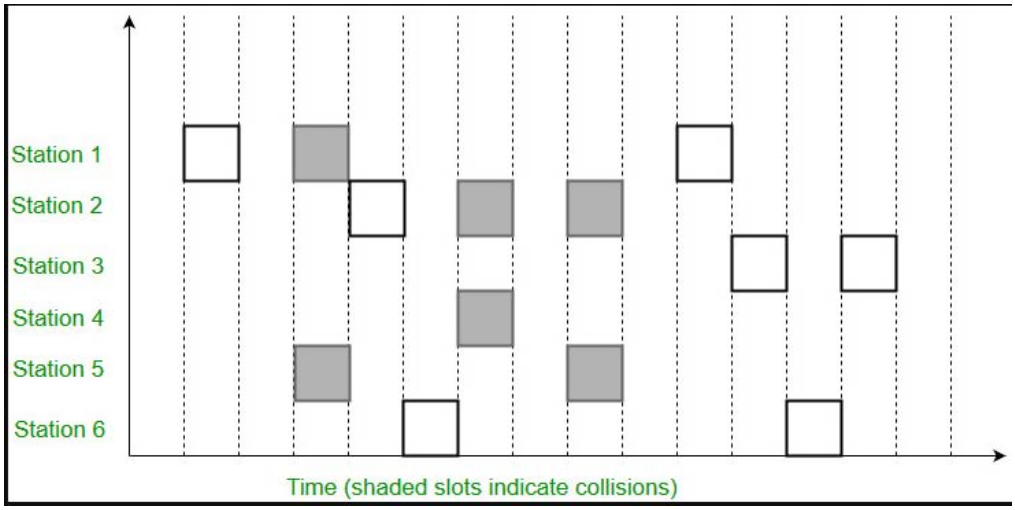
Maximum Efficiency:
Maximum Efficiency will be obtained when G=1/2

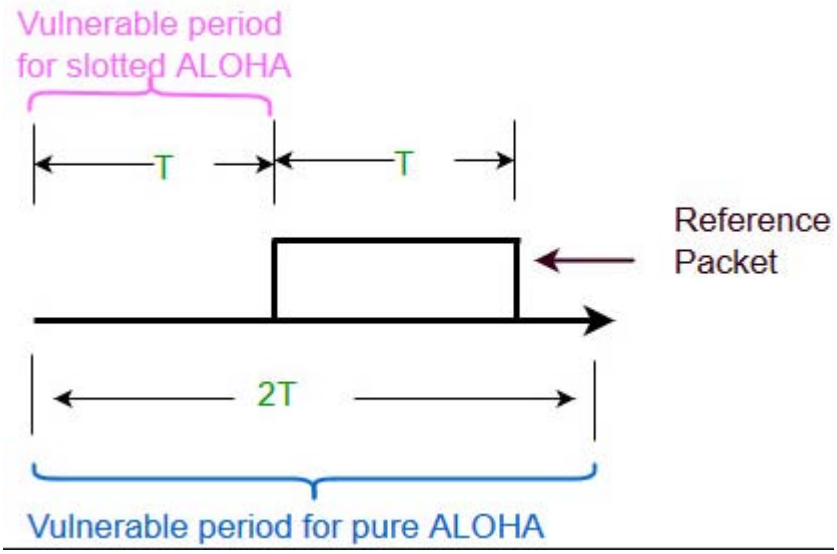
(**S**pure)*max* = 1/2 * e^-1
= 0.184

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

2. Slotted Aloha

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





Collision is possible for only the current slot. Therefore, Vulnerable Time is Tt.

Efficiency of Slotted ALOHA:

```
 Sslotted = G * e^-G

Maximum Efficiency:
(Sslotted)max = 1 * e^-1
              = 1/e = 0.368
Maximum Efficiency, in Slotted ALOHA, is 36.8%.
```

Pros (advantage)

• single active node can continuously transmit at full rate of channel

• highly decentralized: only slots in nodes need to be in sync

• simple

Cons (disadvantage)

• collisions, wasting slots

• idle slots

• nodes may be able to detect collision in less than time to transmit packet

• clock synchronization

Carrier Sense Multiple Access (CSMA):

- Invented to minimize collisions and increase the performance
- A station now "follows" the activity of other stations
- Simple rules for a polite human conversation
    1. Listen before talking
    2. If someone else begins talking at the same time as you, stop talking
- A node should not send if another node is already sending(Carrier Sensing)
- Vulnerable time is the propagation time which is the time needed for a signal to propagate from one end of the medium to the other

CSMA (Persistence Methods)

• Persistence methods :- Methods for Sensing the channel (busy/ idle)

• 3 Persistence methods are available:

1. I-persistence

2. Non-persistence

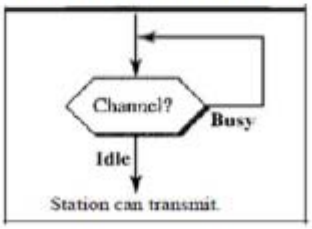
3. P-persistence

6.2.1.1. I-Persistence Method

- **In** this method, after the station finds the line idle, it sends its frame immediately (with probability I)
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately

Figure : Behaviour I persistence

Figure : Flow diagram of I persistence



6.2.1.2. Non-Persistence Method

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

Figure : Behaviour of Non persistence

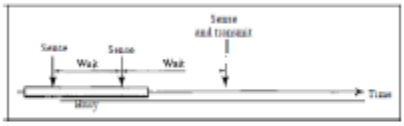
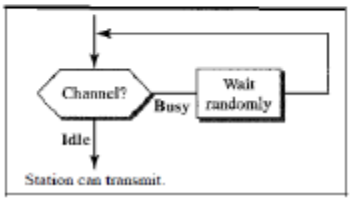


Figure : Flow diagram of Non persistence



6.2.1.3. P-Persistence Method

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

Figure : Behaviour P persistence

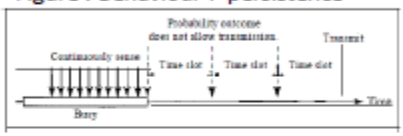
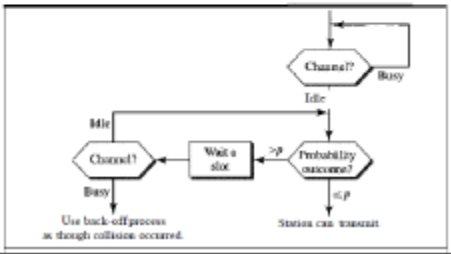


Figure : Flow diagram of P persistence



*This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the datalink layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.*

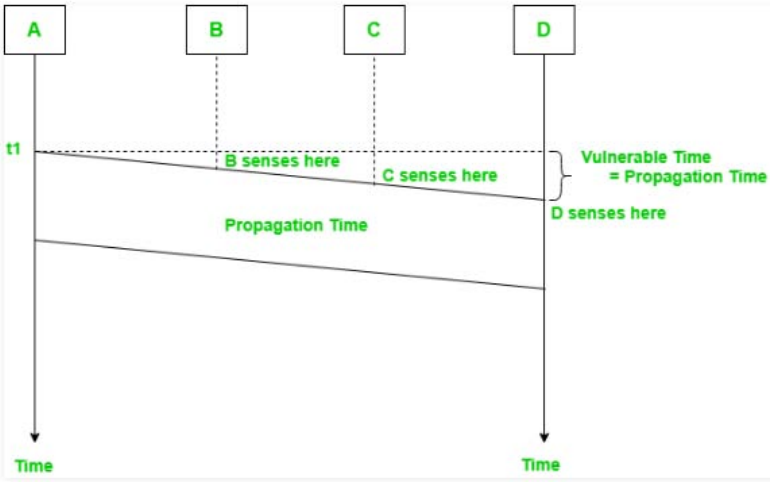
Vulnerable Time –

```
Vulnerable time = Propagation time (Tp)
```

Carrier Sense Multiple Access (CSMA) is a probabilistic Media Access Control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum.

"**Carrier Sense**" describes the fact that a transmitter uses feedback from a receiver that detects a carrier wave before trying to send. That is, it tries to detect the presence of an encoded signal from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission.

"**Multiple Access**" describes the fact that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations using the medium.



The persistence methods can be applied to help the station take action when the channel is busy/idle.

ADVANTAGES

- ☐ Fairly simple to implement
- ☐ Functional scheme that works

DISADVANTAGES

- ☐ Cannot recover from a collision (inefficient waste of medium time)

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

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.If succcessful, the station is finished, if not, the frame is sent again.

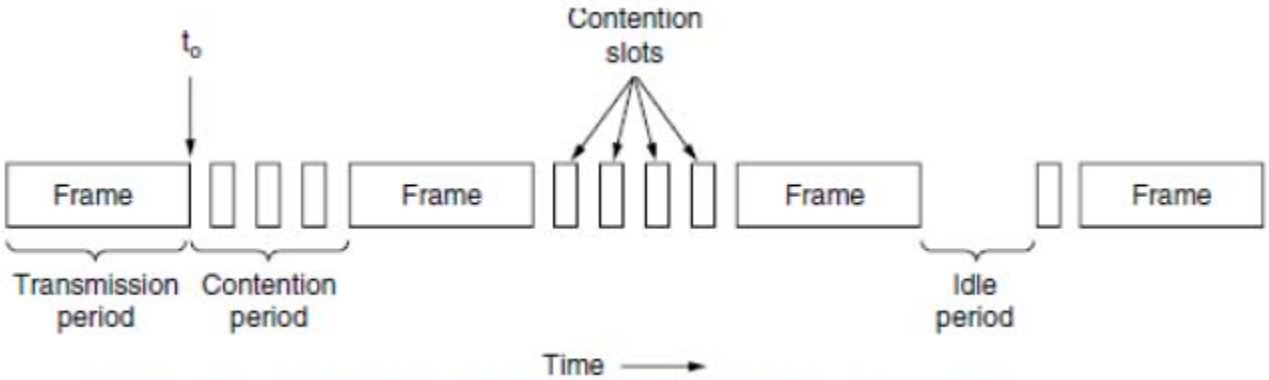
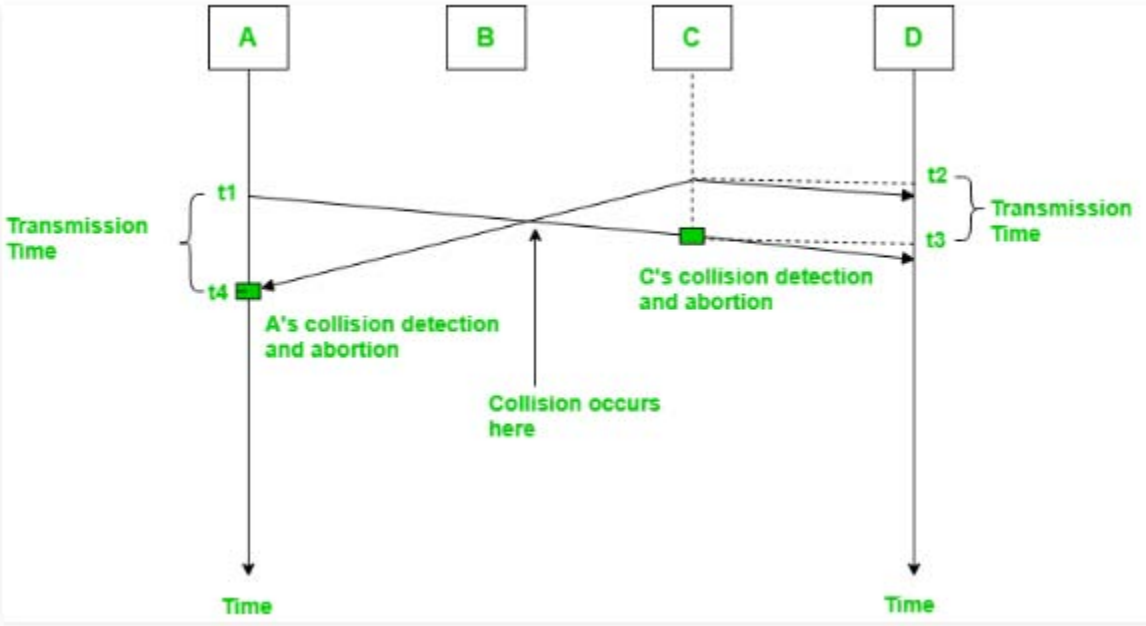


Figure 4-5. CSMA/CD can be in contention, transmission, or idle state.

In CSMA/CD Channel can be in one of the three states: contention, transmission, and idle.

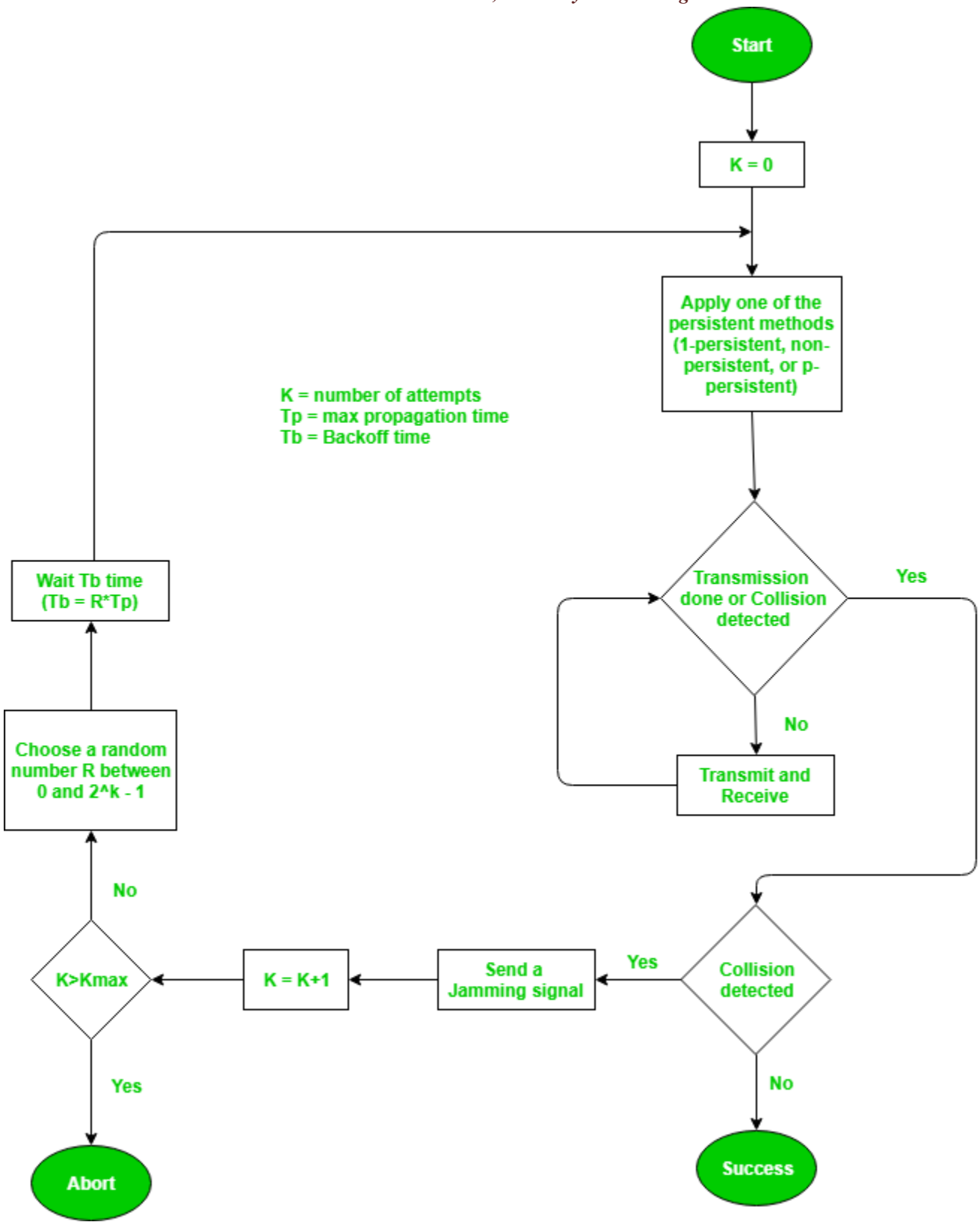


In the diagram, A starts send the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is therefore t3 – t2 and for A's frame is t4- t1.

So, the **frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp)**. This can be deduced when the two stations involved in collision are maximum distance apart.

Process –

The entire process of collision detection can be explained as follows:



Throughput and Efficiency – The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

- For 1-persistent method throughput is 50% when G=1.
- For non-persistent method throughput can go upto 90%.

JAM SIGNAL

The **jam signal** is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations that they must not transmit.

ADVANTAGES

More efficient than basic CSMA

DISADVANTAGES

Requires ability to detect collisions

2. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of received signal almost doubles and the station can sense the possibility of collision. In case of wireless networks, most of the energy is used for transmission and the energy of received signal increases by only 5-10% if collision occurs. It can't be used by station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.
These are three type of strategies:

1. **InterFrame Space (IFS) –** When a station finds the channel busy, it waits for a period of time called IFS time. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
2. **Contention Window –** It is the amount of time divided into slots.A station which is ready to send frames chooses random number of slots as **wait time**.
3. **Acknowledgements –** The positive acknowledgements and time-out timer can help guarantee a successful transmission of the frame.

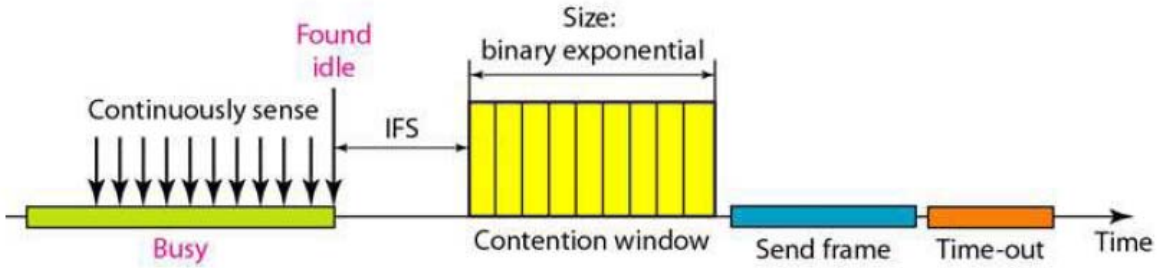
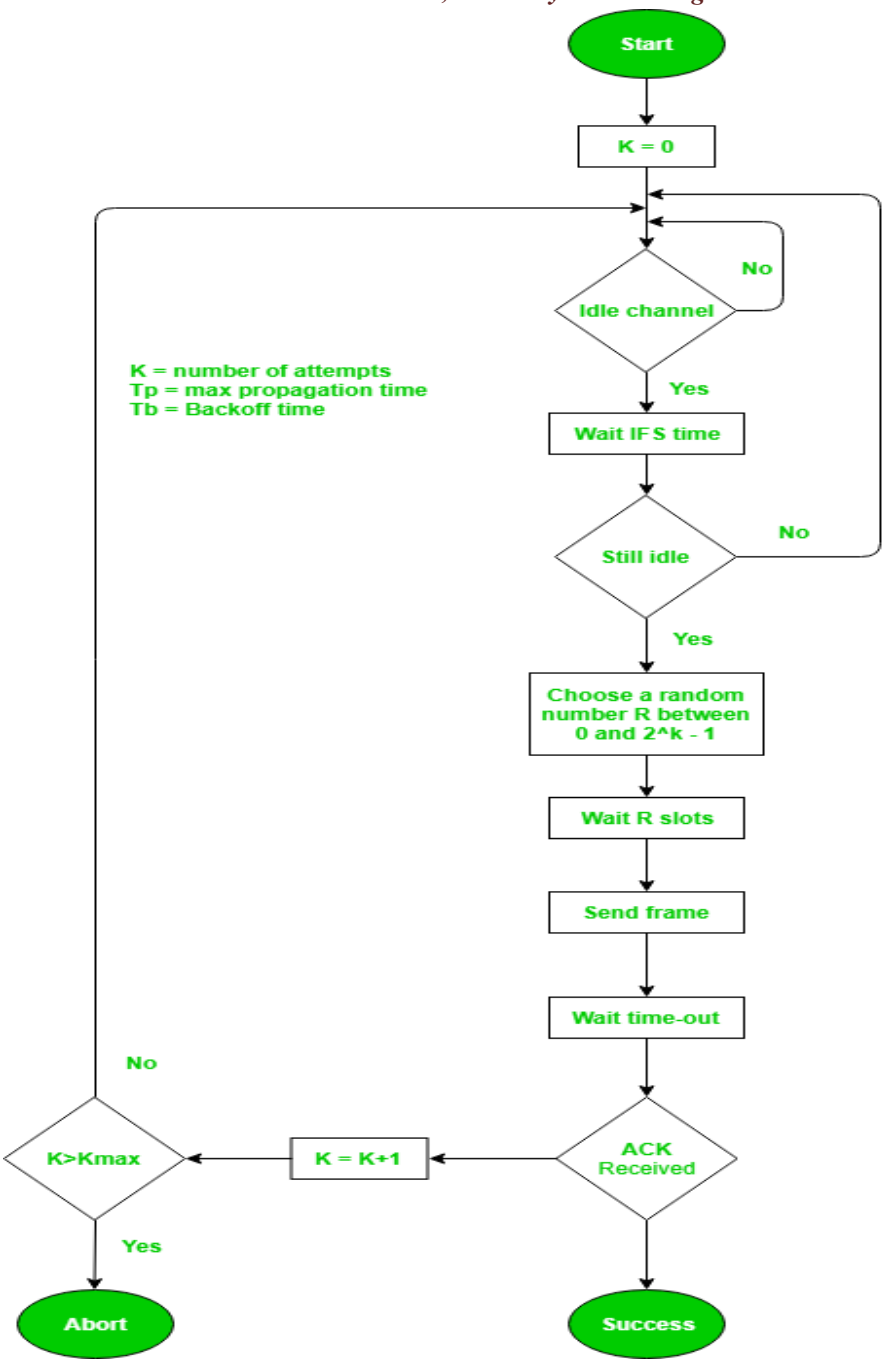


Figure : Timing in CSMA/CA

Process –
The entire process for collision avoidance can be explained as follows:



Let's see the difference between CSMA/CA and CSMA/CD:-

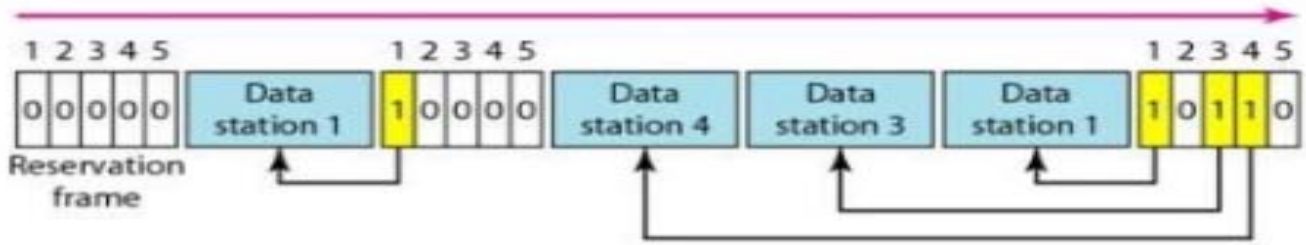
S.NO	CSMA/CD	CSMA/CA
1.	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
2.	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3.	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4.	CSMA / CD resend the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5.	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.
6.	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	While it is similar to simple CSMA(Carrier Sense Multiple Access).

CONTROLLED ACCESS

- In controlled access, the stations consults each other to find which station has right to send.
- Controlled access protocols grants permission to send only one node at a time, to avoid collision of messages on the shared medium.
- A station cannot send data unless it is authorized by the other stations.
- **Now we will discuss three named controlled access methods.**

1. Reservation. Ex: cable modem
2.Polling. Ex: HDLC(normal response mode)
3.Token Passing. Ex: Token Ring, Token Bus.

1.RESERVATION



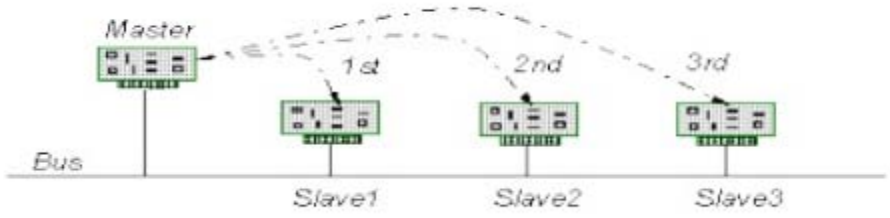
The following figure shows a situation with five stations and a five slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

- In the reservation method, a station needs to make a reservation before sending data.
- Time is divided into intervals.
- In each interval, a reservation frame precedes the data frames sent in that interval
- If there are N stations in the system, there are exactly N reservation mini slots in the reservation frame.
- Each mini slot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own mini slot.
- The stations that have made reservations can send their data frames after the reservation frame a situation with five stations and a five minislot reservation frame.
- a situation with five stations and a five minislot reservation frame.

- *In the reservation method, a station needs to make a reservation before sending data.*
- *The time line has two kinds of periods:*
  1. *Reservation interval of fixed time length*
  2. *Data transmission period of variable frames.*
- *If there are M stations, the reservation interval is divided into M slots, and each station has one slot.*
- *Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.*
- *In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.*
- *The stations which have reserved their slots transfer their frames in that order.*
- *After data transmission period, next reservation interval begins.*
- *Since everyone agrees on who goes next, there will never be any collisions.*

2.POLLING

- To impose order on a network of independent users and to establish one station in the network as a controller that periodically polls all other stations which is called Polling.

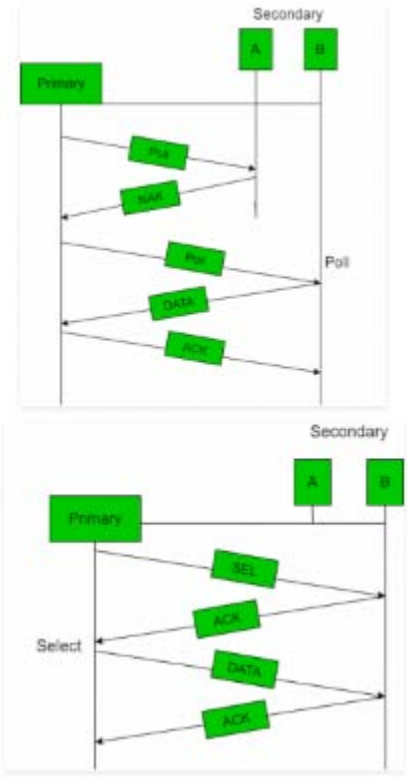


- There are two general polling policies:

i. Round Robin Order
ii. Priority Order

- It works with topologies in which one device is designated as a ***Primary*** Station and the other devices are ***Secondary*** Stations.
- The Primary device controls the link, where as the secondary follows it's instructions.
- Exchange of data must be made through the primary device even though the final destination is secondary.

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



Efficiency

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

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

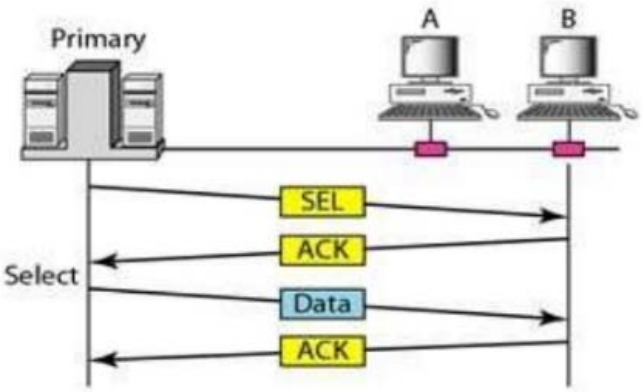
SELECT FUNCTION:

- Whenever primary has something to send, it sends the message to each node.

- Before Sending the data, it creates and transmits a Select(***SEL***) frame, one field of it includes the address of the intended secondary.

- While sending, the primary should know whether the target device is ready to receive or not.

- Hence, it alerts the secondary for the upcoming transmission and wait for an acknowledgement (ACK) of secondary's status.



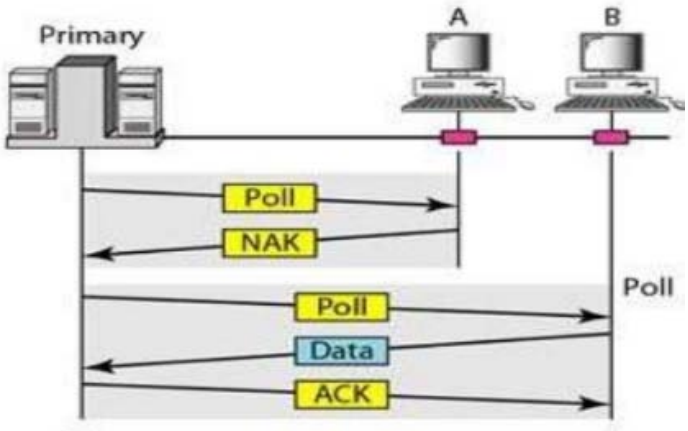
POLL FUNCTION:

- When the primary is ready to receive data, it must ask (*poll*) each device if it has anything to send.

- If the secondary has data to transmit, it sends the data frame. Otherwise, it sends a negative acknowledgement(*NAK*) .

- The primary then polls the next secondary. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (*ACK*).

- There are two possibilities to terminate the transmission: either the secondary sends all data, finishing with an *EOT* frame, or the primary says timer is up.



Advantages:

- Priorities can be assigned to ensure faster access from some secondary .
- Maximum and minimum access times and data rates on the channel are predictable and fixed.

Drawbacks:

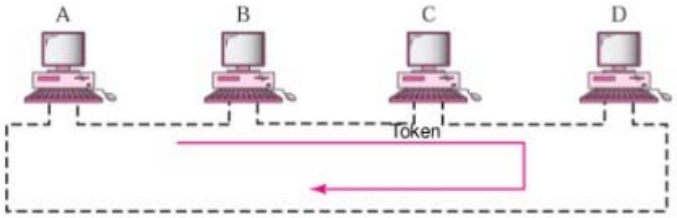
- High dependence on the reliability of the controller.
- Increase in turn around time reduces the channel data rate under low loads and it's throughput.

3.TOKEN PASSING

- A Station is authorized to send data when it receives a special frame called a Token.
- Stations are arranged around a ring (physically or logically)

  - A Token circulates around a ring

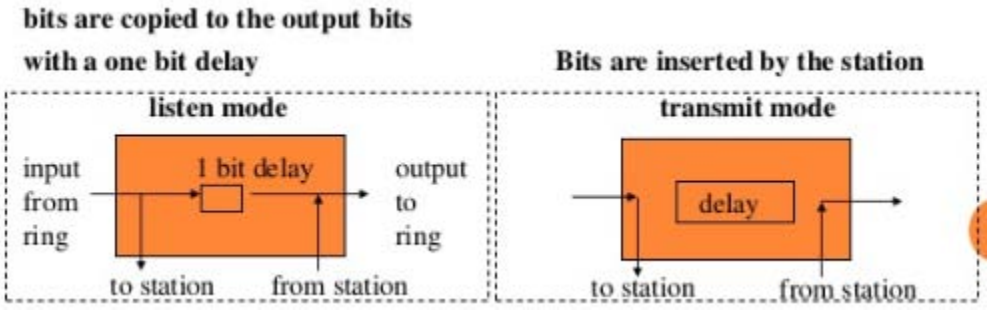
- If a station needs to send data ,it waits for the token
- The Station captures the token and sends one or more frames as long as the allocated time has not expired
- It releases the token to be used by the successor station.



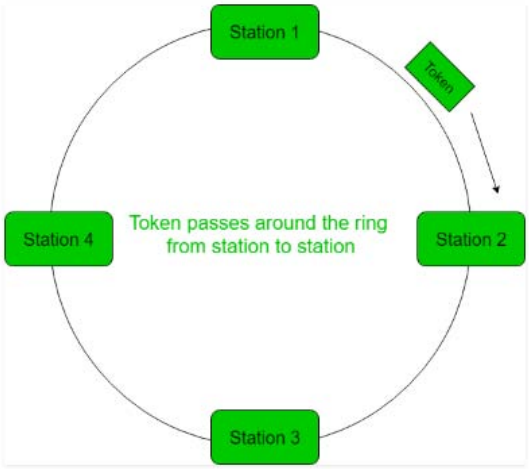
Station Interface is in two states :

o Listen state: Listen to the arriving bits and check the destination address to see if it is its own address. If yes the frame is copied to the station otherwise it is passed through the output port to the next station.

o Transmit state: station captures a special frame called **free token** and transmits its frames. **Sending** station is responsible for **reinserting** the free token into the ring medium and for **removing** the transmitted frame from the medium.



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



Performance

Performance of token ring can be concluded by 2 parameters:-

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

$$\text{Throughput, } S = 1/(1 + a/N) \text{ for } a<1$$

and

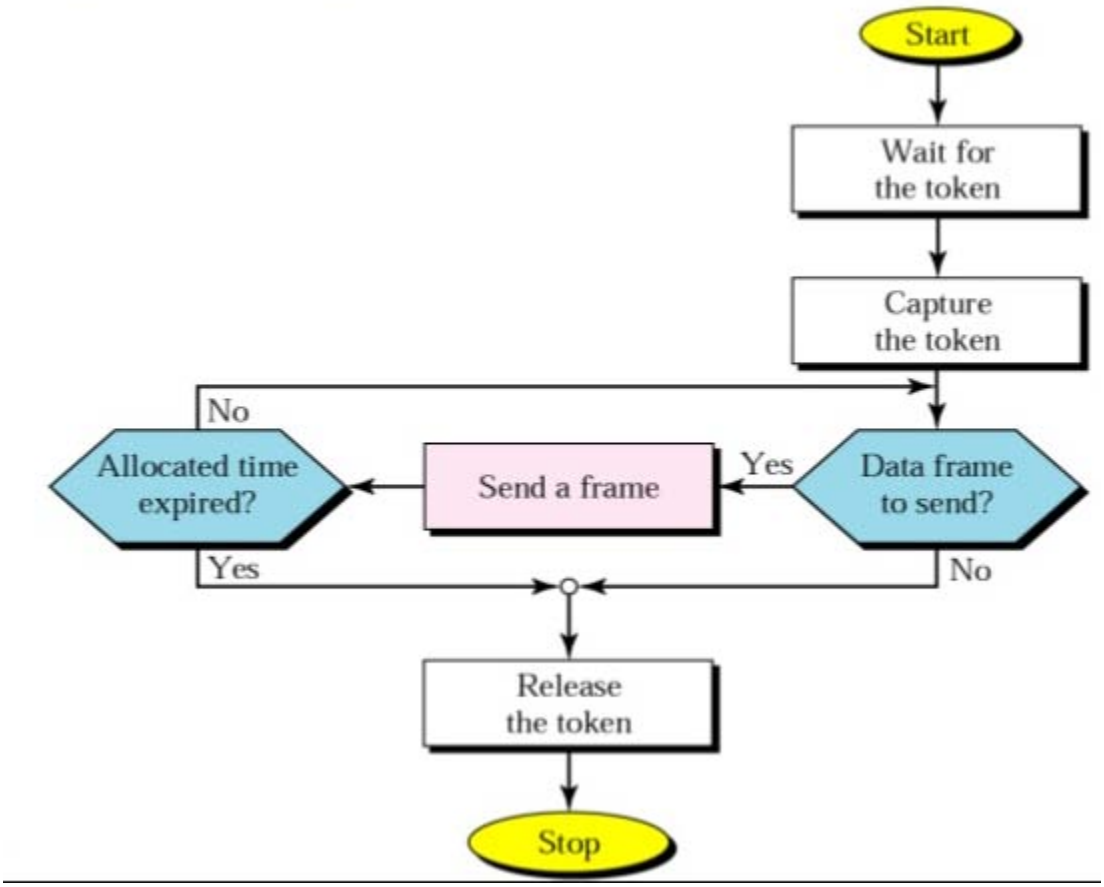
$$S = 1/\{a(1 + 1/N)\} \text{ for } a>1.$$

where N = number of stations

$$a = T_p/T_t$$

(T_p = propagation delay and T_t = transmission delay)

TOKEN PASSING FLOW CHART :



Token Management :

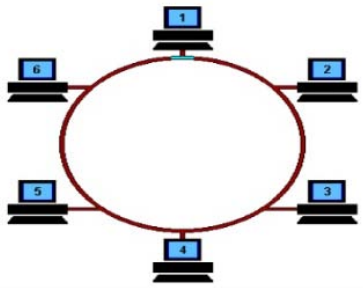
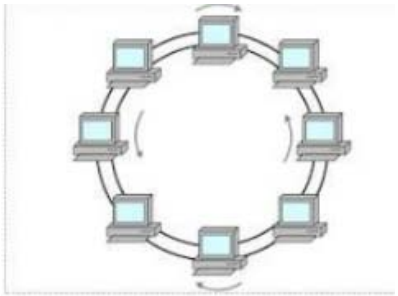
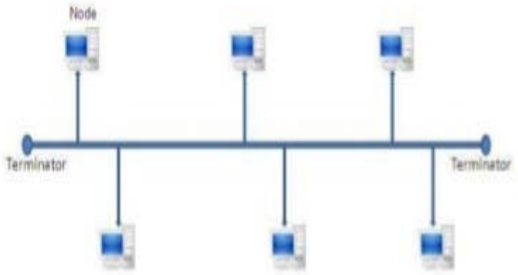
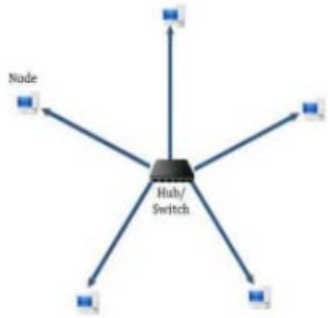
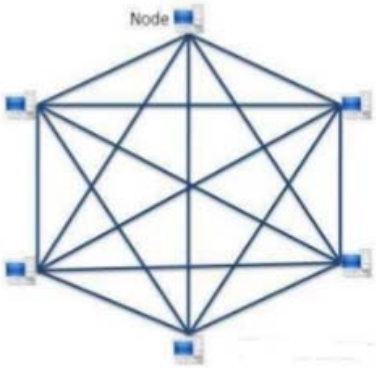
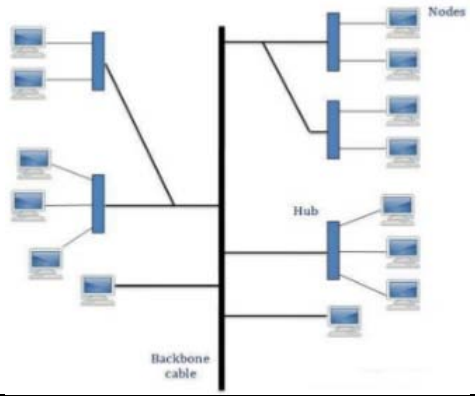
- We need token management , if there is a loss of token or it is destroyed when a station fails
- We can assign priorities as which station can receive the token. Network Topology : o The way in which different systems and nodes are connected and communicate with each other is determined by topology of the network.

➢ Topology can be physical or logical.

Physical Topology is the physical layout of nodes, workstations and cables in the network

logical topology is the way information flows between different components.

TYPES OF LOGICAL RINGS :

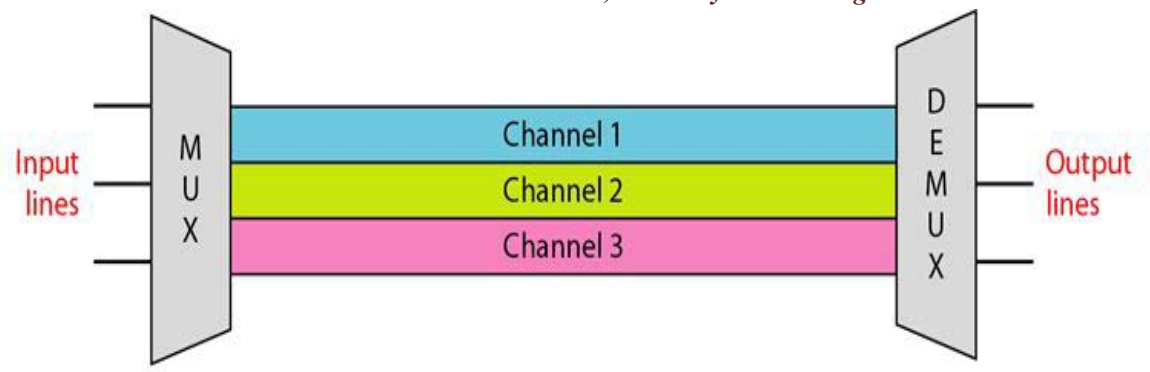
<table>
<tr>
<td>Physical Ring Topology
 
</td>
<td>DUAL RING TOPOLOGY :
  </td>
</tr>
<tr>
<td>BUS RING TOPOLOGY :
 
</td>
<td>STAR TOPOLOGY :
 
</td>
</tr>
<tr>
<td>MESH TOPOLOGY
 
</td>
<td>TREE TOPOLOGY
 
</td>
</tr>
</table>

3. Channelization:

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

Frequency Division Multiple Access (FDMA) – The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no to bands overlap to avoid crosstalk and noise.

- Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted.
- In this illustration, the transmission path is divided into three parts, each representing a channel that carries one transmission.



Multiplexing Process:

The following figure is a conceptual illustration of the multiplexing process. Each source generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulates different carrier frequencies (f1, f2 and f3). The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

Demultiplexing Process:

The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines.

Applications of FDM:

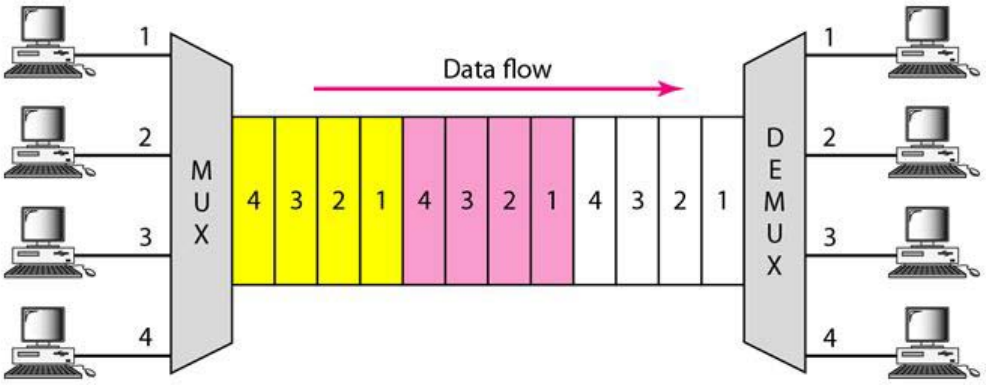
- To maximize the efficiency of their infrastructure, telephone companies have traditionally multiplexed signals from lower-bandwidth lines onto higher-bandwidth lines.
- A very common application of FDM is AM and FM radio broadcasting.
- The first generation of cellular telephones (still in operation) also uses FDM.

Implementation:

FDM can be implemented very easily. In many cases, such as radio and television broadcasting, there is no need for a physical multiplexer or demultiplexer. As long as the stations agree to send their broadcasts to the air using different carrier frequencies, multiplexing is achieved. In other cases, such as the cellular telephone system, a base station needs to assign a carrier frequency to the telephone user. There is not enough bandwidth in a cell to permanently assign a bandwidth range to every telephone user. When a user hangs up, her or his bandwidth is assigned to another caller.

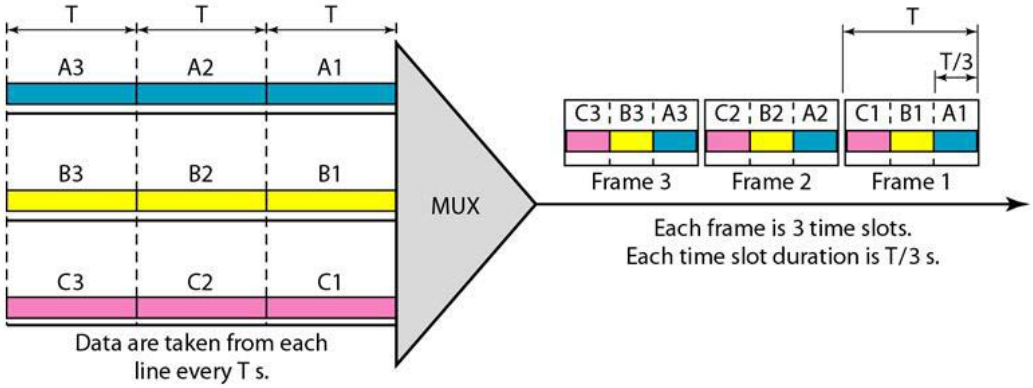
Time Division Multiple Access (TDMA) – In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a linle Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link.



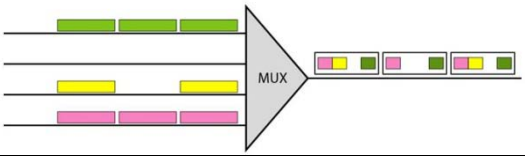
We can divide TDM into two different schemes: synchronous and statistical.

In ***synchronous TDM***, each input connection has an allotment in the output even if it is not sending data. In synchronous TDM, the data flow of each input connection is divided into units, where each input occupies one input time slot.



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

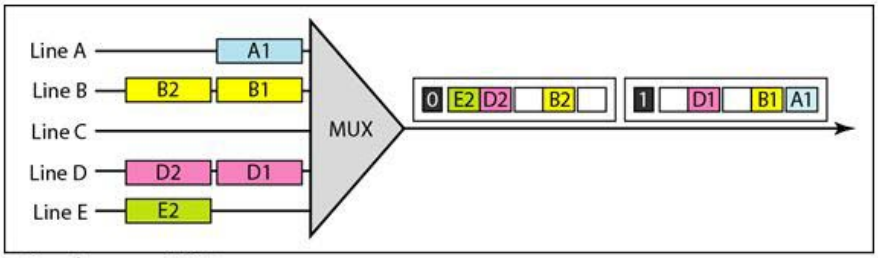
Different Factor:

• ***Interleaving***	• ***Empty Slots*** 
	• ***Data Rate Management***
• Multilevel Multiplexing	• **Multiple-Slot Allocation:**
• **Pulse Stuffing**	• **Frame Synchronizing**

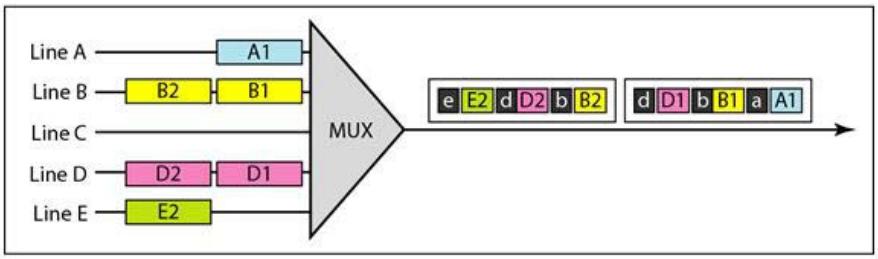
Statistical Time-Division Multiplexing:

In statistical time-division multiplexing, slots are dynamically allocated to improve bandwidth efficiency. Only when an input line has a slot's worth of data to send is it given a slot in the output frame.

In statistical multiplexing, the number of slots in each frame is less than the number of input lines. The multiplexer checks each input line in round robin fashion.



a. Synchronous TDM

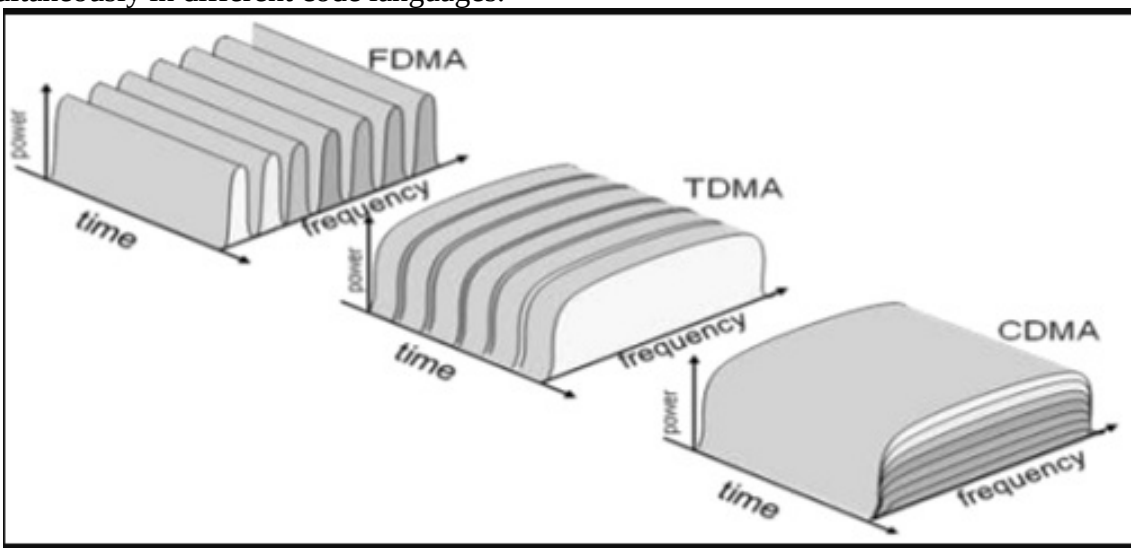


b. Statistical TDM

Depend upon Factor:

- ***Addressing***
- ***Slot Size***
- ***Bandwidth***

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



3.7	**Wired LAN: Ethernet Standards and FDDI**		**1**

Ethernet Standards

- The Ethernet standards come under the IEEE 802 section which deal with **local ar ea networks** and **metropolitan area networks.** In particular, **IEEE 802.3 defines Ethernet.**
- The different IEEE 802.3 standards define different aspects of Ethernet covering the physical layer and data link layer's media access control (MAC) of ***wired Ethernet.***
- Some of the individual standards may introduce new versions or flavours of Ethernet to keep pace with the growing requirements for speed and performance, whereas other standards may define aspects like the data frames used.

The different standards with their numbers are outlined in the table below:

Standard Ethernet Code

In order to understand standard Ethernet code, one must understand what each digit means. Following is a guide:

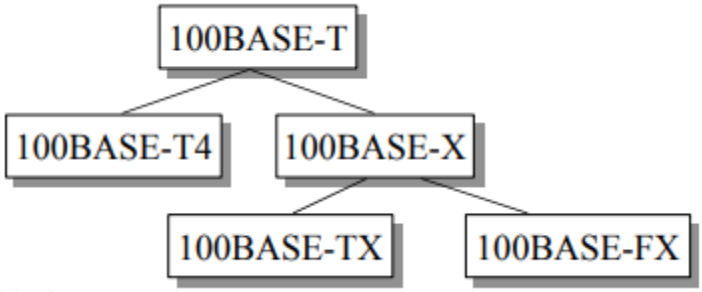
Guide to Ethernet Coding

10	at the beginning means the network operates at 10Mbps.
BASE	means the type of signaling used is baseband.
2 or 5	at the end indicates the maximum cable length in meters.
T	the end stands for twisted-pair cable.
X	at the end stands for full duplex-capable cable.
FL	at the end stands for fiber optic cable.

For example: *100BASE-TX indicates a Fast Ethernet connection (100 Mbps) that uses a twisted pair cable capable of full-duplex transmissions.*

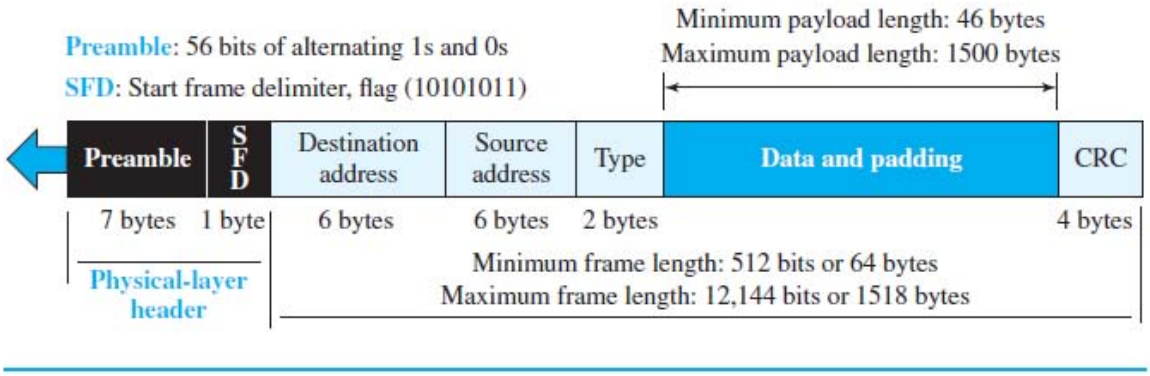
Some of Ethernet version numbering:

- 10BASE5: 10 Mb/s over coaxial cable (ThickWire)
- 10BROAD36: 10 Mb/s over broadband cable, 3600 m max segments
- 10BASE5: 1 Mb/s over 2 pairs of UTP
- 10BASE2: 10 Mb/s over thin RG58 coaxial cable (ThinWire), 185 m max segments
- 10BASE-T: 10 Mb/s over 2 pairs of UTP
- 10BASE-FL: 10 Mb/s fiber optic point-to-point link
- 10BASE-FB: 10 Mb/s fiber optic backbone (between repeaters). Also, known as synchronous Ethernet.



Basic frame format which is required for all MAC implementation is defined in **IEEE 802.3 standard**. Though several optional formats are being used to extend the protocol's basic capability.

Figure 13.3 *Ethernet frame*



- **PREAMBLE –** Ethernet frame starts (PRE).
- ***Start frame delimiter (SFD).*** This field (1 byte: 10101011) signals the beginning
- of the frame.
- ***Type.*** This field defines the upper-layer protocol whose packet is encapsulated in
- the frame.
- ***Data.*** This field carries data encapsulated from the upper-layer protocols. For example, a datagram has a field that defines the
- length(padding) of the data.
- **Cyclic Redundancy Check (CRC):** The last field contains error detection information

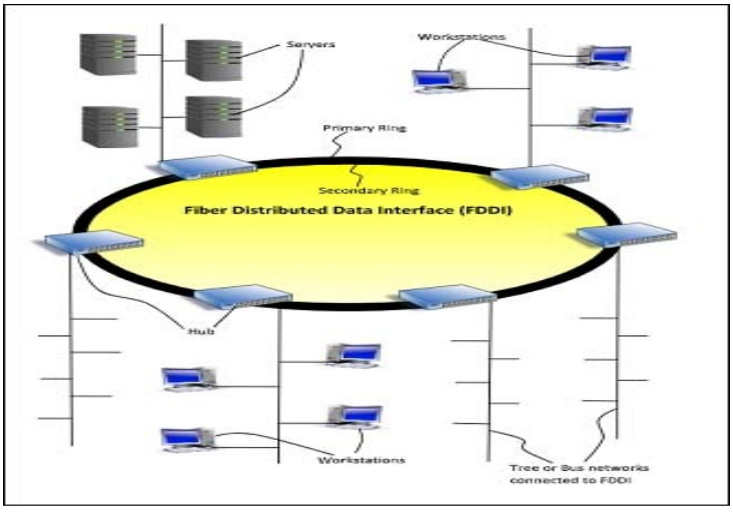
Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables. It is applicable in large LANs that can extend up to 200 kilometers in diameter.

Features

- FDDI uses optical fiber as its physical medium.
- It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.

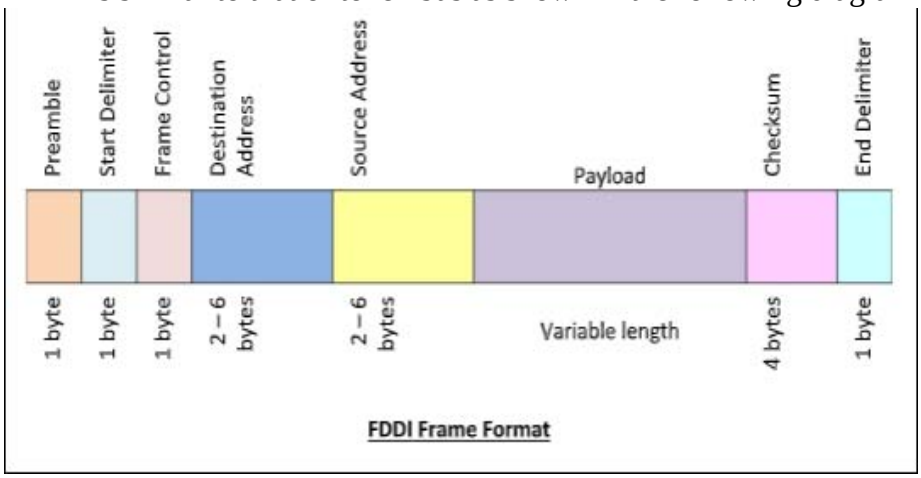
- It provides high data rate of 100 Mbps and can support thousands of users.
- It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
- It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
- It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
- FDDI technology can also be used as a backbone for a wide area network (WAN).

The following diagram shows FDDI −



Frame Format

The frame format of FDDI is similar to that of token bus as shown in the following diagram −



The fields of an FDDI frame are −

Preamble: 1 byte for synchronization.

Start Delimiter: 1 byte that marks the beginning of the frame.

Frame Control: 1 byte that specifies whether this is a data frame or control frame.

Destination Address: 2-6 bytes that specifies address of destination station.

Source Address: 2-6 bytes that specifies address of source station.

Payload: A variable length field that carries the data from the network layer.

Checksum: 4 bytes frame check sequence for error detection.
End Delimiter: 1 byte that marks the end of the frame.

3.8	**Wireless LAN : IEEE 802.11x and Bluetooth Standards**		**1**

802.11x is generic term to refer to the IEEE 802.11 standard for defining communication over a wireless LAN (WLAN). 802.11, commonly known **as Wi -Fi**, specifies an over-the-air interface between a wireless client and a base station or between two wireless clients

- It refers to the common flavors of Wi-Fi, most notably 802.11a, 802.11b, 802.11g, and 802.11n.

IEEE 802.11 defines two MAC sub-layers :-

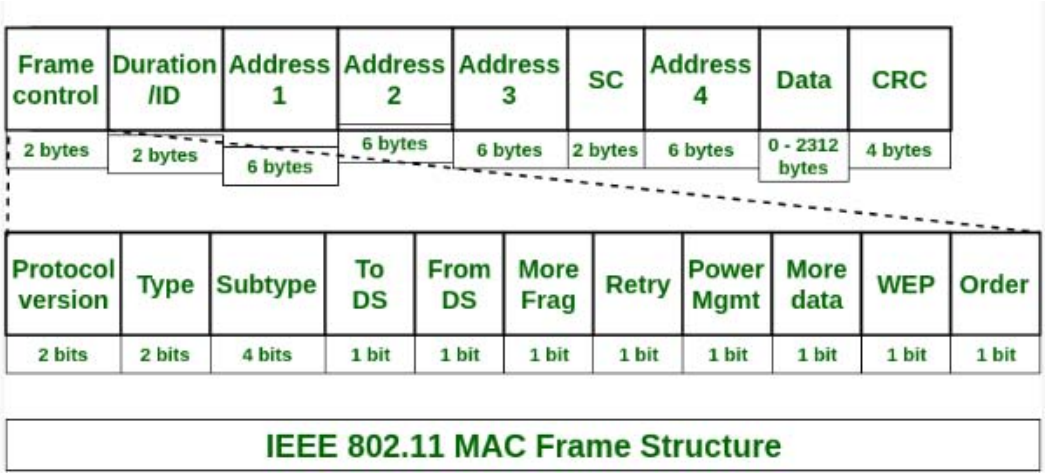
- **Distributed Coordination Function (DCF) –**
  DCF uses CSMA/CD as access method as wireless LAN can't implement CSMA/CD. It only offers asynchronous service.
- **Point Coordination Function (PCF) –**
  PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.

Frame Format of 802.11

The 802.11 MAC sublayer provides an abstraction of the physical layer to the logical link control sublayer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.

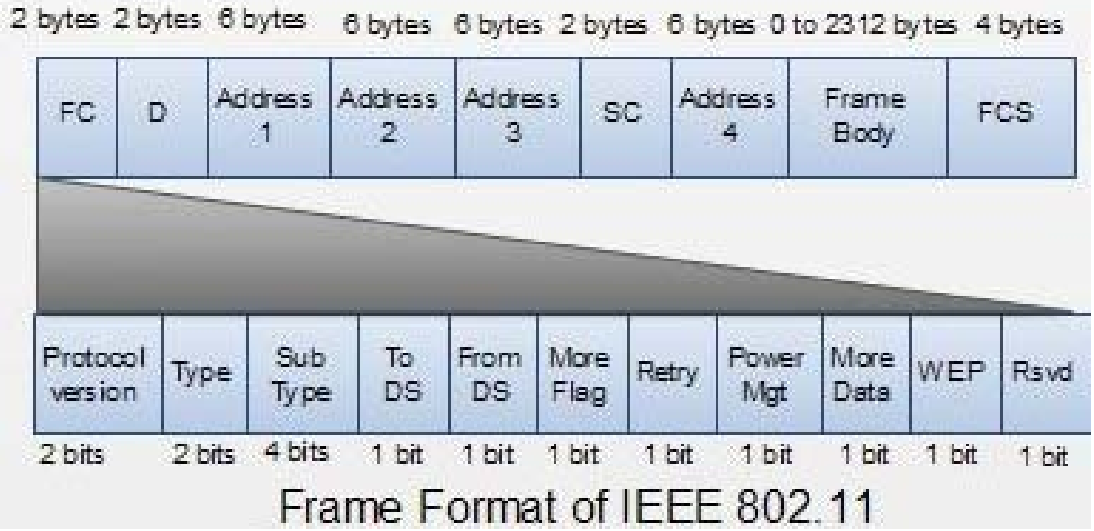
The MAC layer frame consists of nine fields.

1. Frame Control (FC). This is 2 byte field and defines the type of frame and some control information. **This field contains several different subfields**



IEEE 802.11 MAC Frame Structure

Subtype	It defines the subtype of each type,for control frame subtype fields are 1011 RTS,1100-CTS,1101-ACK
TO DS	Indicates Frame is going to distributed system
From DS	Indicates Frame is coming from distributed system
More Flag	if the value is 1,means more fragments
Retry	if the value is 1,means retrans mitted frame
Power Mgt	if the value is 1,means station is in power management mode
More Data	if the value is 1,means station has more data to send
Wep	Wep stands for wired equivalent privacy; if set to 1 means encryption is implimented
Rsvd	Reserved



Frame Format of IEEE 802.11

2. D . It stands for **duration** and is of 2 bytes. This field defines the duration for which the frame and its acknowledgement will occupy the channel. It is also used to set the value of NA V for other stations.

3. Addresses. There are 4 address fields of 6 bytes length. These four addresses represent source, destination, source base station and destination base station.

4. Sequence Control (SC). This 2 byte field defines the sequence number of frame to be used in flow control.

5. Frame body. This field can be between 0 and 2312 bytes. It contains the information.

6. Frame Check Sequence (FCS). This field is 4 bytes long and contains error detection sequence.

BLUE TOOTH

- IEEE 802.15
- It is a wireless LAN technology using short-range radio links, intended to replace the cable(s) connecting portable and/or fixed electronic devices.
- It is an ad hoc network where devices can automatically find each other, establish connections, and discover what they can do for each other.
- range 10-100 mtrs.
- features are robustness, low complexity, low power and low cost.
- uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each
- A Bluetooth device has a built-in short-range radio transmitter.
- It uses Frequency Hop Spread Spectrum (FHSS) to avoid any interference.

Applications

- ✓ Automatic synchronization between mobile and stationary devices
- ✓ Connecting mobile users to the internet using Bluetooth-enabled wire-bound connection ports
- ✓ Dynamic creation of private networks

Types of Bluetooth Wireless Technology

☐ Depending on the power consumption and range of the device, there are 3 Bluetooth Classes as:

1. Class 1: Max Power – 100mW ; Range – 100 m
2. Class : Max Power – 2.5mW ; Range – 10 m
3. Class : Max Power – 1mW ; Range – 1 m

Protocol Architecture

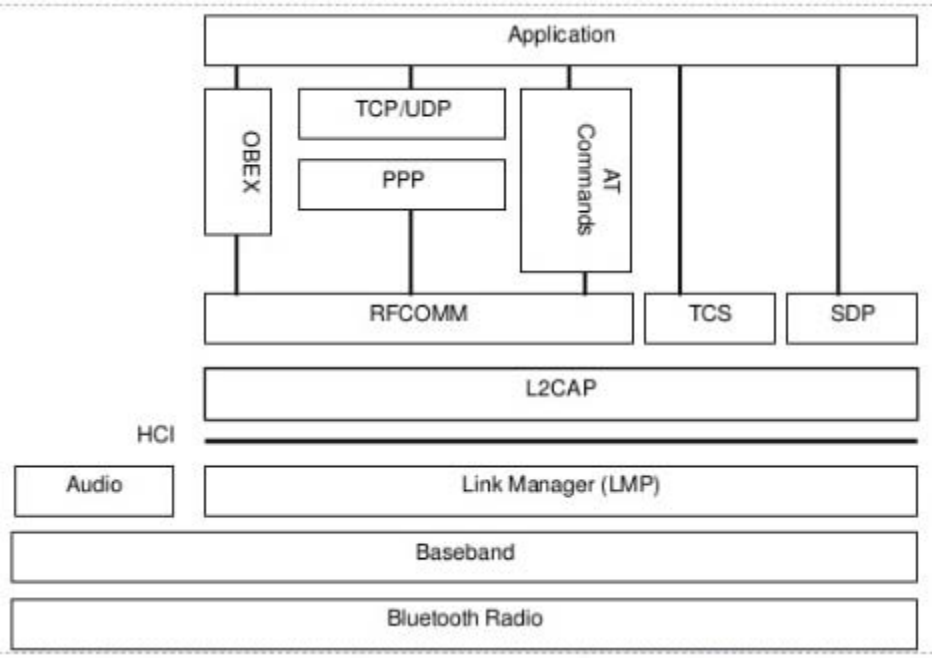
☐ Bluetooth is a layered protocol architecture
- ✓ Core protocols
- ✓ Cable replacement and telephony control protocols
- ✓ Adopted protocols

☐ Core protocols
- ✓ Radio
- ✓ Baseband
- ✓ Link manager protocol (LMP)
- ✓ Logical link control and adaptation protocol (L2CAP)
- ✓ Service discovery protocol (SDP)

☐ Cable replacement protocol
- ☐ RFCOMM

☐ Telephony control protocol
- ☐ Telephony control specification– binary (TCS BIN)

☐ Adopted protocols
- ☐ TCP/UDP/IP
- ☐ OBEX
- ☐ WAE/WAP

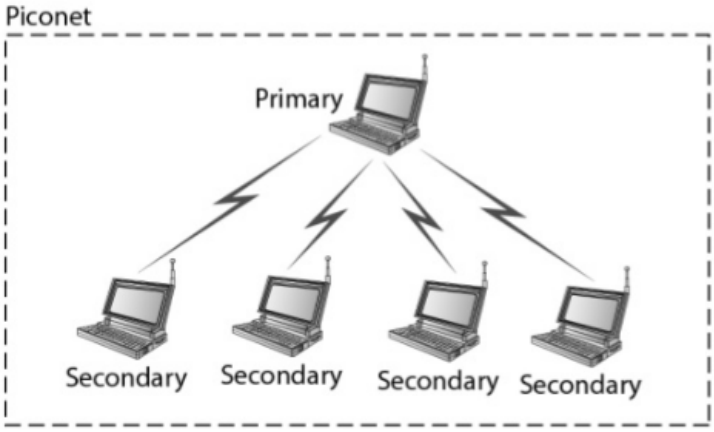


Bluetooth defines two types of network topology:

☐ *Piconet*

PICONET

- known as small net, have up to eight stations.
- One primary, the rest are secondary.
- Communication can be one-to-one or one-to-many.
- Each of the active slaves has an assigned 3-bit Active Member address.
- An additional eight secondary's can be in the "parked state.
- A secondary in a "parked state" is synchronised with the primary but cannot take part in communication until it is moved from the "parked state"



☐ Scatternet

- formed by the combinations of piconet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and acting as a primary, deliver them to secondaries in the second piconet .

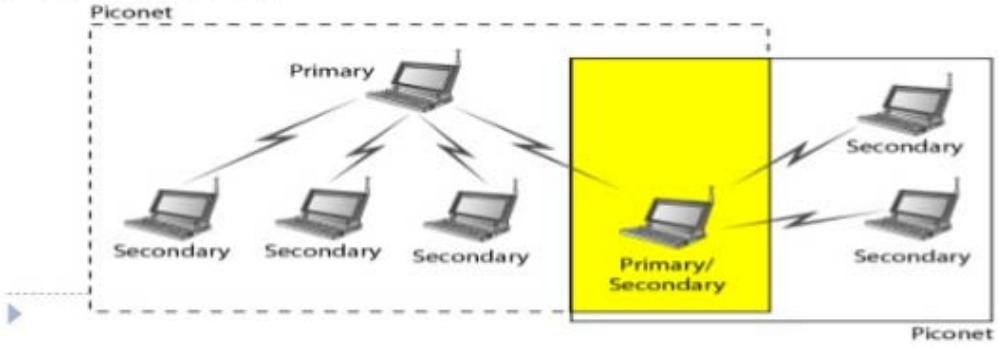


Figure : Scatternet (combine of Piconet)

Bluetooth Link Security

- **Elements:**
  - ✓ Authentication – verify claimed identity
  - ✓ Encryption – privacy
  - ✓ Key management and usage
- **Security algorithm parameters:**
  - ✓ Unit address
  - ✓ Secret authentication key (128 bits key)
  - ✓ Secret privacy key (4-128 bits secret key)
  - ✓ Random number

Notable IEEE Standards formats	
IEEE 802	LAN/MAN
IEEE 802.1	Standards for LAN/MAN bridging and management and remote media access control (MAC) bridging.
IEEE 802.2	Standards for Logical Link Control (LLC) standards for connectivity.
IEEE 802.3	Ethernet Standards for Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
IEEE 802.4	Standards for token passing bus access.
IEEE 802.24	Standards for Logical Link Control (LLC) standards for connectivity.
IEEE 802.5	Standards for token ring access and for communications between LANs and MANs
IEEE 802.6	Standards for information exchange between systems.
IEEE 802.7	Standards for broadband LAN cabling.
IEEE 802.8	Fiber optic connection.
IEEE 802.9	**Standards for integrated services, like voice and data.**
IEEE 802.10	Standards for LAN/MAN security implementations.
IEEE 802.11	Wireless Networking – "WiFi".
IEEE 802.12	Standards for demand priority access method.
IEEE 802.14	Standards for cable television broadband communications.
IEEE 802.15.1	Bluetooth
IEEE 802.15.4	Wireless Sensor/Control Networks – "ZigBee"
IEEE 802.15.6	Wireless Body Area Network[3] (BAN) – (e.g. Bluetooth low energy)
IEEE 802.16	Wireless Networking – "WiMAX"

3.9	Token Bus, Token Ring and Virtual LAN		0.5

802.4 Token Bus

• The 802.4 IEEE standard defines the Token Bus protocol for a token-passing access method on a bus topology.

• In a token-passing access method, a special packet called a token is passed from station to station and only the token holder is permitted to transmit packets onto the LAN.

• No collisions can occur with this protocol (Only One Station can transfer)

• When a station is done transmitting its packets, it passes the token to the "next" station.

• The next station does not need to be physically closest to this one on the bus, just the next logical station.

• A station can hold the token for only a certain amount of time before it must pass it on -even if it has not completed transmitting all of its data.

• This assures access to all stations on the bus within a specified period of time.

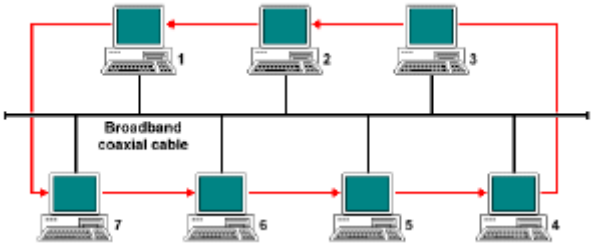


Figure : Token Bus Network (Red Arrow Indicates Token Passing Sequence)

802.5 Token Ring

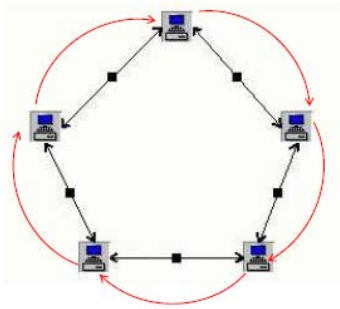
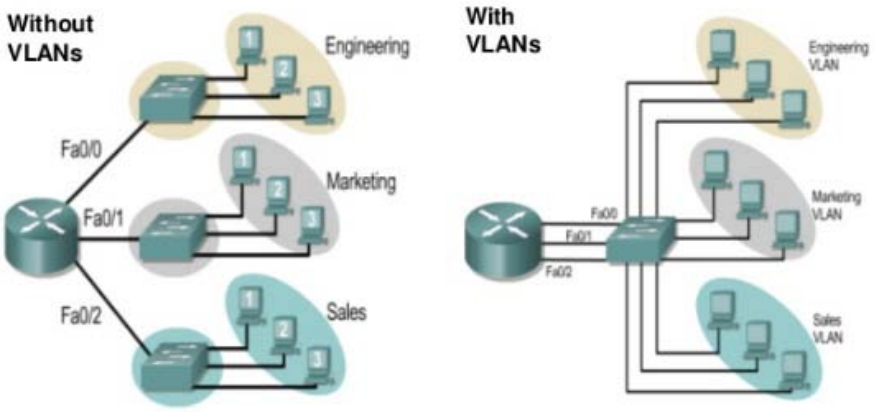


Figure : Token Bus Network (Red Arrow Indicates Token Passing Sequence)

• The 802.5 IEEE standard defines the Token Ring protocol which, like Token Bus, is another token-passing access method, but for a ring topology
• A ring topology consists of a series of individual point-to-point links that form a circle
• A token is passed from station to station in one direction around the ring, and only the station holding the token can transmit packets onto the ring
• Data packets travel in only one direction around the ring
• When a station receives a packet addressed to it, it copies the packet and puts it back on the ring
• When the originating station receives the packet, it removes the packet.

Virtual LANs

• A VLAN is a switched network that is logically segmented by functions, project teams, or applications without regard to the physical location of users.
• For example, several end stations might be grouped as a department, such as engineering or accounting.
• When the end stations are physically located close to one another, you can group them into a LAN segment.
• If any of the end stations are in different buildings (not the same physical LAN segment), you can then group them into a VLAN.



Types:

1.Static VLAN

- ☐ are called port-based and port-centric membership VLANs.
- ☐ Ports on a switch are manually assigned to a VLAN.
- ☐ This is the most common method of assigning ports to VLANs.
- ☐ As a device enters the network, it automatically assumes the VLAN membership of the port to which it is attached.

2. Dynamic VLAN

- ☐ allow membership based on the MAC address of the device connected to the switch port.
- ☐ As a device enters the network, it queries a database within the switch for a VLAN membership.
- ☐ membership is configured using a special server called a VLAN Membership Policy Server (VMPS).

• *VLANs provide the following features:*

Simplification of end-station moves, adds and changes

- When an end station is physically moved to a new location, its attributes can be reassigned from a network management station through Simple Network Management Protocol (SNMP) or through the user interface menus.
- When an end station is moved within the same VLAN, it retains its previously assigned attributes in its new location. When an end station is moved to a different VLAN, the attributes of the new VLAN are applied to the end station.

Controlled traffic activity

- VLANs allow ports on the same or different switches to be grouped so that traffic is confined to members of only that group.
- This feature restricts broadcast, unicast, and multicast traffic (flooding) only to ports included in a certain VLAN.
- The management domain is a group of VLANs that are managed by a single administrative authority.

Workgroup and network security

- You can increase security by segmenting the network into distinct broadcast domains.
- To this end, VLANs can restrict the number of users in a broadcast domain.
- You can also control the size and composition of the broadcast domain by controlling the size and composition of a VLAN.

Components

• Networks that have VLANs contain one or more of the following components:
  - ✓ Switches that logically segment connected end stations
  - ✓ Routers that provide VLAN communications between workgroups
  - ✓ Transport protocols that carry VLAN traffic across shared LAN and ATM backbones
  - ✓ Interoperability with previously installed LAN systems

Disadvantage:

- Costly
- Software based
- Human labor to program
- Depending on variety switches
- Management complexity

Advantages:

- More Security
- Ease of administration
- Broadcast control
- Reduction in network traffic

Answer own Innovation, Creativity & Tinkering.

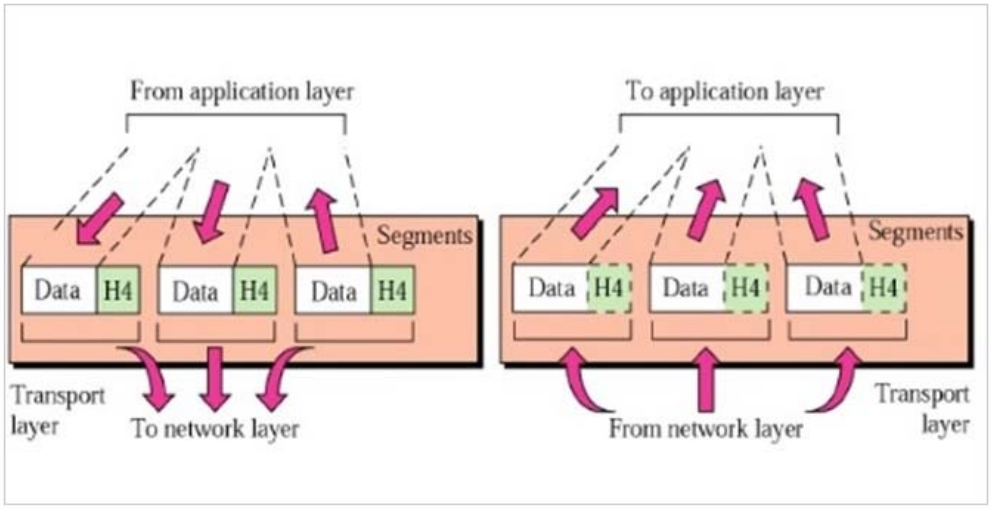
Read Me First (3 times) Assumes Basic Key Terms while writing your unit 5 answer.

bandwidth-delay product	client-server paradigm	congestion
congestion control	demultiplexing	ephemeral port number
finite state machine (FSM)	Go-Back-N protocol (GBN)	multiplexing
piggybacking	pipelining	port number
process-to-process communication	Selective-Repeat (SR) protocol	sequence number
sliding window	socket address	Stop-and-Wait protocol
well-known port number	congestion-avoidance	cookie
deadlock	denial of service attack	fast-recovery
fast retransmission	fragmentation	half-close
initial sequence number (ISN)	keepalive timer	persistence timer
primary address	retransmission time-out (RTO)	round-trip time (RTT)
silly window syndrome	slow-start algorithm	socket address
Stream Control Transmission Protocol	(SCTP)	stream identifier (SI)
stream sequence number (SSN)	SYN flooding attack	three-way handshaking
Transmission Control Protocol (TCP)	transmission sequence number (TSN)	user datagram
User Datagram Protocol (UDP)		

The **Transport Layer** in the Open System Interconnection (OSI) model is responsible for end-to-end delivery over a network. Whereas the network layer is concerned with the end - to- end delivery of individual packets and it does not recognize any relationship between those packets.

- This layer treats each packet independently because each packet belongs to a different message.
- The **transport layer** ensures that each message should reach its destination completely and in order so that it maintains error and flow control to the source to destination to ensure proper data transmission.
- The **transport layer** establishes a connection between two end ports. A connection is a single logical path from source to destination which is associated with all the packets in a message.
- **Transport Layer** uses some standard protocols to enhance its functionalities are TCP(Transmission Control Protocol), UDP(User Datagram Protocol), DCCP(Datagram Congestion Control Protocol), etc.

This figure shows the relationship of the **transport layer** to the network and session layer.



Transport Layer

5.1 Functions of Transport Layer | 1

Specific functions of the **transport layer** are as follows:

1. Service-point addressing

- Computers often run many programs at the same time. Due to this, source-to-destination delivery means delivery from a specific job (currently running program) on one computer to a specific job (currently running program) on the other system not only one computer to the next.
- For this reason, the **transport layer** added a specific type of address to its header, it is referred to as a service point address or port address.
- By this address each packet reaches the correct computer and also the **transport layer** gets the complete message to the correct process on that computer.

2. Segmentation and Reassembly

- In segmentation, a message is divided into transmittable segments; each segment containing a sequence number. This number enables this layer to reassemble the message.
- Upon arriving at its destination system message is reassembled correctly, identify and replaces packets that were lost in transmission.

3. Connection Control

It can be either of two types:

i. Connectionless Transport Layer
ii. Connection Oriented Transport Layer

i) Connectionless Transport Layer

- This Transport Layer treats each packet as an individual and delivers it to the destination machine.
- In this type of transmission, the receiver does not send an acknowledgment to the sender about the receipt of a packet. This is a faster communication technique.

ii) Connection Oriented Transport Layer

- This Transport Layer creates a connection with the Transport Layer at the destination machine before transmitting the packets to the destination.
- To Create a connection following three steps are possible:
    - Connection establishment
    - Data transfer
    - Connection termination

When all the data are transmitted connection is terminated. Connectionless Service is less reliable than connection Oriented Service.

4. Multiplexing and Demultiplexing

- Multiple packets from diverse applications are transmitted across a network needs very dedicated control mechanisms, which are found in the transport layer.
- The transport layer accepts packets from different processes. These packets are differentiated by their port numbers and pass them to the network layer after adding proper headers.
- In Demultiplexing, at the receiver's side to obtain the data coming from various processes. It receives the segments of data from the network layer and delivers it to the appropriate process running on the receiver's machine.

5. Flow control

- The transport layer also responsible for the flow control mechanism between the adjacent layers of the TCP/IP model.
- It does not perform across a single link even it performs an end-to-end node.
- By imposing flow control techniques data loss can be prevented from the cause of the sender and slow receiver.

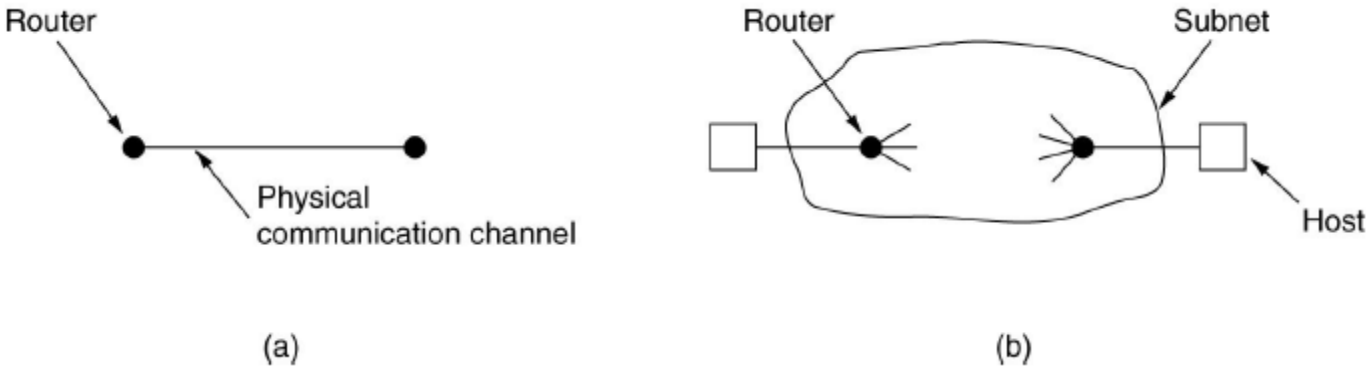
- For instance, it uses the method of sliding window protocol in this method receiver sends a window back to the sender to inform the size of the data is received.

6. Error Control

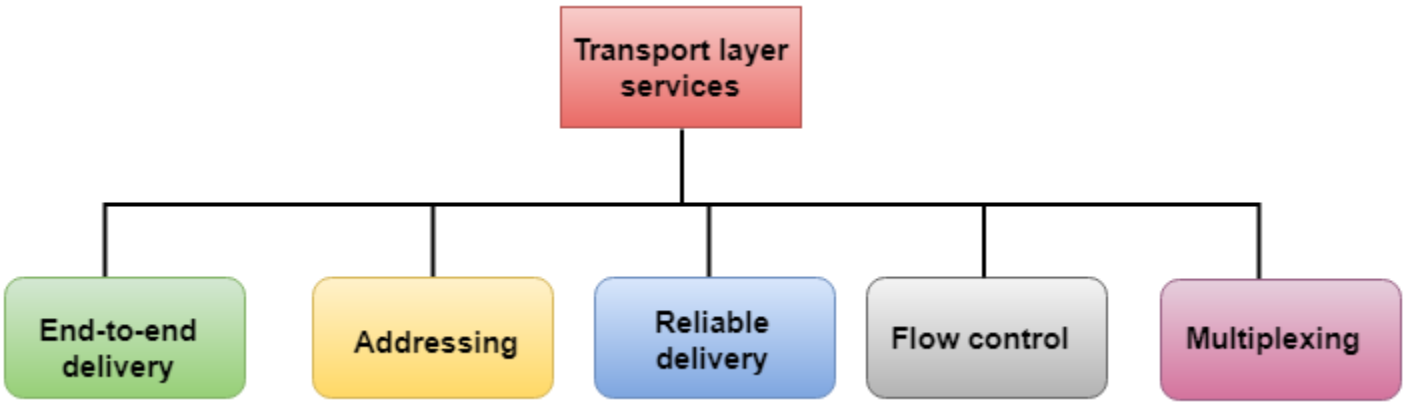
- Error Control is also performed end to end like the data link layer.
- In this layer to ensure that the entire message arrives at the receiving transport layer without any error(damage, loss or duplication). Error Correction is achieved through retransmission of the packet.
- The data has arrived or not and checks for the integrity of data, it uses the ACK and NACK services to inform the sender.

5.2	Elements of Transport Protocols: **Addressing**, Establishing and Releasing Connection, Flow Control & Buffering, **Error Control**, **Multiplexing** & Demultiplexing, Crash Recovery

Transport Protocol



(a)Environment of the data link layer.
(b)Environment of the transport layer.



End-to-end delivery:

The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

Reliable delivery:

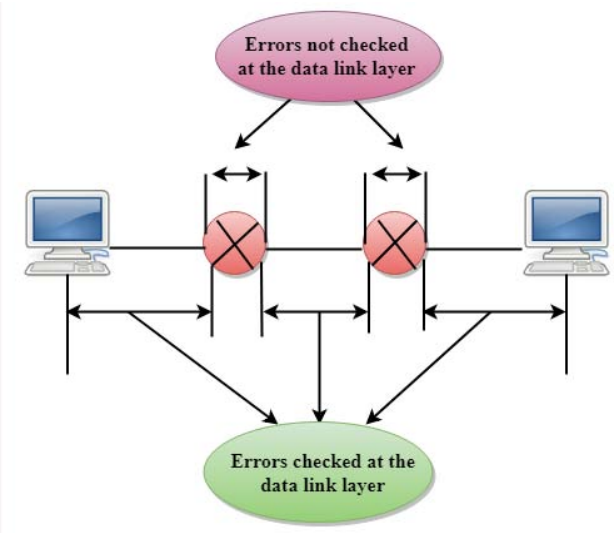
The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects:

- Error control
- Sequence control
- Loss control
- Duplication control

Error Control

- The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
- The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.
- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.



Sequence Control

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

Loss Control

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

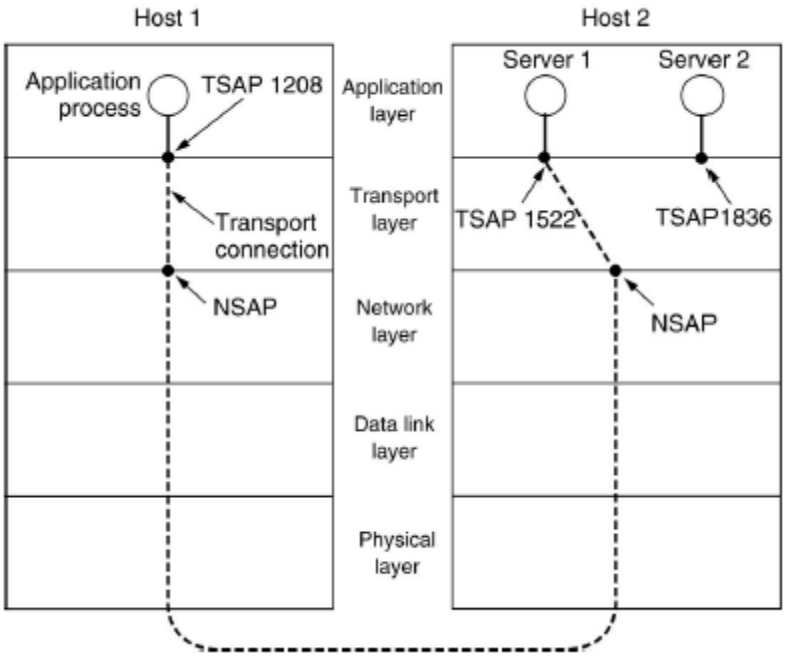
Duplication Control

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow Control

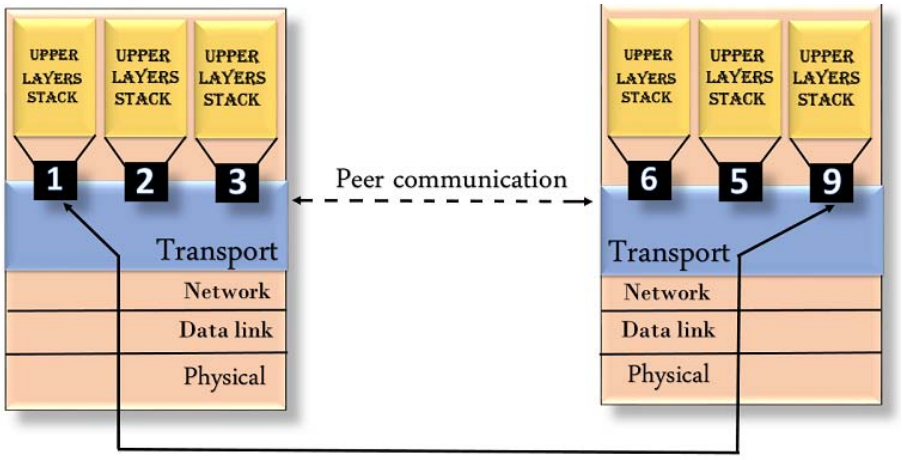
Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Addressing

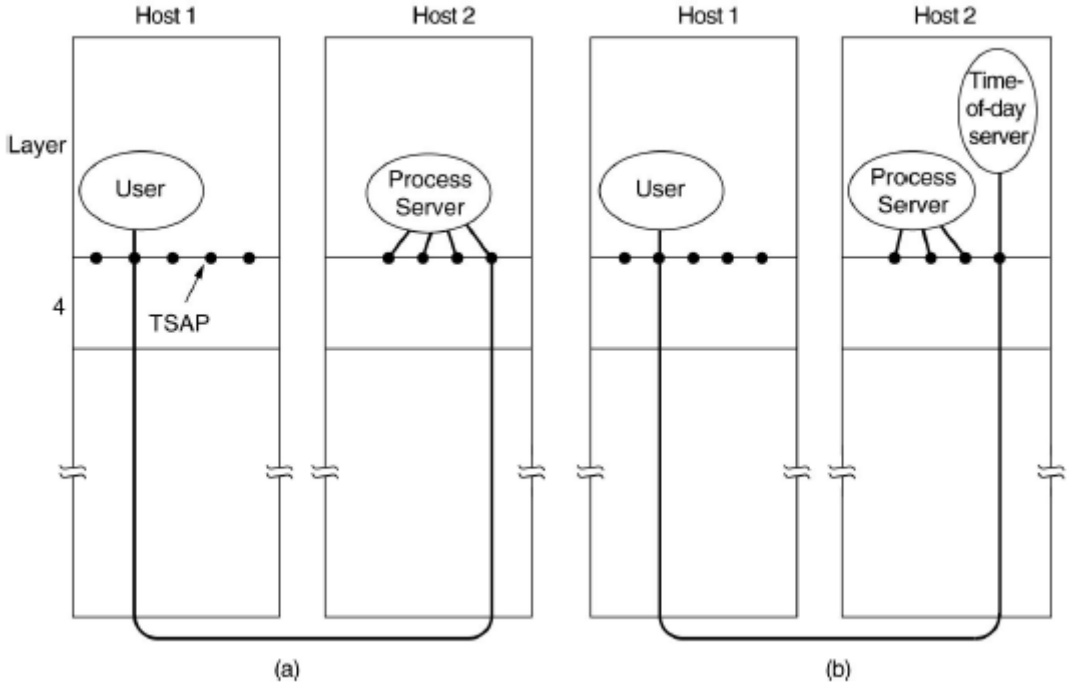


TSAPs, NSAPs and transport connections.

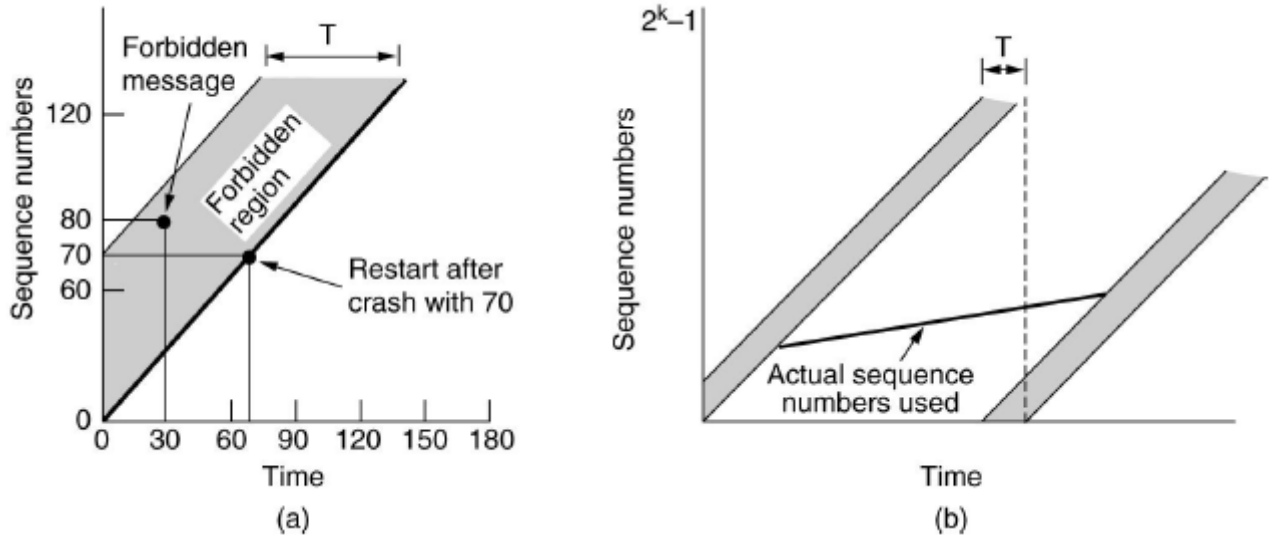
- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.
- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating.



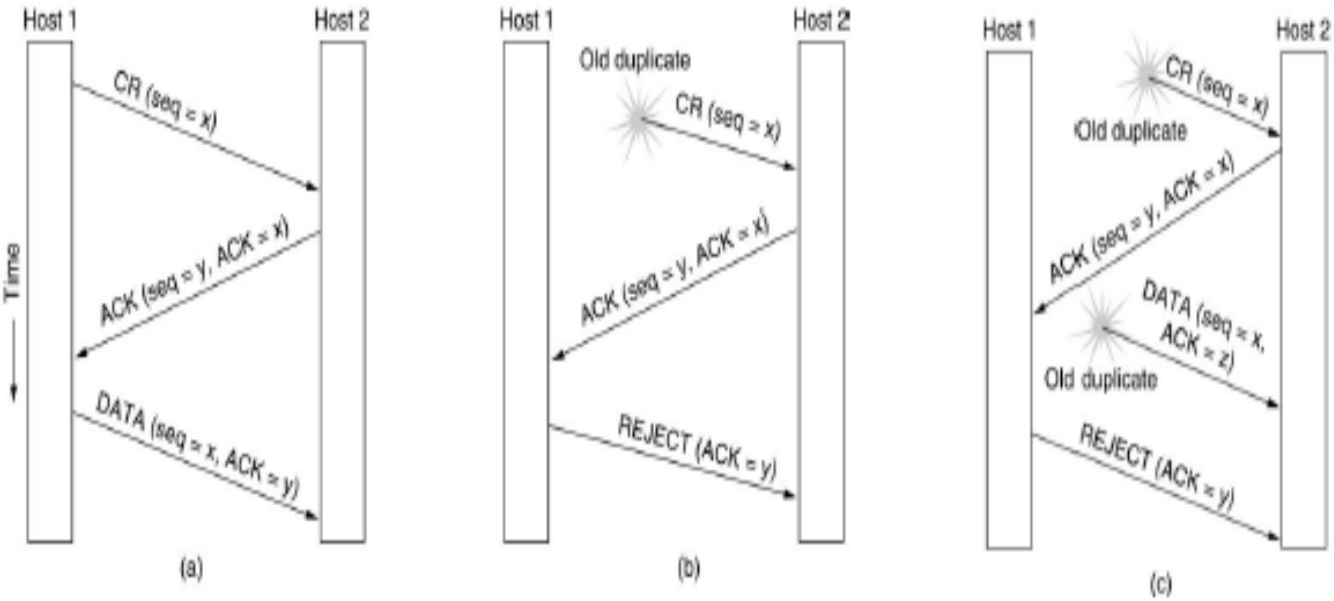
Connection Establishment



How a user process in host 1 establishes a connection with a time-of-day server in host 2..



(a)TPDUs may not enter the forbidden region.
(b)The resynchronization problem.



Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNECTION REQUEST.

(a)Normal operation,

(b)Old CONNECTION REQUEST appearing out of nowhere.

(c)Duplicate CONNECTION REQUEST and duplicate ACK.

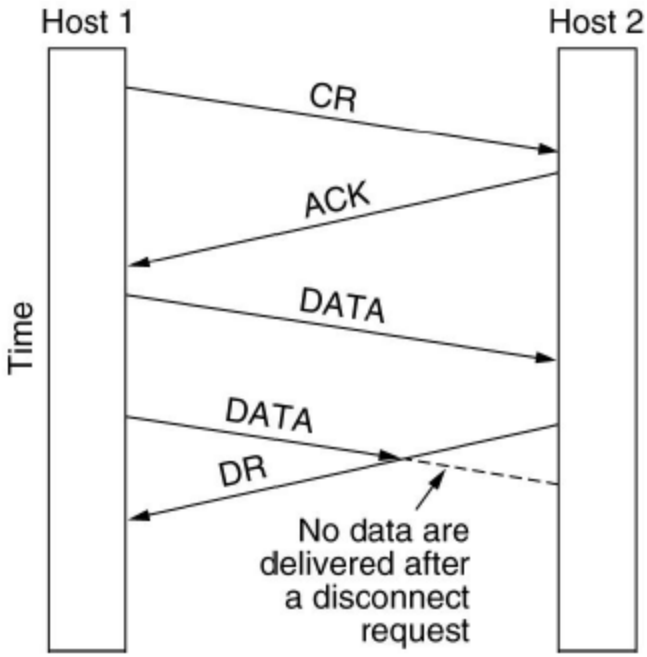
Connection Release

CONNECTION RELEASE Connection at transport can be released in two way.

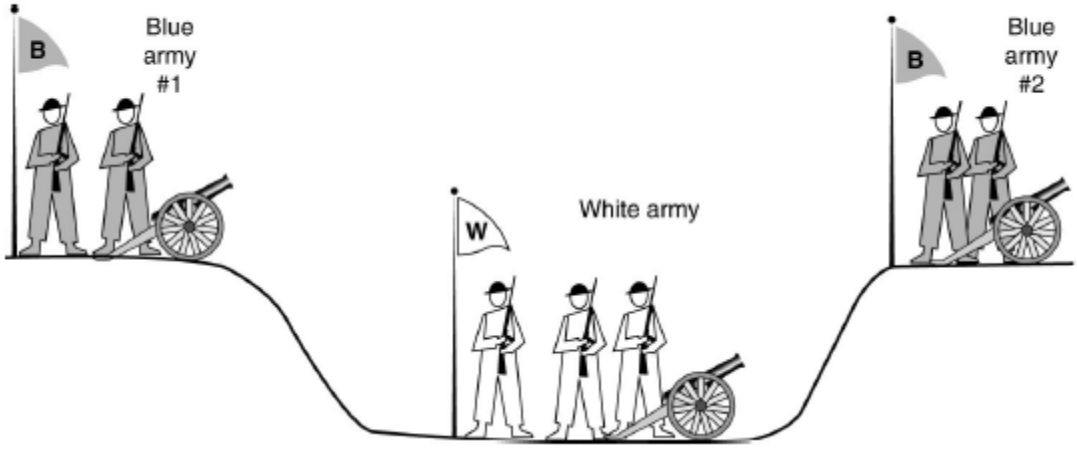
1. asymmetric: if one of host terminates connection, then in both the direction, data communication will be terminated.

2. symmetric: if one of the host disconnects connection, then it can not send the data but it can receive it.

Asymmetric Release

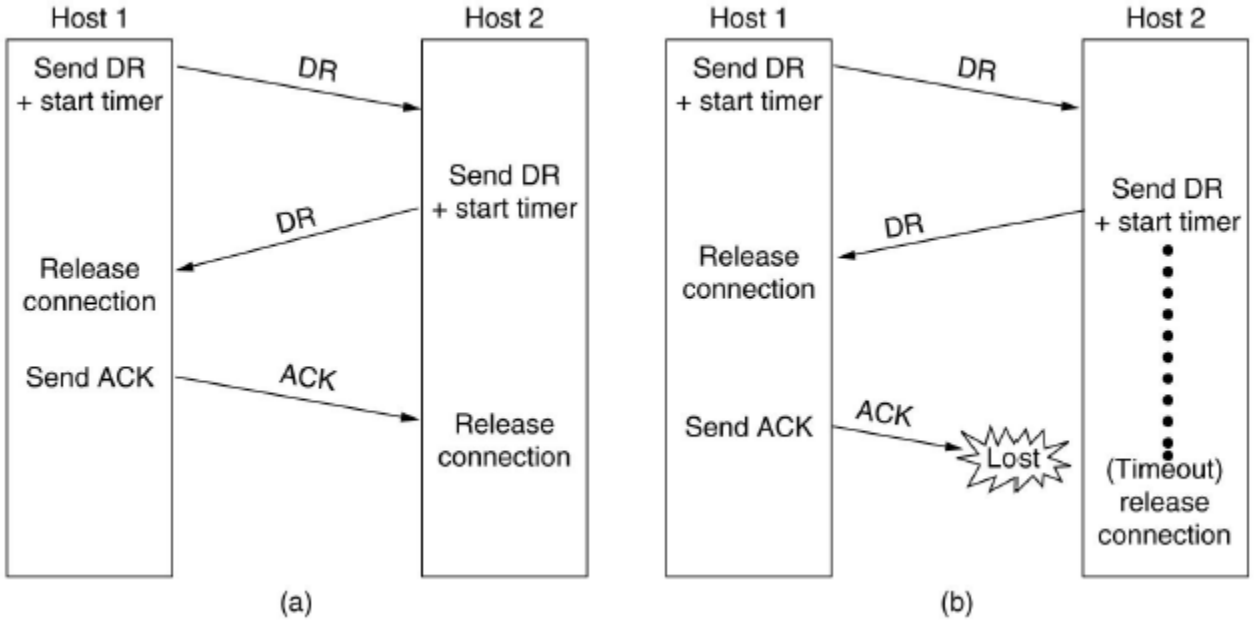


Abrupt disconnection with loss of data.



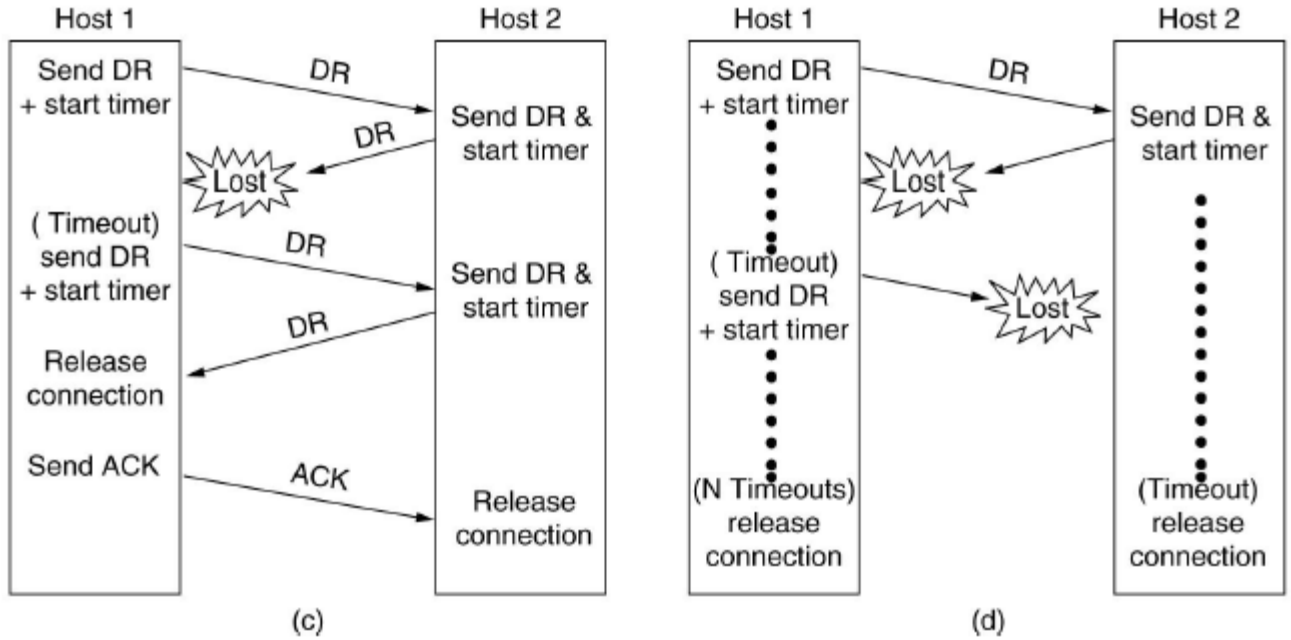
The two-army problem.

Four protocol scenarios for releasing a connection.



(a)Normal case of a three-way handshake.

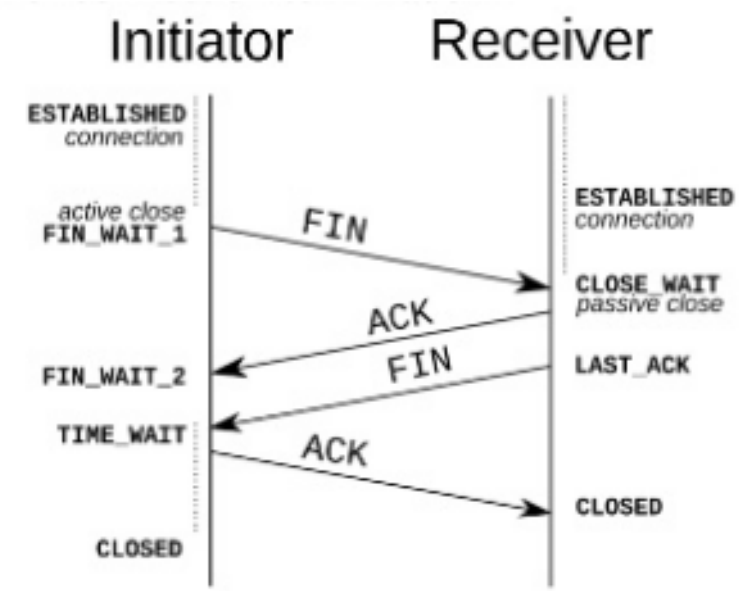
(b)final ACK lost.



(c)Response lost.

(d)Response lost and subsequent DRs lost.

TCP Connection Release uses symmetric approach. It is called Four Way handshaking for connection termination.



Flow Control and Buffering

Transport layer manages end to end to flow. If the receiver is not able to cope with the flow of data, then data flow should be control from sender side, that part is done on Transport layer.

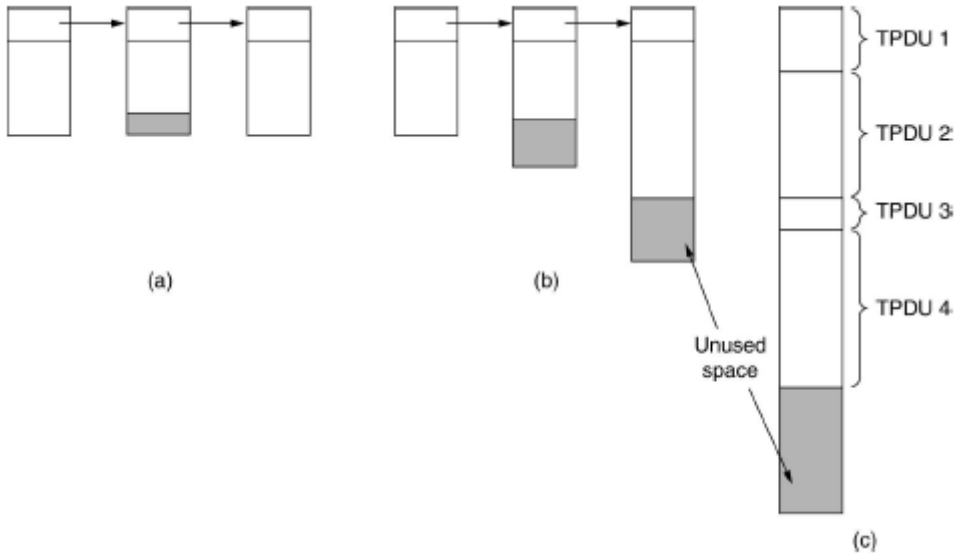
Data link layer is also doing flow control, but it controls flow of data between adjacent nodes in path from source to destination.

Reasons of packet loss at receiver is slow processing speed or insufficient buffer to store the data.

Buffer are allocated at sender and receiver side. If the network service is reliable, so every send TPDU sent will be delivered to receiver and will be buffered and processes at receiver, so no need to keep buffer at sender.

But if network service is unreliable and receiver may not able to handle every incoming TPDU then sender should also keep a buffer, where copy of TPDU resides until it's ACK comes.

Buffers can be allocate in fixed size when connection sets up or buffer can be varied dynamically according to free memory. First case is called static buffer allocation.



(a)Chained fixed-size buffers.

(b)Chained variable-sized buffers.

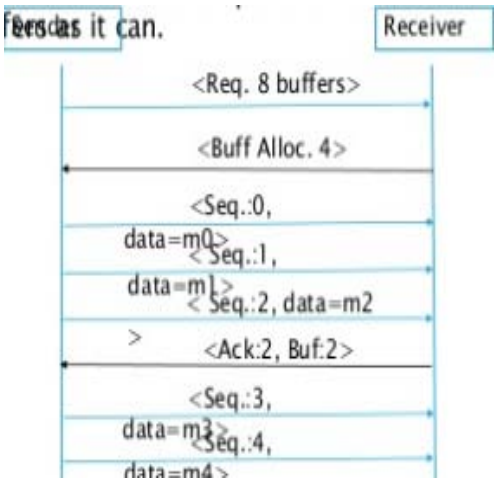
(c)One large circular buffer per connection.

	A	Message	B	Comments
1	→	< request 8 buffers>	→	A wants 8 buffers
2	←	<ack = 15, buf = 4>	←	B grants messages 0-3 only
3	→	<seq = 0, data = m0>	→	A has 3 buffers left now
4	→	<seq = 1, data = m1>	→	A has 2 buffers left now
5	→	<seq = 2, data = m2>	• • •	Message lost but A thinks it has 1 left
6	←	<ack = 1, buf = 3>	←	B acknowledges 0 and 1, permits 2-4
7	→	<seq = 3, data = m3>	→	A has 1 buffer left
8	→	<seq = 4, data = m4>	→	A has 0 buffers left, and must stop
9	→	<seq = 2, data = m2>	→	A times out and retransmits
10	←	<ack = 4, buf = 0>	←	Everything acknowledged, but A still blocked
11	←	<ack = 4, buf = 1>	←	A may now send 5
12	←	<ack = 4, buf = 2>	←	B found a new buffer somewhere
13	→	<seq = 5, data = m5>	→	A has 1 buffer left
14	→	<seq = 6, data = m6>	→	A is now blocked again
15	←	<ack = 6, buf = 0>	←	A is still blocked
16	• • •	<ack = 6, buf = 4>	←	Potential deadlock

Dynamic buffer allocation. The arrows show the direction of transmission. An ellipsis (…) indicates a lost TPDU.

Dynamic Buffer Allocation: as connection are opened and closed, memory available changes, so sender and receiver dynamically adjust buffer allocations.

In dynamic buffer allocation, initially sender will request certain number of buffers based on perceive need. receiver will grant as many buffers as it can.



<Req. 8 buffers>

<Buff Alloc. 4>

<Seq.:0, data=m0>

< Seq.:1, data=m1>

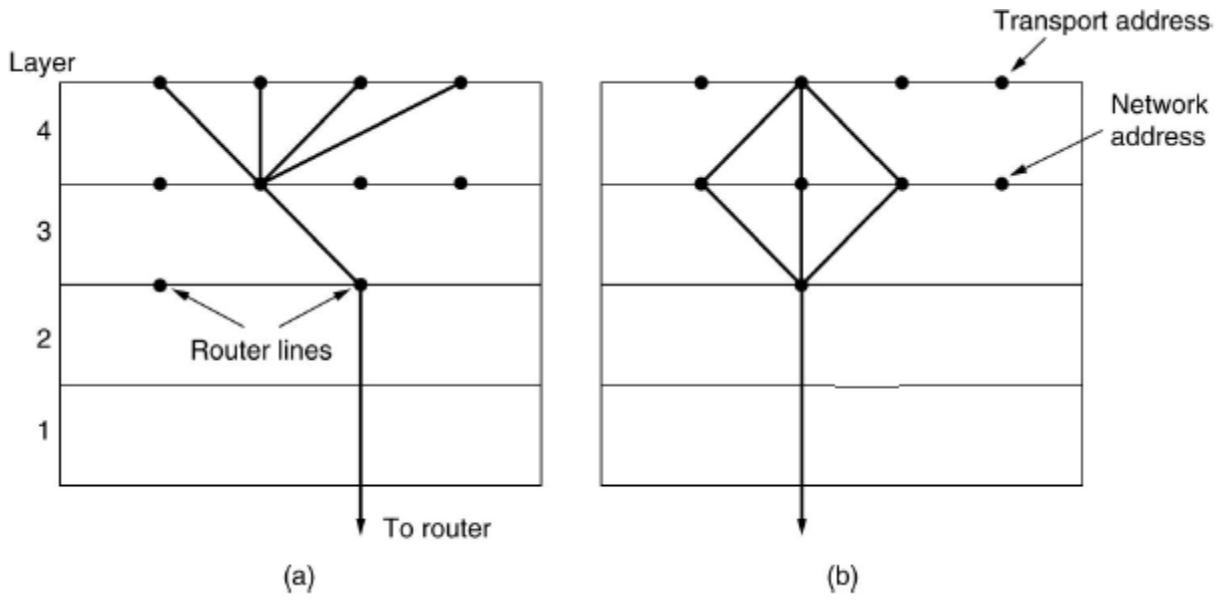
< Seq.:2, data=m2 >

<Ack:2, Buf:2>

<Seq.:3, data=m3>

<Seq.:4, data=m4>

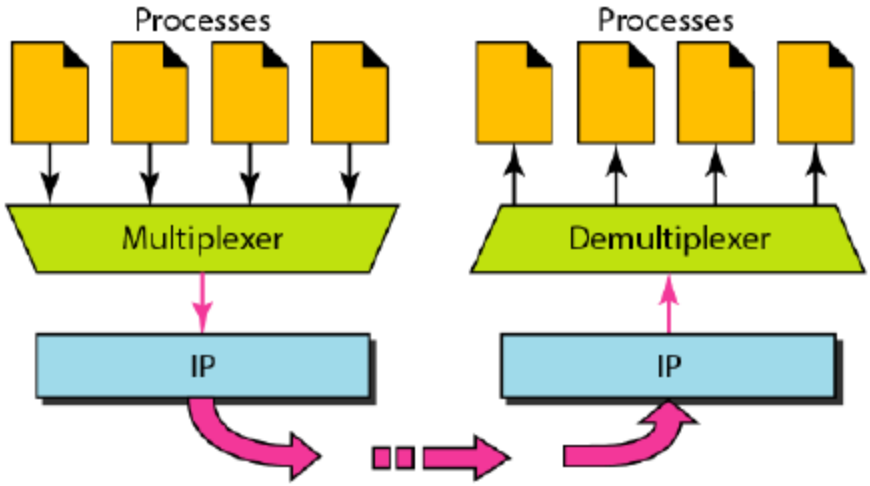
Multiplexing



(a)Upward multiplexing. (b)Downward multiplexing.

1.1. Multiplexing & De-multiplexing

• The addressing mechanism allows multiplexing and De-multiplexing by the transport layer



1.1.1. Multiplexing

• At the sender site, there may be several processes that need to send packets. However, there is only one transport layer protocol at any time. This is a many-to-one relationship and requires multiplexing.

• The protocol accepts messages from different processes, differentiated by their assigned port numbers. After adding the header, the transport layer passes the packet to the network layer

1.1.2. De-multiplexing

• At the receiver site, the relationship is one-to-many and requires Demultiplexing.
The transport layer receives datagrams from the network layer.

• After error checking and dropping of the header, the transport layer delivers each message to the appropriate process based on the port number

CRASH RECOVERY

- Hosts and routers are subject to crash.
- router crash is easier to handle since transport entities are alive at the host, routers are only intermediate nodes which forwards packet, they do not have transport layer entity.

How to recover from host crashes?

One client(host) is sending a file to server(receiver host). Transport layer at server simply passes TPDU to transport layer. While transmission was on going, server crashes.

Server crashes and comes up -> table initiated, does not know where it was?

Server sends a broadcast TPDU to all host, announcing that it had just crashed and requesting that its clients inform it about status of all open connection.

Each client can be in one of two states:

S0: no outstanding TPDU

S1: one TPDU outstanding

Now it seems that if TPDU is outstanding, client should transmit it, but there are can be different hidden situations.

1. if server has first sent ACK and before it can send TPDU to next layer, server crashes. In this case, client will get ACK so it will not retransmit, and TPDU is lost by server.

2. if server first sends packet to next layer, then it crashes before it can send ACK. In this case though server has already received TPDU, client thinks TPDU is lost and it will retransmit.

Server(Receiving host) can be programmed in two ways, 1. ACK first 2. write first

Three events are possible at server, sending ACK(A), sending packet to next layer(W), crashing (C).

Three event can occur in six different case: AC(W) AWC C(AW), C(WA) WAC WC(A)

Client(sending host) can be programmed in four ways,

1. always retransmit last TPDU,

2. never retransmit last TPDU,

3. retransmit only in S0,

4. retransmit only

Strategy used by sending host	Strategy used by receiving host: First ACK, then write			Strategy used by receiving host: First write, then ACK		
	AC(W)	AWC	C(AW)	C(WA)	W AC	WC(A)
Always retransmit	OK	DUP	OK	OK	DUP	DUP
Never retransmit	LOST	OK	LOST	LOST	OK	OK
Retransmit in S0	OK	DUP	LOST	LOST	DUP	OK
Retransmit in S1	LOST	OK	OK	OK	OK	DUP

OK = Protocol functions correctly
DUP = Protocol generates a duplicate message
LOST = Protocol loses a message

Different combinations of client and server strategy.

5.3	User Datagram Protocol(UDP):User Datagram, U DP Operations, Uses of UDP, RPC	1

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is **unreliable and connectionless protocol.** So, there is no need to establish connection prior to data transfer.

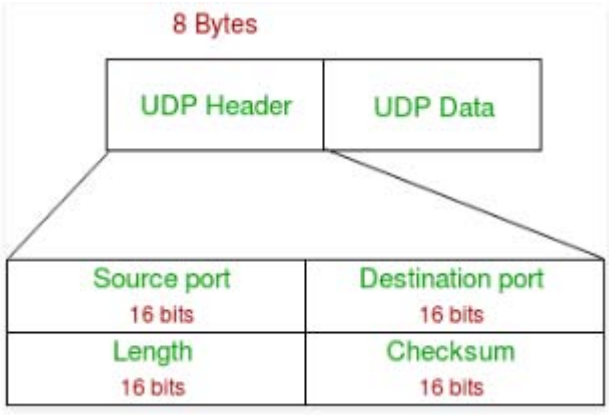
Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture. For the realtime services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also save bandwidth.
User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

Uses of UDP/ Features

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.

- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP Header –



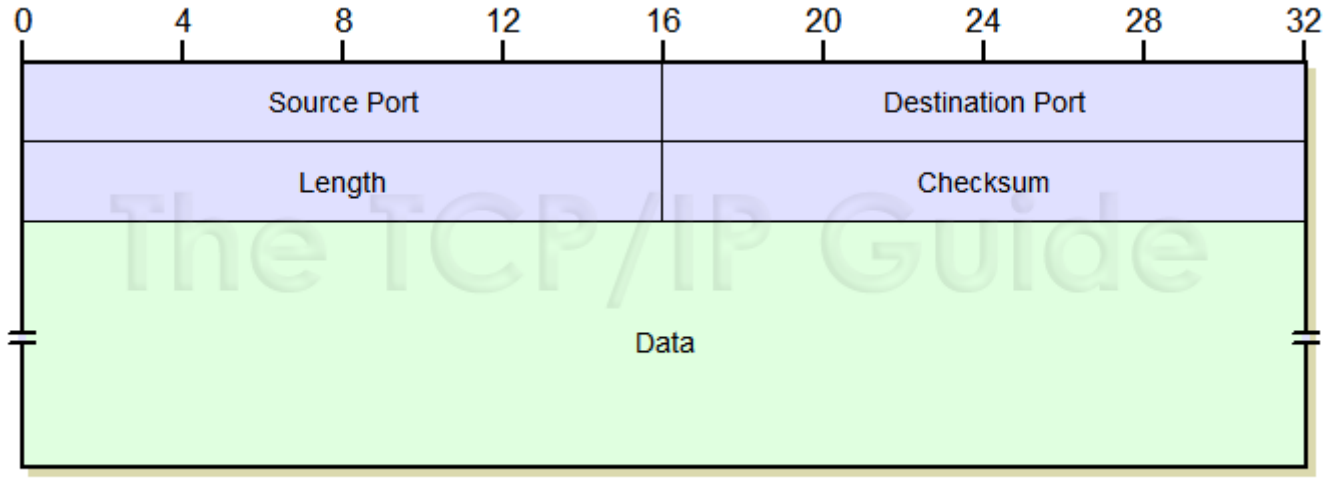


Figure 200: UDP Message Format

Notes – Unlike TCP, Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

UDP Application

Here are few applications where UDP is used to transmit data:

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

UDP Operation

It is designed to do as little as possible, and little is exactly what it does.

What UDP Does

UDP's only real task is to take data from higher-layer protocols and place it in UDP messages, which are then passed down to the Internet Protocol for transmission. The basic steps for transmission using UDP are:

1. **Higher-Layer Data Transfer:** An application sends a message to the UDP software.

2. **UDP Message Encapsulation:** The higher-layer message is encapsulated into the *Data* field of a UDP message. The headers of the UDP message are filled in, including the *Source Port* of the application that sent the data to UDP, and the *Destination Port* of the intended recipient. The checksum value may also be calculated.

3. **Transfer Message To IP:** The UDP message is passed to IP for transmission.

And that's about it. Of course, on reception at the destination device this short procedure is reversed.

What UDP Does Not

In fact, UDP is ***so*** simple, that its operation is very often described in terms of what it does ***not*** do, instead of what it does. As a transport protocol, some of the most important things UDP does not do include the following:

- UDP does not establish connections before sending data. It just packages it and… off it goes.
- UDP does not provide acknowledgments to show that data was received.
- UDP does not provide any guarantees that its messages will arrive.
- UDP does not detect lost messages and retransmit them.
- UDP does not ensure that data is received in the same order that they were sent.
- UDP does not provide any mechanism to manage the flow of data between devices, or handle congestion.

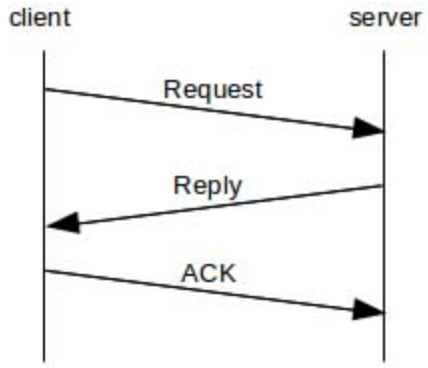
The differences between TCP and UDP

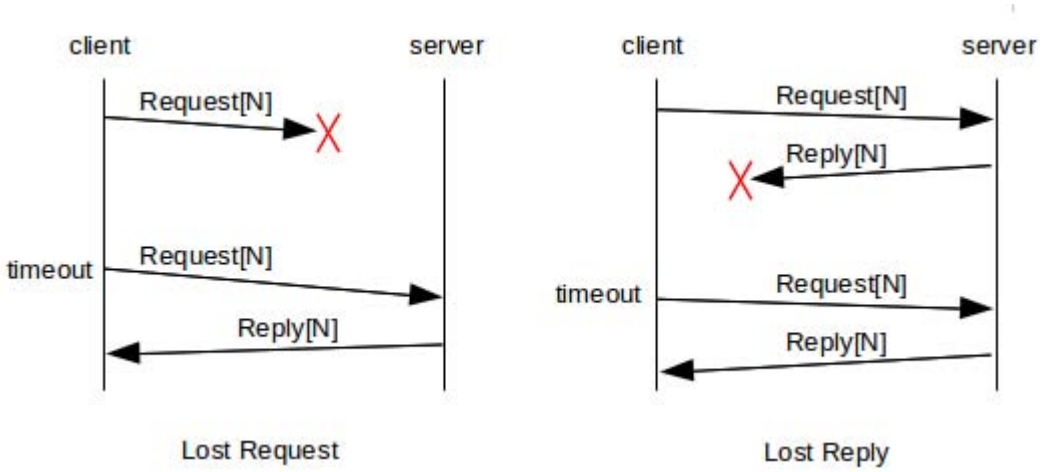
TRANSMISSION CONTROL PROTOCOL	USER DATAGRAM PROTOCOL
A connection-oriented protocol	A connectionless protocol
The most widely used protocol on the internet	Used for voice over IP, streaming video, gaming and live broadcasts
Guarantees that no packets are missing and all the data that's sent makes it to the intended recipient	Faster and needs fewer resources
Sends packets in order so they can be stitched back together easily	Packets don't necessarily arrive in order
Slower and requires more resources	Allows missing packets, but the sender is unable to know whether a packet has been received
Has a bigger header than UDP, best suited for apps that need high reliability and transmission time is relatively less critical	Better suited for applications that need fast, efficient transmission, such as games

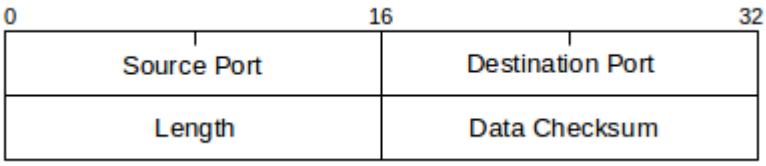
11.7 Remote Procedure Call (RPC)

A very different communications model, usually but not always implemented over UDP, is that of **Remote Procedure Call**, or RPC. The name comes from the idea that a procedure call is being made over the network; host A packages up a *request*, with parameters, and sends it to host B, which returns a *reply*. The term **request/reply protocol** is also used for this. The side making the request is known as the *client*, and the other side the *server*.

common example is that of DNS, Other examples include password verification, system information retrieval, database queries and file I/O (below).







0	15	16	31
Source Port		Destination Port	
Length		Checksum	
Data octets			

Length

The number of bytes in the packet. This includes the UDP header and the data (RPC packet in this case).

Checksum

The checksum is the 16-bit one's complement of the one's complement sum of all 16-bit words in the pseudo-header, UDP header and raw data.

The UDP pseudo-header consists of the source and destination IP addresses, the Internet Protocol Number for UDP (17 decimal) and the UDP length (see RFC 768). An implementation may choose not to compute a UDP checksum when transmitting a packet, in which case it must set the checksum field to zero.

Data Octets

Provided by the protocol layer above UDP. In this case, this is the RPC request itself.

11.7.1 Network File Sharing

In terms of total packet volume, the application making the greatest use of early RPC was Sun's **Network File Sharing**, or NFS; this allowed for a filesystem on the server to be made available to clients.

For read() operations
For write() operations,

11.7.2 Sun RPC

The original simple model above is quite serviceable. However, in the RPC implementation developed by Sun Microsystems and documented in **RFC 1831** (and officially known as Open Network Computing, or ONC, RPC), the final acknowledgment was omitted.

11.7.3 Serialization

In some RPC systems, even those with explicit ACKs, requests are executed serially by the server.

11.7.4 Refinements

One basic network-level improvement to RPC concerns the avoidance of IP-level fragmentation. While fragmentation is not a major performance problem on a single LAN, it may have difficulties over longer distances. One possible refinement is an RPC-level large-message protocol, that fragments at the RPC layer and which supports a mechanism for retransmission, if necessary, only of those fragments that are actually lost.

5.4	**Principles of Reliable Data Transfer: Building a Reliable DataTransfer Protocol, Pipelined Reliable Data Transfer Protocol, Go Back-N(GBN), Selective Repeat(SR)**	**2**

Principles of Reliable Data Transfer (rdt)

- **(Here rdt stands for ``reliable data transfer'' protocol**

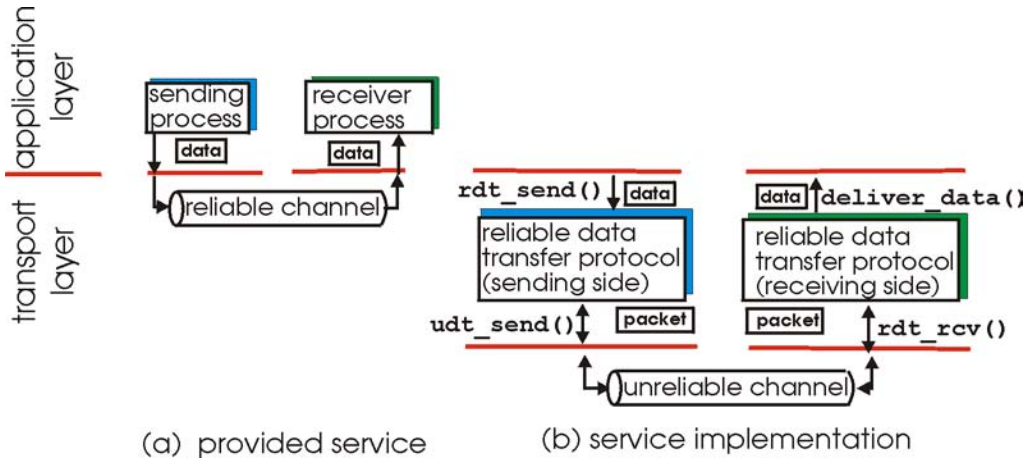


Figure : Reliable data transfer: service model and service implementation.

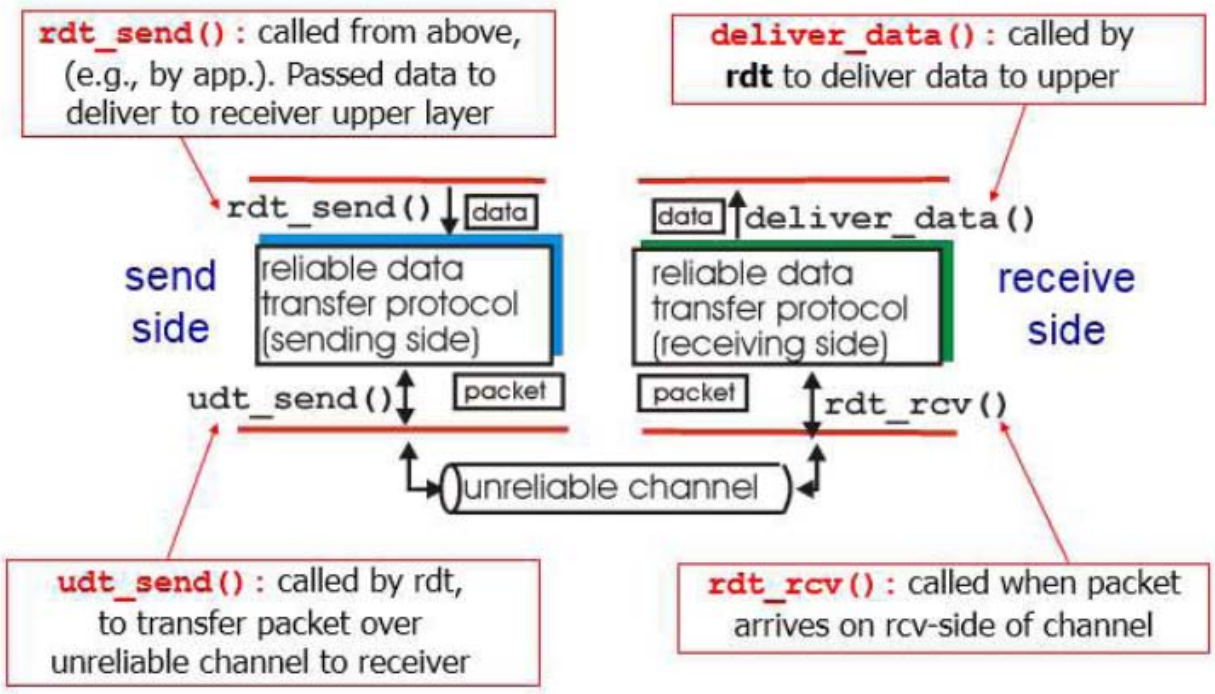


Fig. 7 Reliable data transfer commands

• The sending side of the data transfer protocol will be invoked from above by a call to rdt_send().

• On the receiving side, rdt_rcv() will be called when a packet arrives from the receiving side of the channel.

• When the rdt protocol wants to deliver data to the upper layer, it will do so by calling deliver_data().

• Both the send and receive sides of rdt send packets to the other side by a call to udt_send().

Building a Reliable Data Transfer Protocol

Reliable Data Transfer over a Perfectly Reliable Channel: rdt1.0

- We first consider the simplest case in which the underlying channel is completely reliable.
- The protocol itself, which we will call rdt1.0, is trivial.

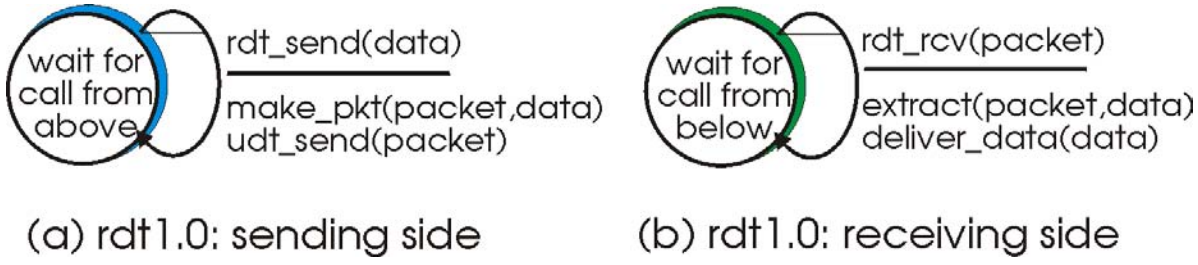


Figure : rdt1.0 - a protocol for a completely reliable channel

- The **finite state machine** (FSM) definitions for the rdt1.0 sender and receiver are shown in Figure

- The **sending side** of rdt simply accepts data from the upper-layer via the rdt_send(data)event, puts the data into a packet (via the action make_pkt(packet,data)) and sends the packet into the channel. In practice, the rdt_send(data)event would result from a procedure call (e.g., to rdt_send()) by the upper layer application.
- On the **receiving side**, rdt receives a packet from the underlying channel via the rdt_rcv(packet) event, removes the data from the packet (via the action extract(packet,data)) and passes the data up to the upper-layer. In practice, the rdt_rcv(packet)event would result from a procedure call (e.g., to rdt_rcv()) from the lower layer protocol.

Reliable Data Transfer over a Channel with Bit Errors: rdt2.0

- ✓ A more realistic model of the underlying channel is one in which bits in a packet may be corrupted.
- ✓ Such bit errors typically occur in the physical components of a network as a packet is transmitted, propagates, or is buffered.
- ✓ We'll continue to assume for the moment that all transmitted packets are received (although their bits may be corrupted) in the order in which they were sent.
- ✓ This message dictation protocol uses both **positive ac knowledgements** (``OK'') and **negative acknowledgements** (``Please repeat that'').

Fundamentally, **two additional protocol capabilities** are required in ARQ protocols to handle the presence of bit errors:

- ***Error detection***
- ***Receiver feedback.***

Figure 3.4-3 shows the FSM representation of rdt2.0, a data transfer protocol employing error detection, positive acknowledgements (ACKs), and negative acknowledgements (NAKs).

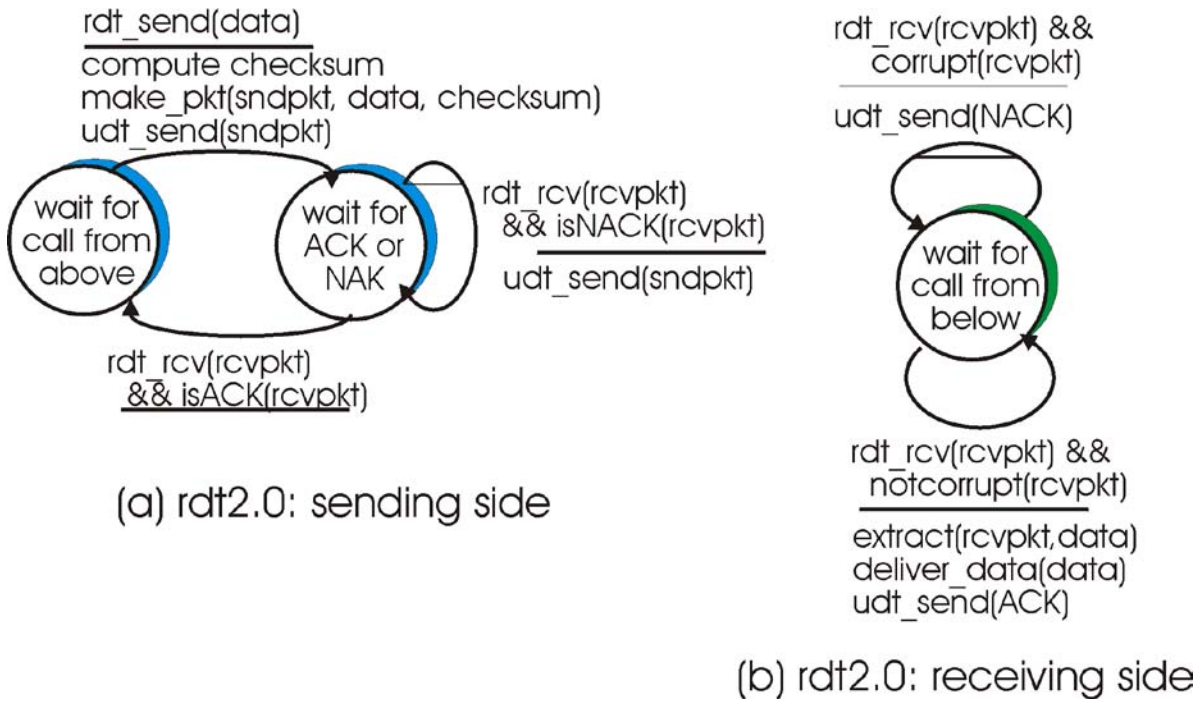


Figure 3.4-3: rdt2.0 - a protocol for a channel with bit-errors

Consider three possibilities for handling corrupted ACKs or NAKs:

- For the **first possibility,** consider what a human might do in the message dictation scenario. If the speaker didn't understand the ``OK" or ``Please repeat that" reply from the receiver, the speaker would probably ask ``What did you say?" (thus introducing a new type of sender-to-receiver packet to our protocol).
- A **second alternative is to add enough checksum bits to allow the sender to not only detect,** but **recover from, bit errors.** This solves the immediate problem for a channel which can corrupt packets but not lose them.
- A **third approach is for the sender to simply resend the current data packet when it receives a garbled ACK or NAK packet**. This, however, introduces **duplicate packets** into the sender-to-receiver channel.

rdt2.1: sender, handles garbled ACK/NAKs

.

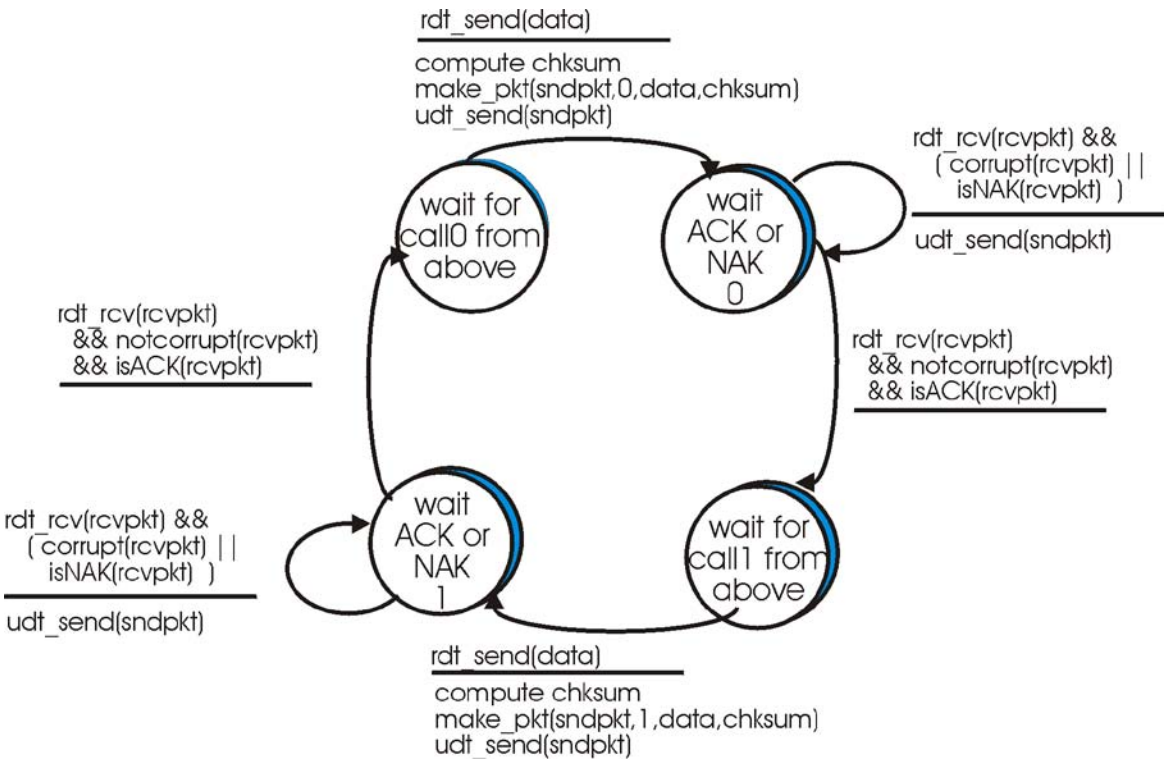


Figure 3.4-4: rdt2.1 sender

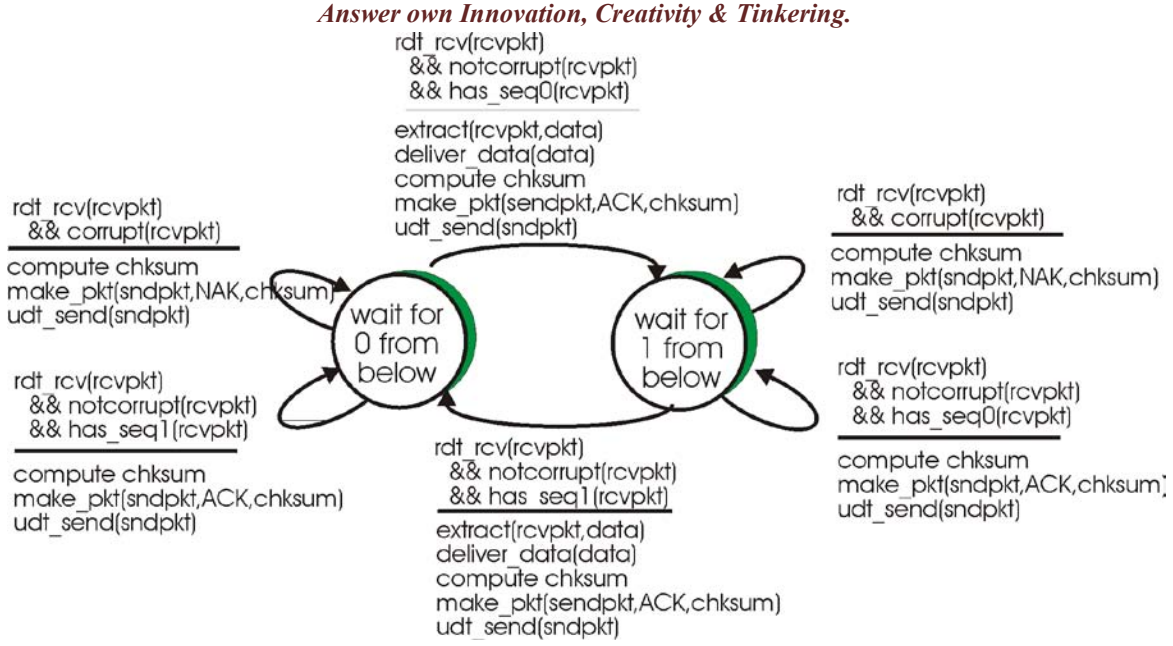


Figure 3.4-5: rdt2.1 recevier

Figures 3.4-4 and 3.4-5 show the FSM description for rdt2.1, our fixed version of rdt2.0. The rdt2.1 sender and receiver FSM's each now have twice as many states as before.

Our NAK-free reliable data transfer protocol for a channel with bit errors is rdt2.2, shown in Figure 3.4-6 and 3.4-7.

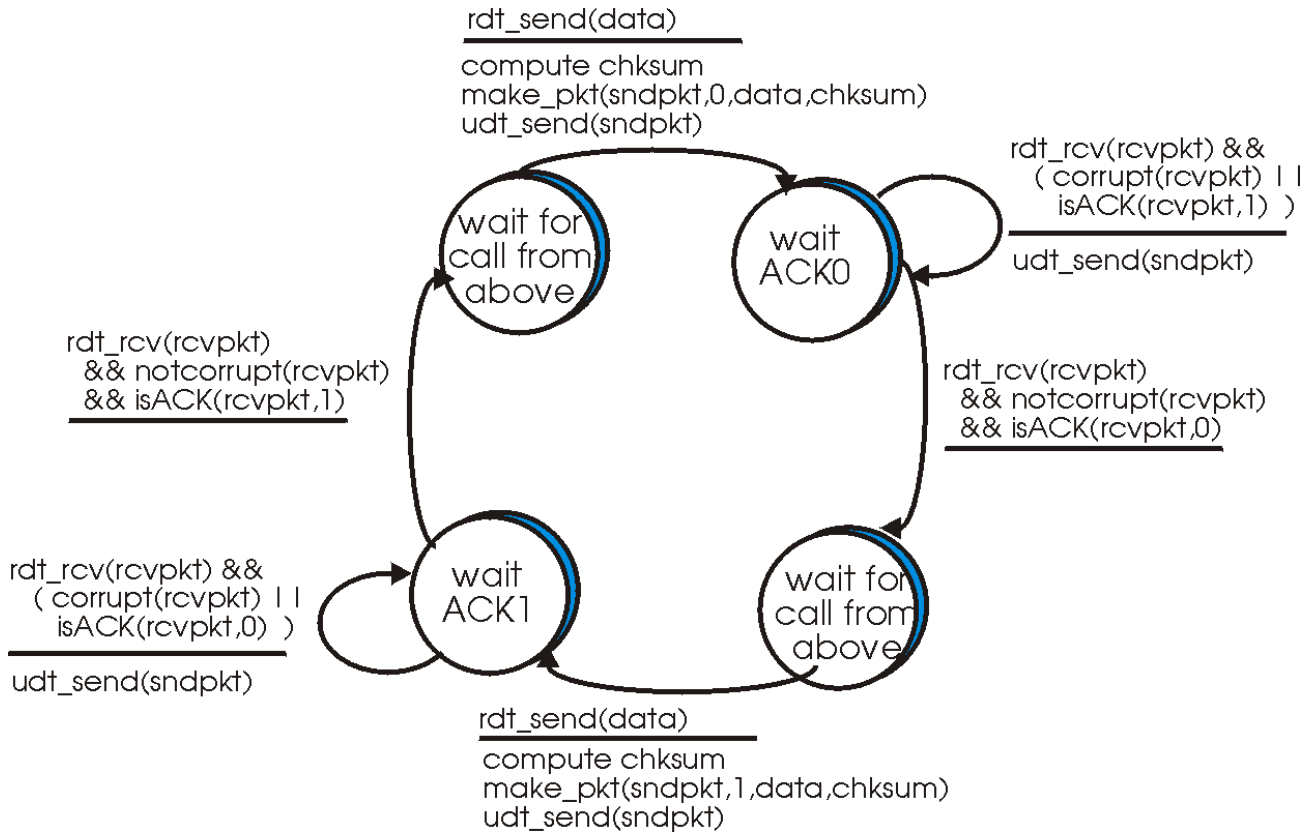


Figure 3.4-6: rdt2.2 sender

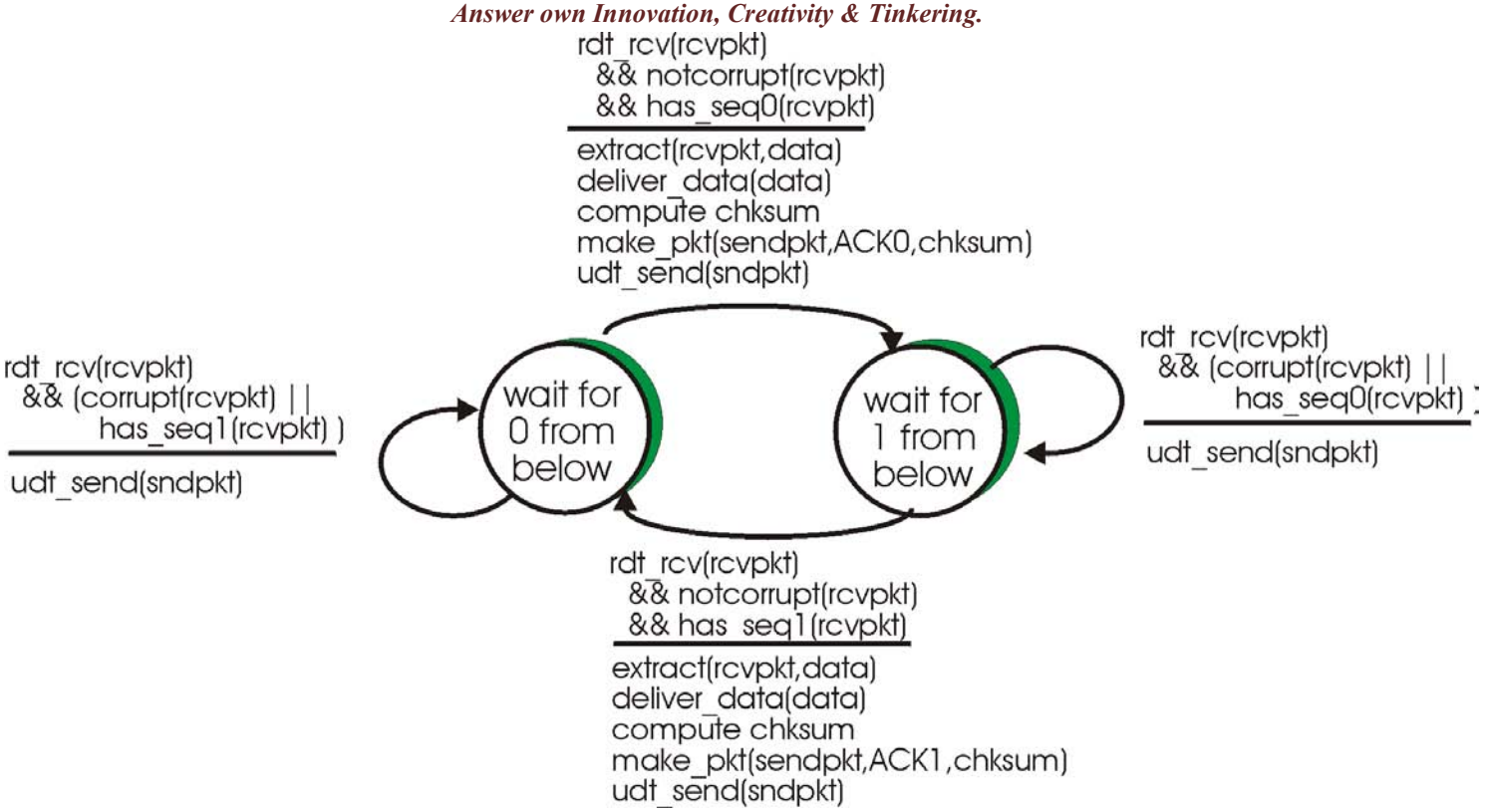


Figure 3.4-7: rdt2.2 receiver

Reliable Data Transfer over a Lossy Channel with Bit Errors: rdt3.0

- Suppose now that in addition to corrupting bits, the underlying channel can *lose* packets as well, a not uncommon event in today's computer networks (including the Internet).
- Two additional concerns must now be addressed by the protocol: how to detect packet loss and what to do when this occurs.
- The use of checksumming, sequence numbers, ACK packets, and retransmissions - the techniques already developed in rdt 2.2 - will allow us to answer the latter concern. Handling the first concern will require adding a new protocol mechanism.

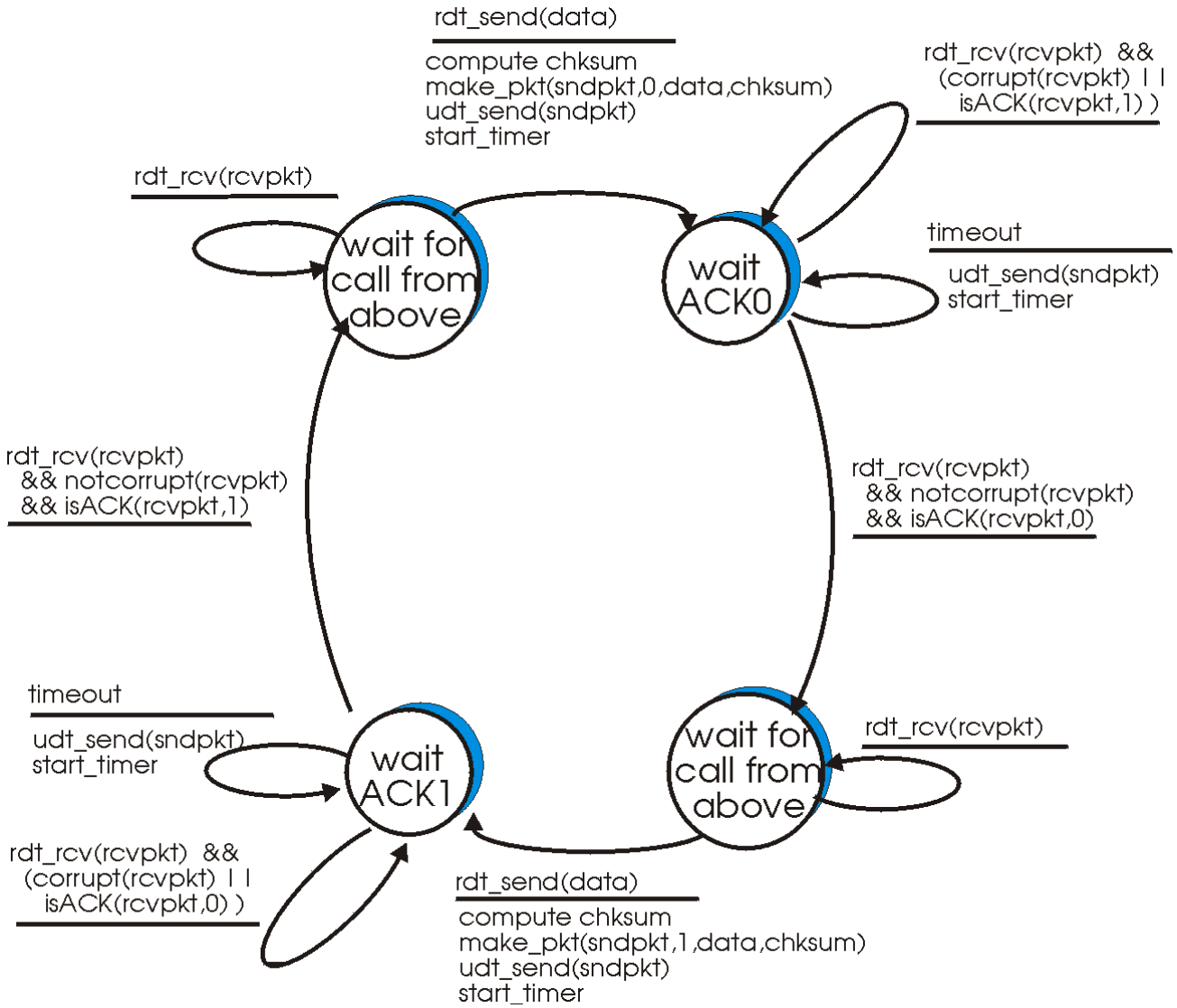


Figure 3. 4-8: rdt 3.0 sender FSM

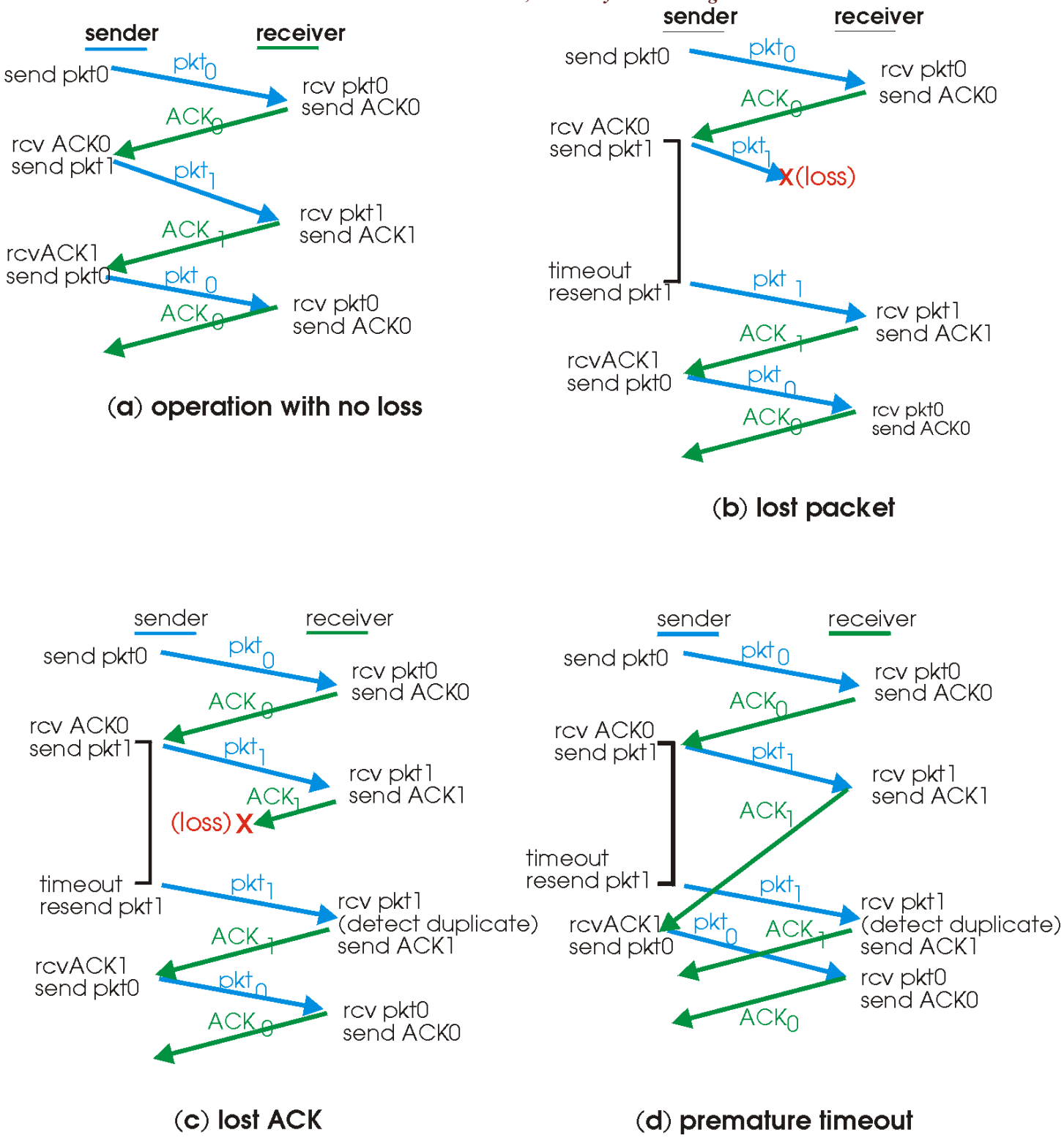


Figure 3.4-9: Operation of rdt 3.0, the alternating bit protocol

Figure 3.4-8 shows the sender FSM for rdt3.0, a protocol that reliably transfers data over a channel that can corrupt or lose packets.

Figure 3.4-9 shows how the protocol operates with no lost or delayed packets, and how it handles lost data packets. In Figure 3.4-9, time moves forward from the top of the diagram towards the bottom of the diagram; note that a receive time for a packet is neccessarily later than the send time for a packet as a result of transmisison and propagation delays.

In Figures 3.4-9(b)-(d), the send-side brackets indicate the times at which a timer is set and later times out. Several of the more subtle aspects of this protocol are explored in the exercises at the end of this chapter. Because packet sequence numbers alternate between 0 and 1, protocol rdt3.0 is sometimes known as the **alternating bit protocol.**

Pipelined Reliable Data Transfer Protocols

- Protocol pipelining is a technique in which multiple requests are written out to a single socket without waiting for the corresponding responses (acknowledged).
- Pipelining can be used in various application layer network protocols, like HTTP/1.1, SMTP and FTP.
- Range of sequence numbers must be increased.
- Data or Packet should be buffered at sender and/or receiver.

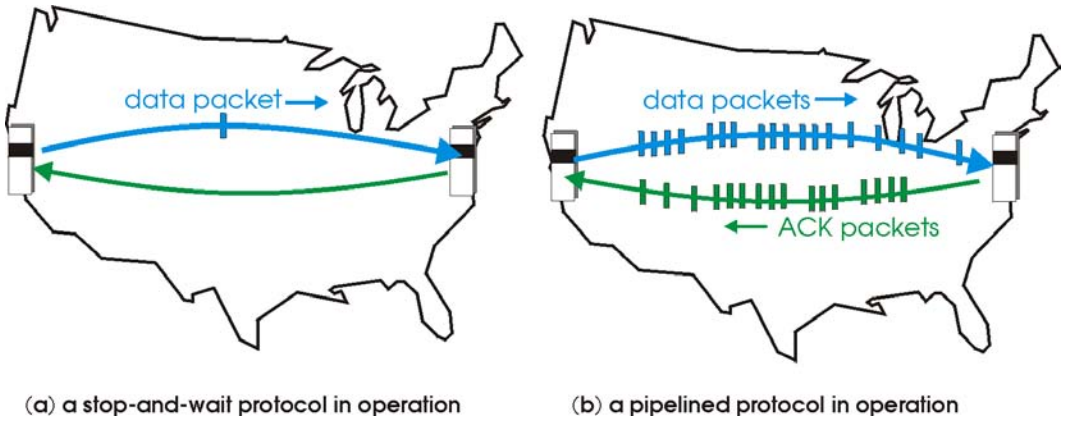
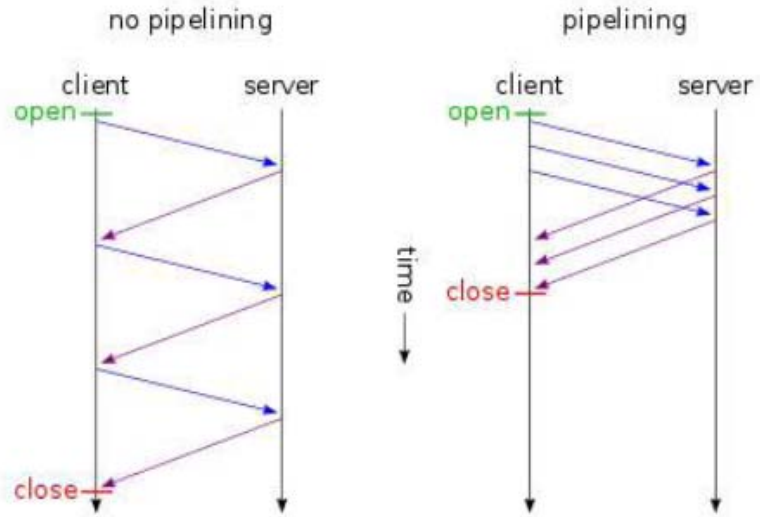


Figure 3.4-10: Stop-and-wait versus pipelined protocols



The solution to this particular performance problem is a simple one: rather than operate in a stop-and-wait manner, the sender is allowed to send multiple packets without waiting for acknowledgements, as shown in Figure 3.4-10(b). Since the many in-transit sender-to-receiver packets can be visualized as filling a pipeline, this technique is known as **pipelining**.

Two generic forms of pipelined protocols are

1. **Go-Back-N**
2. **Selective repeat**

Sr. No.	Key	Go-Back-N	Selective Repeat
1	Definition	In Go-Back-N if a sent frame is found suspected or damaged then **all the frames are** retransmitted till the last packet.	In Selective Repeat, **only** the suspected or damaged frames are retransmitted.
2	Sender Window Size	Sender Window is of size N.	Sender Window size is **same** as N.
3	Receiver Window Size	Receiver Window Size is 1.	Receiver Window Size is N.
4	Complexity	Go-Back-N is easier to implement.	In Selective Repeat, receiver window needs to **sort the** frames.
5	Efficiency	Efficiency of Go-Back-N = N / (1 + 2a).	Efficiency of Selective Repeat = N / (1 + 2a).
6	Acknowledgement	Acknowledgement type is **cumulative**.	Acknowledgement type is **individual**.

"Go-Back-N Protocol and "Selective Repeat Protocol" are the sliding window protocols. The sliding window protocol is primarily an error control protocol, i.e. it is a method of error detection and error correction.

Go-Back-N (GBN)

- Retransmits all the frames that sent after the frame which suspects to be damaged or lost.
- If error rate is high, it wastes a lot of bandwidth.
- Less complicated.
- Window size N-1
- Sorting is neither required at sender side nor at receiver side.
- Receiver do not store the frames received after the damaged frame until the damaged frame is retransmitted.
- No searching of frame is required neither on sender side nor on receiver
- NAK number refer to the next expected frame number.
- It more often used.

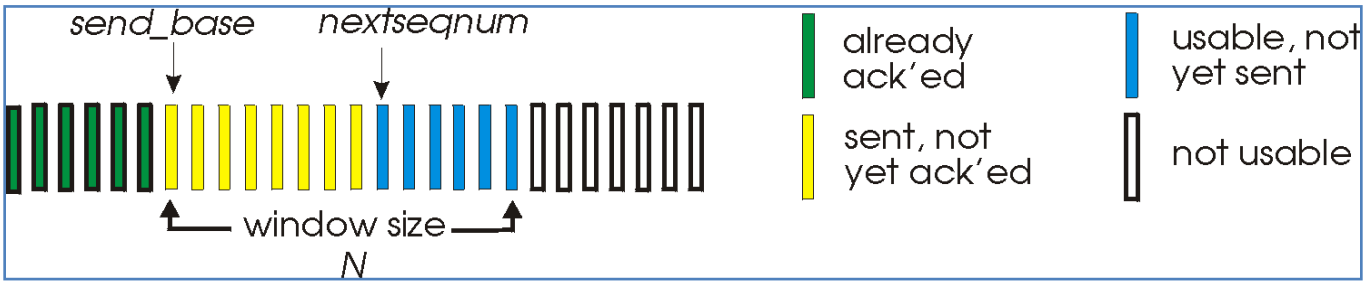


Figure 3.4-11: Sender's view of sequence numbers in Go-Back-N

In a Go-Back-N (GBN) protocol, the sender is allowed to transmit multiple packets (when available) ***without waiting for an acknowledgment, but no more than some maximum allowable number,*** *N*, of unacknowledged packets in the pipeline. finite state machines(FSM)

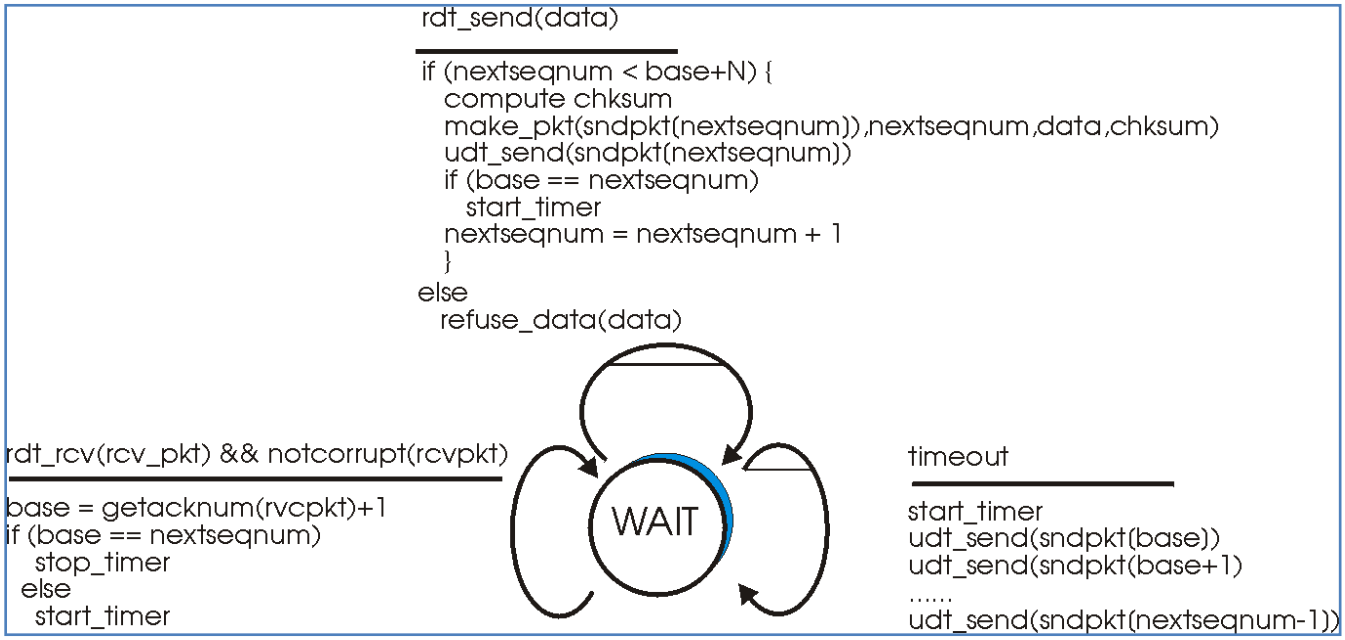


Figure 3.4-12 Extended FSM description of GBN sender.

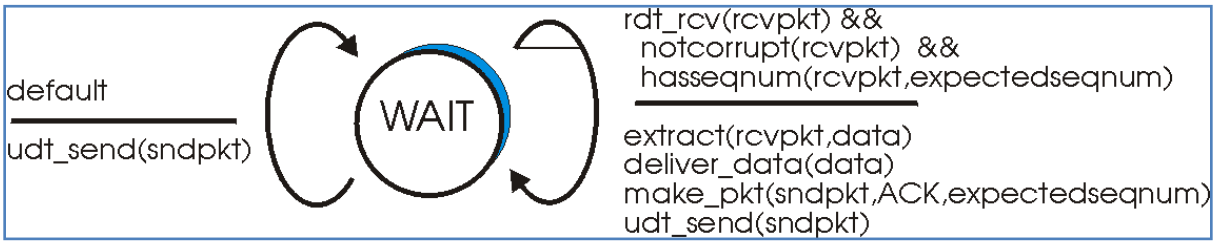


Figure 3.4-13 Extended FSM description of GBN receiver.

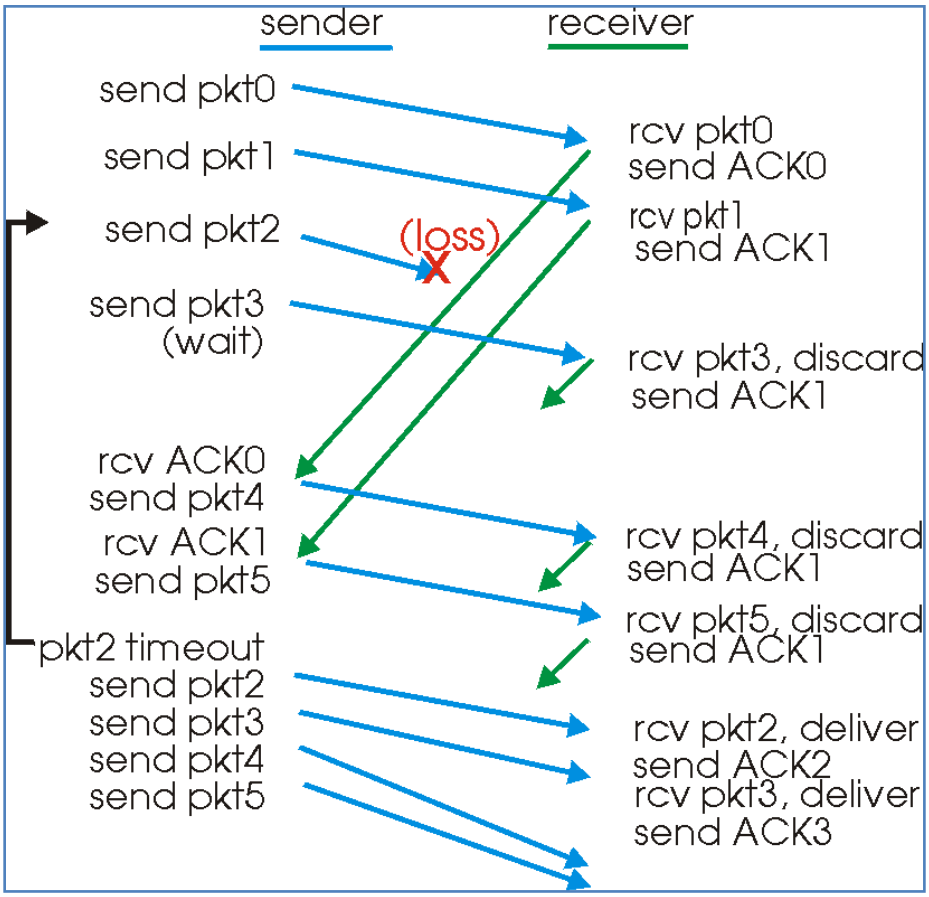


Figure 3.4-14: Go-Back-N in operation

Selective Repeat (SR)

- Retransmits only those frames that are suspected to lost or damaged.
- Comparatively less bandwidth is wasted in retransmitting.
- More complex as it require to apply extra logic and sorting and storage, at sender and receiver.
- Window Size is <= (N+1)/2
- Receiver must be able to sort as it has to maintain the sequence of the frames.
- Receiver stores the frames received after the damaged frame in the buffer until the damaged frame is replaced.
- The sender must be able to search and select only the requested frame.
- NAK number refer to the frame lost.
- It is less in practice because of its complexity.

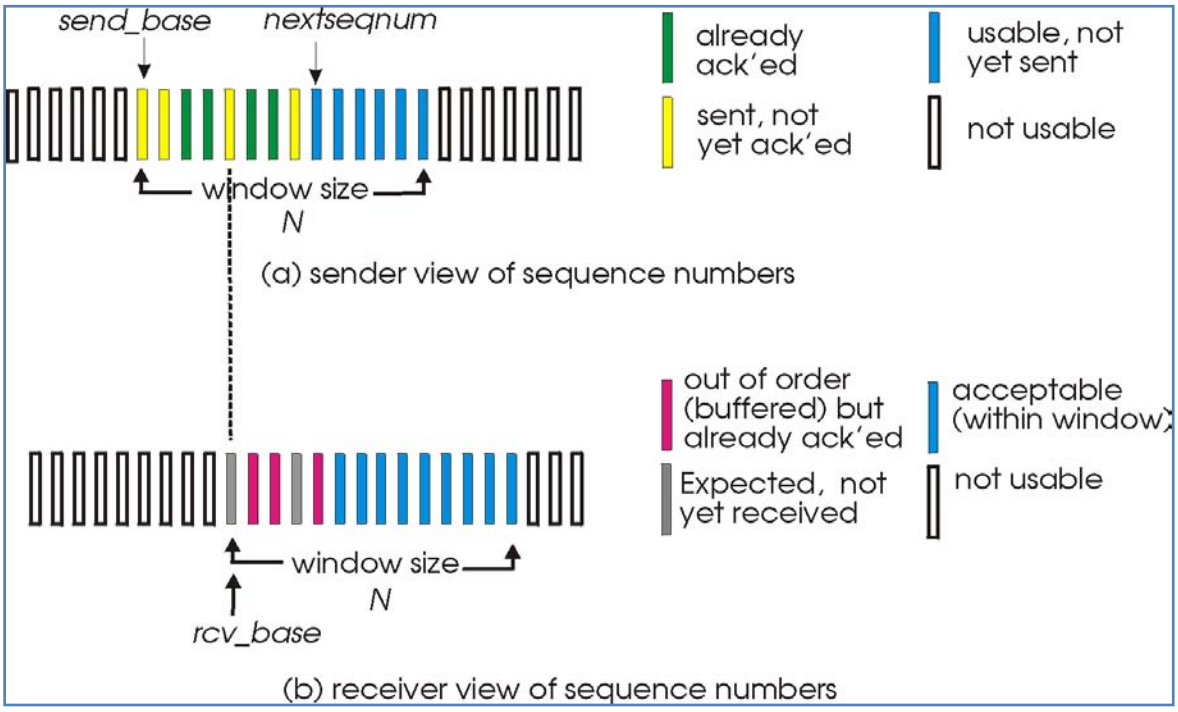


Figure 3.4-15: SR sender and receiver views of sequence number space

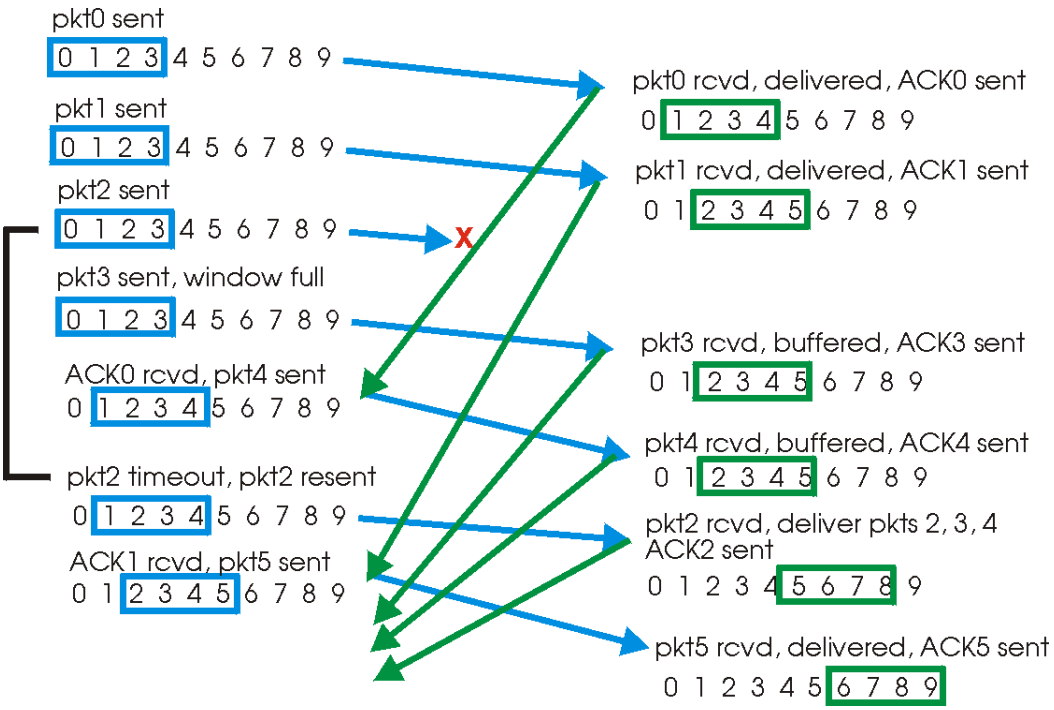


Figure 3.4-18: SR Operation

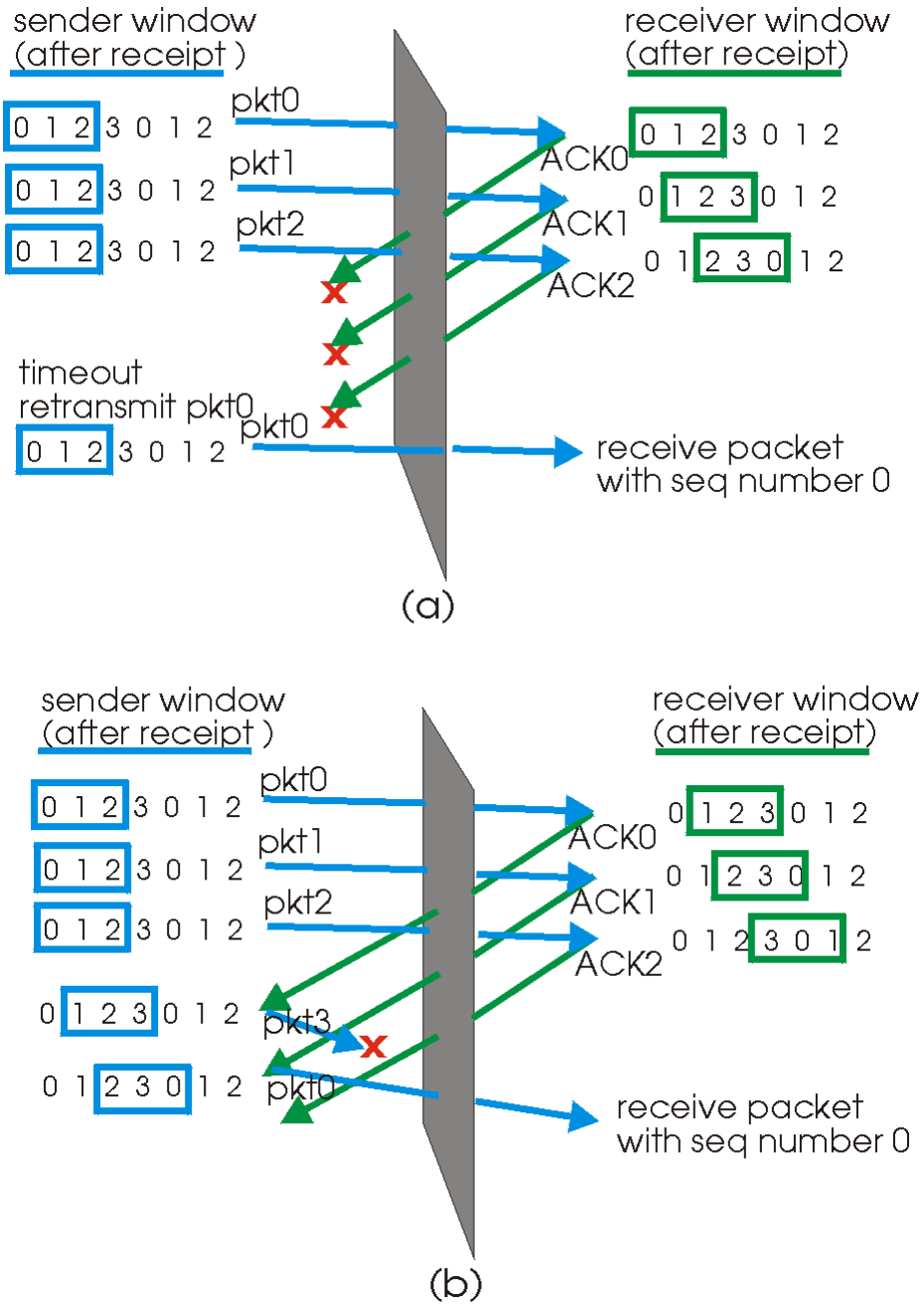


Figure 3.4-19: SR receiver dilemma(a difficult situation or problem) with too large windows: a new packet or a retransmission

5.5	Transmission Control Protocol(TCP): TCP Services, TCP Features, TCP Segment Header	1

Connection-Oriented Transport: 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.

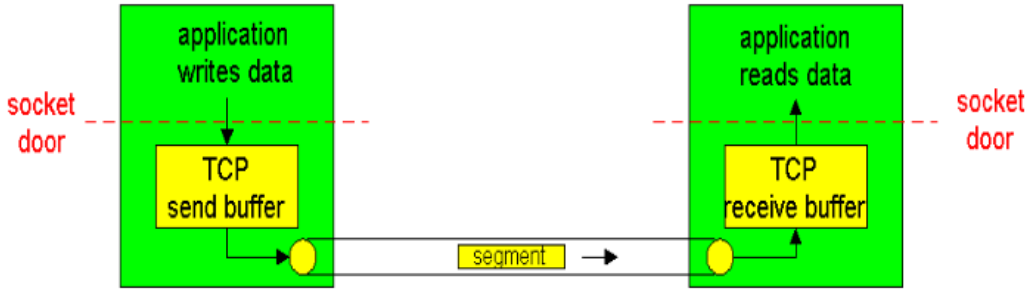


Figure 3.5-1: TCP send and receive buffers

It works together with IP and provides a reliable transport service between processes using the network layer service provided by the IP protocol.

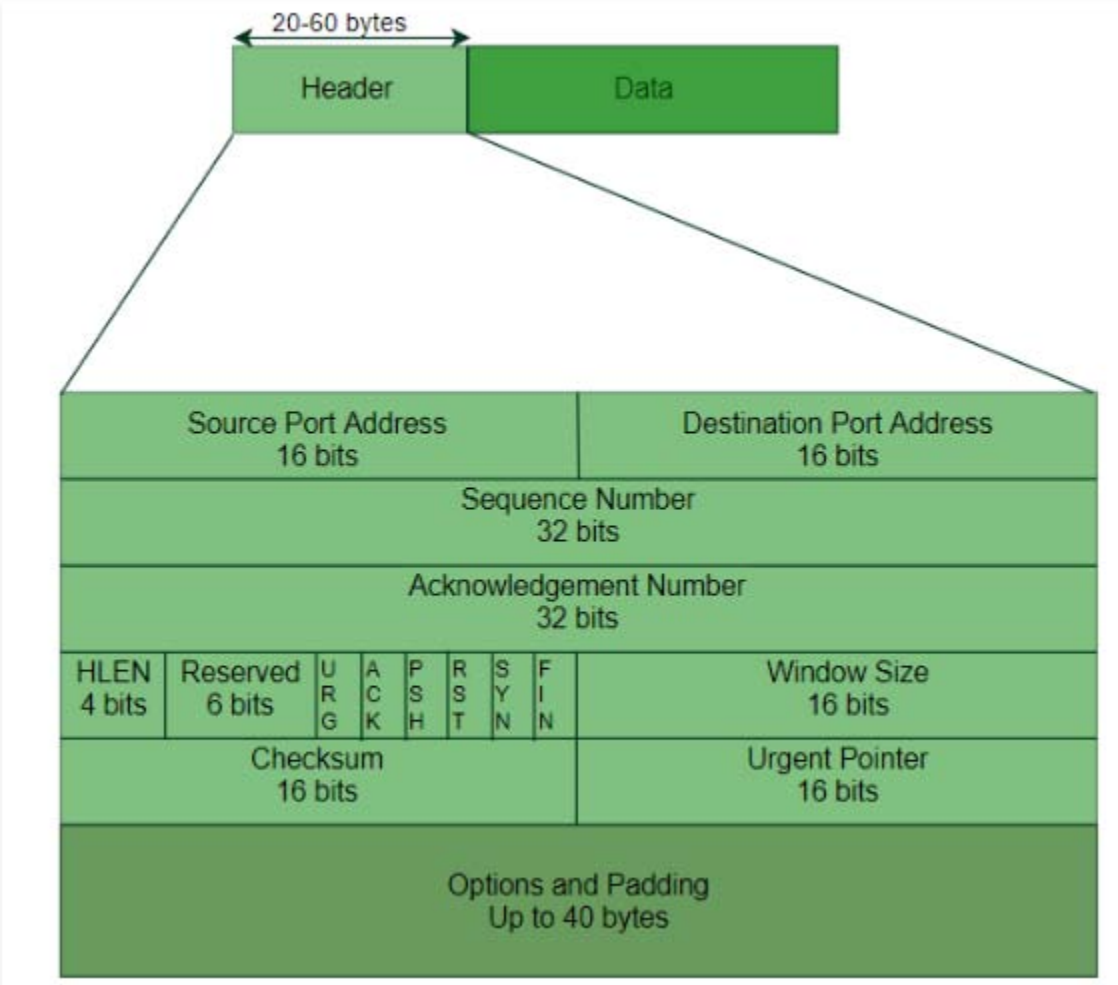
TCP Services to the application layer are as follows:

1. **Process-to-Process Communication –**
   TCP provides process to process communication, i.e, the transfer of data takes place between individual processes executing on end systems. This is done using port numbers or port addresses. Port numbers are 16 bit long that help identify which process is sending or receiving data on a host.
2. **Stream oriented –**
   This means that the data is sent and received as a stream of bytes(unlike UDP or IP that divides the bits into datagrams or packets).
3. **Full duplex service –**
   This means that the communication can take place in both directions at the same time.
4. **Connection oriented service –**
   Unlike UDP, TCP provides connection oriented service. It defines 3 different phases:
   - Connection establishment
   - Data transfer
   - Connection termination
5. **Reliability –**
   TCP is reliable as it uses checksum for error detection, attempts to recover lost or corrupted packets by re-transmission, acknowledgement policy and timers. It uses features like byte number and sequence number and acknowledgement number so as to ensure reliability. Also, it uses congestion control mechanisms.
6. **Multiplexing –**
   TCP does multiplexing and de-multiplexing at the sender and receiver ends respectively as a number of logical connections can be established between port numbers over a physical connection.

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 Header



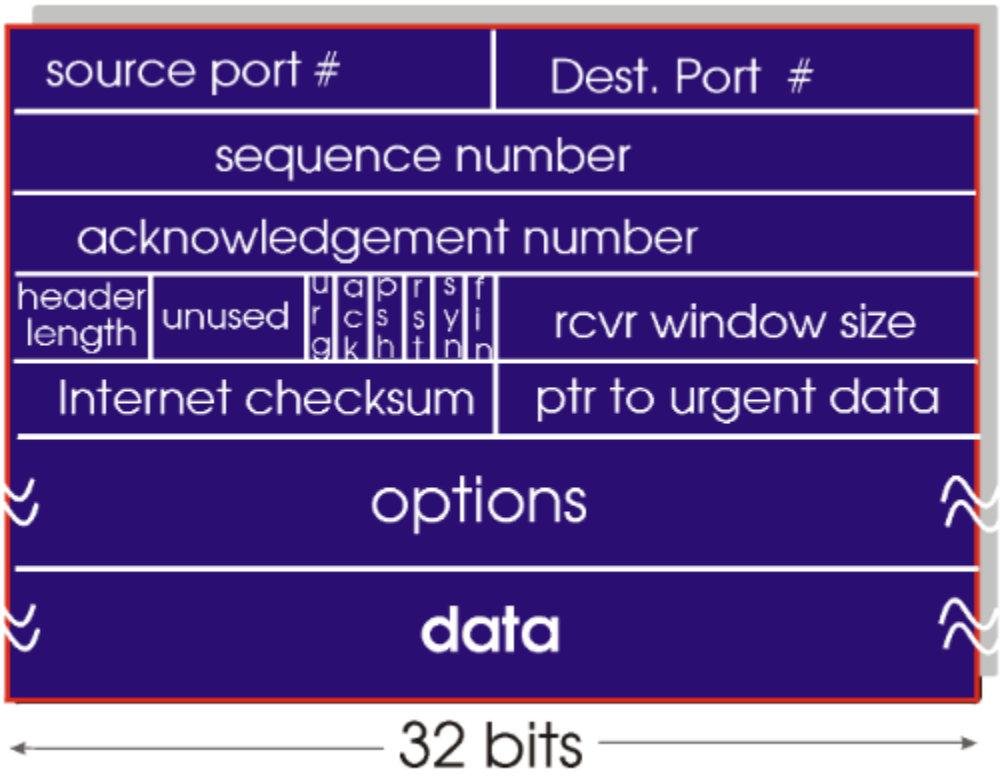


Figure 3.5-2: TCP segment structure

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.

- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
    - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
    - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
    - **ECE** -It has two meanings:
        - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
        - If SYN bit is set to 1, ECE means that the device is ECT capable.
    - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
    - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.

- **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
- **RST** - Reset flag has the following features:
  - It is used to refuse an incoming connection.
  - It is used to reject a segment.
  - It is used to restart a connection.
- **SYN** - This flag is used to set up a connection between hosts.
- **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

5.6	Principle of Congestion Control	1

5.6 Principles of Congestion Control

In this section, we consider the problem of congestion control in a general context, seeking to understand *why* congestion is a "bad thing," *how* network congestion is manifested in the performance received by upper-layer applications, and various approaches that can be taken to avoid, or react to, network congestion. ***The following section contains a detailed study of TCP's congestion control algorithm.***

5.6.1 The Causes and the "Costs" of Congestion

In each case, we'll look at why congestion occurs in the first place, and the "cost" of congestion.

Scenario 1: Two senders, a router with infinte buffers

- Considering perhaps the simplest congestion scenario possible:
- Two hosts (A and B) each have a connection that share a single hop between source and destination, as shown in Figure 3.6-1.

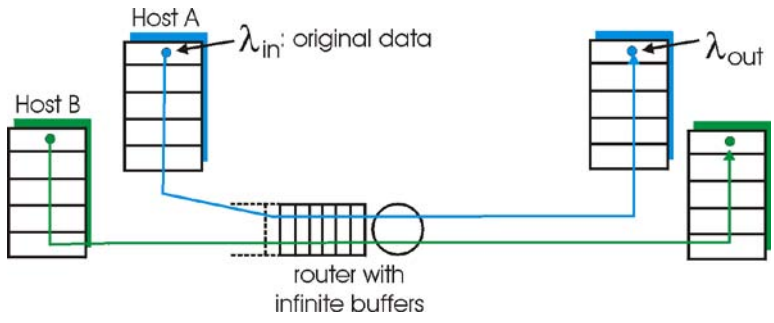


Figure 5.6-1: Congestion scenario 1: two connections sharing a single hop with infinte buffers

Scenario 2: Two senders, a router with finite buffers

Let us now slightly modify scenario 1 in the following two ways.

- First, the amount of router buffering is assumed to be finite.
- Second, we assume that each connection is reliable.

If a packet containing a transport-level segment is dropped at the router, it will eventually be retransmitted by the sender. Because packets can be retransmitted, the term "sending rate."

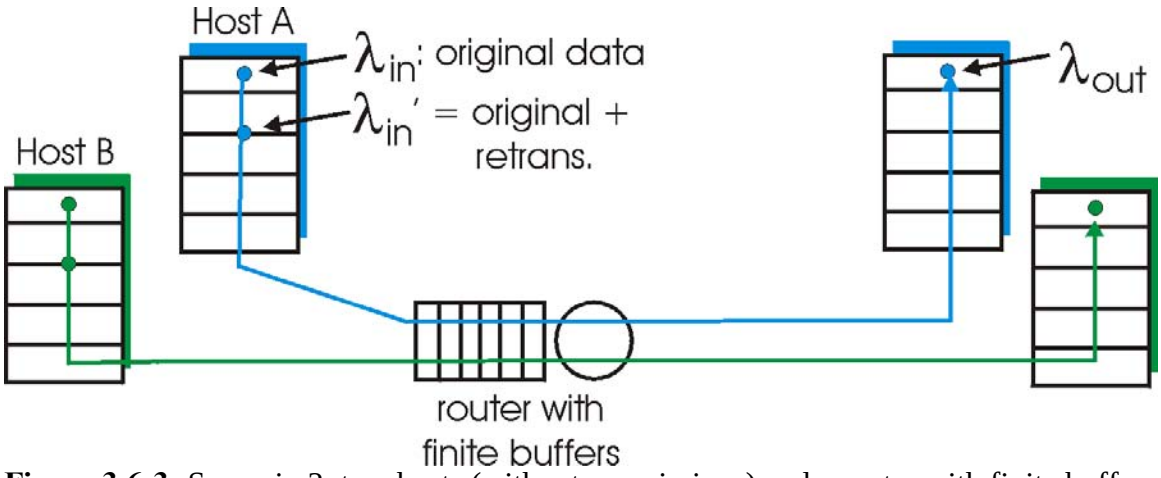


Figure 3.6-3: Scenario 2: two hosts (with retransmissions) and a router with finite buffers

Scenario 3: Four senders, routers with finite buffers, and multihop paths

In our final congestion scenario, four hosts transmit packets, each over overlapping two-hop paths, as shown in Figure 5.6-5. We again assume that each host uses a timeout/retransmission mechanism to implement a reliable data transfer service, that all hosts have the same value of λ_{in}, and that all router links have capacity C bytes/sec.

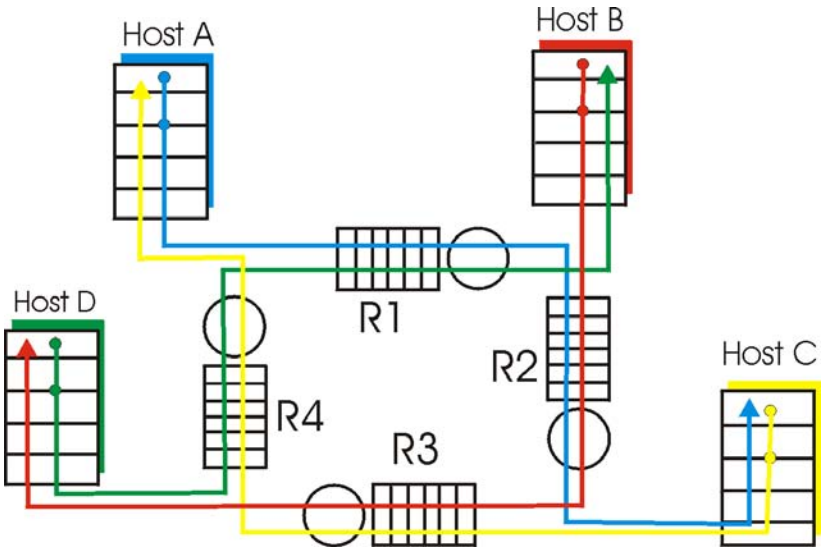


Figure 5.6-5: Four senders, routers with finite buffers, and multihop paths

Let us consider the connection from Host A to Host C, passing through Routers R1 and R2. The A-C connection shares router R1 with the D-B connection and shares router R2 with the B-D connection.

5.6.2 Approaches Toward Congestion Control

At the broadest level, The among congestion control approaches based on the whether or not the network layer provides any explicit assistance to the transport layer for congestion control purposes:

- **End-end congestion control.** In an end-end approach towards congestion control, the network layer provides *no explicit support* to the transport layer for congestion control purposes. Even the presence of congestion in the network must be inferred by the end systems based only on observed network behavior (e.g., packet loss and delay).
- **Network-assisted congestion control.** With network-assisted congestion control, network-layer components (i.e., routers) provide explicit feedback to the sender regarding the congestion state in the network. This feedback may be as simple as a single bit indicating congestion at a link .
  - ✓ For network-assisted congestion control, congestion information is typically fed back from the network to the sender in one of two ways, as shown in Figure 5.6-7.
  - ✓ Direct feedback may be sent from a network router to the sender. This form of notification typically takes the form of a **choke packet** (essentially saying, "I'm congested!").

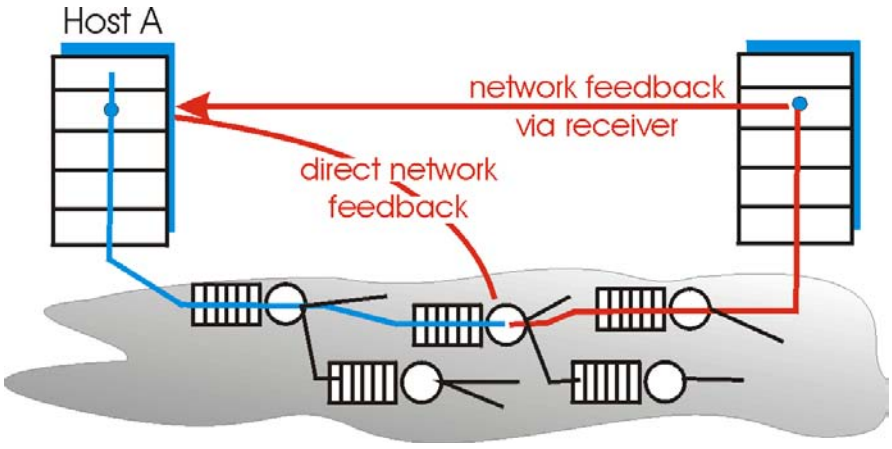


Figure 3.6-7: Two feedback pathways for network-indicated congestion information

ATM ABR Congestion Control

- Adopt ATM terminology (e.g., using the term "switch" rather than "router," and the term "call" rather than "packet).
- With ATM ABR service, data cells are transmitted from a source to a destination through a series of intermediate switches.
- Interspersed (*between other things*)with the data cells are so-called **RM (Resource Management) cells**;
- RM cells can be used to convey congestion-related information among the hosts and switches.
- RM cells can thus be used to provide both direct network feedback and network-feedback-via-the-receiver, as shown in Figure 3.6-8.

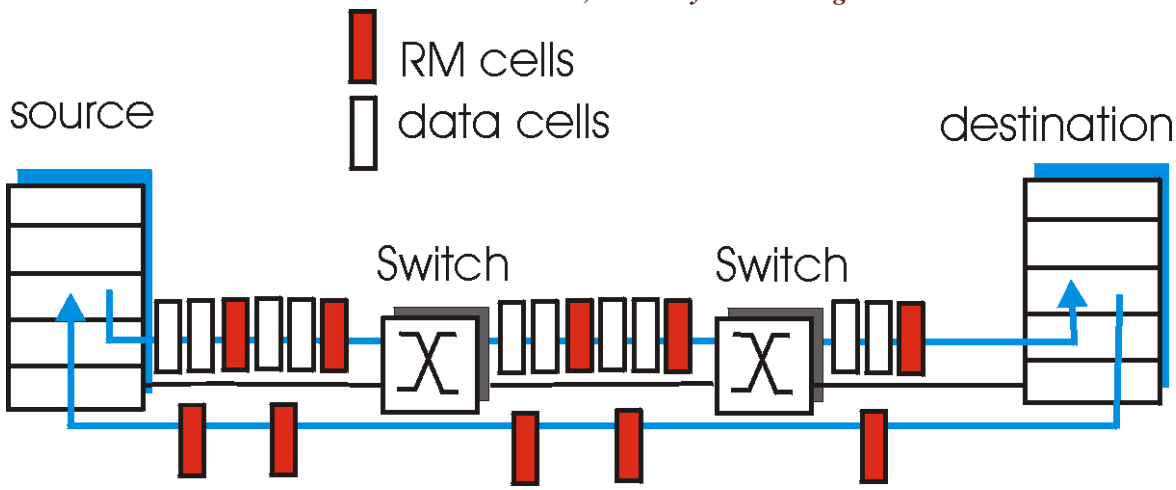


Figure 3.6-8: Congestion control framework for ATM ABR service

- ATM ABR congestion control is a **rate-based ap proach.** That is, the sender explicitly computes a maximum rate at which it can send and regulates itself accordingly.
- ABR provides three mechanisms for signaling congestion-related information from the siwtches to the receiver:

  - **EFCI (Explicit Forward Congestion Indication) bit.**
  - **CI and NI (No Increase) bits.**
  - **Explicit Rate (ER) setting.**

  An ATM ABR source adjusts the rate at which it can send cells as a function of the CI, NI and ER values in a returned RM cell. **The rules for making this rate adjustment are rather complicated and tedious(**too long, slow,**).**

Congestion Control

What is **congestion**?
A state occurring in network layer when the **message traffic is so heavy** that it slows down network response time.

Effects of Congestion

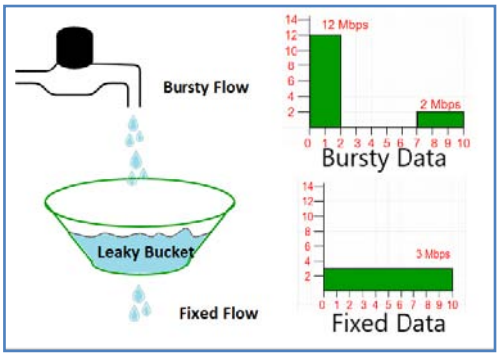
- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

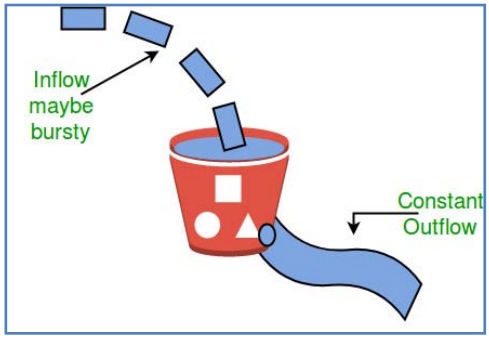
Congestion control algorithms

Difference between Leaky and Token buckets –

LEAKY BUCKET	TOKEN BUCKET
When the host has to send a packet , packet is thrown in bucket.	In this leaky bucket holds tokens generated at regular intervals of time.
Bucket leaks at constant rate	Bucket has maximum capacity.
Bursty traffic is converted into uniform traffic by leaky bucket.	If there is a ready packet , a token is removed from Bucket and packet is send.
In practice bucket is a finite queue outputs at finite rate	If there is a no token in bucket, packet can not be send.

- **Leaky Bucket Algorithm**
  - Suppose we have a bucket in which we are pouring water in a random order but we have to get water in a fixed rate, for this we will make a hole at the bottom of the bucket. It will ensure that water coming out is in a some fixed rate, and also if bucket will full we will stop pouring in it.
  - The input rate can vary, ***but the output rate remains constant.*** Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.





In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In Figure the host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in 10 s. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10 s.

The following is an algorithm for variable-length packets:

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

Example – Let n=1000

Packet= | 200 | 700 | 500 | 450 | 400 | 200 |

Since n> front of Queue i.e. n>200
Therefore, n=1000-200=800
Packet size of 200 is sent to the network.

| 200 | 700 | 500 | 450 | 400 |

Now Again n>front of the queue i.e. n > 400
Therefore, n=800-400=400
Packet size of 400 is sent to the network.

| 200 | 700 | 500 | 450 |

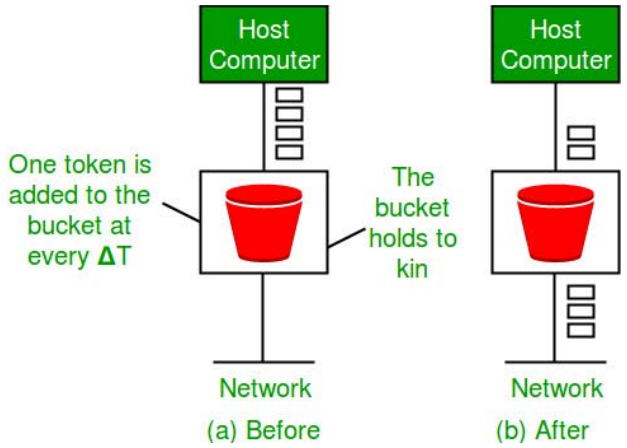
Since n< front of queue
Therefore, the procedure is stop.
Initialize n=1000 on another tick of clock.
This procedure is repeated until all the packets are sent to the network.

Token bucket Algorithm

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket. *f*
2. The bucket has a maximum capacity. *f*
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.



Let's understand with an example,
In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

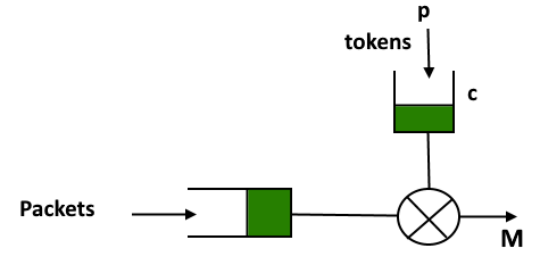
Example:

For a host machine that uses the token bucket algorithm for congestion control, the token bucket has a capacity of 1 megabyte and the maximum output rate is 20 megabytes per second. Tokens arrive at a rate to sustain output at a rate of 10 megabytes per second. The token bucket is currently full and the machine needs to send 12 megabytes of data. The minimum time required to transmit the data is _____ seconds.

According to the token bucket algorithm, the minimum time required to send 1 MB of data or the maximum rate of data transmission is given by:

$$S = C / (M - P)$$

Where,
M = Maximum burst rate,
P = Rate of arrival of a token,
C = capacity of the bucket



M = 20 MB
P = 10 MB
C = 1 MB
S = 1 / (20- 10) = 0.1 sec

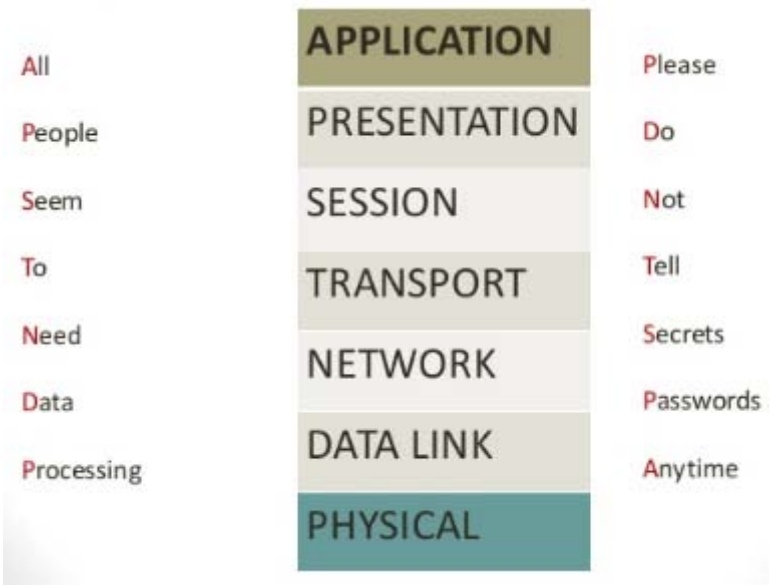
Since, the bucket is initially full, it already has 1 MB to transmit so it will be transmitted instantly. So, we are left with only (12 – 1), i.e. 11 MB of data to be transmitted.

Time required to send the 11 MB will be 11 * 0.1 = **1.1 sec**

Some advantage of token Bucket over leaky bucket –

- If bucket is full in token Bucket , tokens are discard not packets. While in leaky bucket, packets are discarded.
- Token Bucket can send Large bursts at a faster rate while leaky bucket always sends packets at constant rate.

Point to Remember



192.168.10.121/27

Find

a. Subnet mask
b. No. of IP
c. Valid IP addresses
d. Network IP
e. First IP
f. Last IP
g. Broadcast IP
h. Position of given host

Solution:

On bit = 27

Off bit (n) = 32-27 = 5

a. Subnet mask = 255.255.255.11100000

= 255.255.255.224

b. No of IP = $2^n = 2^5 = 32$

c. Valid IP address = $2^n-2 = 2^5-2 = 32-2 = 30$

Now,

The IP starts with

192.168.10.0

192.168.10.31

192.168.10.32

192.168.10.63

192.168.10.64

192.168.10.95

192.168.10.96

192.168.10.127

d. Network IP = 192.168.10.96
e. Broadcast IP = 192.168.10.127
f. First IP = 192.168.10.97
g. Last IP = 192.168.10.126
h. Position of given host = 25 [count from 96-121]

Q. 192.168.5.83/28

Find

a. Subnet mask
b. No. of IP
c. Valid IP addresses
d. Network IP
e. First IP
f. Last IP
g. Broadcast IP
h. Position of given host

Solution:

On bit = 28

Off bit (n) = 32-28 = 4

a. Subnet mask = 255.255.255.11110000

= 255.255.255.240

b. No of IP = $2^n = 2^4 = 16$

c. Valid IP address = $2^n-2 = 2^4-2 = 16-2 = 14$

Now,

The IP starts with

192.168.5.0

192.168.5.15

192.168.10.16

192.168.5.31

192.168.5.32

192.168.5.47

192.168.5.48

192.168.5.63

192.168.5.64

192.168.5.79

192.168.5.80

192.168.5.95

d. Network IP = 192.168.5.80

e. Broadcast IP = 192.168.5.95

f. First IP = 192.168.5.81

g. Last IP = 192.168.5.94

h. Position of given host = 4 [count from 80-83]

Answer own Innovation, Creativity & Tinkering.

- ----- - ---------- ---------- ---------- ---------- ---------

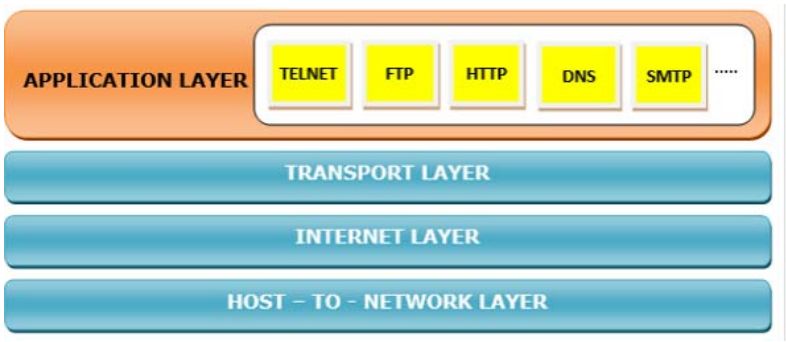
6.1 Functions of Application layer

The application layer is the highest abstraction layer of the TCP/IP model that provides the interfaces and protocols needed by the users. It combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model.

The functions of the application layer are −

- It facilitates the user to use the services of the network.
- It is used to develop network-based applications.
- It provides user services like user login, naming network devices, formatting messages, and e-mails, transfer of files etc.
- It is also concerned with error handling and recovery of the message as a whole.

The following diagram shows the transport layer in the TCP/IP protocol suite −



6.2 Application Layer Protocols: DNS, DHCP, WW W, HTTP, HTTPs, TELNET, FTP, SMTP, POP, IMAP

An application layer protocol defines how application processes (clients and servers), running on different end systems, pass messages to each other. In particular, an application layer protocol defines:

- The types of messages, e.g., request messages and response messages.
- The syntax of the various message types, i.e., the fields in the message and how the fields are delineated.
- The semantics of the fields, i.e., the meaning of the information that the field is supposed to contain;
- Rules for determining when and how a process sends messages and responds to messages.

Answer own Innovation, Creativity & Tinkering.

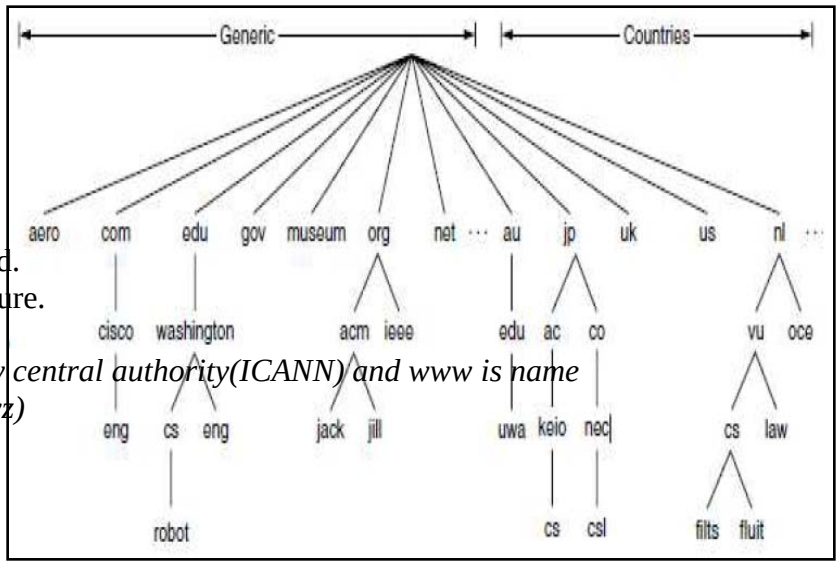
Application Type	Application-layer protocol	Transport Protocol
Electronic mail	Send: Simple Mail Transfer Protocol SMTP [RFC 821]	TCP 25
	Receive: Post Office Protocol v3 POP3 [RCF 1939]	TCP 110
Remote terminal access	Telnet [RFC 854]	TCP 23
World Wide Web (WWW)	HyperText Transfer Protocol 1.1 HTTP 1.1 [RFC 2068]	TCP 80
File Transfer	File Transfer Protocol FTP [RFC 959]	TCP 21
	Trivial File Transfer Protocol TFTP [RFC 1350]	UDP 69
Remote file server	NFS [McKusik 1996]	UDP or TCP
Streaming multimedia	Proprietary (e.g., Real Networks)	UDP or TCP
Internet telephony	Proprietary (e.g., Vocaltec)	Usually UDP

1. DNS:

Domain Name System (DNS) – It is a naming system for devices in networks. It provides services for translating domain names to IP addresses.

1. Name Server (DNS- Domain Name System)

- All system communicate using IP(Numbers)
- Numbers are difficult to remember for human beings than name
- Internet is very large there are millions of computer and servers
- Naming system is introduced(in 1983) for mapping of Host Name to IP address
- In DNS server, there is library procedure (program) called resolver that converts host name to IP.
- **ICANN** (**Internet Corporation for Assigned Names and Numbers**) is responsible for managing the DNS in internet.
- Domain names are unique



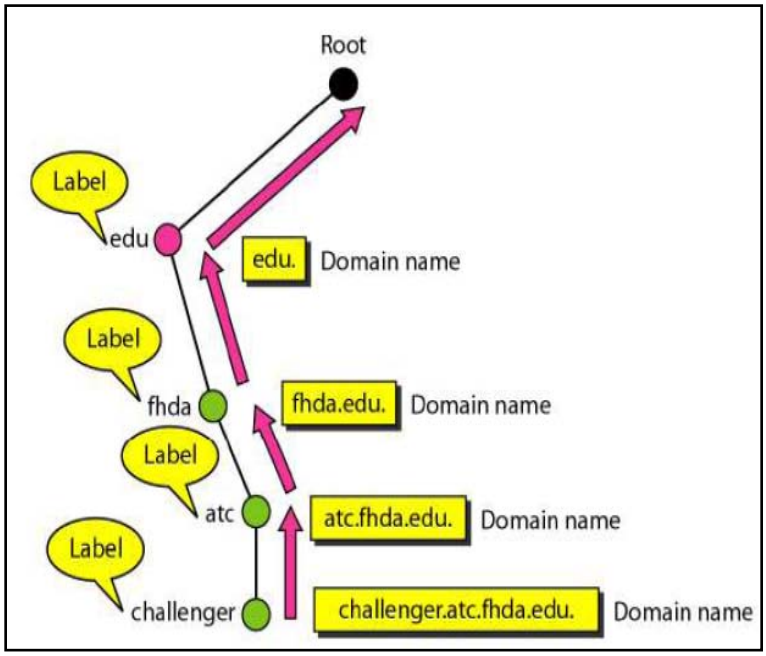
1.1. Name Spaces(Domain Name)

- ***Divided into 2 :***
  1. Flat Structure
  2. Hierarchical Structure
     - Hierarchical structure is used.
     - Name space have tree structure.
     - Example : www.xyz.com
     - *Here xyz.com is managed by central authority(ICANN) and www is name given by organization(here xyz)*

1.1.1. Domain Name Space

- Inverted Tree Structure, contains 0 to127 (128)levels
- 0 is root level
- Internet have nearly 250 **toplevel domains**, where each

domain covers many hosts
• Each domain is partitioned into **subdomains**, and these are further partitioned, and so on com, edu, gov are example of top level domain

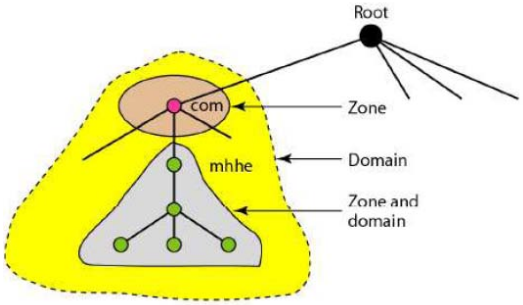


1.1.2. Domain Name

• All label is terminated by a null string(.), it is called a ***FQDN (Fully Qualified Domain Name)***
• **Example:** *challenger.ate.tbda.edu.*
• Label is not terminated by a null string, it is called a ***PQDN (Partially Qualified Domain Name)***
• A PQDN starts from a node, but it does not reach the root
• **Example :** *challenger.ate.tbda.edu*
• NB: **.(dot)** Is called root server

1.1.3. Zone

• Zone will keep track of all nodes in domain and all sub-domains under the domain.



1.2. Servers

• Root Server
• A root server is a server whose zone consists of the whole tree
• A root server usually does not store any information about domains but delegates its authority to other servers
• DNS defines two types of servers

1. Primary Server

• A primary server is a server
• That stores a file about the zone for which it is an authority
• It is responsible for **creating, maintaining, and updating the zone file**

2. Secondary Server

• A secondary server is a server that **transfers the complete information about a zone** from another server (primary or secondary) and stores the file on its local disk

1.3. Query

• ***DNS has two types of messages***

1. Query - sent by DNS client to server, **Query message consists** of a header and question records

2. Response – sent by DNS server to client, **Response message consists** of a header, question, records, answer records, authoritative records, and additional records

• **Query** is a question to the server, Client ask about the **IP address** of the mentioned **URL**

• **Response** is answer to the question provided by client from server, i.e. it sent information (IP address) of the mentioned URL.

2. DHCP:

DHCP(Dynamic Host Configuration Protocol)

• *Two possible way for configuring IP are:*

1. Manually

2. Dynamically (DHCP)

• DHCP is service that provide IP addresses.

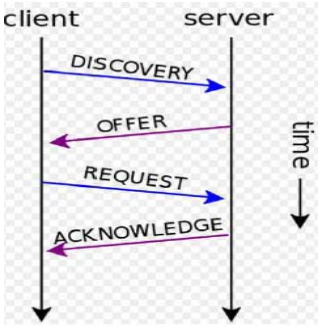
• Server that runs DHCP service is DHCP servers.

• Client that uses DHCP server for IP configuration is DHCP clients.

• DHCP server uses UDP port 67

• DHCP client uses UDP port 68

2.1. DHCP Operation



2.1.1. DHCP Discover Packet

• Sent by DHCP client to DHCP server (Broadcasting).

• DHCP client ***(****computer or device which wants IP****)*** broadcast broadcasts a request for an IP address on its network. It does this by using a DHCP DISCOVER packet.

• Packet must reach the DHCP server.

• A DHCP client may also request its last-known IP address with discover packet.

• DHCP discovers packet is for checking weather DHCP server is available in network and IP address lease request.

2.1.2. DHCP Offer Packet

• Sent by DHCP server to DHCP client (Unicasting)

• When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client

• This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer

2.1.3. DHCP Request Packet

• Sent by DHCP client to DHCP servers (Broadcasting)
• In response to the DHCP offer, the client replies with a DHCP request, broadcast to the server, requesting the offered address.
• A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer
• Based on required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted.
• When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

5.1.4. DHCP Acknowledgement Packet

• Sent by DHCP servers to DHCP client (Unicasting)
• When the DHCP server receives the DHCP REQUEST message from the client, the configuration process enters its final phase.
• The acknowledgement phase involves sending a DHCP ACK packet to the client.
• This packet includes the lease duration and any other configuration information that the client might have requested.
• At this point, the IP configuration process is completed

3. WWW:

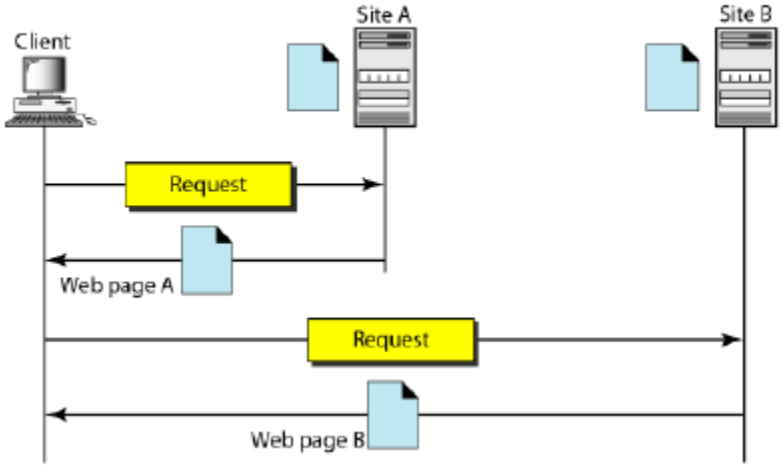
- ✓ This is a protocol used mainly to access data on the World Wide Web (www).
- ✓ The Hypertext Transfer Protocol (HTTP) the Web's main application-layer protocol although current browsers can access other types of servers
- ✓ A respository of information spread all over the world and linked together.
- ✓ The HTIP protocol transfer data in the form of plain text, hyper text, audio, video and so on.
- ✓ HTTP utilizes TCP connections to send client requests and server replies.
- ✓ it is a synchronous protocol which works by making both persistent and non persistent connections.

4. HTTP:

Hyper Text Transfer Protocol, *HTTP* − It is the underlying protocol for world wide web. It defines how hypermedia messages are formatted and transmitted.

• The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web(WWW)
• It is similar to FTP because it transfers files and uses the services of TCP.
• It uses only one TCP connection
• HTTP uses the services of TCP on well-known **port 80**
• Accessing of web page is based on URL

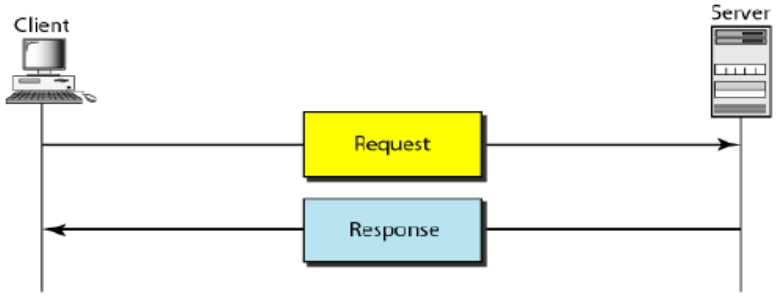
4.1. WWW Architecture



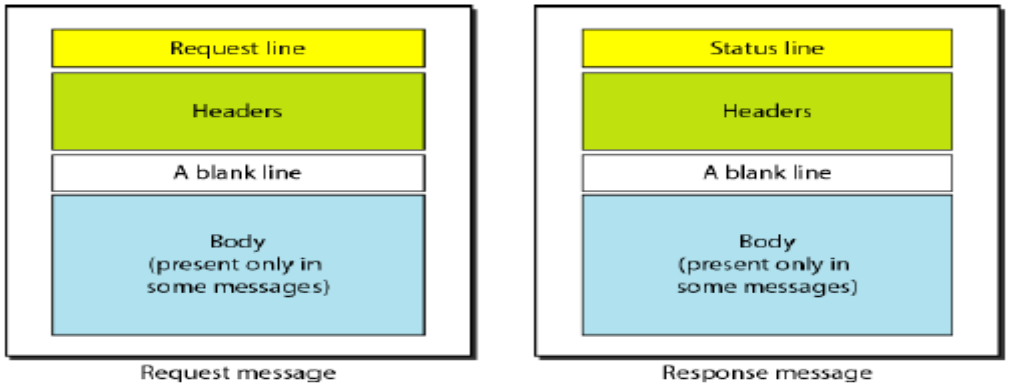
4.2. HTTP Transaction

- HTTP transaction between the client and server
- There are 2 transaction messages
- Request (sent from client to server for requesting a Page or other resource)
- Response (sent from server to client)

4.2. HTTP Transaction Figure



4.2.1 Message Format



5. HTTPs:

- ✓ Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, its predecessor, Secure Sockets Layer (SSL). The protocol is therefore also often referred to as HTTP over TLS, or HTTP over SSL.
- ✓ The principal motivations for HTTPS are authentication of the accessed website, protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks.
- ✓ HTTPS creates a secure channel over an insecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted.
- ✓ **Therefore, a user should trust an HTTPS connection to a website if and only if all of the following are true:**
  - o The user trusts that the browser software correctly implements HTTPS with correctly pre-installed certificate authorities.
  - o The user trusts the certificate authority to vouch only for legitimate websites.
  - o The website provides a valid certificate, which means it was signed by a trusted authority.
  - o The certificate correctly identifies the website (e.g., when the browser visits " https://www.tribhuvan-university.edu.np/", the received certificate is properly for " tribhuvan-university.edu.np " and not some other entity).
  - o The user trusts that the protocol's encryption layer (SSL/TLS) is sufficiently secure against eavesdroppers.

6. TELNET:

TELNET − It provides bi-directional text-oriented services for remote login to the hosts over the network. **TELNET (Terminal Network):**

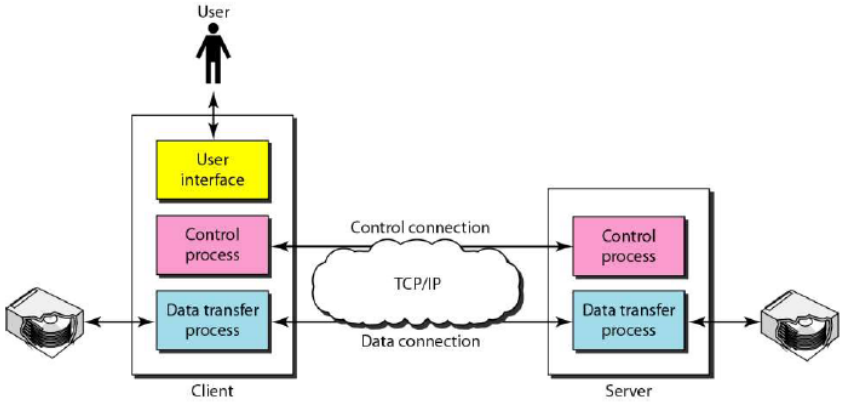
- TELNET is client-server application that allows a user to log onto remote machine and lets the user to access any application program on a remote computer.
- TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system.
- On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- TELNET is a protocol that provides a general, bi-directional, eight-bit byte oriented communications facility.
- Many application protocols are built upon the TELNET protocol
- Telnet services are used on PORT 23.

7. FTP:

File Transfer Protocol, FTP − It is a client-server based protocol for transfer of files between client and server over the network.

• File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for copying a file from one host to another.
• FTP establishes two connections between the hosts
• One connection is used for data transfer, the other for control information (commands and responses)
• Separation of commands and data transfer makes FTP more efficient
• FTP uses **two** well-known TCP ports: **Port 21** is used for the control connection, and **port 20** is used for the data connection.

7.1. FTP Architecture



7.2. FTP Working

• FTP uses Transmission Control Protocol (TCP) for reliable network communication by establishing a session before initiating data transfer

• FTP client send command/ request for connection to FTP server establishing connection(Port 21)

• FTP server Responds to the commands about the status wheatear connected/ not connected (Port 21)

• FTP Client connect to FTP server using control connection i.e. using port 21

• After establishing connection port 20 is used for data transfer

Q. E-mail

• Electronic mail, or more commonly **email**, used to communicate with different users in internet

• Email uses following protocols for storing & delivering messages, They are :

1. SMTP (Simple Mail Transfer Protocol)

2. POP (Post Office Protocol)

3. IMAP (Internet Message Access Protocol)

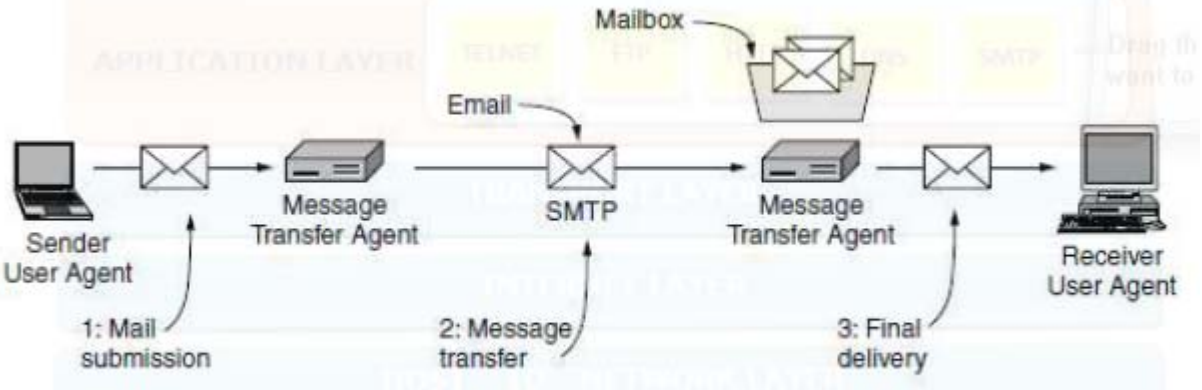


Figure Architecture of the email system.

• ***Email consists of two kinds of subsystems***

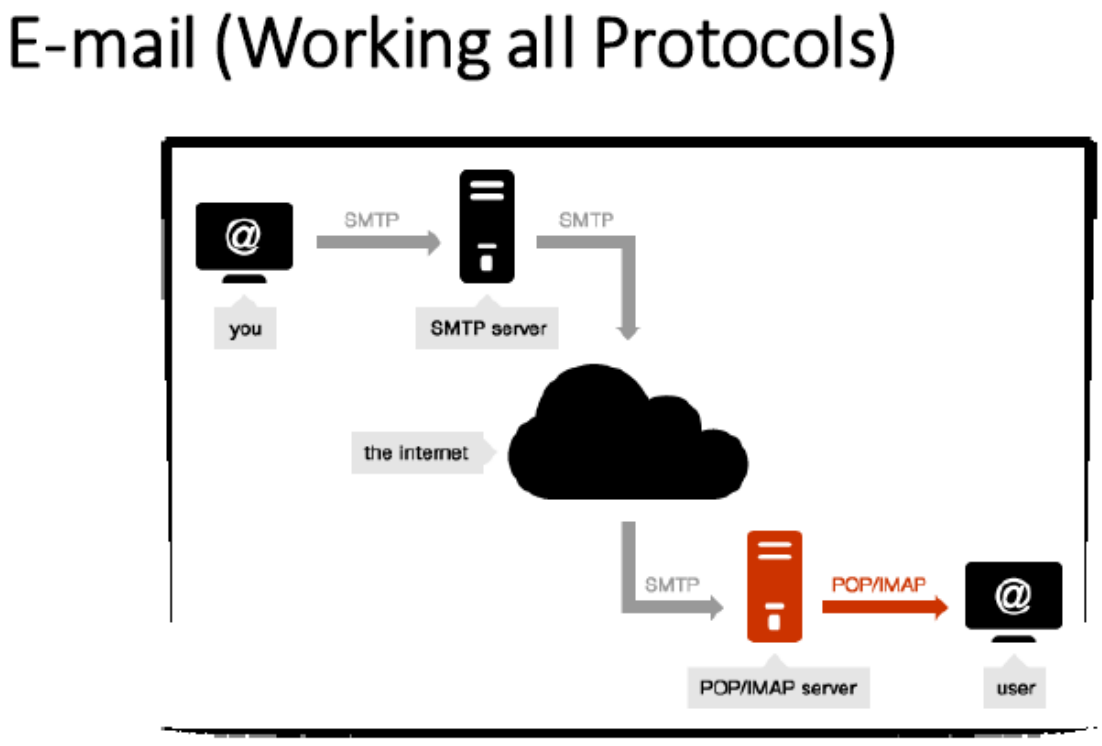
1. Mail User Agents (also called MUA/email client programs): which allow people to read and send email (Ex: Outlook)

2. Message Transfer Agents(also called MTA/ Email Server) : which move the messages from the source to the destination (Ex: Gmail Server)

• Act of sending new messages into the mail system for delivery is called **Mail submission (Email Client to Email Sever)**

• The Process of transferring mail from one MTA to another (Ex : from gmail to yahoo server) is called **Message Transfer**

• **Mailboxes** store the email that is received for a user (Working all Protocols)



8. SMTP:

Simple Mail Transfer Protocol, SMTP − It lays down the rules and semantics for sending and receiving electronic mails (e-mails).

8.1. SMTP (Simple Mail Transfer Protocol)

• Message transfer form originator to the recipient mailbox is done with SMTP

• It uses TCP well known port 25

• SMTP server accepts incoming connections, subject to some security checks, and accepts messages for delivery

• If a message cannot be delivered, an error report containing the first part of the undeliverable message is returned to the sender

• Email is submitted by a mail client **(MUA, mail user agent)** to a mail server (**MSA, mail submission agent)** using SMTP on TCP port 587

• **MSA** delivers the mail to its mail transfer agent **MTA**

8.1.1. Features of SMTP

• SMTP supports sending of email only It cannot retrieve (deliver to user) messages from a remote server on demand

• SMTP provides system for sending message to same (or different) servers (gmail **to** gmail / gmail **to** yahoo)

• SMTP provide a mail exchange between users on same (or different) server

SMTP supports:

1. Sending a message to one or more recipients
2. Sending message that includes text, voice, video or graphics
3. Sending message to users on other network

9. POP:

9.1. POP (Post Office Protocol)

• Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection

• POP has been developed through several versions, with version 3 (POP3) being the last standard

• E-mails are downloaded from the server's mailbox to your computer

• No copy of Email will be kept in mailbox after downloading the email

• E-mails are available when you are not connected

9.1.1. POP Working

• Working of POP servers is as following steps:

1. Connect to server
2. Retrieve all mail
3. Store locally as new mail
4. Delete mail from server*
5. Disconnect

** Deletion of mail is default setting , However user can change the settings to keep the copy of email in mail box*

9.1.2.Features of POP

• POP is a much simpler protocol, making implementation easier

• POP mail moves the message from the email server onto your local computer, although there is usually an option to leave the messages on the email server as well

• POP treats the mailbox as one store, and has no concept of folders

• POP protocol requires the currently connected client to be the only client connected to the mailbox

• When POP retrieves a message, it receives all parts of it

9.1.3. Advantages of POP

• Advantages are:

1. Mail stored locally, i.e. always accessible, even without internet connection
2. Internet connection needed only for sending and receiving mail
3. Saves server storage space
4. Option to leave copy of mail on server

10. IMAP:

IMAP (Internet Message Access Protocol)

- Protocols that is used for final delivery is **IMAP**
- **IMAP** is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection
- IMAP provides mechanisms for storing messages received by SMTP in a mailbox
- IMAP server stores messages received by each user until the user connects to download and read them using an email clients

** Now a days IMAP replaced POP in all E-mail services*

10.1.1. IMAP Working

- Working of IMAP servers is as following steps:

1. Connect to server
2. Fetch user requested content and cache it locally, e.g. list of new mail, message summaries, or content of explicitly selected emails
3. Process user edits, *e.g. marking email as read, deleting email etc.*
4. Disconnect

10.1.2 Features of IMAP

- Connected and disconnected modes of operation (Faster Operation)
- Multiple clients simultaneously connected to the same mailbox
- Access to message parts and partial fetch of messages (No need for complete message to be displayed only **subject / user name** can be retrieved)
- Provides message state information (**Message states are :** read / unread / replied / forwarded)
- Provides multiple mailboxes on the server (create new mail boxes and copy form one to another)
- Provides mechanisms for server-side searches

10.1.3. IMAP Advantage

Advantages

1. Mail stored on remote server, i.e. accessible from multiple different locations
2. Internet connection needed to access mail
3. Faster overview as only headers are downloaded until content is explicitly requested
4. Mail is automatically backed up if server is managed properly
5. Saves local storage space
6. Option to store mail locally

6.3	Concept of traffic analyzer: MRTG, PRTG, SNMP. Packet tracer, Wireshark.			2

Simple Network Management Protocol, SNMP

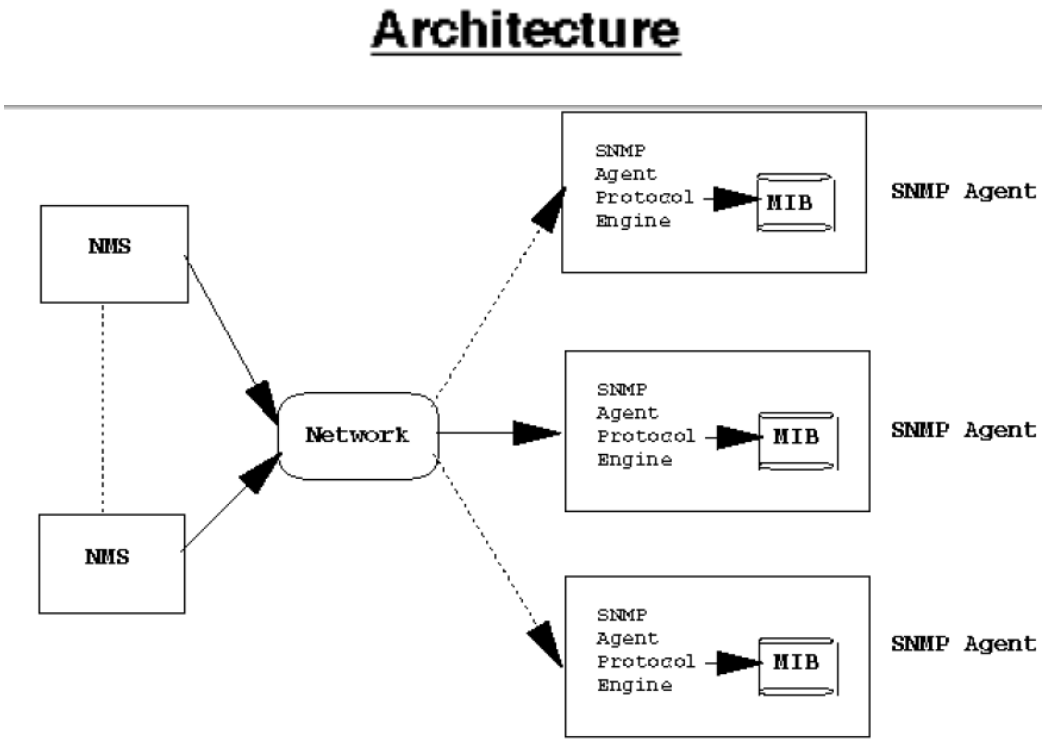
Simple Network Management Protocol, SNMP – It is for managing, monitoring the network and for organizing information about the networked devices.

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

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

An SNMP-managed network consists of three key components:

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



To do management tasks, SNMP uses two other protocols:

1. Structure of Management Information (SMI)
2. Management Information Base (MIB).

A typical agent usually:

- Implements full SNMP protocol.
- Stores and retrieves management data as defined by the Management Information Base
- Can asynchronously signal an event to the manager
- Can be a proxy (The proxy agent then translates the protocol interactions it receives from the management station) for some non-SNMP manageable network node.

A typical manager usually:

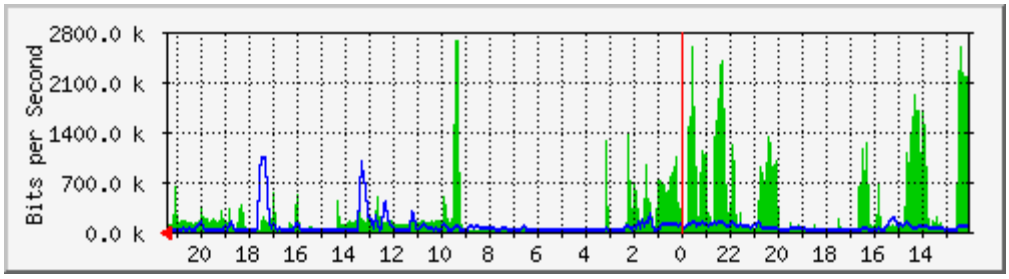
- Implemented as a Network Management Station (the NMS)
- Implements full SNMP Protocol
- Able to Query agents
- Get responses from agents

MRTG

- The **Multi Router Traffic Grapher** (MRTG) is free software for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form.

- It was originally developed by Tobias Oetiker and Dave Rand to monitor router traffic, but has developed into a tool that can create graphs and statistics for almost anything.

- MRTG is written in Perl and can run on Windows, Linux, Unix, Mac OS and NetWare.



How it works

- **SNMP**

✓ MRTG uses the **Simple Network Management Protocol** (SNMP) to send requests with two object identifiers (OIDs) to a device.

✓ The device, which must be SNMP-enabled, will have a management information base (MIB) to look up the OIDs specified.

✓ After collecting the information it will send back the raw data encapsulated in an SNMP protocol. MRTG records this data in a log on the client along with previously recorded data for the device.

✓ The software then creates an HTML document from the logs, containing a list of graphs detailing traffic for the selected devices in the server.

- **Script output**

✓ Alternatively, MRTG can be configured to run a script or command, and parse its output for counter values.

✓ The MRTG website contains a large library of external scripts to enable monitoring of SQL database statistics, firewall rules, CPU fan RPMs, or virtually any integer-value data.

Features

- Measures two values (I for Input, O for Output) per target.
- Gets its data via an SNMP agent, or through the output of a command line.
- Typically collects data every five minutes (it can be configured to collect data less frequently).
- Creates an HTML page per target that features four graphs (GIF or PNG images).
- Results are plotted vs time into day, week, month and year graphs, with the I plotted as a full green area, and the O as a blue line.
- Automatically scales the Y axis of the graphs to show the most detail.
- Adds calculated Max, Average and Current values for both I and O to the target's HTML page.
- Can also send warning emails if targets have values above a certain threshold.

PRTG:

PRTG Network Monitor (Paessler Router Traffic Grapher until version 7) is an agentless network monitoring software from Paessler AG. It can monitor and classify system conditions like bandwidth usage or uptime and collect statistics from miscellaneous hosts as switches, routers, servers and other devices and applications.

1. **Specifications**
   - PRTG Network Monitor has an auto-discovery mode that scans predefined areas of an enterprise network and creates a device list from this data.
   - In the next step, further information on the detected devices can be retrieved using various communication protocols.
   - Typical protocols are Ping, SNMP, WMI, NetFlow, jFlow, sFlow, but also communication via DICOM or the RESTful API is possible.
   - The tool is only available for Windows systems. In addition, Paessler AG offers the cloud-based monitoring solution "PRTG hosted by Paessler"
   -

1.1 Sensors

The software is based on sensors that are configured for a specific purpose. For example, there are HTTP, SMTP/POP3 (e-mail) application sensors and hardware-specific sensors for switches, routers and servers. PRTG Network Monitor has over 200 different predefined sensors that retrieve statistics from the monitored instances, e.g. response times, processor, memory, database information, temperature or system status.

1.2 Web interface and desktop client

The software can be operated completely via a AJAX-based web interface. The web interface is suitable for both real-time troubleshooting and data exchange with non-technical staff via maps (dashboards) and user-defined reports. An additional administration interface in the form of a desktop application for Windows and macOS is available.

1.3 Notifications and reports

In addition to the usual communication channels such as Email and SMS, notification is also provided via push notification on smartphones using an app for iOS or Android. PRTG also offers customizable reports.

1.4 Pricing

PRTG Network Monitor's licensing is based on sensors. Most devices require between five and ten sensors to be fully monitored. A version with 100 integrated sensors is available free of charge.

Packet Analyzer:

- A packet analyzer (also known as a **packet sniffer)** is a computer program or piece of computer hardware (such as a packet capture appliance) that can intercept and log traffic that passes over a digital network or part of a network.
- Packet capture is the process of intercepting and logging traffic.
- A packet analyzer used for intercepting traffic on wireless networks is known as a wireless analyzer or WiFi analyzer.
- A packet analyzer can also be referred to as a network analyzer or protocol analyzer though these terms also have other meanings.

Capabilities

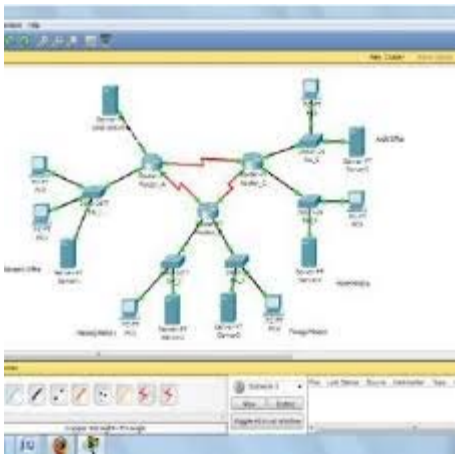
- On wired shared medias networks, such as Ethernet, Token Ring, and FDDI networks, depending on the network structure (hub or switch), it may be possible to capture all traffic on the network from a single machine on the network.
- On modern networks, traffic can be captured using a network switch with a so-called monitoring port that mirrors all packets that pass through designated ports of the switch.
- On wireless LANs, traffic can be captured on one channel at a time, or by using multiple adapters, on several channels simultaneously.

- When traffic is captured, either the entire contents of packets are recorded, or just the headers are recorded. Recording just headers reduces storage requirements, and avoids some legal issues, yet often provides sufficient information to diagnose problems.
- Captured information is decoded from raw digital form into a human-readable format that lets users easily review exchanged information. Protocol analyzers vary in their abilities to display and analyze data.
- Some protocol analyzers can also generate traffic and thus act as the reference device.
- Protocol analyzers can also be hardware-based, either in probe format or, as is increasingly common, combined with a disk array. These devices record packets (or a slice of the packet) to a disk array.

Uses:

Packet sniffers can:

- Analyze network problems
- Detect network misuse by internal and external users
- Monitor WAN bandwidth utilization
- Gather and report network statistics



Notable packet analyzers

- Wireshark formerly known as Ethereal)
- ngrep, Network Grep
- Fiddler

Wireshark

- Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format.
- Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.
- Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

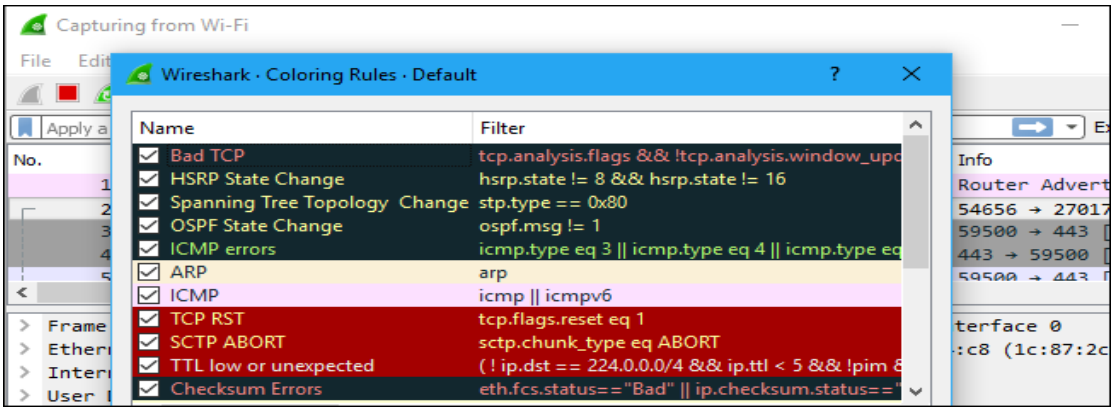
Features

Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols.

- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Data display can be refined using a display filter.
- Wireless connections can also be filtered as long as they traverse the monitored Ethernet.
- Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic

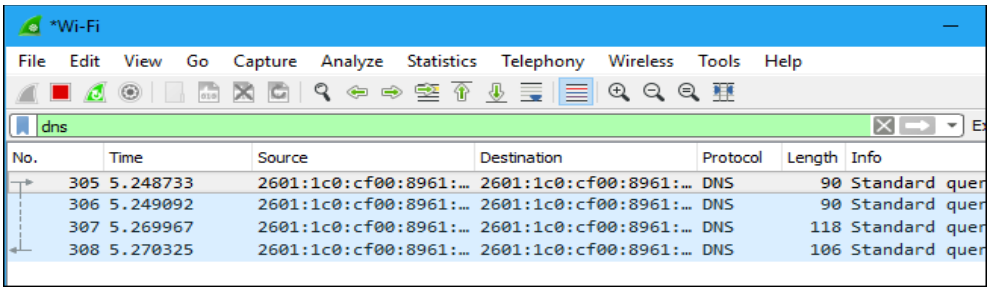
Color Coding

It probably can see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. ***By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.***

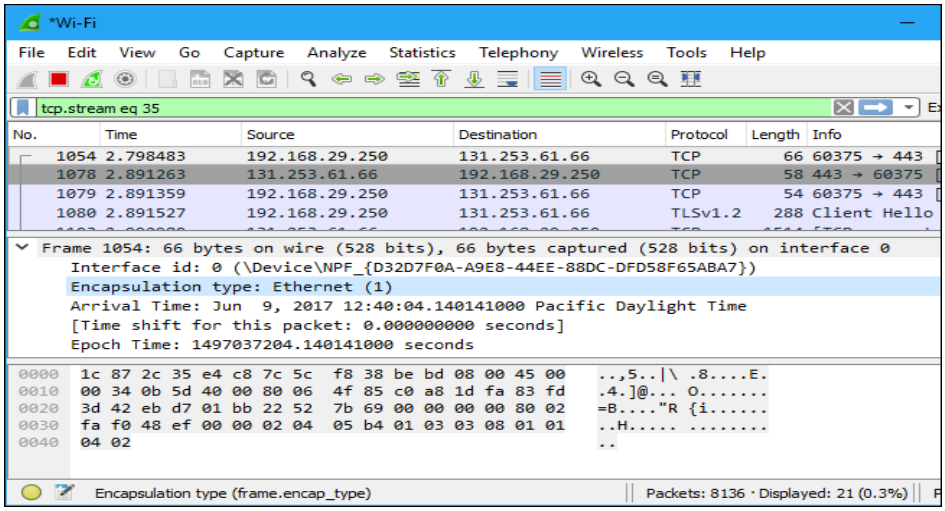


Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.



Inspecting Packets



S.No.	Contents	Check it (if Difficult)	Page	Spend Time in Hour
6.1	Functions of Application layer			1
6.2	Application Layer Protocols: DNS, DHCP, WWW, HTTP, HTTPs, TELNET, FTP, SMTP, POP, IMAP			2
6.3	Concept of traffic analyzer: MRTG, PRTG, SNMP. Packet tracer, Wireshark.			2

INSPIRING LEARNING QUOTES

"NOTHING WILL WORK UNLESS YOU DO."

Don't be judgmental towards anyone, including yourself.

"YESTERDAY I WAS CLEVER, SO I CHANGED THE WORLD. TODAY I AM WISE, SO I AM CHANGING MYSELF."

"NEVER GIVE UP ON A DREAM JUST BECAUSE OF THE TIME IT WILL TAKE TO ACCOMPLISH IT. THE TIME WILL PASS ANYWAY."

"TELL ME AND I FORGET. TEACH ME AND I REMEMBER. INVOLVE ME AND I LEARN."

Ask yourself: how is this changing me?

Answer own Innovation, Creativity & Tinkering.

Point to Note

Basic Concept Cryptography

Cryptography is a method of using advanced mathematical principles in storing and transmitting data in a particular form so that only those whom it is intended can read and process it.

Cryptography Terms

- **Encryption**: It is the process of locking up information using cryptography. Information that has been locked this way is encrypted.
- **Decryption**: The process of unlocking the encrypted information using cryptographic techniques.
- **Key**: A secret like a password used to encrypt and decrypt information. There are a few different types of keys used in cryptography.
- **Steganography**: It is actually the science of hiding information from people who would snoop on you. The difference between steganography and encryption is that the would-be snoopers may not be able to tell there's any hidden information in the first place.

7.1	A Model for Network Security			1

A MODEL FOR NETWORK SECURITY

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

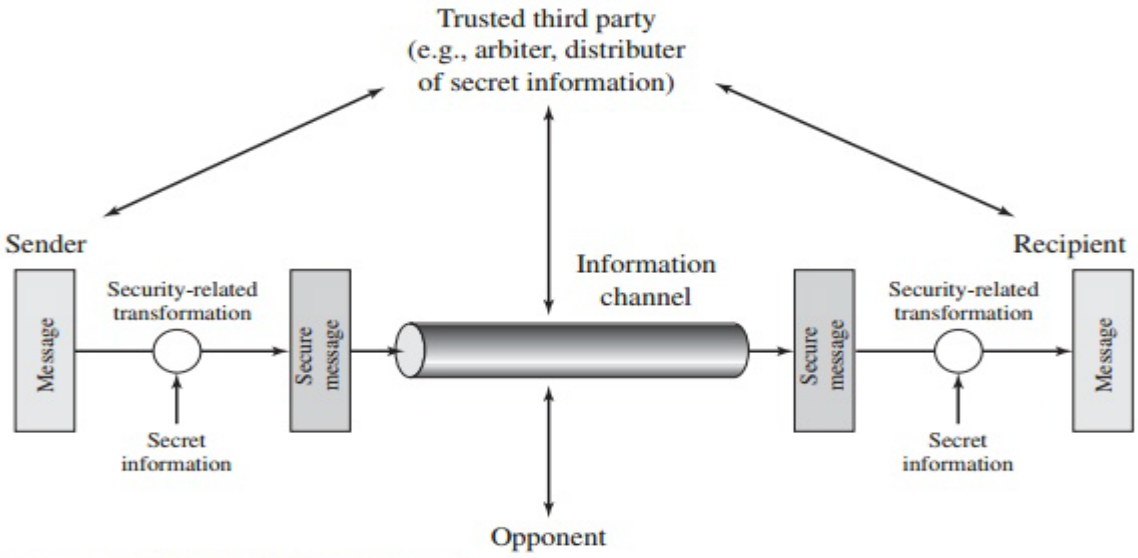


Figure 1.4 Model for Network Security

- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

- A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

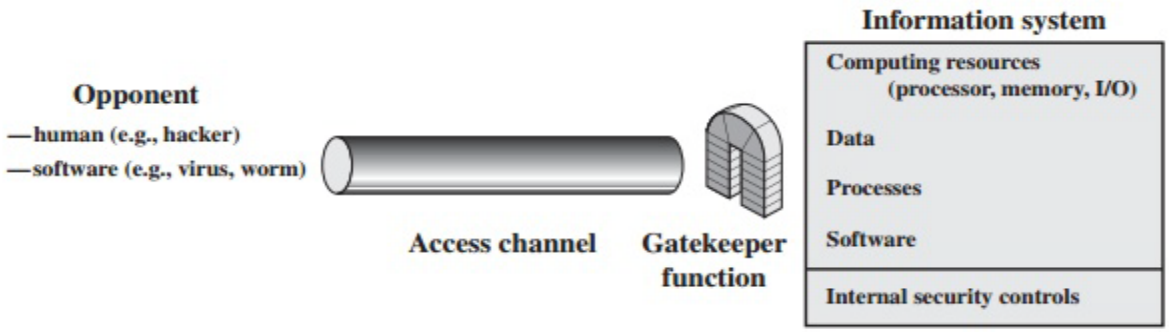


Figure 1.5 Network Access Security Model

A general model of these other situations is illustrated by Figure 1.5, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

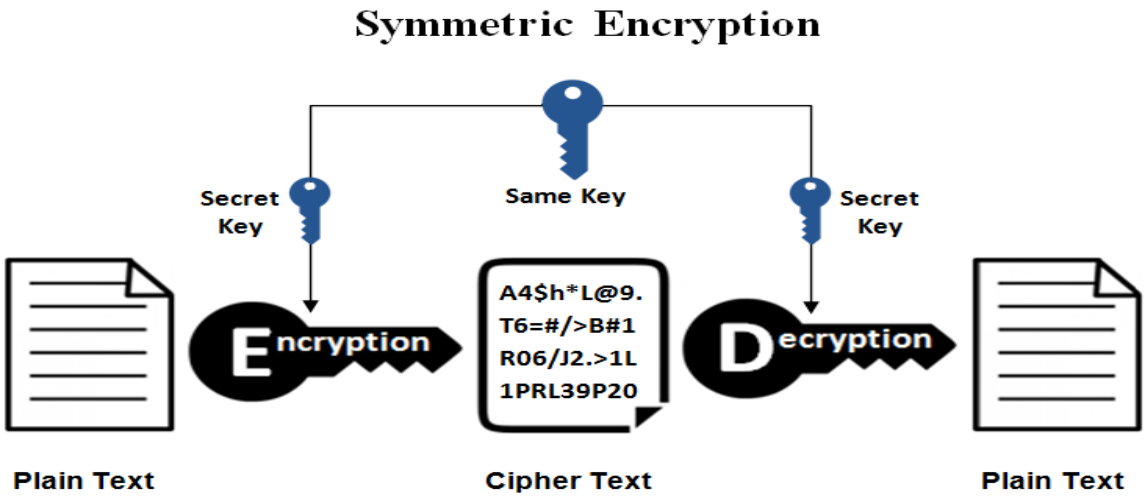
Programs can pre-sent two kinds of threats:-

- **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
- **Service threats:** Exploit service flaws in computers to inhibit use by legitimate users.

The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.5). The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

7.2	Principles of cryptography: Symmetric Key and Public Key		1

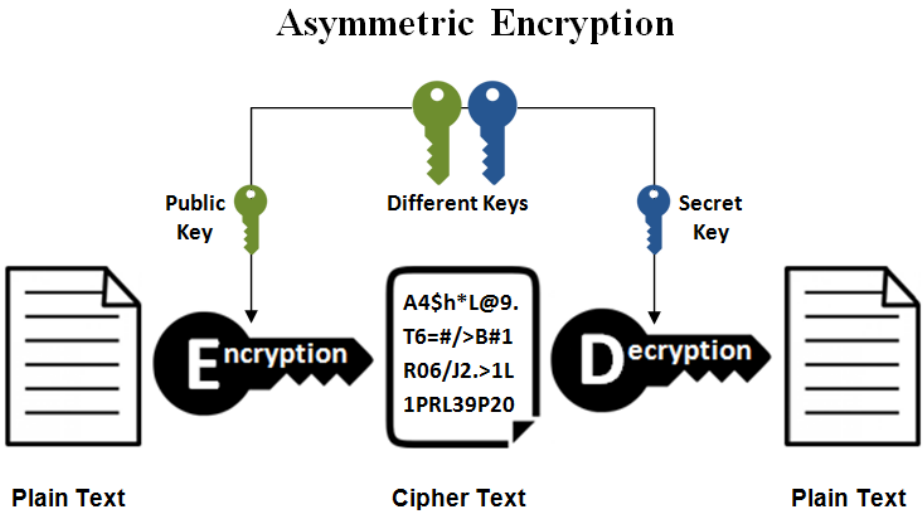
Symmetrical Encryption



- ✓ This is the simplest kind of encryption that involves only one secret key to cipher and decipher information.
- ✓ Symmetrical encryption is an old and best-known technique.
- ✓ It uses a secret key that can either be a number, a word or a string of random letters.
- ✓ It is a blended with the plain text of a message to change the content in a particular way.
- ✓ The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. AES, DES, RC5, and RC6 are examples of symmetric encryption.
- ✓ The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Asymmetrical Encryption



- ✓ Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption.
- ✓ Asymmetric encryption uses **two keys** to encrypt a plain text.
- ✓ Secret keys are exchanged over the Internet or a large network.
- ✓ It ensures that malicious persons do not misuse the keys.
- ✓ It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security.
- ✓ A public key is made freely available to anyone who might want to send you a message. The second **private key** is kept a secret so that you can only know.
- ✓ A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key.
- ✓ Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes RSA, DSA etc

Asymmetric Encryption in Digital Certificates

To use asymmetric encryption, there must be a way of discovering public keys. One typical technique is using digital certificates in a client-server model of communication. A certificate is a package of information that identifies a user and a server. It contains information such as an organization's name, the organization that issued the certificate, the users' email address and country, and users public key.

When a server and a client require a secure encrypted communication, they send a query over the network to the other party, which sends back a copy of the certificate. The other party's public key can be extracted from the certificate. A certificate can also be used to uniquely identify the holder.

DIFFERENCE BETWEEN SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHY

Characteristic	Symmetric key cryptography	Asymmetric key cryptography
Key used for encryption/decryption	Same key is used	One key is used for encryption and another ;different key is used for decryption
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original plain text size.	More than the original plain text size
Known keys	Both parties should know the key in symmetric key encryption	Only, either one of the keys is known by the two parties in public key encryption.
Usage	Confidentiality	Confidentiality, digital signature etc.

7.3	Public Key Algorithm - RSA		1

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

Algorithm

The RSA algorithm holds the following features −

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm −

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −

N=p*q

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

Step 3: Public key

The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.

Step 4: Private Key

Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −

ed = 1 mod (p-1) (q-1)

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is **(n,e).** To encrypt the plain text message in the given scenario, use the following syntax −

$C = P^e \bmod n$

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver **C** has the private key **d**, the result modulus will be calculated as −

$Plaintext = C^d \bmod n$

Let us learn the mechanism behind RSA algorithm (*Reference to Class Problem)*:

>> Generating Public Key :

- Select two prime no's. Suppose **P = 53 and Q = 59**.
- Now First part of the Public key : **n = P*Q = 3127**.

- We also need a small exponent say **e** :
- But e Must be
  - An integer.
  - Not be a factor of n.
  - **1 < e < Φ(n)** [Φ(n) is discussed below],
  - Let us now consider it to be equal to 3.
- Our Public Key is made of n and e

>> Generating Private Key :

- We need to calculate Φ(n) :
- Such that **Φ(n) = (P-1)(Q-1)**
- so, Φ(n) = 3016

- Now calculate Private Key, **d** :
- **d = (k*Φ(n) + 1) / e** for some integer k
- For k = 2, value of d is 2011.

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011)

Now we will encrypt **"HI"** :

- Convert letters to numbers : H = 8 and I = 9

- Thus **Encrypted Data c = 89^e mod n**.
- Thus our Encrypted Data comes out to be 1394

Now we will decrypt **1394** :

- **Decrypted Data = c^d mod n**.
- Thus our Encrypted Data comes out to be 89

8 = H and I = 9 i.e. "HI".

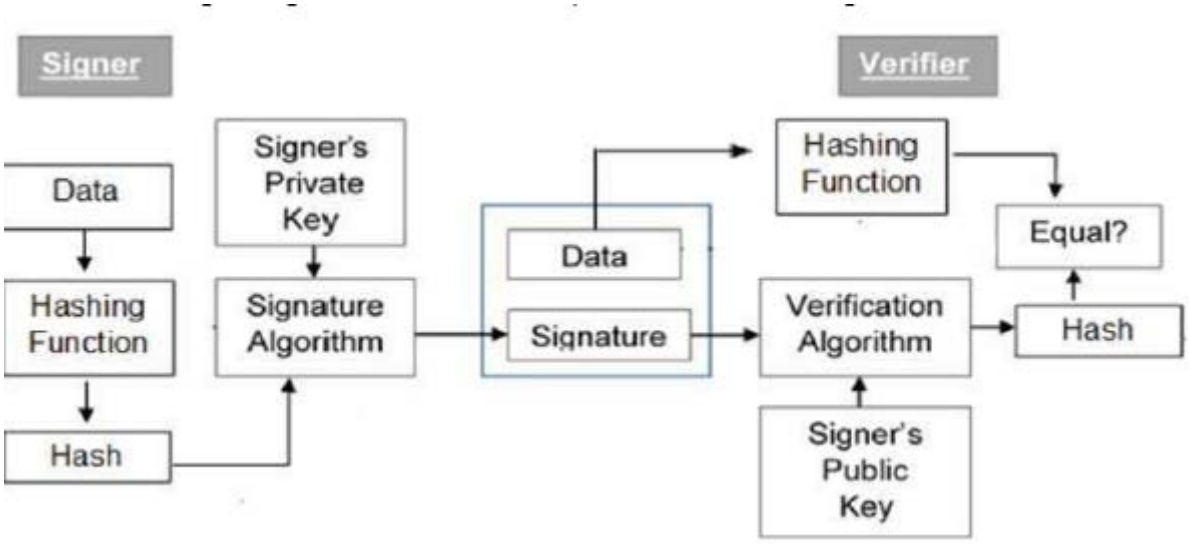
7.4	Digital Signature Algorithm		1

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, **a digital signature is a technique that binds a person/entity to the digital data**. **This binding can be independently verified by receiver as well as any third party**.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

Model of Digital Signature



Importance of Digital Signature

Let us briefly see how this is achieved by the digital signature −

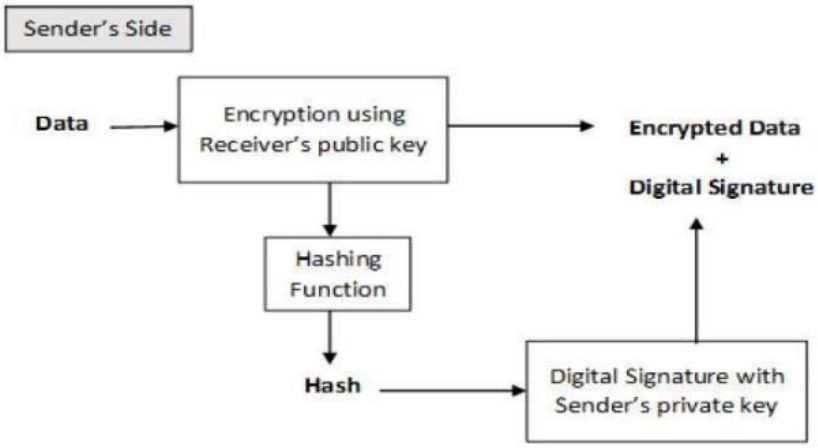
- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

Encryption with Digital Signature

There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −



The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

Advantages of Digital Signature Algorithm

- Along with having strong strength levels, the length of the signature is smaller as compared to other digital signature standards.
- The signature computation speed is less.
- DSA requires less storage to work as compared to other digital standards.
- DSA is patent free so it can be used free of cost.

Disadvantages of Digital Signature Algorithm

- It requires a lot of time to authenticate as the verification process includes complicated remainder operators. It requires a lot of time for computation.
- Data in DSA is not encrypted. We can only authenticate data in this.
- The digital signature algorithm firstly computes with SHA1 hash and signs it. Any drawbacks in cryptographic security of SHA1 are reflected in DSA because implicitly of DSA is dependent on it.
- With applications in both secret and non-secret communications, DSA is of the US National Standard.

7.5	Communication Security: IPSec, VPN, Firewalls, Wireless Security.		1

IP security (IPSec)

Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.Also known as IP Security.

IPsec involves two security services:

- **Authentication Header (AH)**: This authenticates the sender and it discovers any changes in data during transmission.
- **Encapsulating Security Payload (ESP):** This not only performs authentication for the sender but also encrypts the data being sent.

There are two modes of IPsec:

- **Tunnel Mode:** This will take the whole IP packet to form secure communication between two places, or gateways.
- **Transport Mode:** This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication.

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security –

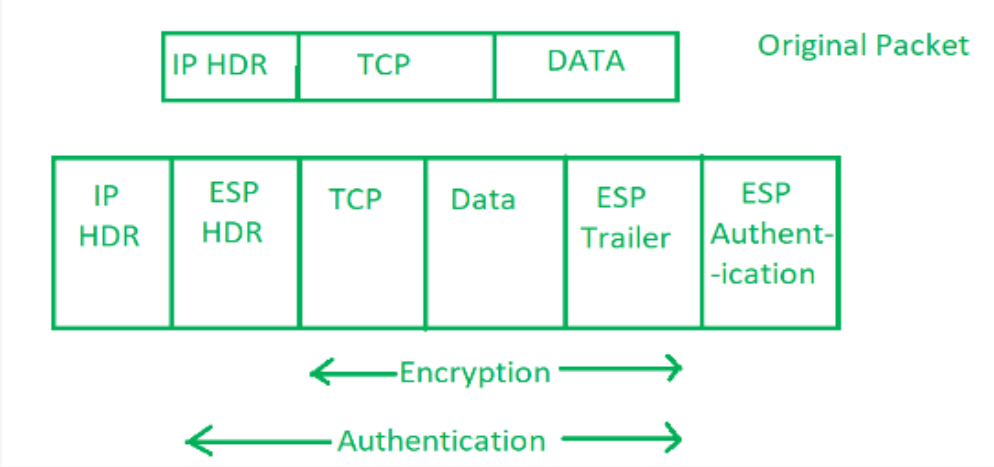
It has the following components:

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

Internet Key Exchange (IKE) –

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



IPsec provides the following security services for traffic at the IP layer:

- Data origin authentication—identifying who sent the data.
- Confidentiality (encryption)—ensuring that the data has not been read en route.
- Connectionless integrity—ensuring the data has not been changed en route.
- Replay protection—detecting packets received more than once to help protect against denial of service attacks.

Applications of IPSec

As we all know to help in the security of a network the Internet community has done lot of work and developed application-specific security mechanisms in numerous application areas, including electronic mail (*Privacy Enhanced Mail, Pretty Good Privacy* [PGP]), network management (*Simple Network Management Protocol Version 3*[SNMPv3]), Web access (Secure HTTP, *Secure Sockets Layer* [SSL]), and others.

Benefits of IPSec

When IPSec is implemented in a firewall or router, it provides strong security whose application is to all traffic crossing this perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

IPSec is below the transport layer (TCP, UDP), and is thus transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router.

Even if IPSec is implemented in end systems, upper layer software, including applications is not affected. IPSec can be transparent to end users.

VPN (Virtual Private Network)

VPN stands for Virtual Private Network (VPN) that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection that is called VPN tunnel and all Internet traffic and communication is passed through this secure tunnel.

Virtual Private Network (VPN) is basically of 2 types:

1. **Remote Access VPN:**
   Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.
2. **Site to Site VPN:**
   A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

Types of Virtual Private Network (VPN) Protocols:

1. **Internet Protocol Security (IPSec):**
   Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection.
   IPSec runs in 2 modes:
   - (i) Transport mode
   - (ii) Tunneling mode

   The work of transport mode is to encrypt the message in the data packet and the tunneling mode encrypts the whole data packet. IPSec can also be used with other security protocols to improve the security system.
2. **Layer 2 Tunneling Protocol (L2TP):**
   L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.
3. **Point–to–Point Tunneling Protocol (PPTP):**
   PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

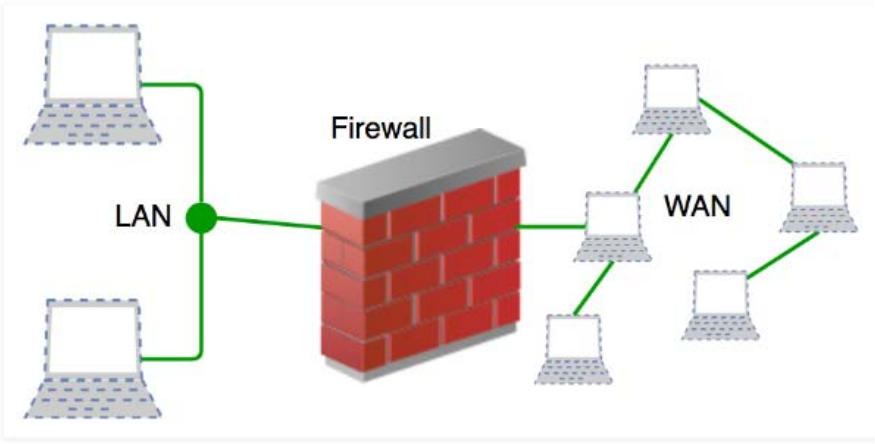
4. **SSL and TLS:**
   SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have "https" in the initial of the URL instead of "http".
5. **OpenVPN:**
   OpenVPN is an open source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol.
6. **Secure Shell (SSH):**
   Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

Firewall

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply
A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

A firewall is a **network security** device that monitors incoming and outgoing network traffic and permits or blocks data **packets** based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How does a firewall work?

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Generation of Firewall

Firewalls can be categorized based on its generation.

First Generation- Packet Filtering Firewall : Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

Second Generation- Stateful Inspection Firewall : Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient.

Third Generation- Application Layer Firewall : Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

Next Generation Firewalls (NGFW) : Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks.

Wireless-Security

Like the system's security and data security, keeping a sound knowledge about different wireless security measures is also essential to know for security professionals. It is because different wireless security mechanisms have a different level of strength and capabilities.

There are automated wireless hacking tools available that have made cybercriminals more powerful. List of some of these tools are:

- ✓ AirCrack.
- ✓ AirSnort.
- ✓ Cain & Able.
- ✓ Wireshark.
- ✓ NetStumbler etc.

Different various techniques of hacking include remote accessing, shoulder surfing, wireless router's dashboard accessing, and brute-forcing attack that are used to penetrate wireless security.

1. What is Wireless Security?
2. Wired Equivalent Privacy (WEP)
3. Wi-Fi Protected Access (WPA)
4. Wi-Fi Protected Access II (WPA2)
5. Wi-Fi Protected Access 3 (WPA3)

What is Wireless Security?

Wireless security revolves around the concept of securing the wireless network from malicious attempts and unauthorized access.

The wireless security can be delivered through different ways such as:

1. **Hardware-based:** where routers and switches are fabricated with encryption measures protects all wireless communication. So, in this case, even if the data gets compromised by the cybercriminal, they will not be able to decrypt the data or view the traffic's content.

2. **Wireless setup of IDS and IPS:** helps in detecting, alerting, and preventing wireless networks and sends an alarm to the network administrator in case of any security breach.
3. **Wireless security algorithms:** such as WEP, WPA, WPA2, and WPA3. These are discussed in the subsequent paragraphs.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the oldest security algorithm of 1999. It uses the initialization vector (IV) method. The very first versions of the WEP algorithm were not predominantly strong enough, even for that time when it got released. But the reason for this weak release was because of U.S. limits on the exporting of different cryptographic technologies, which led the manufacturing companies to restrict their devices to 64-bit encryption only. As the limitation was withdrawn, the 128 bit and 256 bit WEP encryption were developed and came into the wireless security market, though 128 became the standard one.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) was the next Wi-Fi Alliance's project that replaced the increasingly noticeable vulnerabilities of WEP standard. WPA was officially adopted in the year 2003, one year before the retirement of WEP. WPA's most common configuration is with WPA-PSK, which is abbreviated as Pre-Shared Key. WPA uses 256-bit, which was a considerable enhancement above the 64-bit as well as 128-bit keys.

Wi-Fi Protected Access II (WPA2)

Wi-Fi Protected Access II (WPA2) became official in the year 2006 after WPA got outdated. It uses the AES algorithms as a necessary encryption component as well as uses CCMP (Counter Cipher Mode - Block Chaining Message Authentication Protocol) by replacing TKIP.

Wi-Fi Protected Access 3 (WPA3)

Wi-Fi Protected Access 3 (WPA3) is the latest, and the third iteration of this family developed under Wi-Fi Alliance. It has personal as well as enterprise security-support feature and uses 384-bit Hashed Message Authentication Mode, 256-bit Galois / Counter Mode Protocol (GCMP-256), as well as Broadcast/Multicast Integrity Protocol of 256-bit. WPA3 also provides perfect forward secrecy mechanism support.

INSPIRING LEARNING QUOTES

"NOTHING WILL WORK UNLESS YOU DO."

Don't be judgmental towards anyone, including yourself.

"YESTERDAY I WAS CLEVER, SO I CHANGED THE WORLD. TODAY I AM WISE, SO I AM CHANGING MYSELF."

"NEVER GIVE UP ON A DREAM JUST BECAUSE OF THE TIME IT WILL TAKE TO ACCOMPLISH IT. THE TIME WILL PASS ANYWAY."

"TELL ME AND I FORGET. TEACH ME AND I REMEMBER. INVOLVE ME AND I LEARN."

Ask yourself: how is this changing me?