



## **Computer Network : Lecture Notes**

Nepal Engineering College

Prepared by: Junior Professor: Daya Ram Budhathoki

Nepal Engineering college, Changuarayan

dayaramb(at)nec.edu.np

Available online at

<http://dayaramb.wordpress.com>



---

### **References:**

#### **Text book:**

1. **Computer Networking**  
**A Top-Down Approach Featuring the Internet**  
**James F. Kurose and Keith W. Ross**
2. **Data and Computer Communication William Stalling**
3. **Computer Network A.S Tanenebaum**
4. **Data communication and Networking- Forouzan**
5. **Microsoft Encyclopedia of Networking**
6. **IIT Computer Network Video lectures.**
7. **Wiki-pedia**

# Table of Contents

Chapter1: Emergence of Network , principle of communication Network and Multiplexing.....	7
What is computer Network?.....	7
Historical Events:.....	8
Modes of communication:.....	9
Protocol:.....	10
Principle of Communication:.....	11
Elements of Network:.....	13
Multiplexing:.....	14
Simplex:.....	14
Duplex.....	14
Half-duplex.....	14
Chapter2: Network Topology and Architecture.....	15
Local Area Network (LAN).....	15
MAN:.....	15
WAN: .....	16
LAN Vs WAN.....	17
Internet:.....	17
Intranet:.....	18
Extranet:.....	19
Ethernet:.....	19
Physical Topology and Logical Topology:.....	20
Bus Topology:.....	21
Ring Topology.....	21
Mesh Topology:.....	22
Star Topology:.....	22
Logical Topology:.....	23
Network Architecture:.....	23
Peer-to-Peer Model:.....	23
Client-server Model:.....	24
Wireless LAN:.....	26
Wireless Standards - 802.11b 802.11a 802.11g and 802.11n.....	27
Wireless Topologies:.....	27
Chapter3: OSI Reference Model:.....	29
Network Software:.....	29
Protocol Hierarchies.....	29
Layer Communication:.....	29
OSI Model.....	30
Peer-to-Peer Communication:.....	31
Data Encapsulation:.....	31
Seven Layers of OSI Reference Model:.....	32
1. Physical Layer:.....	32
2. Data Link Layer:.....	32
3. Network Layer:.....	33

4. Transport Layer:.....	33
5. Session Layer:.....	34
6. Presentation Layer: .....	34
7. Application layer:.....	35
Devices and Protocols on each Layer:.....	35
Chapter4: Physical layers and its Design issues:.....	36
Transmission Medium:.....	36
Shielded Twisted-Pair (STP) Cable .....	36
Unshielded twisted-pair (UTP) .....	37
UTP Cabling Standards .....	38
Co-axial Cable:.....	38
Coaxial Cable Connectors .....	39
Fiber-optics.....	39
Fiber Compared to Copper Cabling : .....	40
Propagation modes:.....	40
Advantages and Disadvantages of Optical Fiber .....	43
Wireless Networking.....	43
Radio Waves .....	45
Microwaves .....	45
Infrared .....	46
Satellite Microwave:.....	47
Hub.....	48
Repeater.....	48
Introduction to Frame Relay, ATM, ISDN, PSTN, and X.25.....	49
Virtual Circuit:.....	49
X.25:.....	49
Frame Relay:.....	51
Asynchronous Transfer Mode (ATM).....	55
Integrated Service Digital Network: (ISDN).....	59
Public Switched Telephone Network(PSTN).....	62
Chapter5: Data Link layers.....	64
Multiple Access.....	64
Bridge:.....	64
Hub:.....	65
Switch:.....	65
Framing:.....	67
Fixed-Size Framing .....	68
Variable-Size Framing .....	68
Flow Control:.....	71
Stop and wait Flow Control:.....	72
Sliding Window Flow Control:.....	72
Error Control:.....	74
Hamming distance: .....	74
Error Detection:.....	74
1. Parity Check:.....	75
2. Cyclic Redundancy Check:.....	75
3. Checksum:.....	77

Error Correction:	77
Stop-and-wait ARQ:	78
Go-Back-N ARQ:	79
Selective-reject ARQ	80
High -Level Data Link Control(HDLC):	80
HDLC Frame Format:	80
I Frames:	82
U Frames:	83
PPP: (Point-to-point protocol):	83
Framing	84
SLIP: (SERIAL LINE INTERNET PROTOCOL):-	87
Chapter: 6 TCP/IP Reference Model, IP Addressing and Subnetting:	88
TCP/IP Model:	88
Application Layer:	88
Transport Layer:	88
TCP Header Format:	89
UDP (User Datagram Protocol):	90
TCP vs UDP:	90
Internet Layer:	91
Network Access Layer:	91
Comparison of OSI Model and TCP/IP Model:	91
IP Address:	92
Ipv4 Header:	93
Class A Blocks	95
Class B Blocks	95
Class C Blocks:	95
Class D Blocks:	96
Class E Block:	96
Private and Public IP addresses:	97
Subnet Mask:	97
CIDR:	98
Subnetting Class C Addresses	98
Subnetting Class C Address: 192.168.10.0/26:	99
Subnetting Class B Address: 172.16.0.0/17:	100
Subnetting Class A network: 10.0.0.0/16:	102
IPV6:	102
Features of IPV6:	102
IPv4 VS IPv6:	103
IPV6 Addressing:	105
IPV6 Transition Mechanism:	106
Dual Stack:	106
Tunneling Technique:	106
NAT-Protocol Translation (NAT-PT):	107
Chapter: 7 Network and Internet Layer:	108
Design issues for the network layer:	108
Circuit Switching:	109
Packet Switching:	110

Virtual Circuit:.....	110
Datagram:.....	111
Datagram Packet Switching Vs Virtual-circuit Packet Switching:.....	112
Router: (Introduction).....	112
Routing and Routing Protocols:.....	114
Distance Vector Routing Algorithm:.....	116
Link State Routing Algorithm:.....	119
Advantages of Link state Routing protocol:.....	120
Distance vector vs. Link state:.....	120
Spanning Tree Protocol(STP).....	121
Congestion control:.....	124
Open Loop Congestion Control:.....	124
Retransmission Policy .....	124
Window Policy .....	125
Acknowledgment Policy : .....	125
Discarding Policy : .....	125
Admission Policy : .....	125
Closed-Loop Congestion Control .....	125
Back-pressure:.....	125
Choke Packet .....	126
Implicit Signaling .....	126
Explicit Signaling .....	126
Traffic Shaping .....	127
Leaky Bucket .....	127
Chapter: 8 Network Servers and Protocols.....	129
Hypertext Transfer Protocol HTTP:.....	129
HTTPS VS HTTP.....	130
DHCP(Dynamic Host Configuration Protocol).....	130
Domain Name System (DNS):.....	131
Domain Name Space:.....	132
DNS in the Internet:.....	133
Generic Domains .....	133
Country Domains .....	134
Inverse Domain .....	134
Simple Mail Transfer Protocol (SMTP).....	135
IMAP:(Internet Mail Access Protocol).....	136
Post Office Protocol version 3 (POP3).....	137
IMAP VS POP:.....	137
What's the difference? .....	137
IMAP makes it easier to view mail from home, work, and other locations.....	138
Virtual Private Network (VPN).....	139
IPSEC.....	140
proxy server.....	141
Types of Proxy:.....	141
1. Forward Proxy:.....	141
2. Open Proxy:.....	141
3. Reverse Proxy:.....	142

File Transfer Protocol (FTP).....	142
Chapter9: Network Management and Security:.....	144
Introduction to Network Management:.....	144
Functions of Network Management System:.....	144
Simple Network Management Protocol(SNMP).....	145
Network Management Architectures.....	146
Computer security requirements and Attacks:.....	147
Types of Network Attacks .....	148
Data Encryption/Decryption, Cryptography, Integrity & Firewalls:.....	148
Cryptography.....	148
Encryption and Decryption.....	148
Symmetric-key.....	149
Asymmetric-Key Cryptography .....	150
DES (Data Encryption Standard):.....	152
Digital signatures .....	153
HASH Function: .....	154
Firewall.....	154
Types of Firewall.....	154
Network Level Firewall:.....	154
Circuit-level Firewall:.....	155
Application Level Firewall:.....	155
Chapter 10 :Introduction to Socket Programming:.....	157
Client Server Computing:.....	157
Client-Server Architecture:.....	157
2-Tier Architecture.....	157
3-Tier Architecture:.....	157
Comparing both types of architecture.....	158
Multi-Tiered Architecture.....	158
Distributed processing:.....	159
Socket Programming:.....	159

# Chapter1: Emergence of Network , principle of communication

## Network and Multiplexing

What is Computer Network?

Uses and advantages of Computer Network.

Principles of Communication.

Modes of communication

Multiplexing(Simplex,Duplex and half-duplex)

## What is computer Network?

A communication system for connecting computers/hosts.

- A computer network is a number of computers ( also known as nodes) connected by some communication lines.
- Two computers connected to the network can communicate with each other through the other nodes if they are not directly connected.
- Some of the nodes in the network may not be computers at all but they are network devices( Like switches, routers etc.) to facilitate the communication.

### Uses of the computer Network

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

### Advantages of Computer Network?

- Better communication
- Better connectivity
- Better sharing of Resources
- Bring people together

### Network supporting the way we live

Communication is almost as important to us as our reliance on air, food, water and shelter. The methods that we used to share the information are constantly changing and evolving. As with every advance in communication technology, the creation and interconnection of data network is having a profound effect. These days computer networks have evolved to carry voice, video streams, text and graphics between many different types of devices.

The immediate nature of communications over the Internet encourages the formation of global communities. These communities foster social interaction that is independent of location or time zone.

### Examples of Todays popular communication tools.

1. Instant messaging
2. Weblogs
3. wikis
4. Podcasting
5. Collaboration tools
6. Facebook
7. Twitter

### Networks Supporting the way we learn

communication, collaboration and engagement are fundamental building blocks of education. institutions are

continually striving to enhance these processes to maximize the dissemination of knowledge. Robust and reliable networks support and enrich student learning experiences.

Traditional Learning Process:

1. Text book
2. Instructor

these are limited in type of format and the timing of the presentation. In contrast, on-line courses can contain voice, data, and video, and are available to the students at any time from any place. on line distance learning has removed geographic barriers and improved student opportunity.

- course-ware
- collaboration
- References
- Administration

**Network supporting the way we work:**

**Remote Access:** Business application can be accessed remotely as if employees were on site.

**Multiple Resources:** workers in any location can reach each other and access multiple resources on the network.

**Network supporting the way we play:**

on-line games

**Types of Computer Network:**

LAN	WAN
Connects host within a relatively small geographical area. <ul style="list-style-type: none"><li>• Same Building</li><li>• Same room</li><li>• Same Campus</li></ul>	Hosts may be widely dispersed. <ul style="list-style-type: none"><li>• Across Campuses</li><li>• Across Cities/countries/continent</li></ul>
Faster	Slower
Cheaper	Expensive
Under a control of single ownership.	Not under a control of a single person.
Typical Speeds: 10 Mbps to 10Gbps	Typical Speed: 64 Kbps to 8 Mbps

## Historical Events:

- 1948 first commercial computer installed UNIVAC 1
- 1958 First U.S communication satellite.
- 1964 SABRE airline reservation system packet switching network (Proposed by RAND).
- 1969 ARPANET first packet switching network begins operation.
- 1971 first computer chip
  - 4 bit, 2,300 transistors
- 1972 Ethernet specifications formulated
- 1974 introduces SNA
- 1975 Altair 8800 first commercial microcomputer sold as kit.
- 1975 Paul Allen/Bill Gates wrote a BASIC language interpreter for the Altair, they formed Microsoft.



- 1976 Wozniak and Jobs built Apple I and formed Apple computer company.
- 1979 Visicalc first commercial spreadsheet introduced.
- 1981 IBM introduces IBM PC one floppy
- 1983 TCP/IP becomes the official protocol on ARPANET.
- 1984 Apple introduced GUI with Apple Macintosh.
- 1986 Laptop PC.

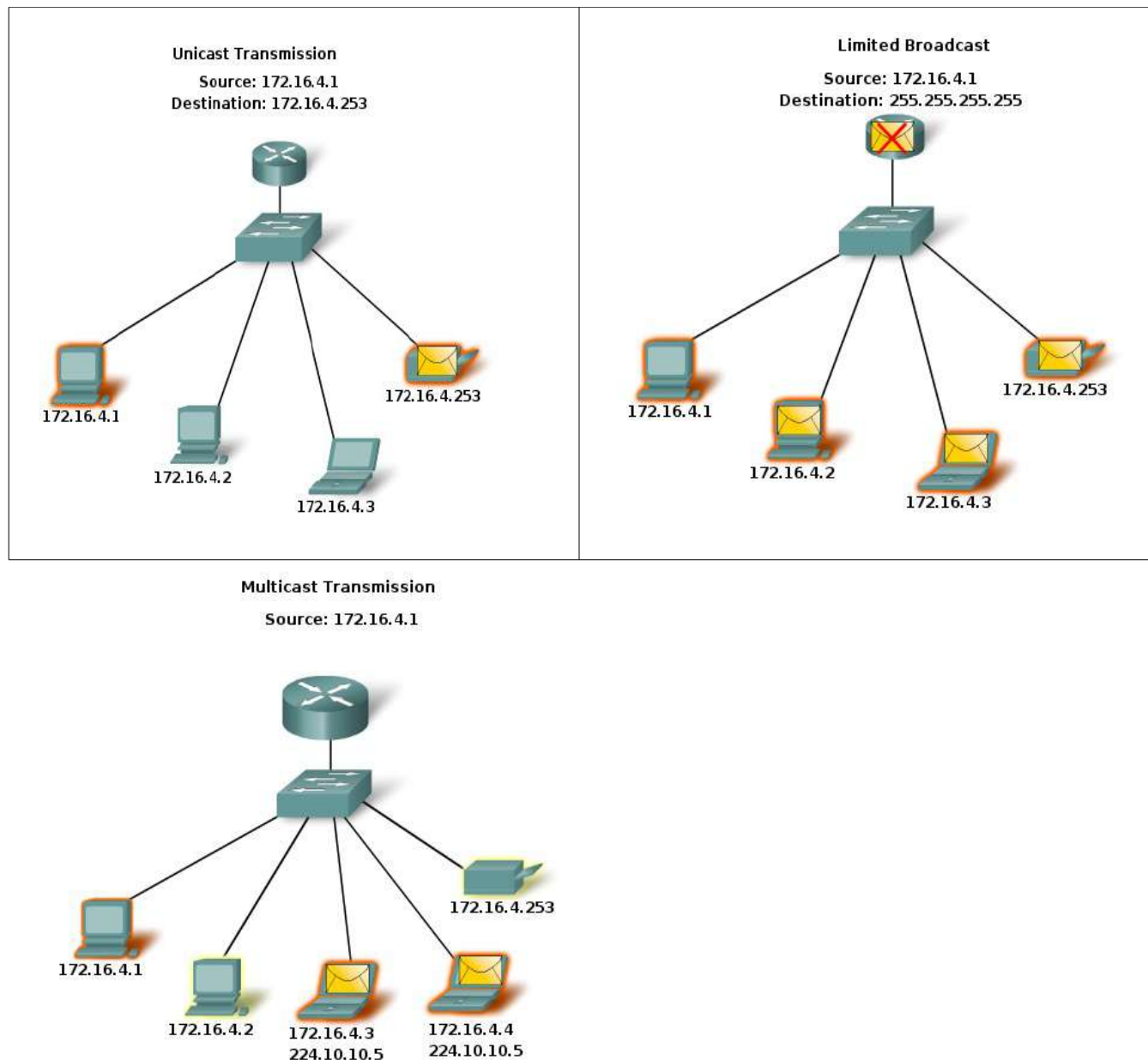
## Modes of communication:

In an IPv4 network, the hosts can communicate one of three different ways:

**Unicast** - the process of sending a packet from one host to an individual host

**Broadcast** - the process of sending a packet from one host to all hosts in the network

**Multicast** - the process of sending a packet from one host to a selected group of hosts



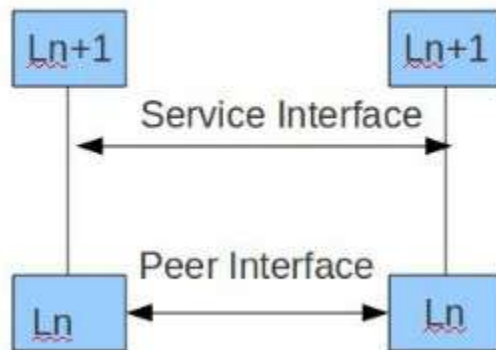
## Protocol:

A protocol defines the format and the order of messages exchanged between two or more

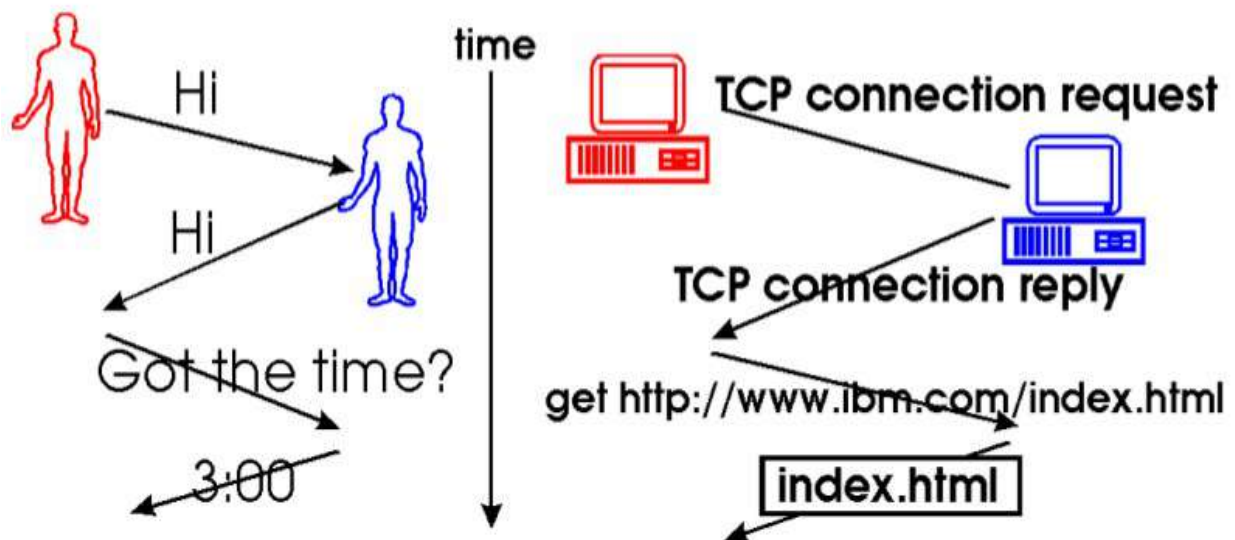
- Each protocol object has two different interfaces.
  - Service interfaces: Defines operation on this protocol.
  - Peer-to-peer interfaces: Defines message exchanged with peer.

communicating entities, as well as the actions taken on the transmission and/or receipt of a message.

- Building blocks of a Network Architecture.

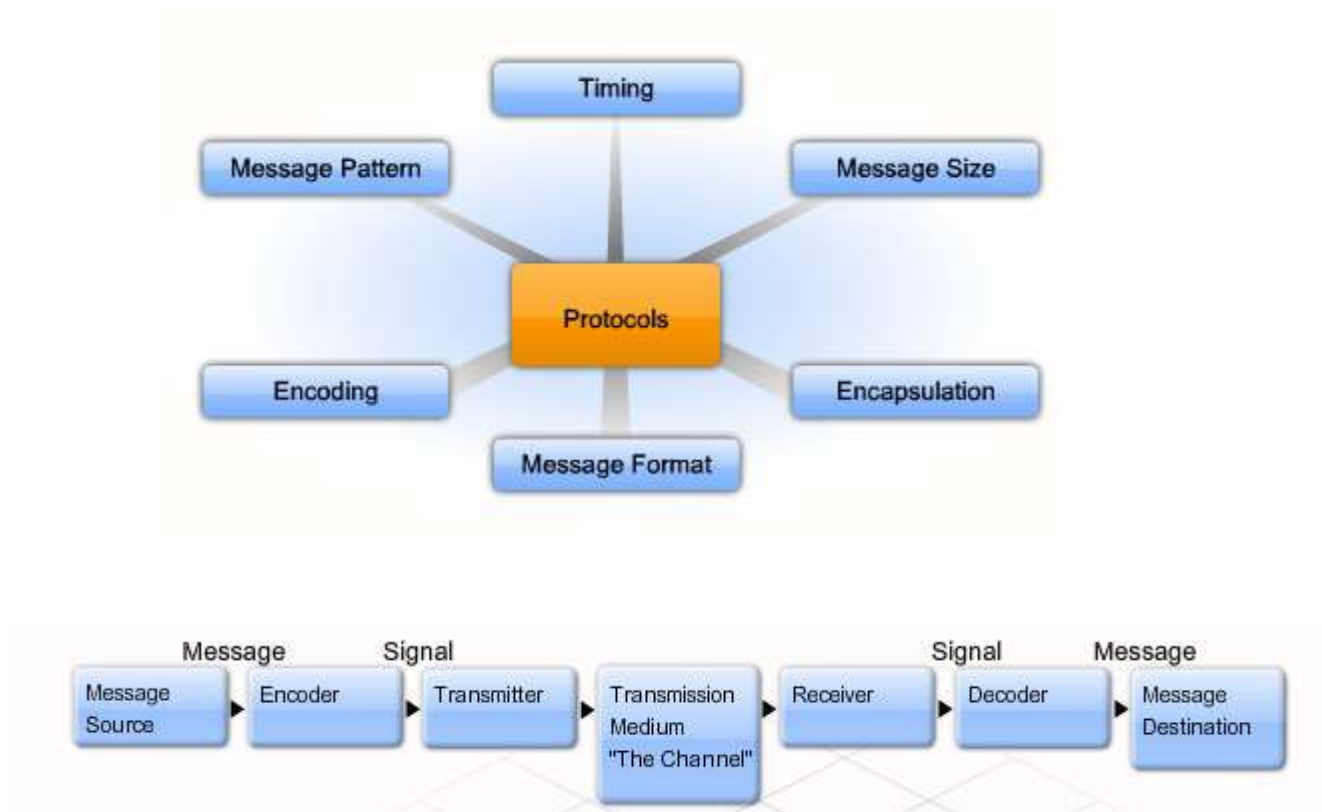


- Most networks are organized as a series of layers.
- The task of each layer is to give some service to the upper layers.
- Any layer maintains a virtual connection with the corresponding layer in a peer.
- There is a peer to peer protocol running between any two corresponding layers.
- The interface between any two layers is well defined.
- The implementation of each layer in each node is transparent to other devices.



*A Human protocol and Computer Network protocol*

# Principle of Communication:



The primary purpose of any network is to provide a method to communicate. All communication methods have three elements in common. The first of these elements is the message **source, or sender**. Message sources are people, or electronic devices, that need to communicate a message to other individuals or devices. The second element of communication is the **destination, or receiver**, of the message. The destination receives the message and interprets it. A third element, called a **channel**, provides the pathway over which the message can travel from source to destination.

Protocols are specific to the characteristics of the source, channel and destination of the message. The rules used to communicate over one medium, like a telephone call, are not necessarily the same as communication using another medium, such as a letter.

Protocols define the details of how the message is transmitted, and delivered. This includes issues of:

1. Message format
2. Message size
3. Timing
4. Encapsulation
5. Encoding
6. Standard message pattern

**Encoding:**

Encoding is the process of putting a sequence of [characters](#) (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage. Encoding between hosts must be in an appropriate form for the medium. Messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted. The destination host receives and decodes the signals in order to interpret the message.

**Message Format:**

Message that is sent over a computer network follows specific format rules for it to be delivered and processed. Just as a letter is encapsulated in an envelope for delivery, so computer messages are encapsulated. Each computer message is encapsulated in a specific format, called a frame, before it is sent over the network. A frame acts like an envelope; it provides the address of the intended destination and the address of the source host.

**Message Size:**

When a long message is sent from one host to another over a network, it is necessary to break the message into smaller pieces.

**Message Timing:**

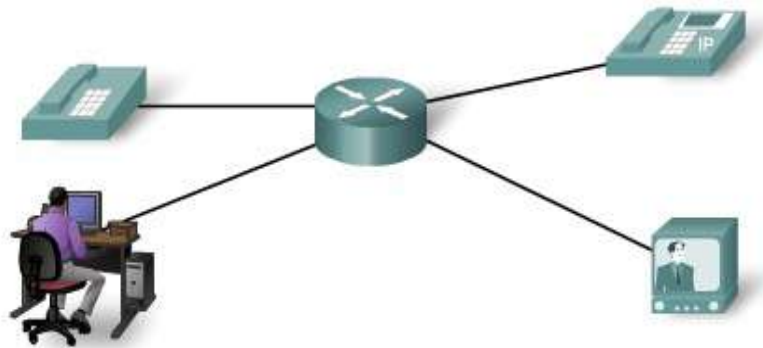
One factor that affects how well a message is received and understood is timing . People use timing to determine when to speak, how fast or slow to talk, and how long to wait for a response. These are the rules of engagement.

1. Access Methods
2. Flow Control
3. Response Timeout

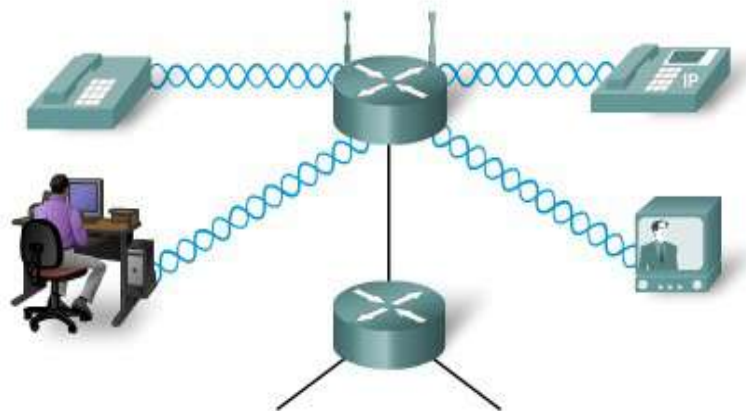
Service	Protocol ("Rule")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Instant Message (Jabber; AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
IP Telephony	SIP (Session Initiation Protocol)

# Elements of Network:

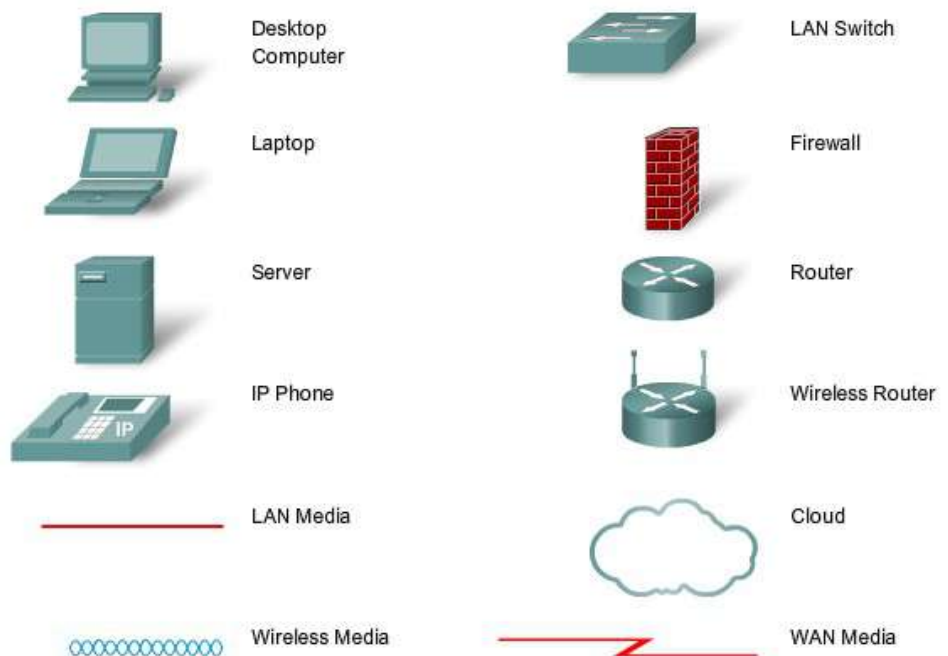
Wired networks used physical cables to connect devices.



Wireless networks use radio waves to communicate between devices.



Wireless networks are also connected to wired networks, at some point.



# Multiplexing:

## Why Multiplexing?

### Basic concept of multiplexing

Frequency division multiplexing

Wavelength division multiplexing

Time division multiplexing

- Synchronous
- Asynchronous

Inverse TDM

Course syllabus deal with Simplex, Duplex and half Duplex?

## Simplex:

A form of communication in which signals are sent in only one direction. This is different from duplex transmission, in which signals can simultaneously be sent and received by a station, and from half-duplex transmission, in which signals can be sent or received but not both at the same time. Simplex transmission occurs in many common communication applications, the most obvious being broadcast and cable television. It is not used in true network communication because stations on a network generally need to communicate both ways. Some forms of network communication might seem to be simplex in nature, such as streaming audio or video, but the communication actually takes place using bidirectional network traffic, usually Transmission Control Protocol (TCP) traffic. Simplex communication is not included in the V series recommendations of the International Telecommunication Union (ITU).

## Duplex

A telecommunications term referring to bidirectional communication. In full-duplex communication, both stations send and receive at the same time, and usually two communication channels are required. However, you can also achieve full-duplex communication using a multiplexing technique whereby signals traveling in different directions are placed into different time slots. The disadvantage of this technique is that it cuts the overall possible transmission speed by half.

In half-duplex communication, only one station can transmit at any given time while the other station receives the transmission. The opposite of duplex communication is simplex communication, which can occur only in one direction.

## Half-duplex

A mode of communication in which data can be transmitted or received, but cannot be transmitted and received simultaneously. The simplest example is a walkie-talkie: You have to press a button to talk and release the button to listen. When two people use walkie-talkies to communicate, at any given moment, only one of them can talk while the other listens. If both try to talk simultaneously, a collision occurs and neither hears what the other says.

Communication through traditional Ethernet networks is another example of half-duplex communication. When one station on an Ethernet transmits, the other stations detect the carrier signal and listen instead of transmitting. If two stations transmit signals simultaneously, a collision occurs and both stations stop transmitting and wait random intervals of time before retransmitting.

In contrast, full-duplex communication enables stations to transmit and receive signals simultaneously, with the advantage of providing twice the bandwidth of equivalent half-duplex technologies. However, full-duplex requires two communication channels to achieve these results—one to transmit and one to receive signals.

A third mode of communication is called simplex, which involves transmission in one direction only, with one station transmitting signals and the other receiving them.

## Chapter2: Network Topology and Architecture

*Definition, use and prospect of LAN; Types of networking: LAN, WAN, MAN, Extra-Net, Intra-net and Inter – Net, Star, Clustered Star, Bus Ring; Logical and Physical, Client Server Network Model: Peer – to peer Network architecture model; Wireless LAN*

### Local Area Network (LAN)

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

LANs are designed to:

Operate within a limited geographic area.  
Allow Multi-access to high bandwidth media.

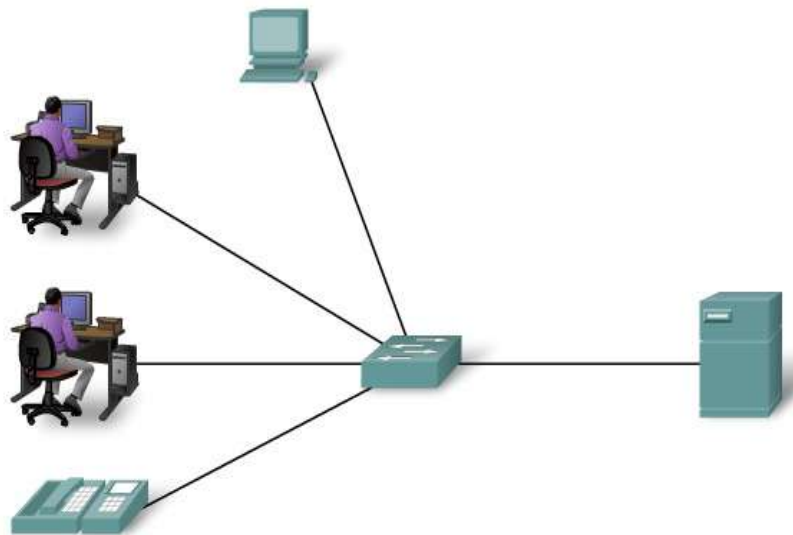
LANs consist of the following components:

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

LANs allow businesses to locally share computer files and printers efficiently and make internal communications possible. A good example of this technology is e-mail. LANs manage data, local communications, and computing equipment. Some common LAN technologies include the following:

- Ethernet
- Token Ring
- FDDI

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



### MAN:

is a network that spans a city. The network consists of various buildings interconnected via either wireless or fiber optics backbones.

A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus. A MAN

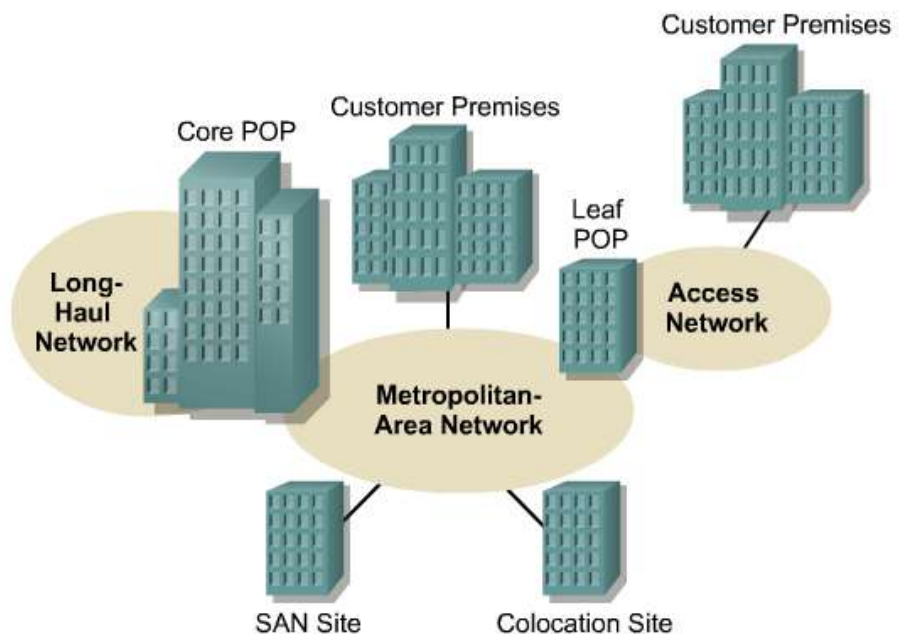


Fig:MAN



usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet.

## WAN:

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

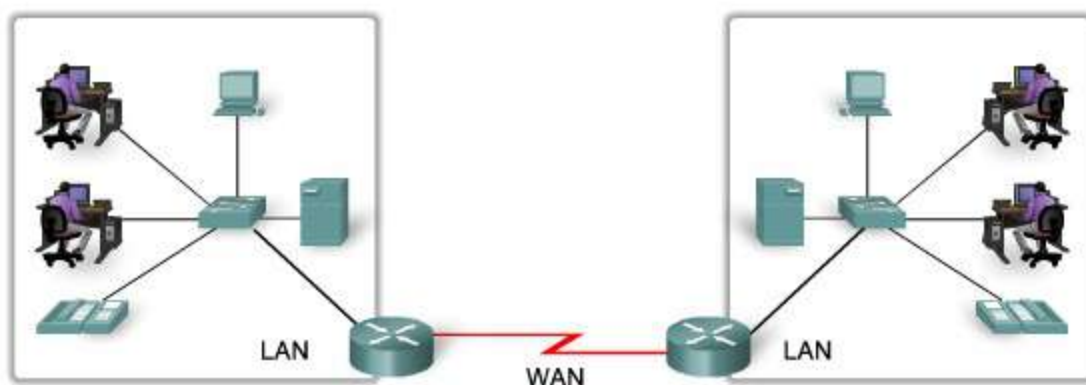
WANs are designed to do the following:

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

Some common WAN technologies include the following:

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

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





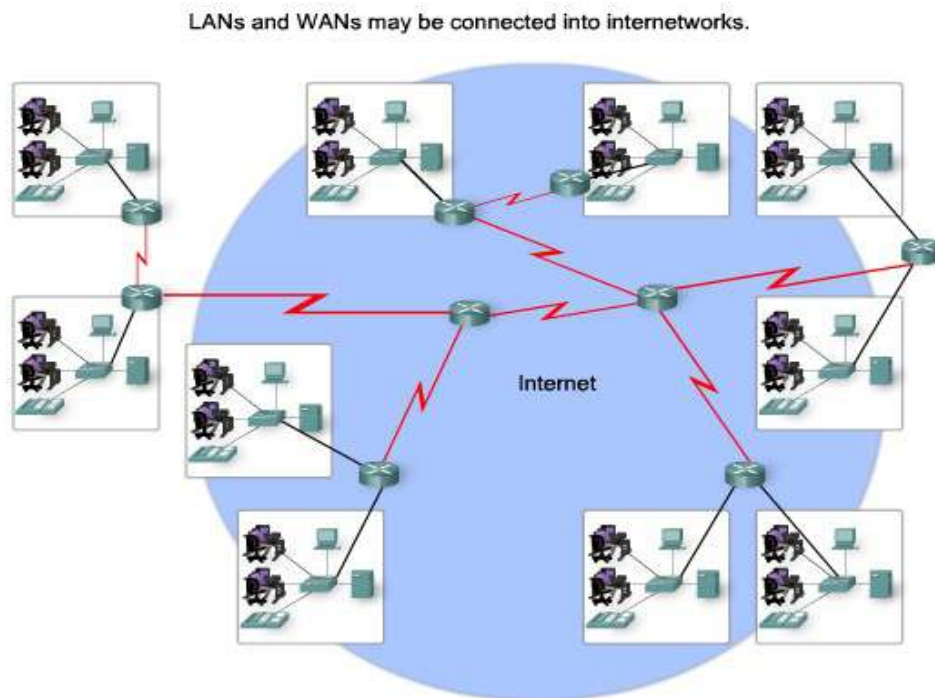
# LAN Vs WAN

LAN	WAN
Connects host within a relatively small geographical area. <ul style="list-style-type: none"><li>• Same Building</li><li>• Same room</li><li>• Same Campus</li></ul>	Hosts may be widely dispersed. <ul style="list-style-type: none"><li>• Across Campuses</li><li>• Across Cities/countries/continent</li></ul>
Faster	Slower
Cheaper	Expensive
Under a control of single ownership.	Not under a control of a single person.
Typical Speeds: 10 Mbps to 10Gbps	Typical Speed: 64 Kbps to 8 Mbps

## Internet:

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

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



**Internet is comprises of :**

*A community of people :* who use and develop the network.

*A collection of resources:* that can be reached from those networks.

*A setup to facilitate collaboration:* Among the members of the research and educational communities world wide.

*The connected networks use the TCP/IP protocols:*

**important Internet applications:**

world wide web(WWW)

File Transfer Protocol(FTP)

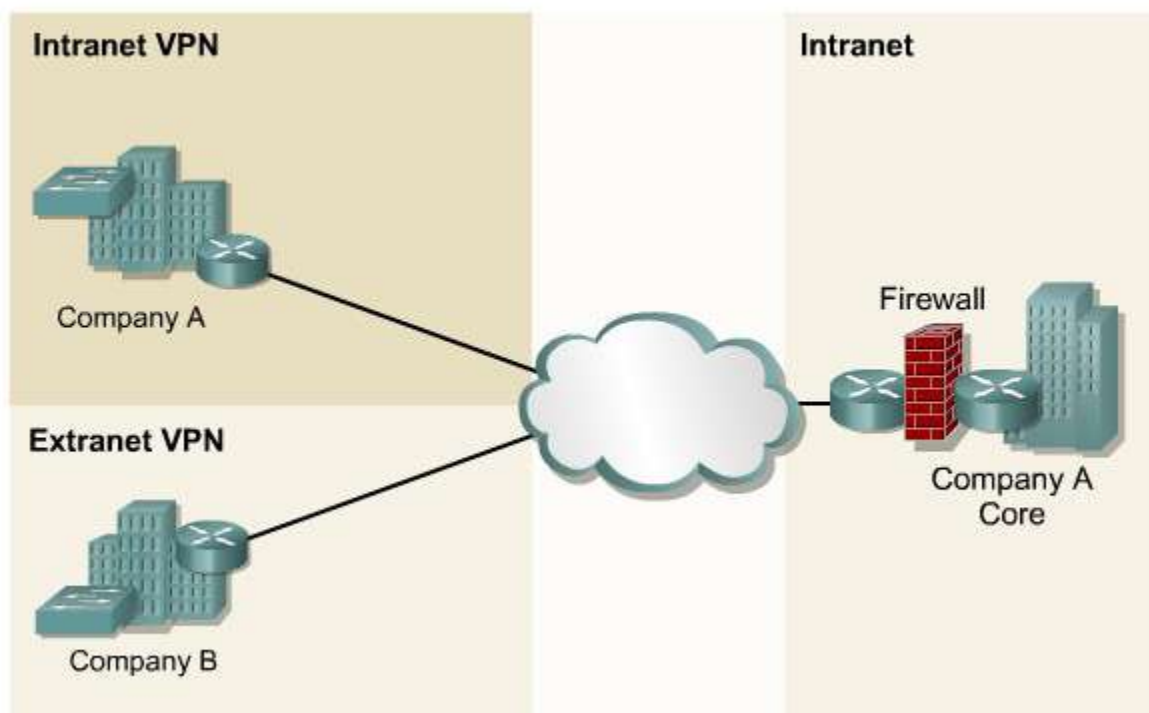
Electronic Mail

Internet Relay Chat

**Intranet:**

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

Intranet Web servers differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization. Intranets are designed to permit users who have access privileges to the internal LAN of the organization. Within an intranet, Web servers are installed in the network. Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data.



## Extranet:

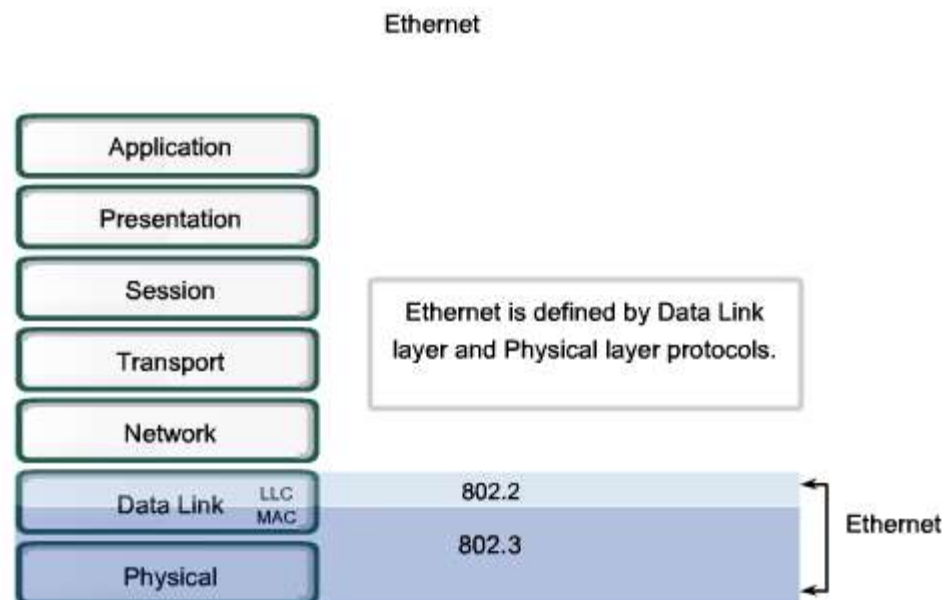
Extranets refer to applications and services that are Intranet based, and use extended, secure access to external users or enterprises. This access is usually accomplished through passwords, user IDs, and other application-level security. An extranet is the extension of two or more intranet strategies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

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

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

## Ethernet:

Ethernet is a family of LAN technologies, that may be best understood with the OSI reference model.



Ethernet technologies have three part names:

1. Speed
2. Signal Method (BaseBand and BroadBand).
3. Medium

Eg. 100BASET

- 100 Mbps
- Baseband
- Unshielded Twisted Pair

10BASE5, 10Mbps, Baseband, 5\*100Meters.

**Baseband:**

A signaling technology that sends digital signals over a single frequency as discrete electrical pulses. The baseband signal is bidirectional so that a baseband system can both transmit and receive signals simultaneously. Use time-division multiplexing (**TDM**) to accommodate multiple channels over a single baseband transmission line. Baseband signals can be regenerated using repeaters in order to travel longer distances before weakening and becoming unusable because of attenuation. Eg. Ethernet

**Braodband:**

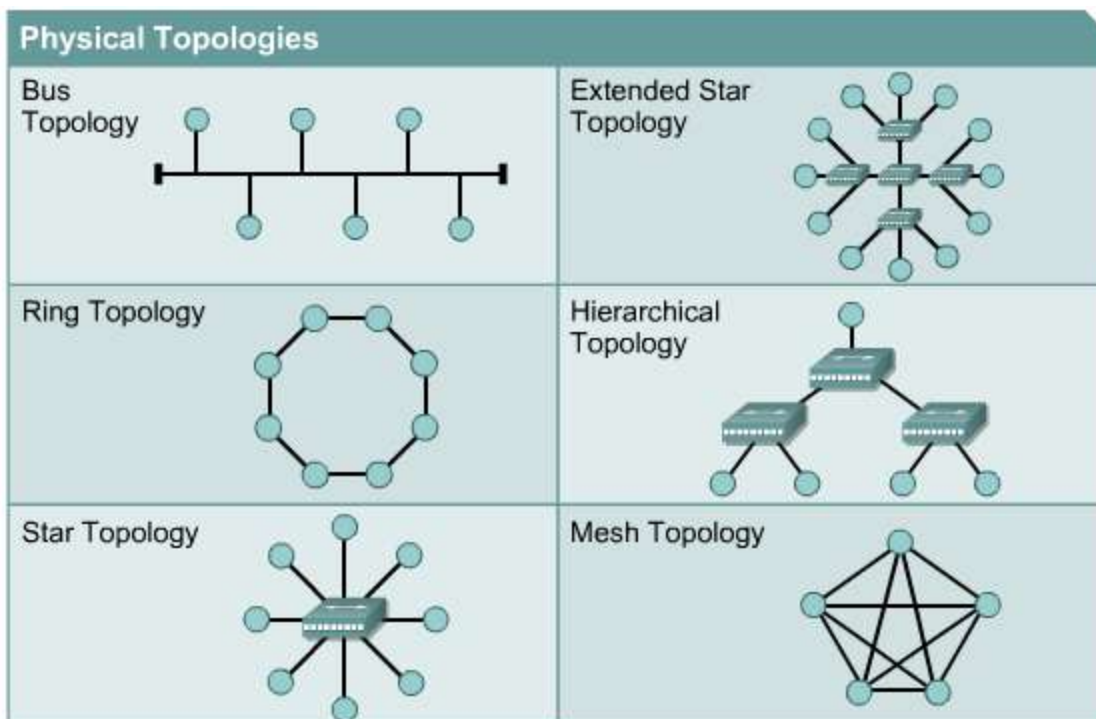
A signaling technology that sends signals simultaneously over a range of different frequencies as electromagnetic waves. These signals are unidirectional—traveling in only one direction at a time—so a broadband system can generally either transmit or receive but cannot do both simultaneously. Broadband signals can be regenerated using amplifiers in order to travel longer distances before becoming attenuated. Broadband transmissions are divided into multiple bands or channels by multiplexers using a multiplexing scheme such as frequency-division multiplexing (**FDM**).

Eg. One good example of broadband signaling would be how you view different channels through your cable box and a signal coaxial cable carrying multiple signals in cable television.

## Physical Topology and Logical Topology:

**Physical topology** The term physical topology refers to the way in which a network is laid out physically. The actual layout of the wire or media. Two or more devices connect to a link; two or more links form a topology.

**Logical topology:** Defines how the hosts access the media to send data. Shows the flow of data on a network.



## Bus Topology:

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

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

### Advantages:

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

### Disadvantages:

- out of date technology.
- include difficult reconnection and fault isolation
- Can be difficult to troubleshoot.
- Unmanageable in a large network
- If cable breaks, whole network is down

## Ring Topology

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

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location. However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

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

### Advantages:

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

**Disadvantage:**

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

## Mesh Topology:

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

**Advantages:**

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. Robust, If one link becomes unusable, it does not incapacitate the entire system.
3. Advantage of privacy or security.
4. point-to-point links make fault identification and fault isolation easy , Traffic can be routed to avoid links with suspected problems.

**Disadvantage:**

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

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

## Star Topology:

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

**Advantages:**

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

**Disadvantage:**

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

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

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

## Logical Topology:

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

The use of a **broadcast topology** indicates that each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to use the network. It is first come, first serve. Ethernet works this way as will be explained later in the course.

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

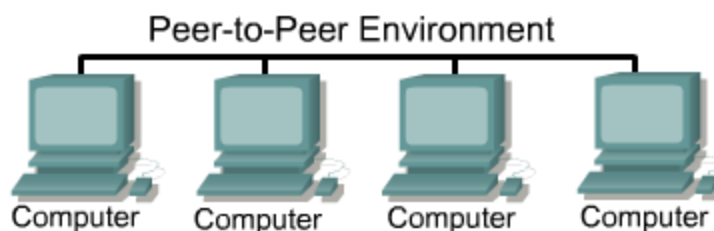
## Network Architecture:

*Two types of Network Architecture:*

1. Peer-to-Peer Model
2. Client-server Model

### Peer-to-Peer Model:

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



In a peer-to-peer network, individual users control their own resources. The users may decide to share certain files with other users. The users may also require passwords before they allow others to access their resources. Since individual users make these decisions, there is no central point of control or administration in the network. In addition, individual users must back up their own systems to be able to recover from data loss in case of

failures. When a computer acts as a server, the user of that machine may experience reduced performance as the machine serves the requests made by other systems.

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

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

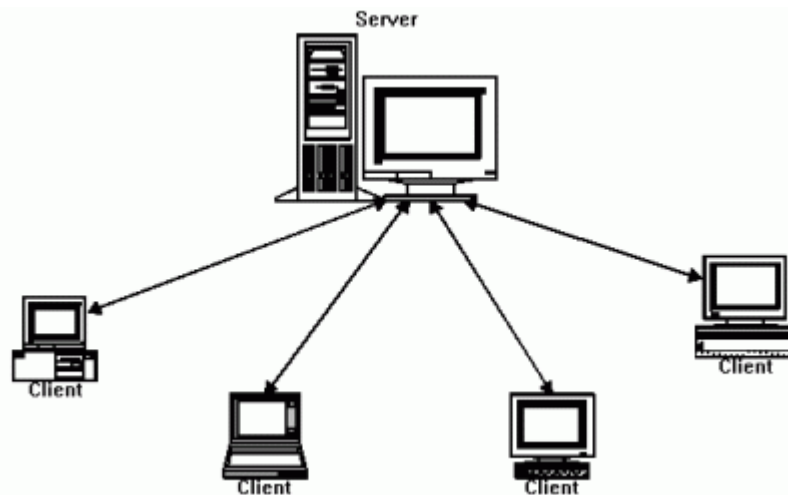
#### **The advantages of peer-to-peer:**

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

#### **Client-server Model:**

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

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



Servers are designed to handle requests from many clients simultaneously. Before a client can access the server resources, the client must be identified and be authorized to use the resource. Each client is assigned an account



name and password that is verified by an authentication service. The authentication service guards access to the network. With the centralization of user accounts, security, and access control, server-based networks simplify the administration of large networks. The concentration of network resources such as files, printers, and applications on servers also makes it easier to back-up and maintain the data. Resources can be located on specialized, dedicated servers for easier access. Most client/server systems also include ways to enhance the network with new services that extend the usefulness of the network.

The centralized functions in a client/server network has substantial advantages and some disadvantages. Although a centralized server enhances security, ease of access, and control, it introduces a single point of failure into the network. Without an operational server, the network cannot function at all. Servers require a trained, expert staff member to administer and maintain. Server systems also require additional hardware and specialized software that add to the cost.

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

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

#### **Client-server Vs Peer-to-Peer Network:**

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

## Wireless LAN:

The infrastructure less network where, there is not required of any physical cable for network connection. In wireless LAN each client computer is connected to the Access Point though which they can share the file and access to the Internet.

These days People are becoming more mobile and want to maintain access to their business LAN resources from locations other than their desks. Workers in the office want to take their laptops to meetings or to a co-worker's office. When using a laptop in another location, it is inconvenient to rely on a wired connection.

### WLAN VS LAN:

Characteristics	802.11 Wireless LAN	802.3 Ethernet LANS
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance (CSMA/CA)	Collision Detection(CSMA/CD)
Availability	Anyone with a radio NIC in range of an Access point	Cable connection required
Signal interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

- RF does not have boundaries, such as the limits of a wire in a sheath. The lack of such a boundary allows data frames traveling over the RF media to be available to anyone that can receive the RF signal.
- RF is unprotected from outside signals, whereas cable is in an insulating sheath. Radios operating independently in the same geographic area but using the same or a similar RF can interfere with each other.
- RF transmission is subject to the same challenges inherent in any wave-based technology, such as consumer radio. For example, as you get further away from the source, you may hear stations playing over each other or hear static in the transmission. Eventually you may lose the signal all together. Wired LANs have cables that are of an appropriate length to maintain signal strength.
- RF bands are regulated differently in various countries. The use of WLANs is subject to additional regulations and sets of standards that are not applied to wired LANs.



## Wireless Standards - 802.11b 802.11a 802.11g and 802.11n

Parameters	802.11a	802.11b	802.11g	802.11n
Bandwidth(BW)	11Mbps	54Mbps	54Mbps	100Mbps
Signal Frequency	2.4Ghz	Upto 5Ghz	2.4Ghz	Unconfirmed possibly 2.4 and 5Ghz.

### 802.11a:

- **Pros of 802.11a** - fast maximum speed; regulated frequencies prevent signal interference from other devices
- **Cons of 802.11a** - highest cost; shorter range signal that is more easily obstructed

### 802.11b:

- **Pros of 802.11b** - lowest cost; signal range is good and not easily obstructed
- **Cons of 802.11b** - slowest maximum speed; home appliances may interfere on the unregulated frequency band

### 802.11g:

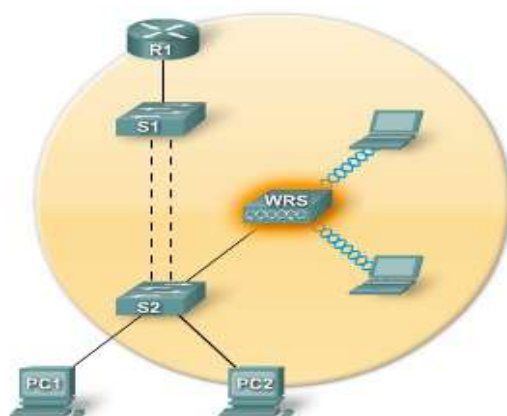
- **Pros of 802.11g** - fast maximum speed; signal range is good and not easily obstructed
- **Cons of 802.11g** - costs more than 802.11b; appliances may interfere on the unregulated signal frequency.

### 802.11n:

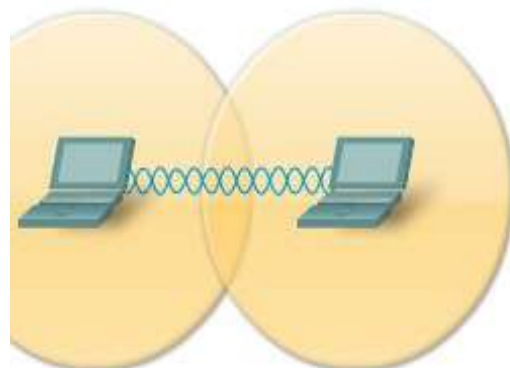
- **Pros of 802.11n** - fastest maximum speed and best signal range; more resistant to signal interference from outside sources
- **Cons of 802.11n** - standard is not yet finalized; costs more than 802.11g; the use of multiple signals may greatly interfere with nearby 802.11b/g based networks.

## Wireless Topologies:

1. BSS (Basic Service Set). (in the presence of a Control Module often called “Base Station” or Access points.
2. Ad-hoc or Peer-to-Peer (When there is no Control Module)



*BSS Topology*



*Adhoc Topology*

### BSS:

Access points provide an infrastructure that adds services and improves the range for clients. A single access point in infrastructure mode manages the wireless parameters and the topology is simply a BSS.

**Ad-Hoc:**

Wireless networks can operate without access points; this is called an ad hoc topology. Client stations which are configured to operate in ad hoc mode configure the wireless parameters between themselves. The IEEE 802.11 standard refers to an ad hoc network as an independent BSS (IBSS).

## Chapter3: OSI Reference Model:

### Network Software:

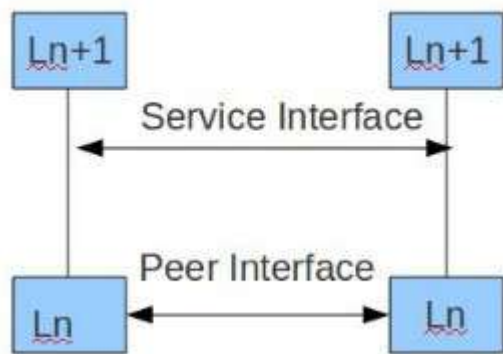
Network Software is a set of primitives that define the protocol between two machines. The network software resolves an ambiguity among different types of network making it possible for all the machines in the network to connect and communicate with one another and share information.

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

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

### Protocol Hierarchies

To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.



This concept is actually a familiar one and used throughout computer science, where it is variously known as information hiding, abstract data types, data encapsulation, and object-oriented programming. The fundamental idea is that a particular piece of software (or hardware) provides a service to its users but keeps the details of its internal state and algorithms hidden from them.

Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer n protocol. Basically, a protocol is an agreement

between the communicating parties on how communication is to proceed. As an analogy, when a woman is introduced to a man, she may choose to stick out her hand. He, in turn, may decide either to shake it or kiss it, depending, for example, on whether she is an American lawyer at a business meeting or a European princess at a formal ball. Violating the protocol will make communication more difficult, if not completely impossible.

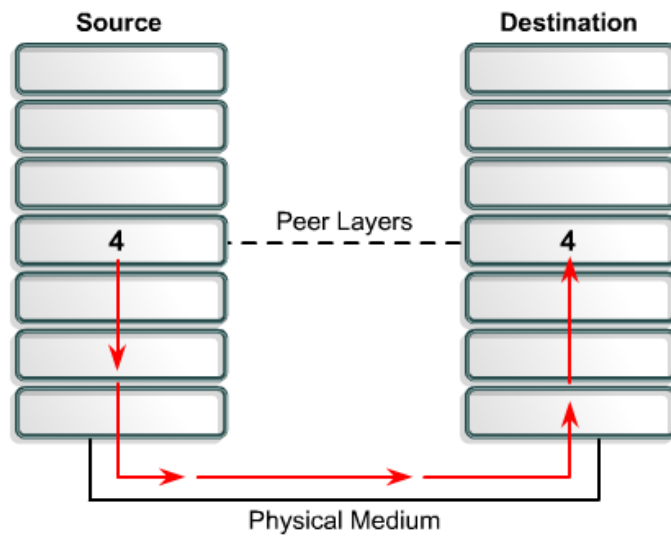
### Layer Communication:

In order for data packets to travel from a source to a destination on a network, it is important that all the devices on the network speak the same language or protocol. *A protocol is a set of rules that make communication on a network more efficient. For example, while flying an airplane, pilots obey very specific rules for communication with other airplanes and with air traffic control.*

**A data communications protocol is a set of rules or an agreement that determines the format and transmission of data.**

As shown in fig alongside Layer 4 on the source computer communicates with Layer 4 on the destination computer. The rules and conventions used for this layer are known as Layer 4 protocols. It is important to remember that protocols prepare data in a linear fashion. A protocol in one layer performs a certain set of operations on data as it prepares the data to be sent over the network. The data is then passed to the next layer where another protocol performs a different set of operations.

Once the packet has been sent to the destination, the protocols undo the construction of the packet that was done on the source side. This is done in reverse order. The protocols for each layer on the destination return the information to its original form, so the application can properly read the data.



## OSI Model

An architectural model for open networking systems that was developed by the International Organization for Standardization (ISO) in Europe in 1974. The Open Systems Interconnection (OSI) reference model was intended as a basis for developing universally accepted networking protocols, but this initiative essentially failed for the following reasons.

- The standards process was relatively closed compared with the open standards process used by the Internet Engineering Task Force (IETF) to develop the TCP/IP protocol suite.
- The model was overly complex. Some functions (such as connectionless communication) were neglected, while others (such as error correction and flow control) were repeated at several layers.
- The growth of the Internet and TCP/IP—a simpler, real-world protocol model—pushed the OSI reference model out.

*The OSI reference model is best seen as an idealized model of the logical connections that must occur in order for network communication to take place. Most protocol suites used in the real world, such as TCP/IP, DECnet, and Systems Network Architecture (SNA), map somewhat loosely to the OSI reference model. The OSI model is a good starting point for understanding how various protocols within a protocol suite function and interact.*

### Benefits of OSI Model:

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

## Peer-to-Peer Communication:

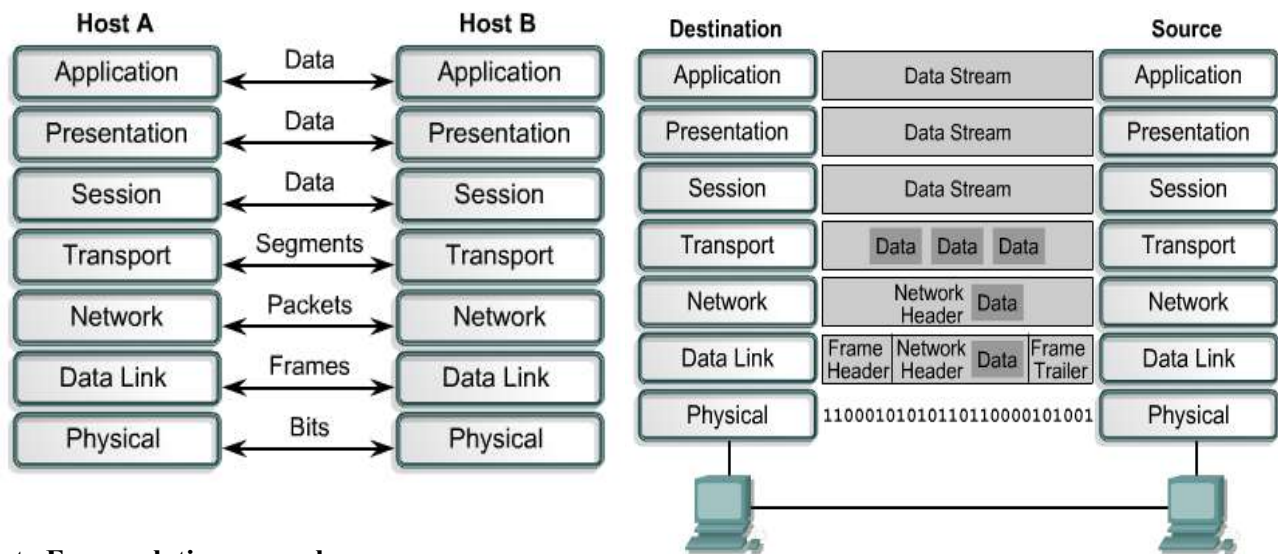
In order for data to travel from the source to the destination, each layer of the OSI model at the source must communicate with its peer layer at the destination. This form of communication is referred to as peer-to-peer. During this process, the protocols of each layer exchange information, called protocol data units (PDUs). Each layer of communication on the source computer communicates with a layer-specific PDU, and with its peer layer on the destination computer as illustrated in Figure

Data packets on a network originate at a source and then travel to a destination. Each layer depends on the service function of the OSI layer below it. To provide this service, the lower layer uses encapsulation to put the PDU from the upper layer into its data field. Then it adds whatever headers and trailers the layer needs to perform its function. Next, as the data moves down through the layers of the OSI model, additional headers and trailers are added.

## Data Encapsulation:

All communications on a network originate at a source, and are sent to a destination. The information sent on a network is referred to as data or data packets. If one computer (host A) wants to send data to another computer (host B), the data must first be packaged through a process called encapsulation.

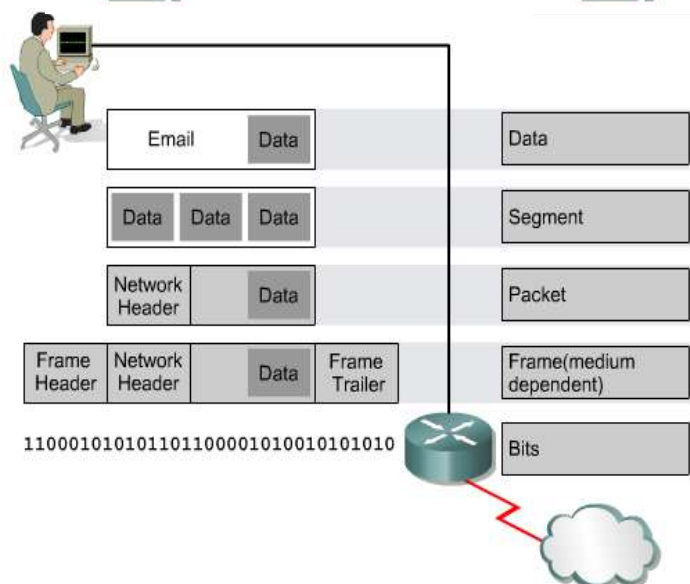
Encapsulation wraps data with the necessary protocol information before network transit. Therefore, as the data packet moves down through the layers of the OSI model, it receives headers, trailers, and other information.



### Data Encapsulation example:

Perform the following five conversion steps in order to encapsulate the data.

1. Build the data.
2. Package the data for end-to-end transport.
3. Add the network IP address to the header.
4. Add the data link layer header and trailer.
5. Convert to bits for transmission.



# Seven Layers of OSI Reference Model:

## 1. Physical Layer:

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

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

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

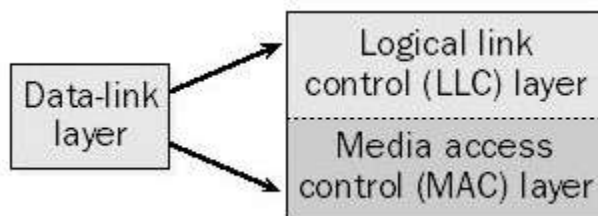
**Functional.** Specifies the functions performed by individual circuits of the physical interface between a system and the transmission medium.

**Procedural.** Specifies the sequence of events by which bit streams are exchanged across the physical medium.

## 2. Data Link Layer:

The physical layer provides only a raw bit-stream service, the data link layer attempts to make the physical link reliable while providing the means to activate, maintain, and deactivate the link .

For LANs, the Project 802 standards of the Institute of Electrical and Electronics Engineers (IEEE) separate the data-link layer into two sublayers:



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

### Functions:

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

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



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

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

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

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

- IEEE 802.3, which provides the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method for baseband Ethernet networks
- IEEE 802.5, which provides the token-passing access method for baseband token ring implementations

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

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

### 3. Network Layer:

Layer 3 of the Open Systems Interconnection (OSI) reference model for networking. The network layer is responsible for functions such as the following:

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

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

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

### 4. Transport Layer:

Layer 4 of the Open Systems Interconnection (OSI) reference model. The transport layer is responsible for providing reliable transport services to the upper-layer protocols. These services include the following:

- Flow control to ensure that the transmitting device does not send more data than the receiving device can handle.

- Packet sequencing for segmentation of data packets and remote reassembly.
- Error handling and acknowledgments to ensure that data is retransmitted when required.
- Multiplexing for combining data from several sources for transmission over one data path.
- Virtual circuits for establishing sessions between communicating stations.

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

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

*Virtual circuits can be either permanent (called PVCs) or temporary (called SVCs).*

## 5. Session Layer:

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

### Functions:

**Dialog control:** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half- duplex (one way at a time) or full-duplex (two ways at a time) mode.

**Synchronization:** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

## 6. Presentation Layer:

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

### Specific responsibilities of the presentation layer include the following:

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

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

**Compression.** Data compression reduces the number of bits contained in the information. Data compression

becomes particularly important in the transmission of multimedia such as text, audio, and video.

## 7. Application layer:

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

**File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

**Mail services.** This application provides the basis for e-mail forwarding and storage.

**Directory services.** This application provides distributed database sources and access for global information about various objects and services.

### Summary:

**Physical Layer:** How to transmit bits.

**Data Link Layer:** How to transmits frames

**Network:** How to route packets to the node.

**Transport:** How to send packets to the applications.

**Session:** Manage connections.

**Presentation:** Encode/Decode messages, security.

**Application:** Everything else.

## Devices and Protocols on each Layer:

Layer	Protocols	Devices
Physical		Hub, Repeater, Cables
Data-link	LLC,MAC,Ethernet	Switch
Network	IP,Routing protocol(RIP, OSPF)	Router
Transport	TCP,UDP	
Session		
Presentation	ASCII,Encryption, Decryption	
Application	DNS,NFS,TELNET,NFS	

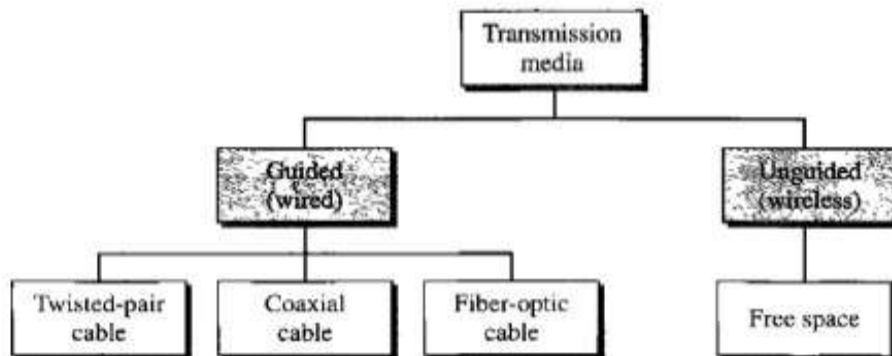
## Chapter4: Physical layers and its Design issues:

Twisted Pair Cable; Co-axial Cable; Base – band Cable; Broad – band Cable; Fiber Optics; Wireless Networking; Physical Layer Devices ( Hub, Repeaters); Introduction of Frame Relay, ATM, ISDN, PSTN and X.25.

### Transmission Medium:

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

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



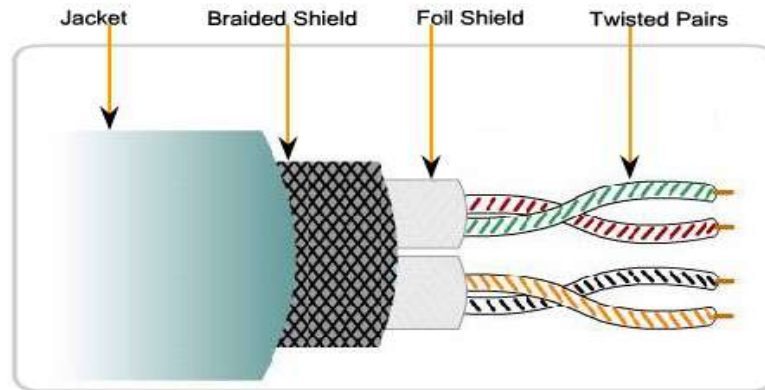
#### Guided Media:

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

### Shielded Twisted-Pair (STP) Cable

Another type of cabling used in networking is shielded twisted-pair (STP). As shown in the figure, STP uses two pairs of wires that are wrapped in an overall metallic braid or foil. STP cable shields the entire bundle of wires within the cable as well as the individual wire pairs. STP provides better noise protection than UTP cabling, however at a significantly higher price.

For many years, STP was the cabling structure specified for use in Token Ring network installations. With the use of Token Ring declining, the demand for shielded twisted-pair cabling has also waned. The new 10 GB standard for Ethernet has a provision for the use of STP cabling. This may provide a renewed interest in shielded twisted-pair cabling.



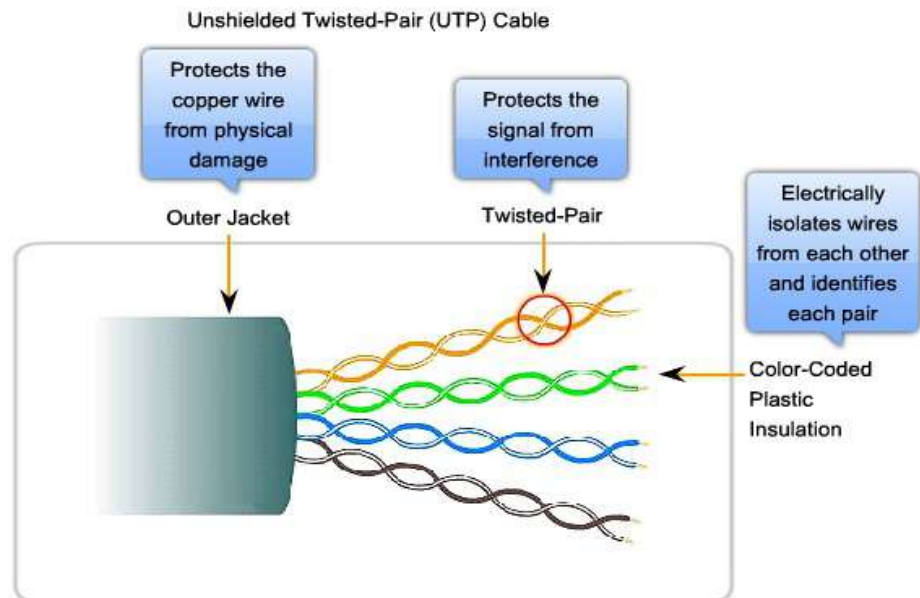
*Shielded Twisted-Pair Cable(STP)*

## Unshielded twisted-pair (UTP)

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

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

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



in the cable use a different number of twists per meter to help protect the cable from crosstalk between pairs.

## UTP Cabling Standards

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

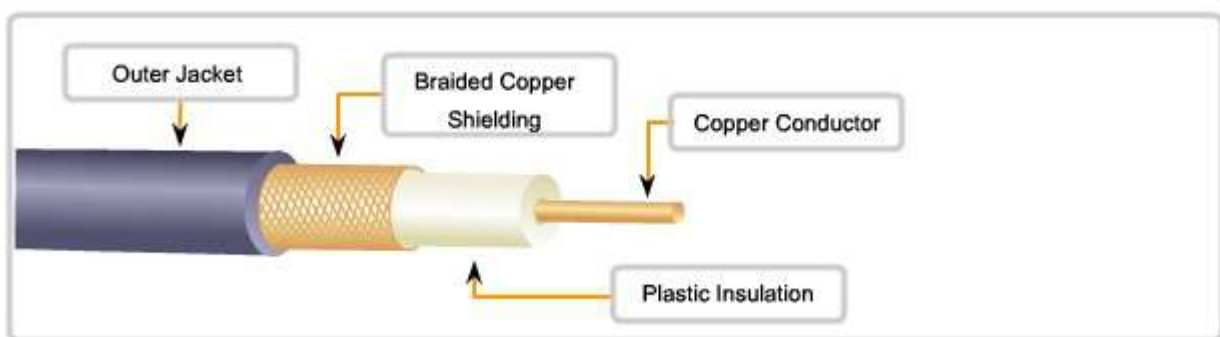
- Cable types
- Cable lengths
- Connectors
- Cable termination
- Methods of testing cable

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

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

## Co-axial Cable:

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



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

### Uses of Coaxial Cable

The coaxial cable design has been adapted for different purposes. Coax is an important type of cable that is used in **wireless and cable access technologies**. Coax cables are used to attach antennas to wireless devices. The coaxial cable carries radio frequency (RF) energy between the antennas and the radio equipment.

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

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

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

### Coaxial Cable Connectors

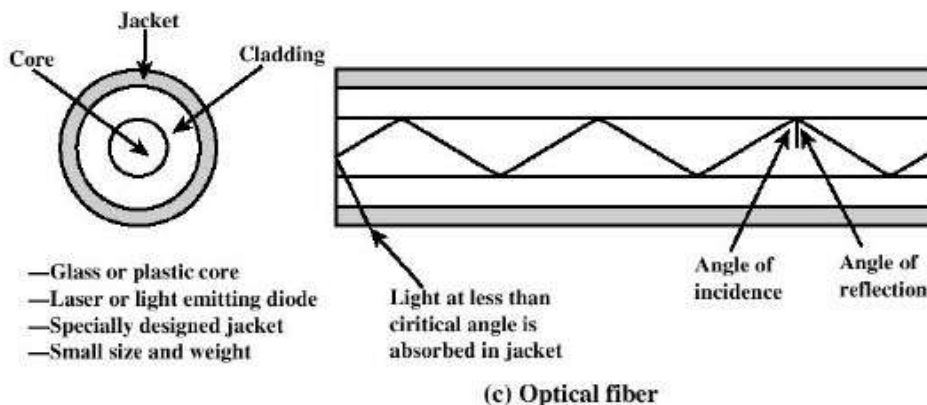
To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet-Neill-Concelman (BNC), connector. Three types of connectors: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the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

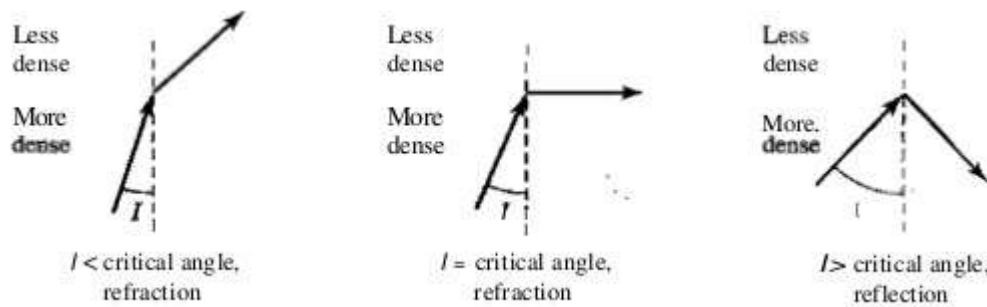
## Fiber-optics

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

### Principle of Fiber-optics:

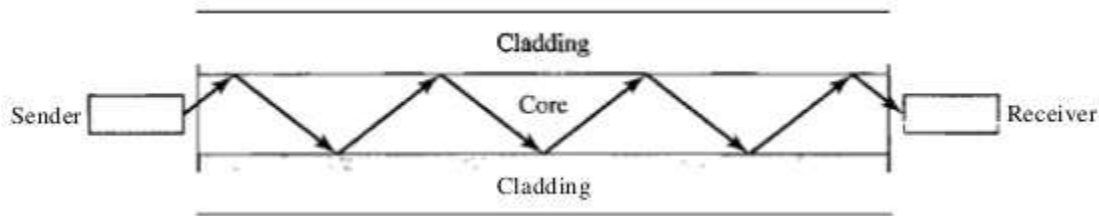
It is based on the principle of Total internal Reflection.





*Fig: Bending of Light Ray*

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



## **Fiber Compared to Copper Cabling :**

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

Optical fiber media implementation issues include:

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

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

## **Propagation modes:**

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multi- mode can be implemented in two forms: step-index or graded-index .



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

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



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

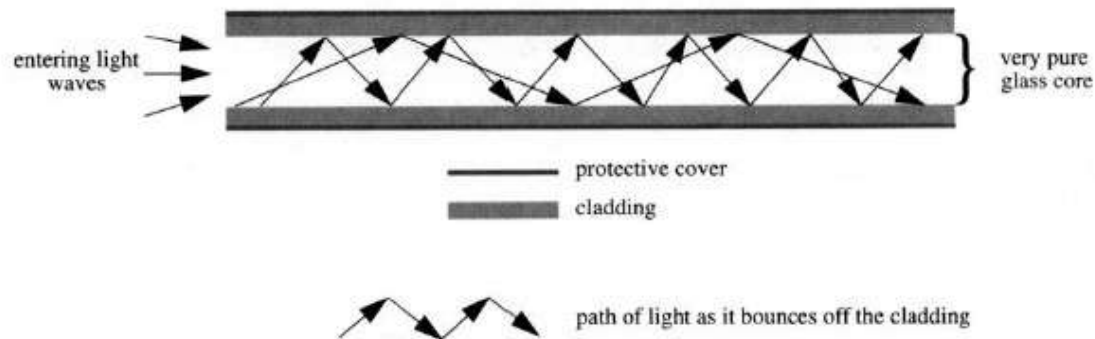
**Multimode** fiber typically uses LED emitters that do not create a single coherent light wave. Instead, light from an LED enters the multimode fiber at different angles. Because light entering the fiber at different angles takes different amounts of time to travel down the fiber, long fiber runs may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

#### **Multimode Step-index:**

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

### Three types of fiber transmission

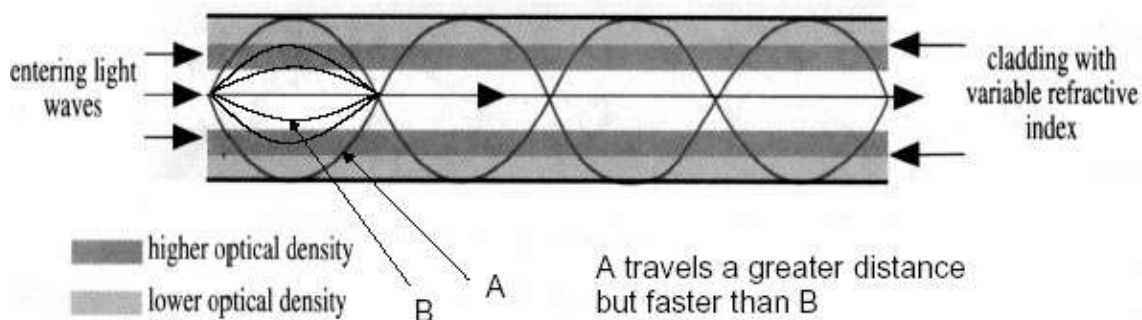
- Step index multimode
  - Variety of angles that reflect. Each angle defines a path or a mode
  - Limited data rate due to the different path lengths



### Multimode Graded-index

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

- Graded index multimode
  - Use the fact that speed of light depends on the medium; light travels faster through less optically dense media
  - The boundary between core and cladding is not sharply defined; Moving out radially from the core, the material becomes gradually less dense



## Advantages and Disadvantages of Optical Fiber

### Advantages

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

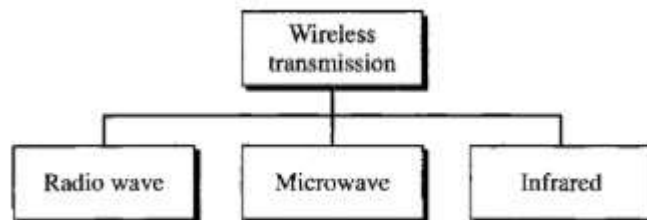
- **Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology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

**Disadvantages** There are some disadvantages in the use of optical fiber.

- **Installation and maintenance.** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- **Unidirectional light propagation.** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- **Cost.** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

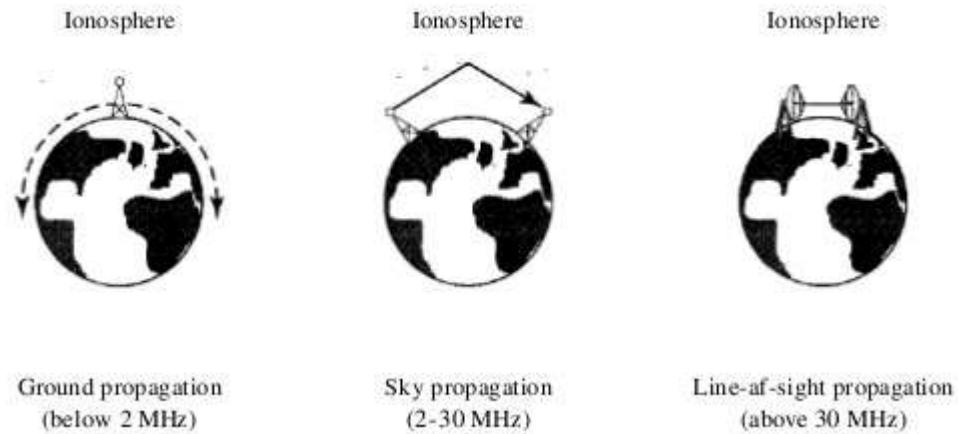
## Wireless Networking

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



*Fig: Wireless Transmission Waves*

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



*Fig: Propagation Method*

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

*Fig:Bands*

## Radio Waves

Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves. However, the behavior of the waves, rather than the frequencies, is a better criterion for classification. Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna.

The omnidirectional property has a disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band. Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio. Radio waves, particularly those of low and medium frequencies, can penetrate walls.

This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building. The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into subbands, the subbands are also narrow, leading to allow data rate for digital communications.

### Omnidirectional Antenna

Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure 7.20 shows an omnidirectional antenna.

### Applications

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

## Microwaves

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

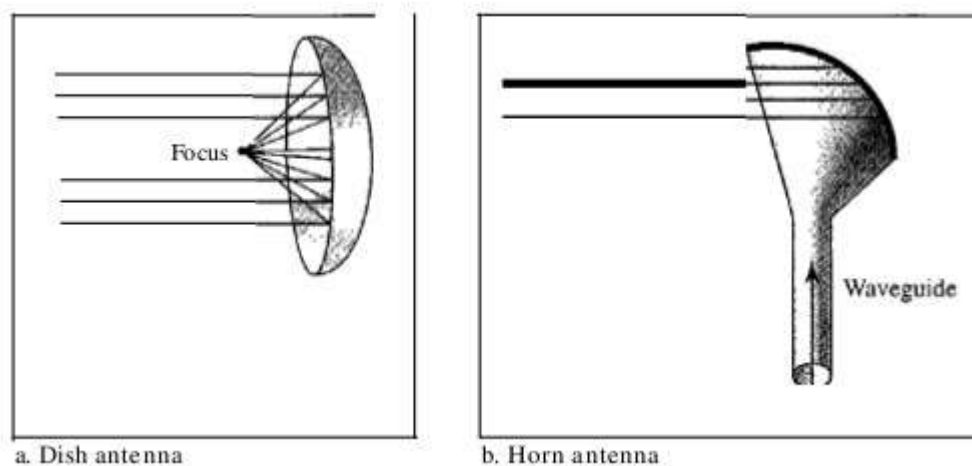
- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for long- distance communication.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible
- Use of certain portions of the band requires permission from authorities.

## Applications

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

## Unidirectional Antenna

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



A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus. The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

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

## Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

## Applications

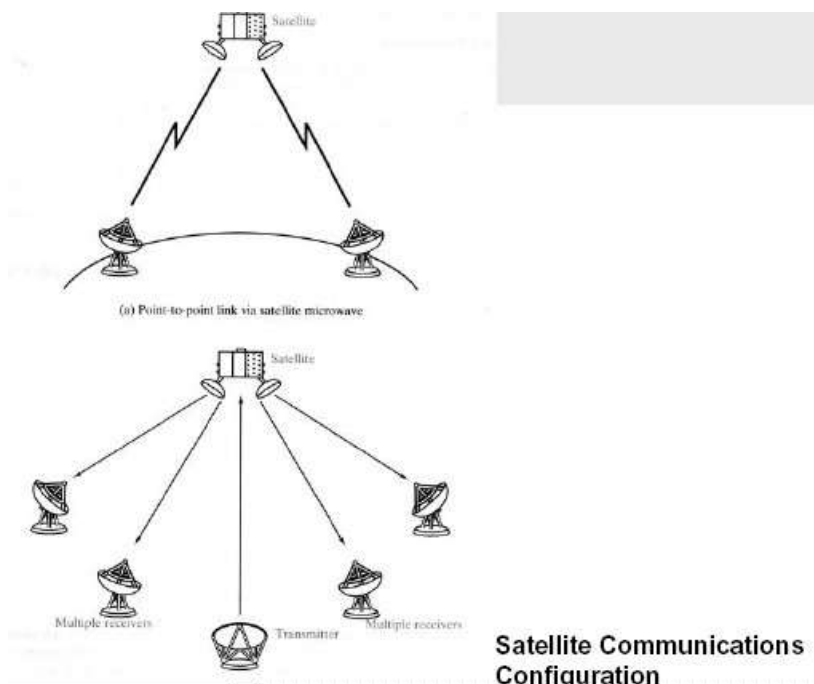
The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate. The Infrared Data Association (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers. For example, some manufacturers provide a special

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

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

## Satellite Microwave:

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



## VSAT (Very Small Aperture System)

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

# Hub

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

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

## How It Works

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

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

# Repeater

A networking component that extends a network by boosting the signal so that it can travel farther along the cabling.

## How It Works

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

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

Other uses for repeaters include the following:

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

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



# Introduction to Frame Relay, ATM, ISDN, PSTN, and X.25

## Virtual Circuit:

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

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

**A Permanent Virtual Circuit (PVC)** is a virtual circuit that is permanently available to the user. A PVC is defined in advance by a network manager. A PVC is used on a circuit that includes routers that must maintain a constant connection in order to transfer routing information in a dynamic network environment. Carriers assign PVCs to customers to reduce overhead and improve performance on their networks.

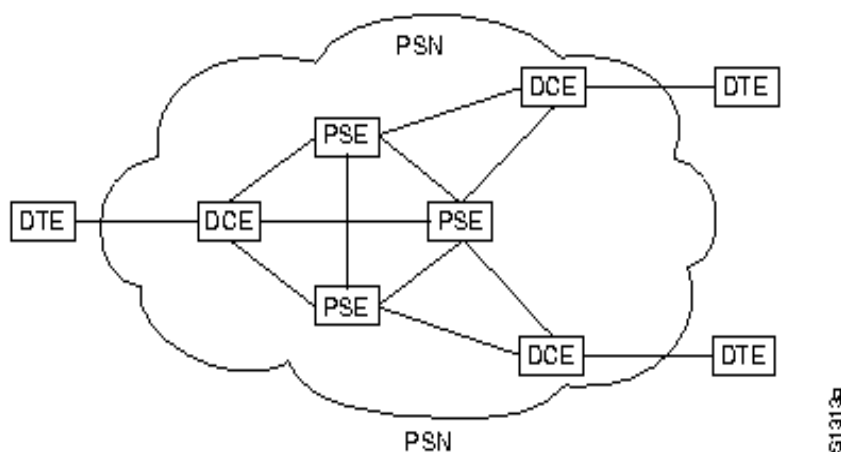
**A switched virtual circuit (SVC)** is a virtual circuit in which a connection session is set up dynamically between individual nodes temporarily only for the duration of a session. Once a communication session is complete, the virtual circuit is disabled.

## X.25:

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

X.25 defines a telephone network for data communications. To begin communication, one computer calls another to request a communication session. The called computer can accept or refuse the connection. If the call is accepted, the two systems can begin full-duplex information transfer. Either side can terminate the connection at any time.

The X.25 specification defines a point-to-point interaction between *data terminal equipment* (DTE) and *data communication equipment* (DCE). DTEs (terminals and hosts in the user's facilities) connect to DCEs (modems, packet switches, and other ports into the PDN, generally located in the carrier's facilities), which connect to *packet switching exchanges* (PSEs, or simply *switches*) and other DCEs inside a PSN and, ultimately, to another DTE. The relationship between the entities in an X.25 network is shown in Figure .



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

### How It Works

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

- The physical layer interface for connecting data terminal equipment (DTE), such as computers and terminals at the customer premises, with the data communications equipment (DCE), such as X.25 packet switches at the X.25 carrier's facilities. The physical layer interface of X.25 is called X.21bis and was derived from the RS-232 interface for serial transmission.
- The data-link layer protocol called Link Access Procedure, Balanced (LAPB), which defines encapsulation (framing) and error-correction methods. LAPB also enables the DTE or the DCE to initiate or terminate a communication session or initiate data transfer. LAPB is derived from the High-level Data Link Control (HDLC) protocol.
- The network layer protocol called the Packet Layer Protocol (PLP), which defines how to address and deliver X.25 packets between end nodes and switches on an X.25 network using permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). This layer is responsible for call setup and termination and for managing transfer of packets.

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

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

## **Disadvantages of X.25**

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

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

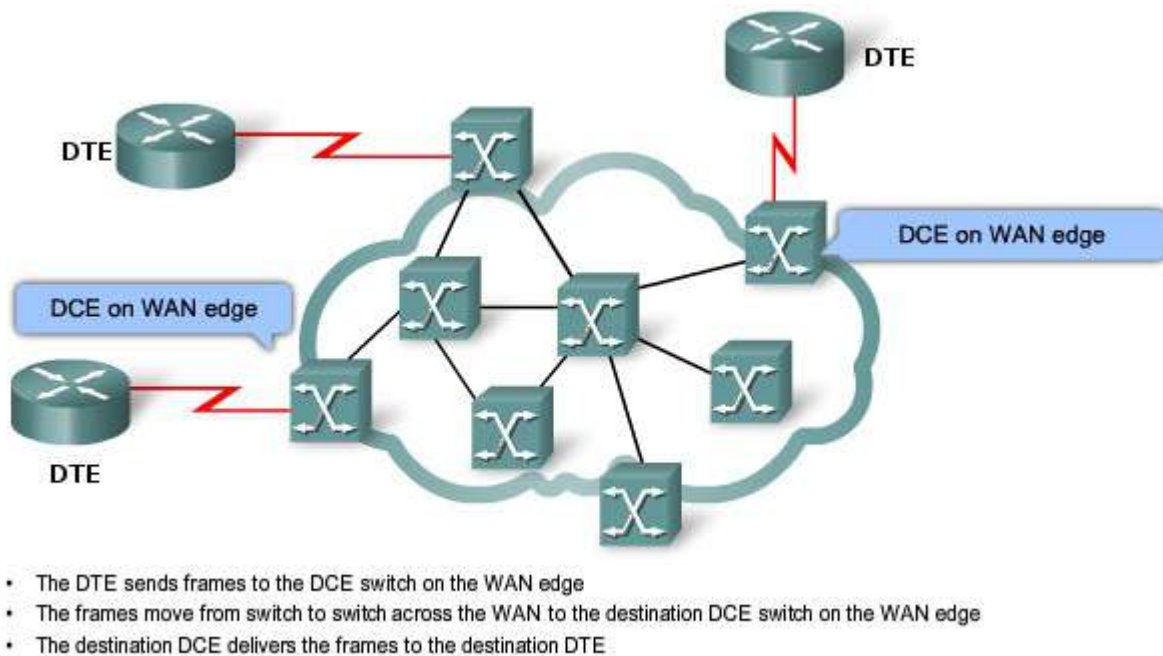
## **Frame Relay:**

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

1. Frame Relay operates at a higher speed (1.544 Mbps and recently 44.376 Mbps). This means that it can easily be used instead of a mesh of T-1 or T-3 lines.
2. Frame Relay operates in just the physical and data link layers. This means it can easily be used as a backbone network to provide services to protocols that already have a network layer protocol, such as the Internet.
3. Frame Relay allows bursty data.
4. Frame Relay allows a frame size of 9000 bytes, which can accommodate all local- area network frame sizes.
5. Frame Relay is less expensive than other traditional WANs.
6. Frame Relay has error detection at the data link layer only. There is no flow control or error control. There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame Relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers.

## **Frame Relay Operation:**

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



*Fig: Frame Relay Operation*

### Virtual Circuits :

The connection through a Frame Relay network between two DTEs is called a virtual circuit (VC). The circuits are virtual because there is no direct electrical connection from end to end. The connection is logical, and data moves from end to end, without a direct electrical circuit. With VCs, Frame Relay shares the bandwidth among multiple users and any single site can communicate with any other single site without using multiple dedicated physical lines.

### There are two ways to establish VCs:

#### Permanent Virtual Circuit(PVC):

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

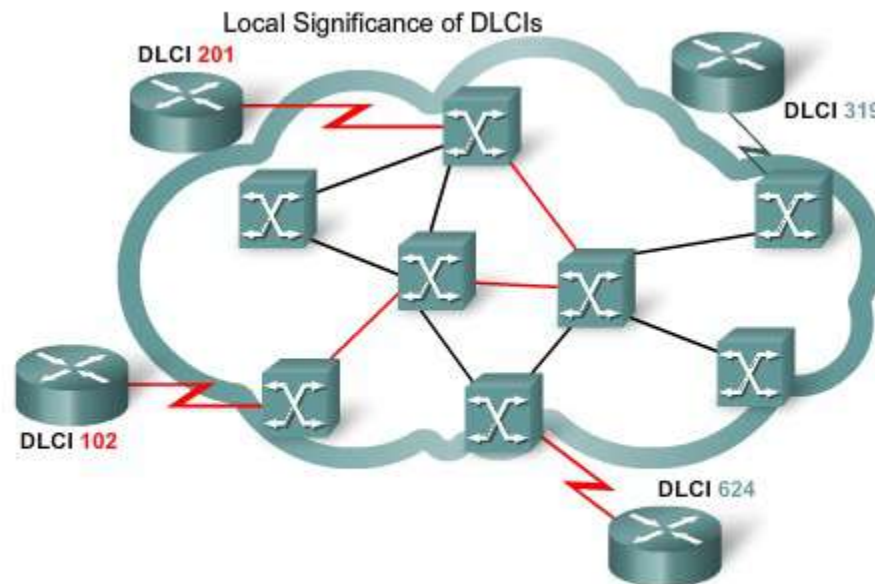
#### Switched Virtual-circuit(SVC):

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

#### DLCI (Data link connection identifier):

Frame Relay is a virtual circuit network. A virtual circuit in Frame Relay is identified by a number called a data link connection identifier (DLCI). DLCI values typically are assigned by the Frame Relay service provider (for example, the telephone company). Usually, DLCIs 0 to 15 and 1008 to 1023 are reserved for special purposes. Therefore, service providers typically assign DLCIs in the range of 16 to 1007. Frame Relay DLCIs have local

significance, which means that the values themselves are not unique in the Frame Relay WAN. A DLCI identifies a VC to the equipment at an endpoint. A DLCI has no significance beyond the single link. Two devices connected by a VC may use a different DLCI value to refer to the same connection.



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

### Frame Relay Layers:

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

#### Physical Layer

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

#### Data Link Layer

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

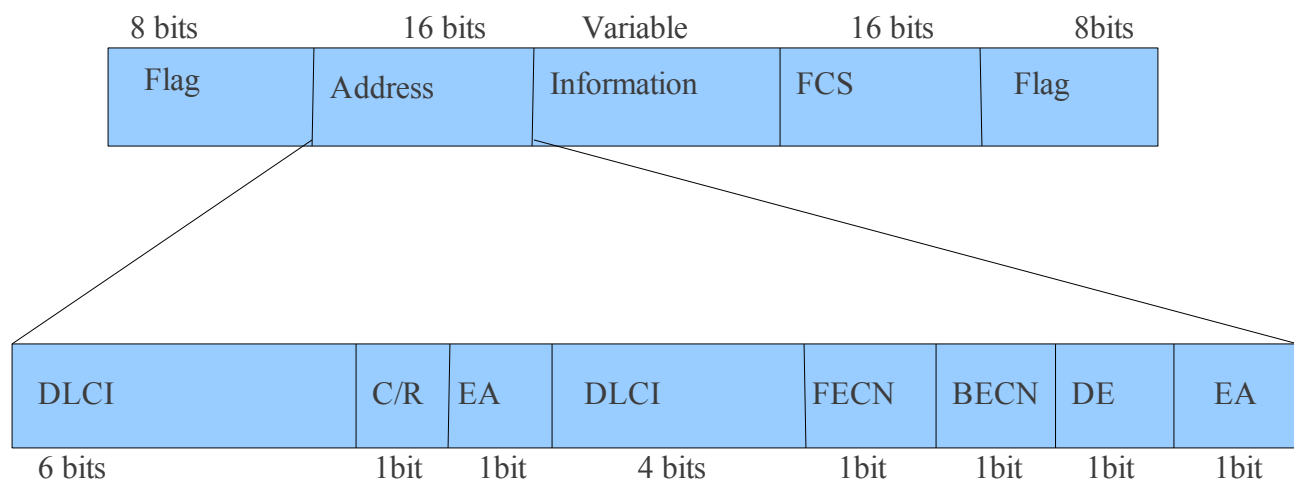


Fig:Frame Relay Frame Format

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

**Address (DLCI) field.** The first 6 bits of the first byte makes up the first part of the DLCI. The second part of the DLCI uses the first 4 bits of the second byte. These bits are part of the 10-bit data link connection identifier defined by the standard.

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

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

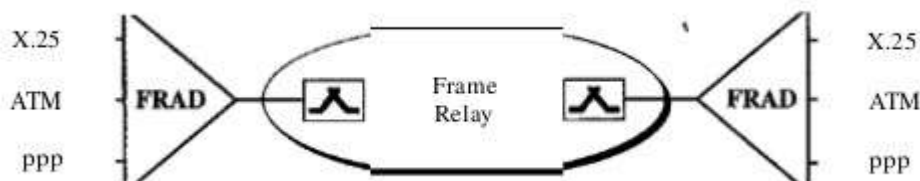
**Forward explicit congestion notification (FECN).** The forward explicit congestion notification (FECN) bit can be set by any switch to indicate that traffic is congested. This bit informs the destination that congestion has occurred. In this way, the destination knows that it should expect delay or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

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

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

### FRADs

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



## VOFR

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

## Local Management Information (LMI )

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

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

## Asynchronous Transfer Mode (ATM)

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

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

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

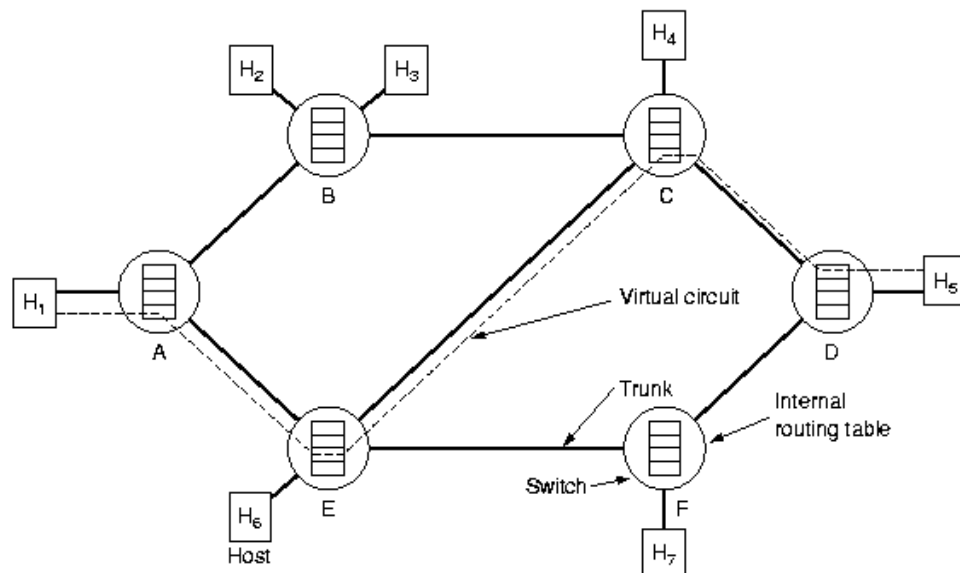


*Fig:ATM cell Format*

- Transmits all information in fixed size blocks called cells.
- Cells are transmitted asynchronously.
- The network is connection oriented.
- Each cell is 53 bytes long – 5 bytes header and 48 bytes payload.
- Making an ATM call requires first sending a message to set up a connection. Subsequently all cells follow the same path to the destination.

- ATM was envisioned as the technology for providing B-ISDN services.
- It can handle both constant rate traffic and variable-length traffic. Thus, it can carry multiple types of traffic with end-to-end quality of service.
- ATM is independent of transmission medium. It doesn't prescribe any particular rule.
- They may be sent on a wire or Fiber by themselves or they may be also packaged inside the payload of the other carrier system.
- Delivery of the system is not guaranteed but the order is.

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

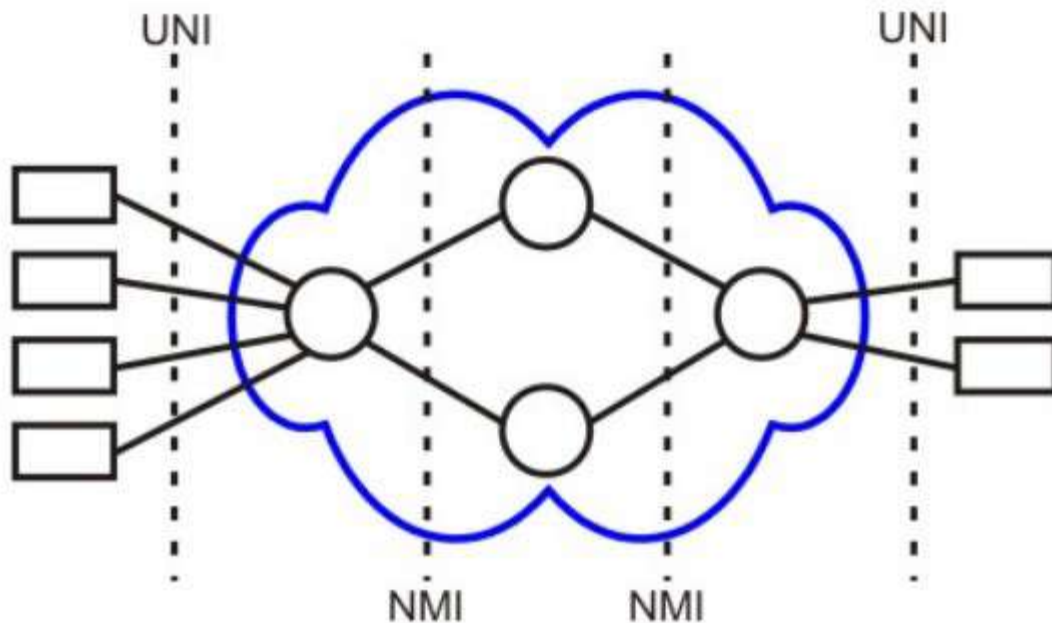


*Fig: Cells Traveling from Host#1 to Host#5:-*

### **ATM Network Interfaces :**

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





*Fig: UNI and NNI interfaces of the ATM*

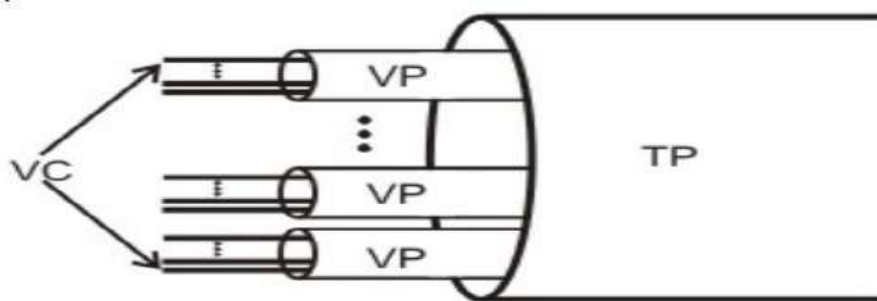
### ATM Virtual Connections

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

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

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

*A virtual path connection (VPC) is a bundle of VCCs that have the same endpoints. Thus, all of the cells flowing over all of the VCCs in a single VPC are switched together*



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

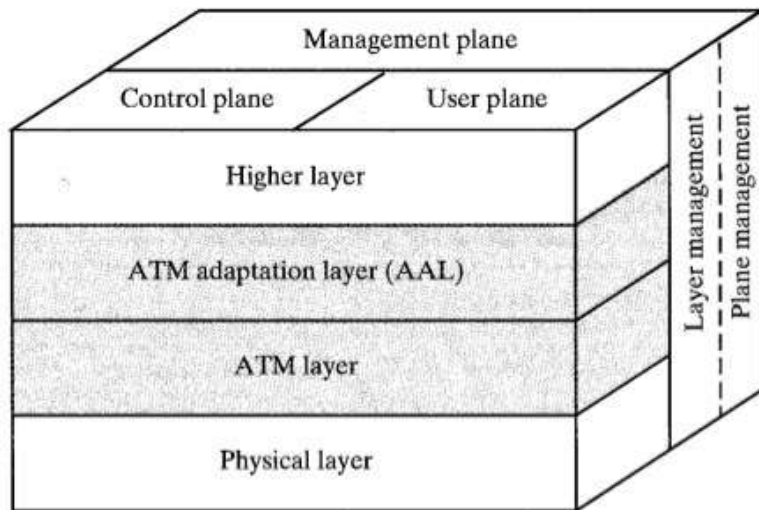
**ATM Reference Model:**

The protocol reference model makes reference to three separate planes:

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

**Control Plane.** Performs call control and connection control functions.

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



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

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

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

**ATM Advantages:**

- ATM supports voice, video and data allowing multimedia and mixed services over a single network.
- high evolution potential, works with existing, legacy technologies
- provides the best multiple service support
- supports delay close to that of dedicated services
- supports the broadest range of burstiness, delay tolerance and loss performance through the implementation of multiple QoS classes
- provides the capability to support both connection-oriented and connectionless traffic using AALs
- able to use all common physical transmission paths (such as DS1, SONET).
- cable can be twisted-pair, coaxial or fiber-optic
- ability to connect LAN to WAN
- legacy LAN emulation
- efficient bandwidth use by statistical multiplexing

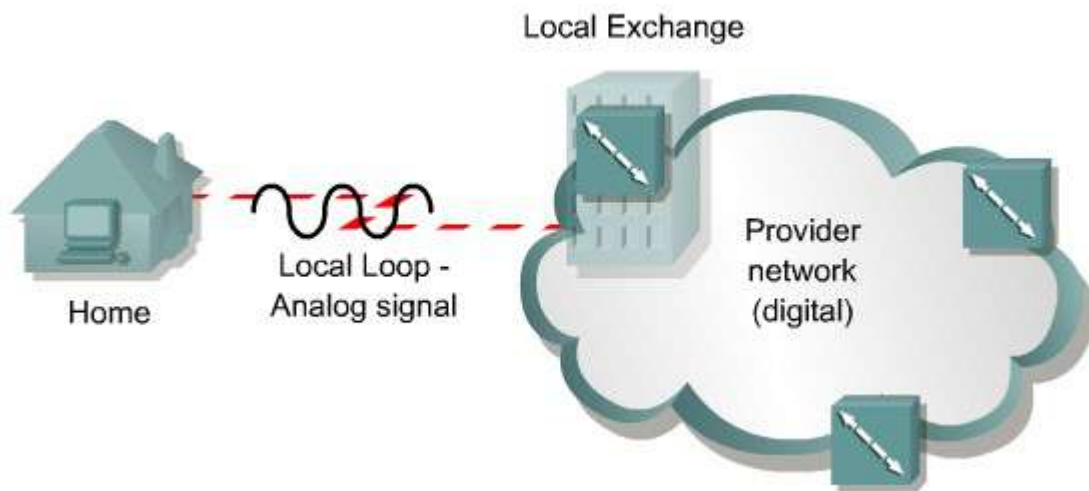
- scalability
- higher aggregate bandwidth
- high speed Mbps and possibly Gbps

#### ATM disadvantages

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

## Integrated Service Digital Network: (ISDN)

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



*fig1: Analog Communication without ISDN*

The traditional PSTN was based on an analog connection between the customer premises and the local exchange, also called the local loop. Fig 1 The analog circuits introduce limitations on the bandwidth that can be obtained on the local loop. Circuit restrictions do not permit analog bandwidths greater than approximately 3000 Hz. ISDN technology permits the use of digital data on the local loop, providing better access speeds for the remote users fig2.

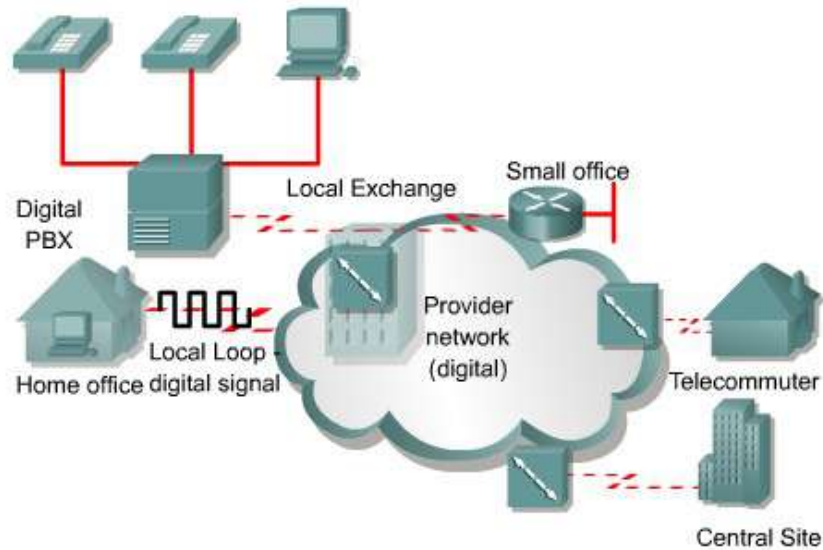
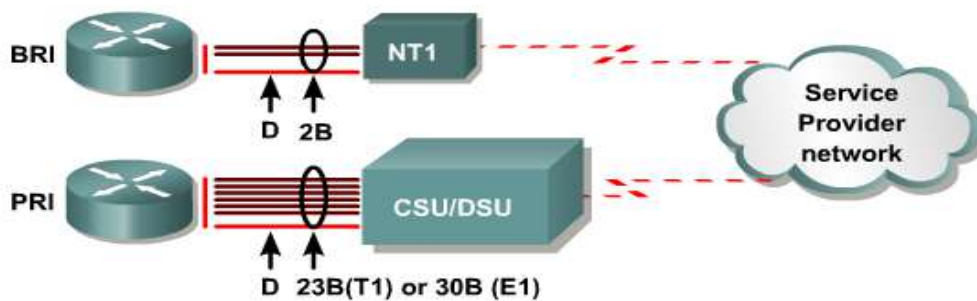


Fig2: Digital Communication with ISDN

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

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

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



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

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

### Basic Rate Interface (BRI):

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



The capacity of the BRI is therefore:

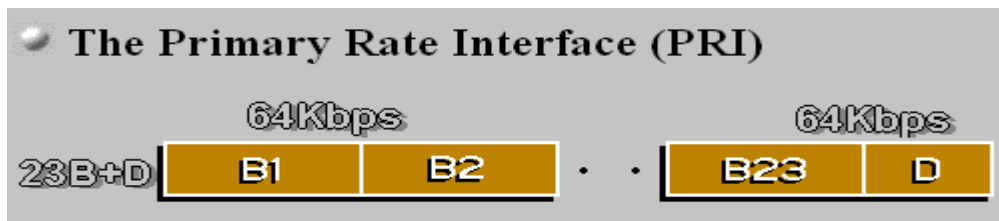
- two voice, two high-speed data or
- one voice and one high-speed data plus 16kbps packet data

BRI can carry a wide and flexible range of communications. A single BRI, for example, can carry two simultaneous voice or data conversations (to the same or different locations).

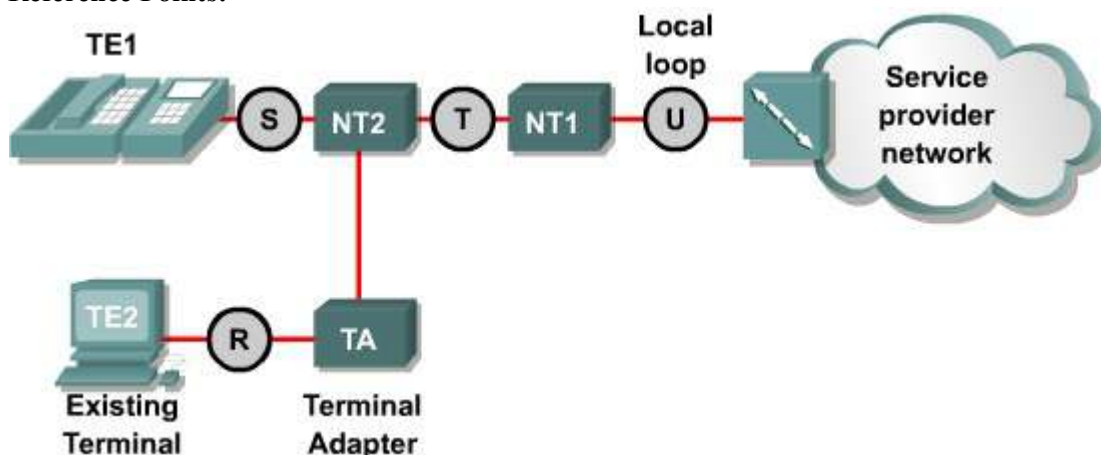
The D-channel can also be used for packet communications to a third location, also simultaneously.

### PRI (Primary Rate Interface):

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



### ISDN Reference Points:



- **R** — References the connection between a non-ISDN compatible device Terminal Equipment type 2 (TE2) and a Terminal Adapter (TA), for example an RS-232 serial interface.
- **S** — References the points that connect into the customer switching device Network Termination type 2 (NT2) and enables calls between the various types of customer premises equipment.
- **T** — Electrically identical to the S interface, it references the outbound connection from the NT2 to the ISDN network or Network Termination type 1 (NT1).
- **U** — References the connection between the NT1 and the ISDN network owned by the telephone company.

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

## Public Switched Telephone Network(PSTN)

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

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

PSTN, the Public Switched Telephone Network, is a circuit-switched network that is used primarily for voice communications worldwide, with more than 800 million subscribers. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital and also includes mobile as well as fixed telephones. The basic digital circuit in the PSTN is a 64-kilobit-per-second channel, known as "DS0" or Digital Signal 0. DS0's are also known as timeslots because they are multiplexed together in a time-division fashion. To carry a typical phone call from a calling party to a called party, the audio sound is digitized at an 8 kHz sample rate using 8-bit pulse code modulation.

Multiple DS0's can be multiplexed together on higher capacity circuits, such that 24 DS0's make a DS1 signal or T1 (the European equivalent is an E1, containing 32 64 kbit/s channels).

For more than a hundred years, the PSTN was the only bearer network available for telephony. Today, the mobile telephone over wireless access network, which is carried through the PSTN trunking network, is becoming

increasingly popular. Other bearer networks for voice transmission include integrated service digital network (ISDN), Digital Subscriber Line (DSL), Asynchronous Transfer Mode (ATM), frame relay and the Internet VOIP.

#### **T-1 & E-1 Circuit:**

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

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

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

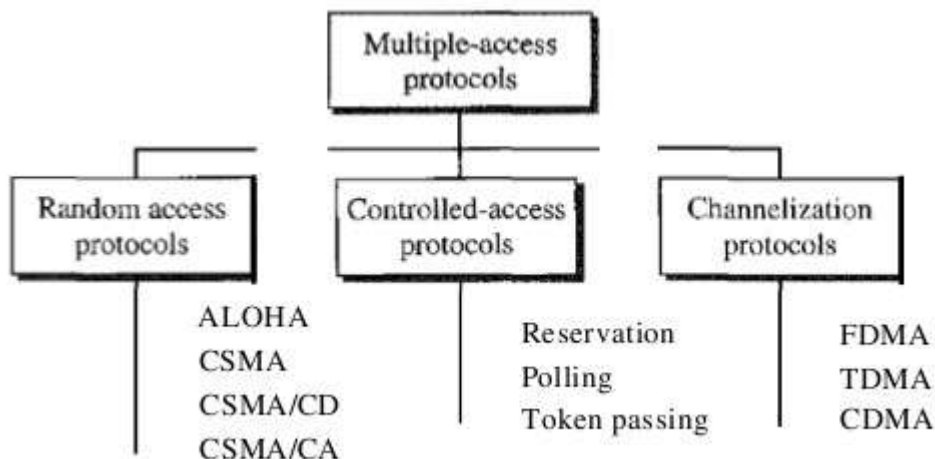
A T1/E1 circuit is the first multiplexed level of the digital signalling multiplexing scheme. T1s use what is called a Stratum 3 clock to maintain what is called clocking on the line.

## Chapter5: Data Link layers

Services and Data Link Devices (Switch, Bridge); Framing, Flow Control and Error Control; Elementary Data link Protocols; Sliding Window Protocols; HDLC, SLIP and PPP Media Access Control Layer ( Carrier Sense Multiple Access/ Collision Detection)

### Multiple Access

The upper sublayer of Datalink layer, that is responsible for flow and error control is called the logical link control (LLC) layer; the lower sublayer that is mostly responsible for multiple- access resolution is called the media access control (MAC) layer.



According to CSMA/CD, a node should not send a packet unless the network is clear of traffic. If two nodes send packets at the same time, a collision occurs and the packets are lost. Then both nodes send a jam signal, wait for a random amount of time, and retransmit their packets. Any part of the network where packets from two or more nodes can interfere with each other is considered a collision domain. A network with a larger number of nodes on the same segment has a larger collision domain and typically has more traffic. As the amount of traffic in the network increases, the likelihood of collisions increases.

#### CSMA/CD Algorithm:

1. If the medium is idle, transmit; otherwise, go to step 2.
2. If the medium is busy, continue to listen until the channel is idle, then transmit immediately.
3. If a collision is detected during transmission, transmit a brief jamming signal to assure that all stations know that there has been a collision and then cease transmission.
4. After transmitting the jamming signal, wait a random amount of time, then attempt to transmit again.  
(Repeat from step 1.)

Traditional Ethernet uses CSMA/CD.

### Bridge:

A networking component used either to extend or to segment networks. Bridges work at the OSI data-link layer. They can be used both to join dissimilar media such as unshielded twisted-pair (UTP) cabling and fiber-optic cabling, and to join different network architectures such as Token Ring and Ethernet. Bridges regenerate signals



but do not perform any protocol conversion, so the same networking protocol (such as TCP/IP) must be running on both network segments connected to the bridge. Bridges can also support Simple Network Management Protocol (SNMP), and they can have other diagnostic features.

### How it works?

Bridges operate by sensing the source MAC addresses of the transmitting nodes on the network and automatically building an internal routing table. This table is used to determine which connected segment to route packets to, and it provides the filtering capability that bridges are known for. If the bridge knows which segment a packet is intended for, it forwards the packet directly to that segment. If the bridge doesn't recognize the packet's destination address, it forwards the packet to all connected segments except the one it originated on. And if the destination address is in the same segment as the source address, the bridge drops the packet. Bridges also forward broadcast packets to all segments except the originating one.

## Hub:

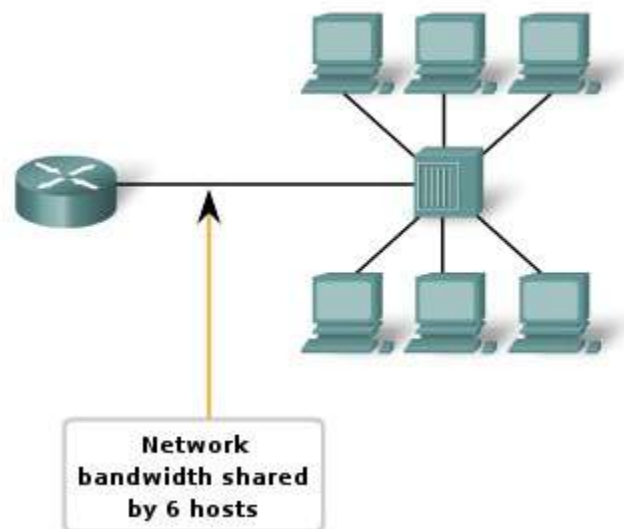
**The basic networking component used in traditional 10-Mbps Ethernet networks to connect network stations to form a local area network (LAN). Hubs can be used for**

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

### How It Works

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

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



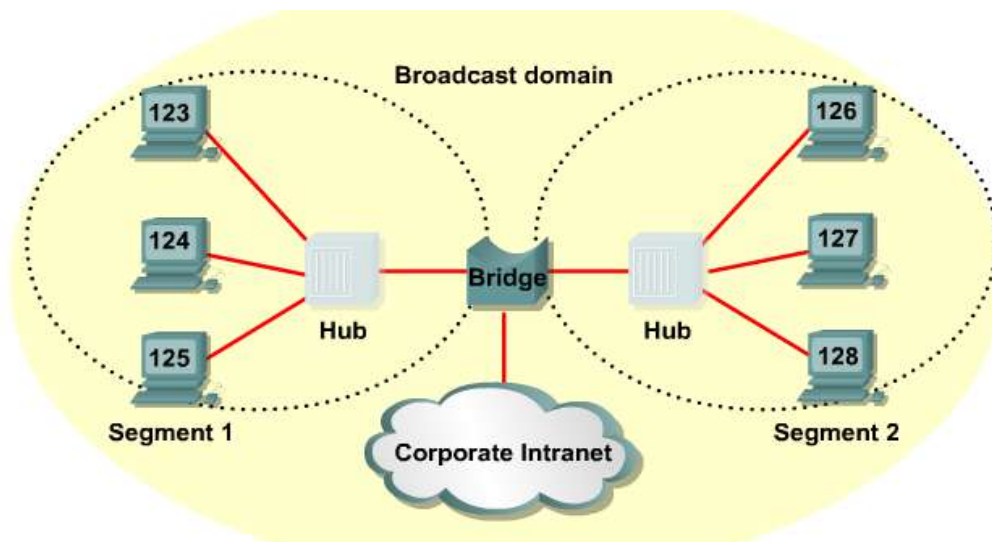
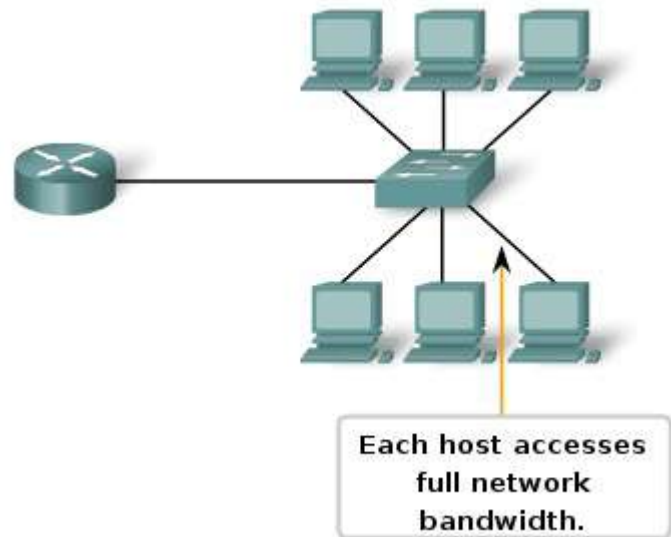
## Switch:

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

### Why Switches:

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

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



### Hub VS Switch:

Hub	Switch
Works on physical layer	Works on Datalink layer
Half-duplex	Full Duplex
Hub extends the collision domain	Switch splits the collision domain (Each port of the switch acts as a collision domain)
Multiport Repeater	Multiport Bridge
Overall Bandwidth is shared	Each port receives its own bandwidth.

Cheap	Expensive
Not used in todays market due to degraded performance	Mostly used today.

**There are three forwarding methods a switch can use:**

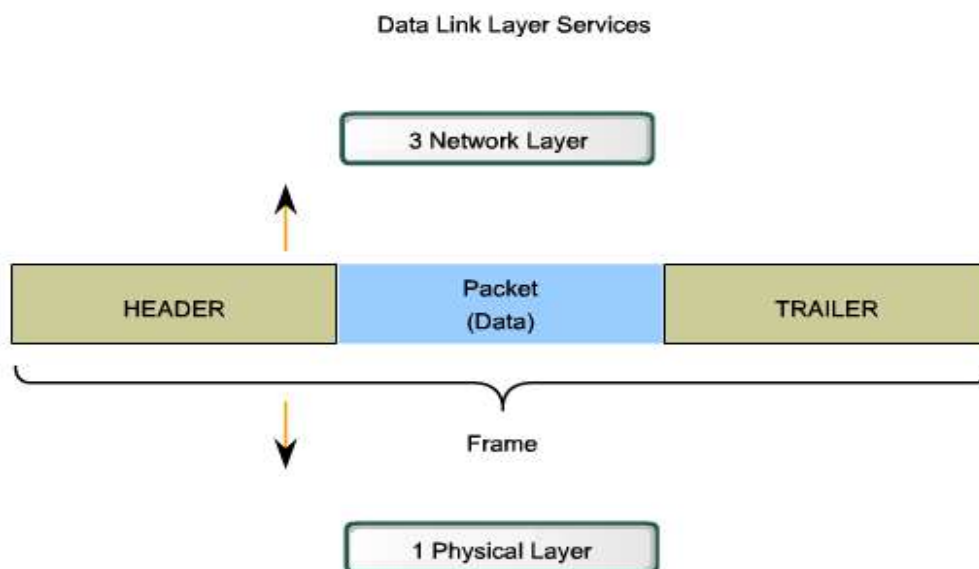
- Cut through (cut-through switching is a switching method for packet switching systems, wherein the switch starts forwarding that frame (or packet) before the whole frame has been received, normally as soon as the destination address is processed. This technique reduces latency through the switch, but decreases reliability.)
- Store and forward - the switch, unlike cut through, buffers and typically, performs a checksum on each frame before forwarding it on.
- Fragment free (Fragment-free switching is suitable for backbone applications in a congested network, or when connections are allocated to a number of users. The packets are sent through the switch as a continuous flow of data--the transmit and receive rates are always the same. Because of this, fragment-free switching cannot pass packets to higher speed networks, for example, to forward packets from a 10 Mbit/s to a 100 Mbit/s Ethernet network. Therefore, if you opt for fragment-free switching, you cannot make direct connections to higher speed networks from that port.)

## Framing:

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

The Data Link layer frame includes:

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



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

## Fixed-Size Framing

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

## Variable-Size Framing

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

### Character-Oriented Protocols

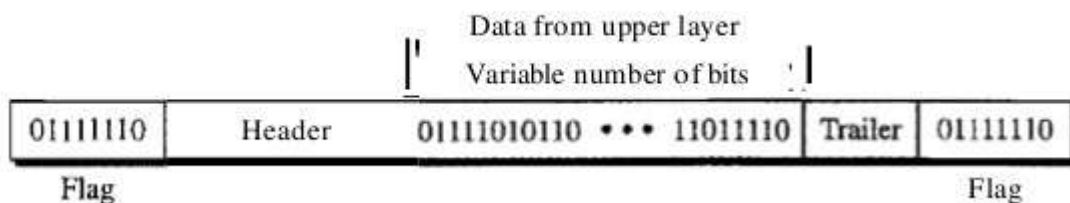
In a character-oriented protocol, data to be carried are 8-bit characters from a coding system such as ASCII (see Appendix A). The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits. To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame .

Any pattern used for the flag could also be part of the information. To fix this problem, **a byte-stuffing** strategy was added to character-oriented framing. In **byte stuffing (or character stuffing)**, a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

Character-oriented protocols present a problem in data communications. The universal coding systems in use today, such as Unicode, have 16-bit and 32-bit characters that conflict with 8-bit characters. We can say that in general, the tendency is moving toward the bit-oriented protocols that we discuss next.

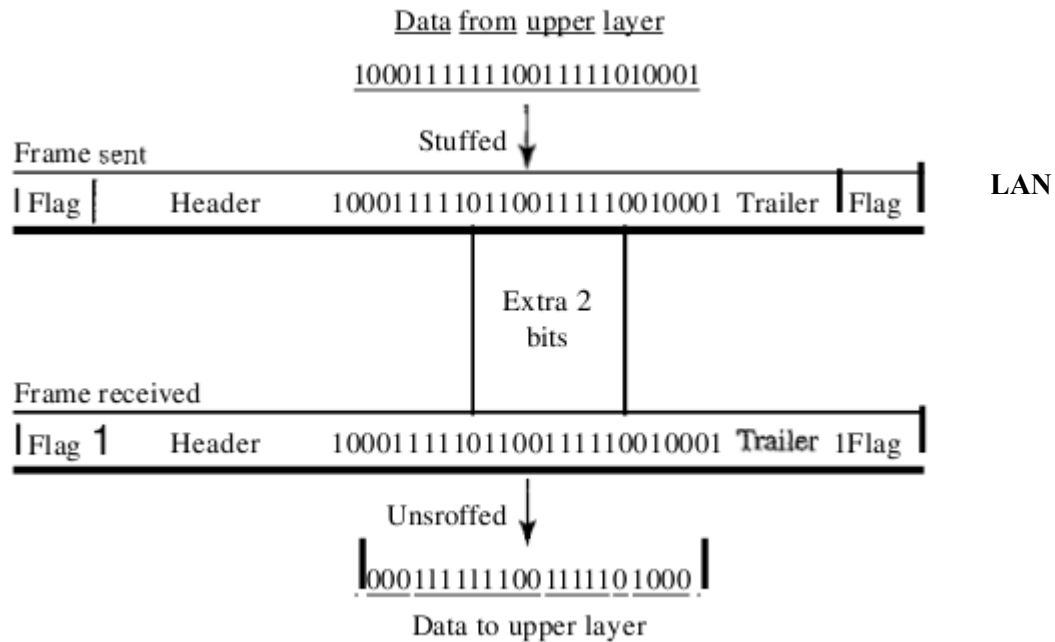
### Bit-Oriented Protocols

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



*Fig:A frame in a bit-oriented protocol*

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



*Fig: Bit Stuffing and unstuffing*

*This means that if the flaglike pattern 01111110 appears in the data, it will change to 011111010 (stuffed) and is not mistaken as a flag by the receiver. The real flag 01111110 is not stuffed by the sender and is recognized by the receiver.*

#### **Architecture:**

The architecture of a LAN can be considered as a set of layered protocols.

In OSI terms, the higher layer protocols are totally independent of the LAN architecture. Hence, only lower order layers are considered for the design of LAN architecture.

The datalink layer of LAN is split into two sub layers.

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

The IEEE 802 committee had formulated the standards for LAN.

## IEEE Standards:

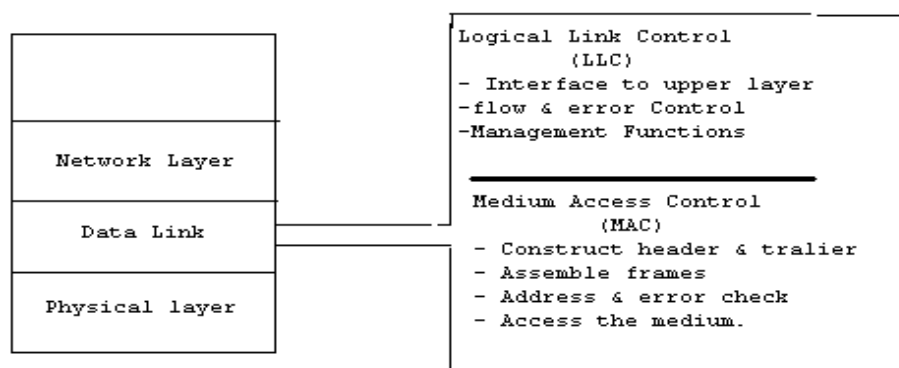
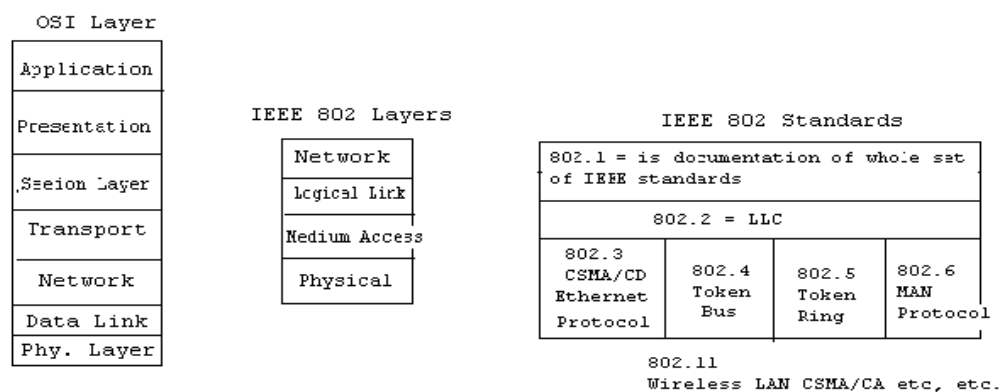


Fig:-OSI Layers for LAN

## LLC Frame Format:

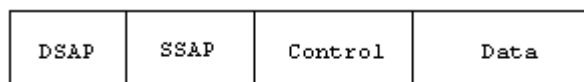


Fig :- LLC Frame Format

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

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

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

- **Information (I) frame** -- Carries upper-layer information and some control information.
- **Supervisory (S) frame** -- Provides control information. An S frame can request and suspend

transmission, reports on status, and acknowledge receipt of I frames. S frames do not have an Information field.

- **Unnumbered (U) frame** -- Used for control purposes and is not sequenced. A U frame can be used to initialize secondaries. Depending on the function of the U frame, its Control field is 1 or 2 bytes. Some U frames have an Information field.

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

### MAC Frame Format:

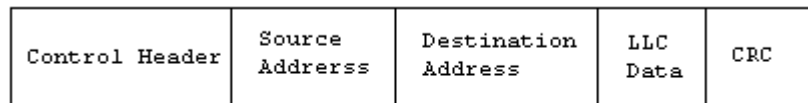
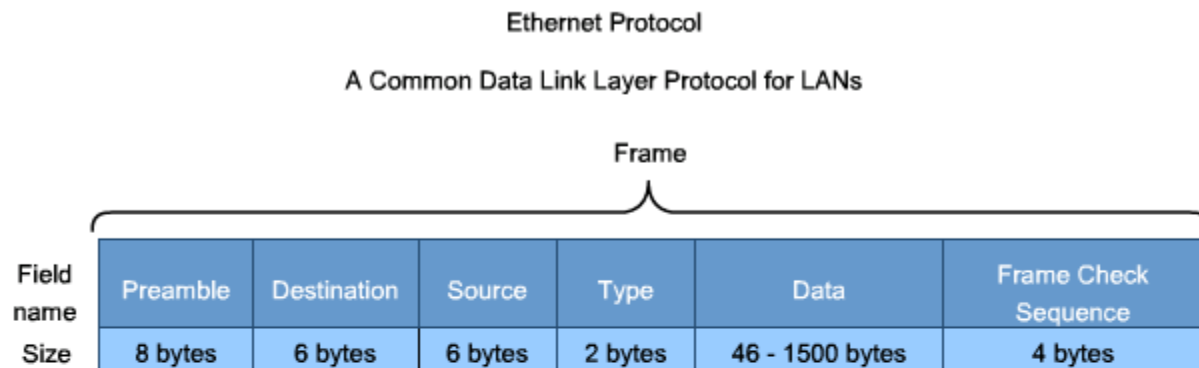


Fig : General MAC frame Format

### **IEEE 802.3 Ethernet Frame Format:**



**Preamble** - used for synchronization; also contains a delimiter to mark the end of the timing information.

**Destination Address** - 48 bit MAC address for the destination node.

**Source Address** - 48 bit MAC address for the source node.

**Type** - value to indicate which upper layer protocol will receive the data after the Ethernet process is complete.

**Data or payload** - this is the PDU, typically an IPv4 packet, that is to be transported over the media.

**Frame Check Sequence (FCS)** - A value used to check for damaged frames.

## **Flow Control:**

Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data. Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver.

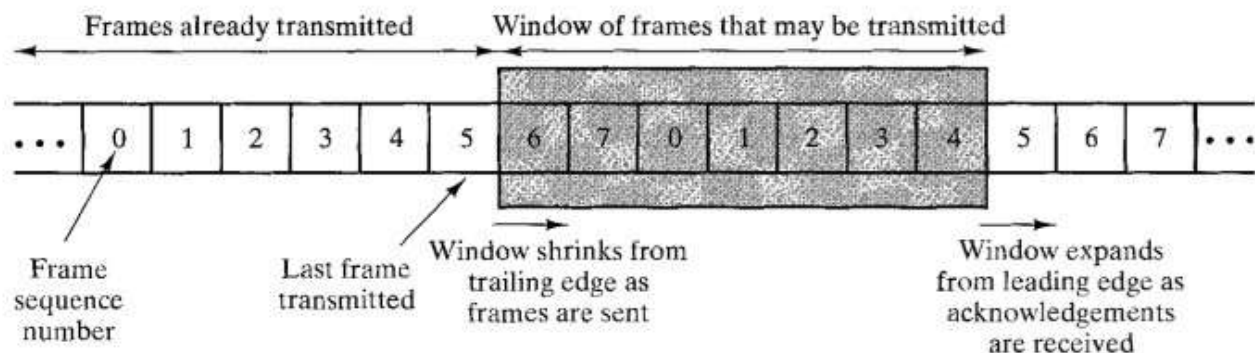
## Stop and wait Flow Control:

A source entity transmits a frame. After reception, the destination entity indicates its willingness to accept another frame by sending back an acknowledgment to the frame just received. The source must wait until it receives the acknowledgment before sending the next frame. The source must wait until it receives the acknowledgment before sending the next frame. The destination can thus stop the flow of data by simply withholding acknowledgment. With the use of multiple frames for a single message, the stop-and-wait procedure may be inadequate. The essence of the problem is that only one frame at a time can be in transit. For very high data rates, or for very long distances between sender and receiver, stop- and-wait flow control provides inefficient line utilization.

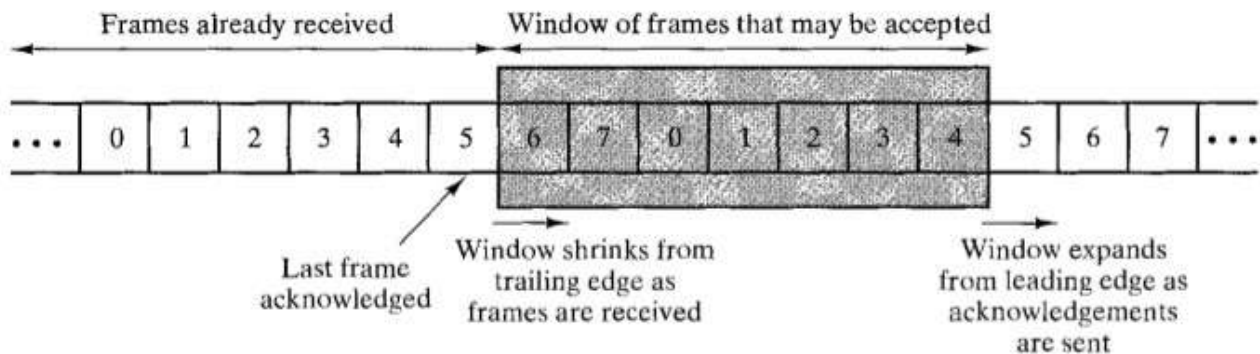
## Sliding Window Flow Control:

Major draw back of stop-and-wait flow control is only one frame can be transmitted at a time; this leads to inefficiency if propagation delay is much longer than transmission delay. Sliding window flow control allows the transmission of multiple frame. It assigns each frame a k-bit sequence number and the range of sequence no. is  $[0..2^k - 1]$ .

Let us examine how this might work for two stations, A and B, connected via a full-duplex link. Station B allocates buffer space for n frames. Thus, B can accept n frames, and A is allowed to send n frames without waiting for any acknowledgments. To keep track of which frames have been acknowledged, each is labeled with a sequence number. B acknowledges a frame by sending an acknowledgment that includes the sequence number of the next frame expected. This acknowledgment also implicitly announces that B is prepared to receive the next n frames, beginning with the number specified. This scheme can also be used to acknowledge multiple frames



(a) Transmitter's perspective



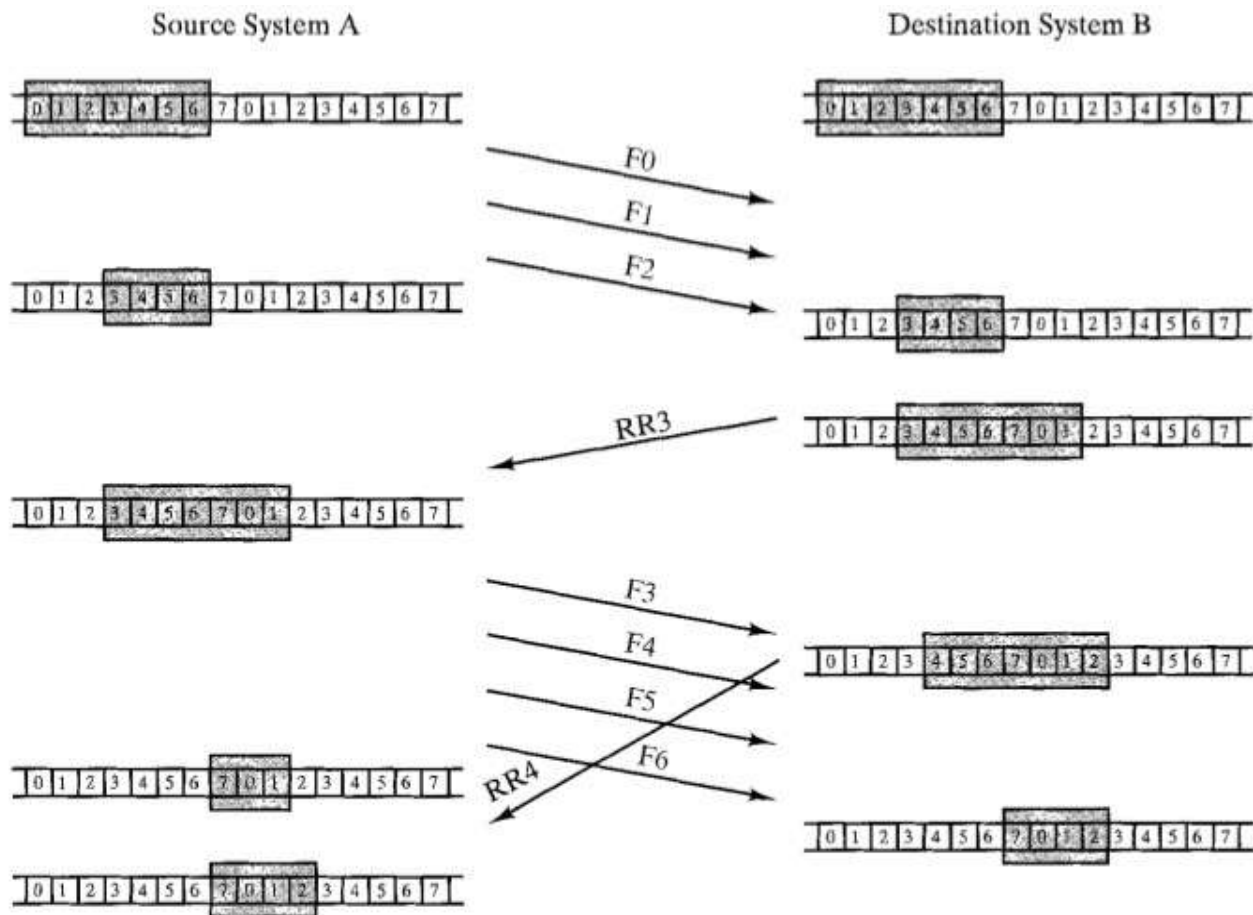
(b) Receiver's perspective



### How Flow control is achieved?

- Receiver can control the size of the sending window.
- By limiting the size of the sending window data flow from sender to receiver can be limited .

The example assumes a 3-bit sequence number field and a maximum window size of seven frames. Initially, A and B have windows indicating that A may transmit seven frames, beginning with frame 0 (F0). After transmitting three frames (F0, F1, F2) without acknowledgment, A has shrunk its window to four frames. The window indicates that A may transmit four frames, beginning with frame number 3. B then transmits an RR (receive-ready) 3, which means: "I have received all frames up through frame number 2 and am ready to receive frame number 3; in fact, I am prepared to receive seven frames, beginning with frame number 3." With this acknowledgment, A is back up to permission to transmit seven frames, still beginning with frame 3. A proceeds to transmit frames 3, 4, 5, and 6. B returns an RR 4, which allows A to send up to and including frame F2.



*Example of Sliding window Protocol*

## Error Control:

When data is transmitted over a cable or channel, there is always a chance that some of the bits will be changed (corrupted) due to noise, signal distortion or attenuation. If errors do occur, then some of the bits will either change from 0 to 1 or from 1 to 0.

Error Control allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. Error control is divided in two main categories:

Error Detection It allows a receiver to check whether received data has been corrupted during transmission. It can, for example, request a retransmission.

Error Correction This type of error control allows a receiver to reconstruct the original information when it has been corrupted during transmission.

In the data link layer, the term error control refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

*Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.*

There are 2 ways to correct found errors:

- Forward error correction (FEC is accomplished by adding redundancy to the transmitted information using a predetermined algorithm. Each redundant bit is invariably a complex function of many original information bits. The original information may or may not appear in the encoded output; codes that include the unmodified input in the output are systematic, while those that do not are nonsystematic.) and
- Automatic repeat request (ARQ) ( in which the receiver detects transmission errors in a message and automatically requests a retransmission from the transmitter. Usually, when the transmitter receives the ARQ, the transmitter retransmits the message until it is either correctly received or the error persists beyond a predetermined number of retransmissions. A few types of ARQ protocols are Stop-and-wait ARQ, Go-Back-N ARQ and Selective Repeat ARQ).

## Hamming distance:

One of the central concepts in coding for error control is the idea of the Hamming distance. The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. We show the Hamming distance between two words  $x$  and  $y$  as  $d(x, y)$ . The Hamming distance can easily be found if we apply the XOR operation on the two words and count the number of 1s in the result. Note that the Hamming distance is a value greater than zero.

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

1. The Hamming distance  $d(000, 011)$  is 2 because  $000 \text{ XOR } 011$  is  $011$  (two 1s).
2. The Hamming distance  $d(10101, 11110)$  is 3 because  $10101 \text{ XOR } 11110$  is  $01011$  (three 1s).

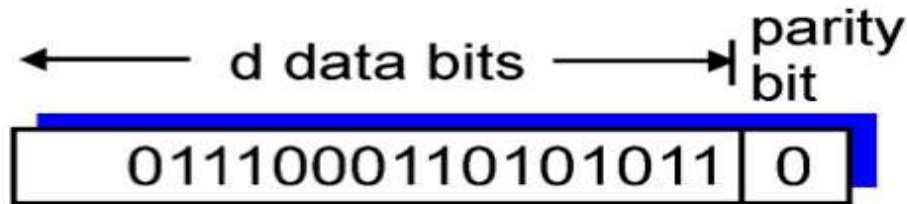
## Error Detection:

There are three ways to detect errors.

1. Parity check
2. CRC
3. Checksum

## 1. Parity Check:

The simplest error-detection scheme is to append a parity bit to the end of a block of data. A typical example is ASCII transmission, in which a parity bit is attached to each 7-bit ASCII character. The value of this bit is selected so that the character has an even number of 1s (even parity) or an odd number of 1s (odd parity).

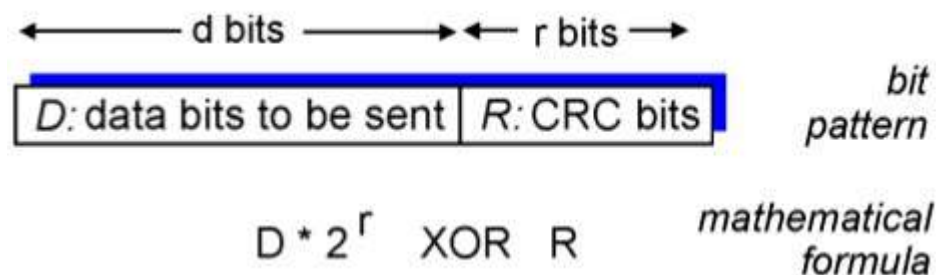


*One bit Even Parity*

So, for example, if the transmitter is transmitting an ASCII G (1110001) and using odd parity, it will append a 1 and transmit 11100011. The receiver examines the received character and, if the total number of 1s is odd, assumes that no error has occurred. If one bit (or any odd number of bits) is erroneously inverted during transmission (for example, 11QO0011), then the receiver will detect an error. Note, however, that if two (or any even number) of bits are inverted due to error, an undetected error occurs. Typically, even parity is used for synchronous transmission and odd parity for asynchronous transmission. The use of the parity bit is not foolproof, as noise impulses are often long enough to destroy more than one bit, particularly at high data rates.

## 2. Cyclic Redundancy Check:

CRC codes operate as follows. Consider the  $d$ -bit piece of data,  $D$ , that the sending node wants to send to the receiving node. The sender and receiver must first agree on a  $r+1$  bit pattern, known as a generator, which we will denote as  $G$ . We will require that the high and low order bits of  $G$  must be 1 (e.g., 10111 is acceptable, but 0101 and 10110 are not). The key idea behind CRC codes is shown in Figure. For a given piece of data,  $D$ , the sender will choose  $r$  additional bits,  $R$ , and append them to  $D$  such that the resulting  $d+r$  bit pattern (interpreted as a binary number) is exactly divisible by  $G$  using modulo 2 arithmetic. The process of error checking with CRC's is thus simple: the receiver divides the  $d+r$  received bits by  $G$ . If the remainder is non-zero, the receiver knows that an error has occurred; otherwise the data is accepted as being correct.



All CRC calculations are done in modulo 2 arithmetic without carries in addition or borrows in subtraction. This means that addition and subtraction are identical, and both are equivalent to the bitwise exclusive-or (XOR) of the operands. Thus, for example,

$$1011 \text{ XOR } 0101 = 1110$$

$$1001 \text{ XOR } 1101 = 0100$$

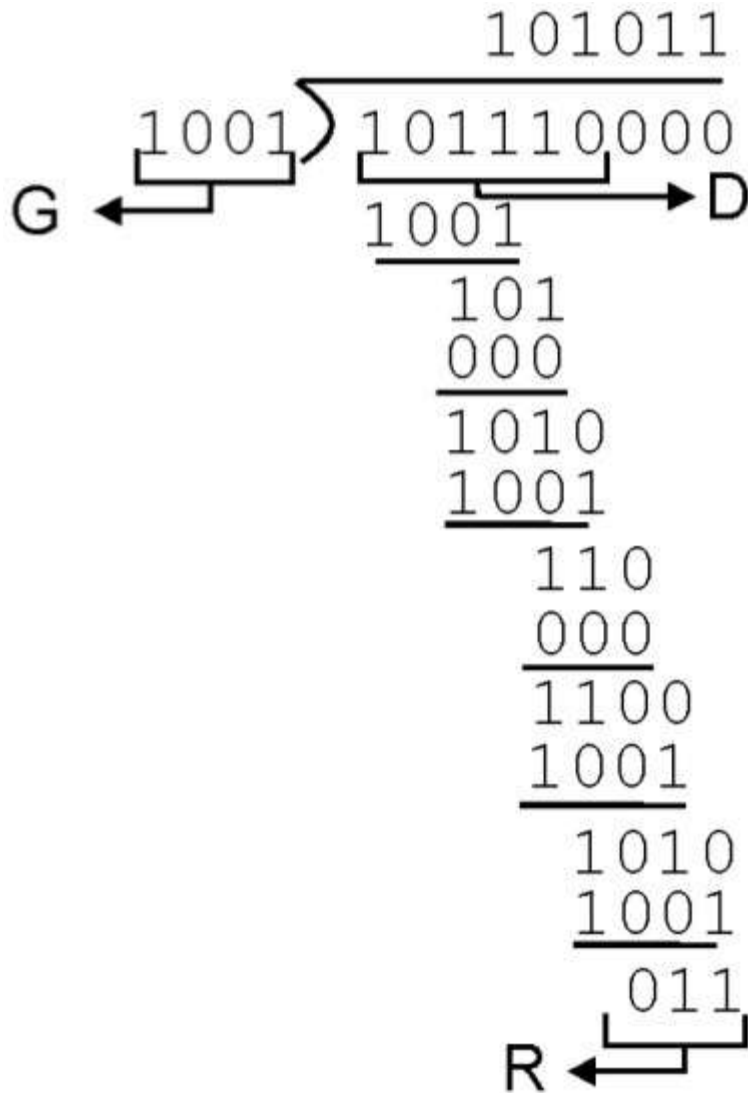
Also, we similarly have

$$\begin{array}{r} 1011 - 0101 = 1110 \\ 1001 - 1101 = 0100 \end{array}$$

Multiplication and division are the same as in base 2 arithmetic, except that any required addition or subtraction is done without carries or borrows. As in regular binary arithmetic, multiplication by  $2^k$  left shifts a bit pattern by k places. Thus, given D and R, the quantity  $D \cdot 2^r \text{ XOR } R$  yields the d+r bit pattern shown in Figure above.

International standards have been defined for 8-, 12-, 16- and 32-bit generators,  $G$ . An 8-bit CRC is used to protect the 5-byte header in ATM cells.

Figure below illustrates this calculation for the case of  $D = 101110$ ,  $d = 6$  and  $G = 1001$ ,  $r=3$ . The nine bits transmitted in this case are 101110 011. You should check these calculations for yourself and also check that indeed  $D2^r = 101011 * G \text{ XOR } R$ .



A second way to viewing the CRC process is to express all values as polynomials in a dummy variable  $X$ , with binary coefficients. The coefficients corresponds to the bits in the binary number. Thus for  $D=110011$  we have,  $D(X)=X^5+X^4+X+1$  for  $P=11001$  we have  $P(X)=X^4+X^3+1$ . Arithmetic operations are again modulo 2.

### 3. Checksum:

The checksum is used in the Internet by several protocols although not at the data link layer. However, we briefly discuss it here to complete our discussion on error checking.

Example1:

Suppose our data is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12, 0, 6, 36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise, there is an error somewhere and the data are not accepted.

Example2:

We can make the job of the receiver easier if we send the negative (complement) of the sum, called the checksum. In this case, we send (7, 11, 12, 0, 6, -36). The receiver can add all the numbers received (including the checksum). If the result is 0, it assumes no error; otherwise, there is an error

#### Internet Checksum

Traditionally, the Internet has been using a 16-bit checksum. The sender calculates the checksum by following these steps.

##### Sender site:

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

The receiver uses the following steps for error detection.

##### Receiver site:

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

### Error Correction:

Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ). *Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.*

#### Three versions of ARQ have been standardized:

Stop-and-wait ARQ

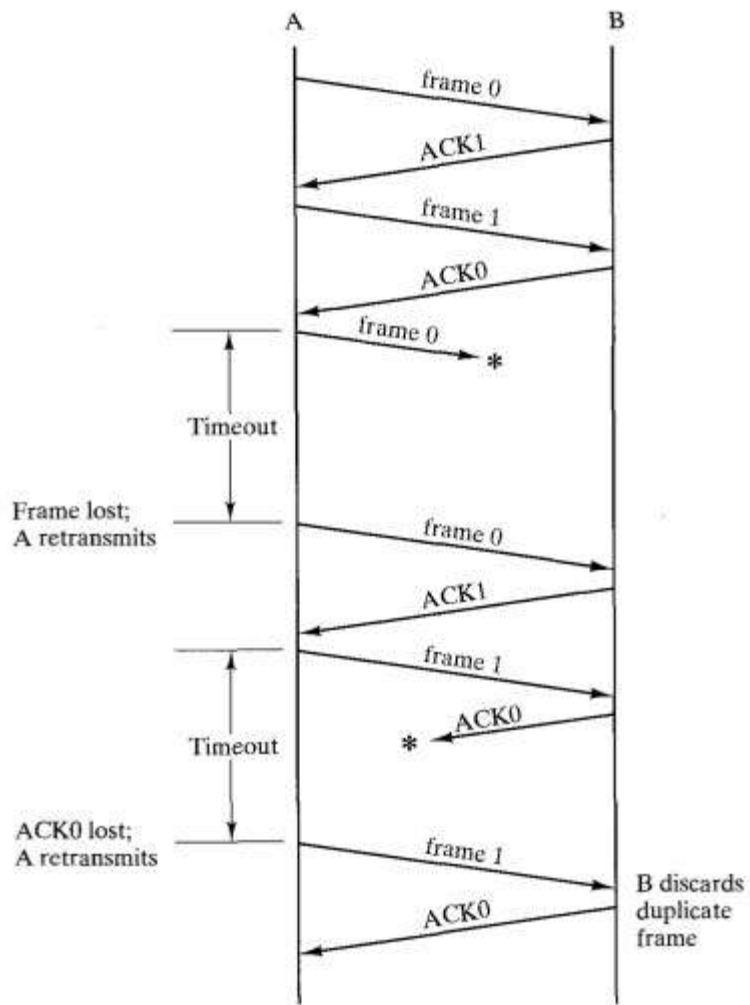
Go-back-N ARQ

Selective-reject ARQ

## Stop-and-wait ARQ:

Stop-and-wait ARQ is based on the stop-and-wait flow-control technique outlined previously and is depicted in Figure alongside.

- The source station transmits a single frame and then must await an acknowledgement (ACK). No other data frames can be sent until the destination stations reply arrives at the source station.
- The sending device keeps a copy of the last frame until it receives an acknowledgement for that frame. Keeping a copy allows the sender to retransmits lost or damaged frames until they are received correctly.
- For identification purposes, both data frames and acknowledgement frames (ACK) are numbered 0 & 1. A data 0 frame is acknowledged by and ACK1 frame, indicating that the receiver has received data frame 0 and is now expecting data frame 1.
- The sender starts a timer when it sends a frame. If an acknowledgement is not received within an allotted time period, the sender assumes that the frame was lost or damage and resends it.



*Fig. Stop and Wait ARQ*

- The receiver sends only +ve ACK for frame received safe and sound. It is silent about the frames damaged or lost. The acknowledgement number always define the number of next expected frame. If frame 0 is received, ACK1 is sent; if frame 1 is received ACK 0 is sent.

### Bidirectional Transmission:

The stop-and-wait mechanism we have discussed is unidirectional. However, we can have bi-directional transmission if the two parties have two separate channels for the full-duplex transmission or share the same channel for half-duplex transmission.

**Piggybacking:** is a method to combine a data frame with an acknowledgement. For example, stations A and B both have data to send. Instead of sending separate data and ACK frames, Station A sends a data frame that includes an ACK, station B behaves in a similar manner.

Piggybacking can save BW because the overhead from a data frame and ACK frame (addresses, CRC, etc) can be combined into just one frame.

## Go-Back-N ARQ:

- The form of error control based on sliding-window flow control that is most commonly used is called go-back-N ARQ.
- In go-back-N ARQ, a station may send a series of frames sequentially numbered modulo some maximum value.
- The number of unacknowledged frames out-standing is determined by window size, using the sliding-window flow control technique.
- While no errors occur, the destination will acknowledge (RR = receive ready) incoming frames as usual.
- If the destination station detects an error in a frame, it sends a negative acknowledgment (REJ = reject) for that frame. The destination station will discard that frame and all future incoming frames until the frame in error is correctly received. Thus, the source station, when it receives an REJ, must retransmit the frame in error plus all succeeding frames that were transmitted in the interim.

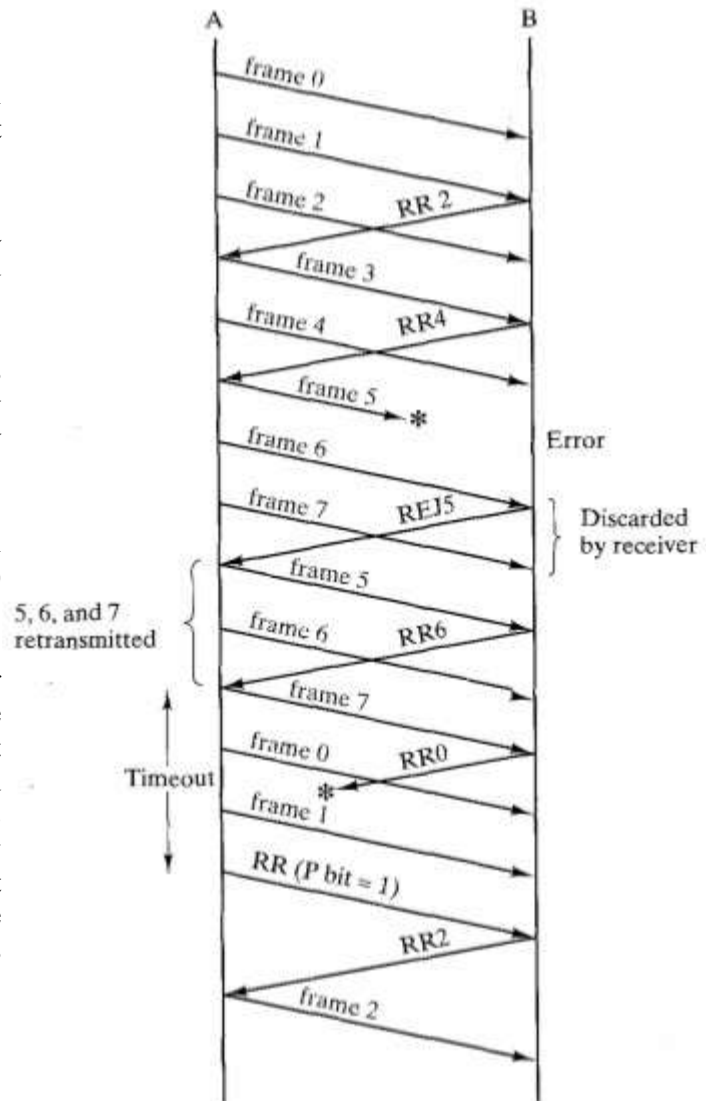


Fig: Go-Back-N ARQ

Consider that station A is sending frames to station B. After each transmission, A sets an acknowledgment timer for the frame just transmitted. The go-back-N technique takes into account the following contingencies:

### 1. Damaged frame. There are three sub-cases:

- a) A transmits frame  $i$ . B detects an error and has previously successfully received frame  $(i - 1)$ . B sends REJ  $i$ , indicated that frame  $i$  is rejected. When A receives the REJ, it must retransmit frame  $i$  and all subsequent frames that it has transmitted since the original transmission of frame  $i$ .
- b) Frame  $i$  is lost in transit. A subsequently sends frame  $(i + 1)$ . B receives frame  $(i + 1)$  out of order and sends an REJ  $i$ . A must retransmit frame  $i$  and all subsequent frames.
- c) Frame  $i$  is lost in transit, and A does not soon send additional frames. B receives nothing and returns neither an RR nor an REJ. When A's timer expires, it transmits an RR frame that includes a bit known as

the P bit, which is set to 1. B interprets the R R frame with a P bit of 1 as a command that must be acknowledged by sending an R R indicating the next frame that it expects. When A receives the RR, it retransmits frame i.

## **2. Damaged RR. There are two sub-cases:**

- a) B receives frame i and sends R R (i + 1), which is lost in transit. Because acknowledgments are cumulative (e.g., RR 6 means that all frames through 5 are acknowledged), it may be that A will receive a subsequent R R to a subsequent frame and that it will arrive before the timer associated with frame i expires.
- b) If A's timer expires, it transmits an RR command as in Case 1c. It sets another timer, called the P-bit timer. If B fails to respond to the RR command, or if its response is damaged, then A's P-bit timer will expire. At this point, A will try again by issuing a new RR command and restarting the P-bit timer. This procedure is tried for a number of iterations. If A fails to obtain an acknowledgment after some maximum number of attempts, it initiates a reset procedure.

## **3. Damaged REJ. If an REJ is lost, this is equivalent to Case 1c.**

## **Selective-reject ARQ**

With selective-reject ARQ, the only frames retransmitted are those that receive a negative acknowledgment, in this case called SREJ, or that time-out. This would appear to be more efficient than go-back-N, because it minimizes the amount of retransmission. On the other hand, the receiver must maintain a buffer large enough to save post-SREJ frames until the frame in error is retransmitted, and it must contain logic for reinserting that frame in the proper sequence. The transmitter, too, requires more complex logic to be able to send a frame out of sequence. Because of such complications, selective-reject ARQ is much less used than go-back-N ARQ.

## **High-Level Data Link Control(HDLC)**

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. HDLC is a synchronous Data Link layer bit-oriented protocol developed by the International Organization for Standardization (ISO). The current standard for HDLC is ISO 13239. HDLC was developed from the Synchronous Data Link Control (SDLC) standard proposed in the 1970s. HDLC provides both connection-oriented and connectionless service. HDLC uses synchronous serial transmission to provide error-free communication between two points. HDLC defines a Layer 2 framing structure that allows for flow control and error control through the use of acknowledgments. Each frame has the same format, whether it is a data frame or a control frame. When you want to transmit frames over synchronous or asynchronous links, you must remember that those links have no mechanism to mark the beginnings or ends of frames. HDLC uses a frame delimiter, or flag, to mark the beginning and the end of each frame.

## **HDLC Frame Format:**



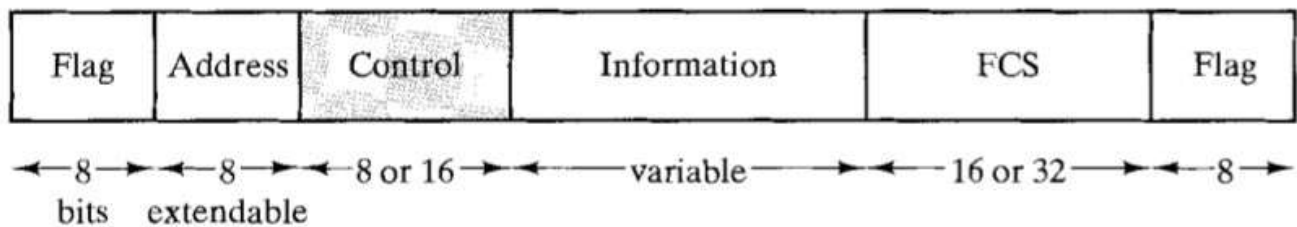
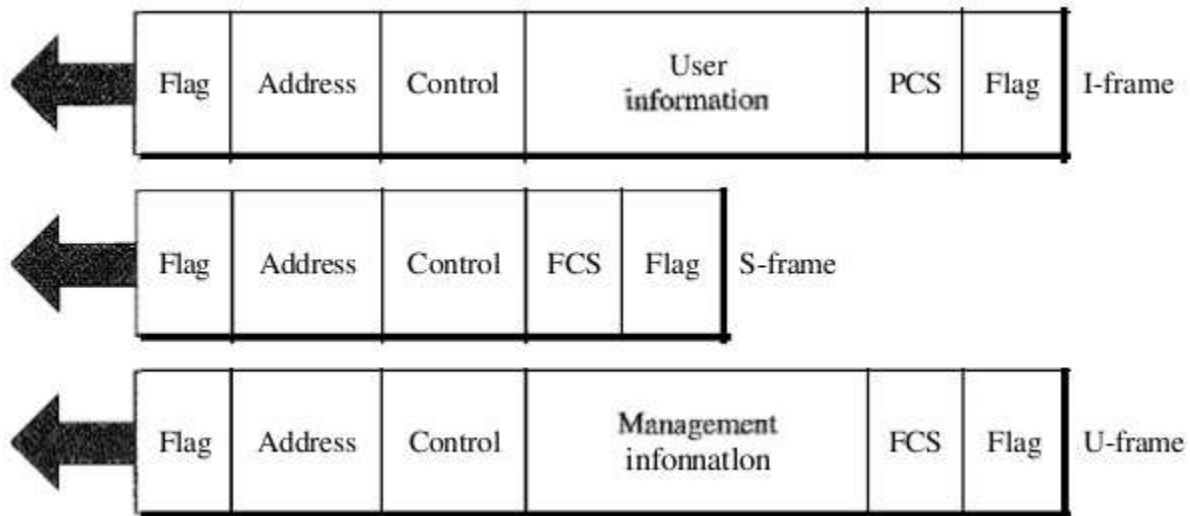


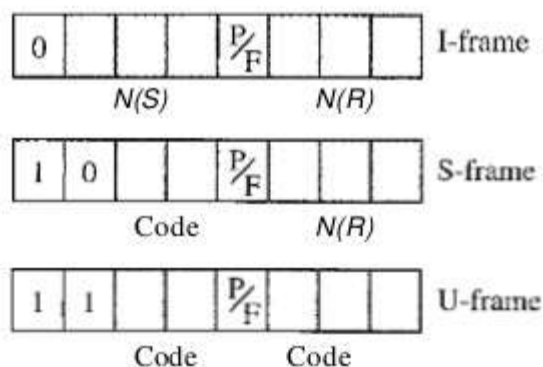
Fig: HDLC Frame Format



HDLC defines three types of frames:

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

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



#### LEGEND

N(S) = Send sequence number  
N(R) = Receive sequence number  
P/F = Poll/final bit

## I Frames:

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

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

## S Frame:

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

- If the first 2 bits of the control field is 10, this means the frame is an S-frame.
  - The last 3 bits, called N(R), corresponds to the acknowledgment number (ACK) or negative acknowledgment number (NAK) depending on the type of S-frame.
  - The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames, as described below :
1. **Receive ready (RR).** If the value of the code subfield is 00, it is an RR S-frame. This kind of frame acknowledges the receipt of a safe and sound frame or group of frames. In this case, the value N(R) field defines the acknowledgment number.
  2. **Receive not ready (RNR).** If the value of the code subfield is 10, it is an RNR S-frame. This kind of frame is an RR frame with additional functions. It acknowledges the receipt of a frame or group of frames, and it announces that the receiver is busy and cannot receive more frames. It acts as a kind of congestion control mechanism by asking the sender to slow down. The value of N(R) is the acknowledgment number.
  3. **Reject (REJ).** If the value of the code subfield is 01, it is a REJ S-frame. This is a NAK frame, but not like the one used for Selective Repeat ARQ. It is a NAK that can be used in Go-Back-N ARQ to improve the efficiency of the process by informing the sender, before the sender time expires, that the last frame is lost or damaged. The value of N(R) is the negative acknowledgment number.
  4. **Selective reject (SREJ).** If the value of the code subfield is 11, it is an SREJ S-frame. This is a NAK frame used in Selective Repeat ARQ. Note that the HDLC Protocol uses the term selective reject instead of selective repeat. The value of N(R) is the negative acknowledgment number.

The fifth field in the control field is the P/F bit as discussed before.

The next 3 bits, called N(R), correspond to the ACK or NAK value.

## U Frames:

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

### Flag Field:

Flag fields delimit the frame at both ends with the unique pattern 01111110. A single flag may be used as the closing flag for one frame and the opening flag for the next. On both sides of the user-network interface, receivers are continuously hunting for the flag sequence to synchronize on the start of a frame. While receiving a frame, a station continues to hunt for that sequence to determine the end of the frame. Since the pattern 01111110 may appear in the frame as well, a procedure known as bit stuffing is used.

After detecting a starting flag, the receiver monitors the bit stream. When a pattern of five 1s appears, the sixth bit is examined. If this bit is 0, it is deleted. If the sixth bit is a 1 and the seventh bit is a 0, the combination is accepted as a flag. If the sixth and seventh bits are both 1, the sender is indicating an abort condition. With the use of bit stuffing, arbitrary bit patterns can be inserted into the data field of the frame. This property is known as data transparency.

### Address Field:

The address field identifies the secondary station that transmitted or is to receive the frame. This field is not needed for point-to-point links, but is always included for the sake of uniformity.

**Control Field:** It defines the three types of frames I, U and S Frame for HDLC.

**Information Field:** This field is present only in I frame and some U Frame.

**Frame Check Sequence Field:** Its error detecting code calculated from the remaining bits of the frame, exclusive of flags. The normal code is 16 bit CRC code.

## PPP: (Point-to-point protocol):

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

### PPP provides several services:

1. PPP defines the format of the frame to be exchanged between devices.
2. PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
3. PPP defines how network layer data are encapsulated in the data link frame.
4. PPP defines how two devices can authenticate each other.
5. PPP provides multiple network layer services supporting a variety of network layer protocols.

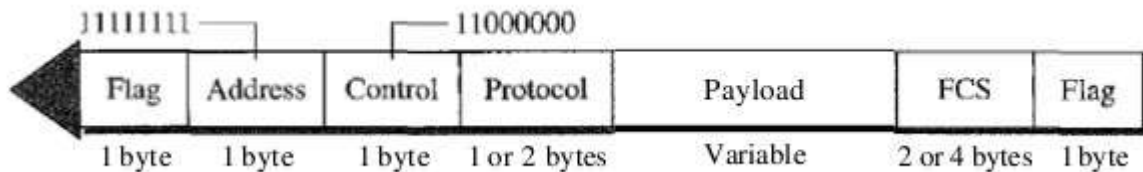
6. PPP provides connections over multiple links.
7. PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

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

1. PPP does not provide flow control. A sender can send several frames one after another with no concern about overwhelming the receiver.
2. PPP has a very simple mechanism for error control. A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs to take care of the problem. Lack of error control and sequence numbering may cause a packet to be received out of order.
3. PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

## Framing

PPP is a byte-oriented protocol. Framing is done according to the discussion of byte-oriented protocols above.



*Fig: PPP Frame Format*

**Flag.** A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110. Although this pattern is the same as that used in HDLC, there is a big difference. PPP is a byte-oriented protocol; HDLC is a bit-oriented protocol. The flag is treated as a byte, as we will explain later.

- **Address.** The address field in this protocol is a constant value and set to 11111111 (broadcast address). During negotiation (discussed later), the two parties may agree to omit this byte.
- **Control.** This field is set to the constant value 11000000 (imitating unnumbered frames in HDLC). As we will discuss later, PPP does not provide any flow control. Error control is also limited to error detection. This means that this field is not needed at all, and again, the two parties can agree, during negotiation, to omit this byte.
- **Protocol.** The protocol field defines what is being carried in the data field: either user data or other information. We discuss this field in detail shortly. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.
- **Payload field.** This field carries either the user data or other information. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte-stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.

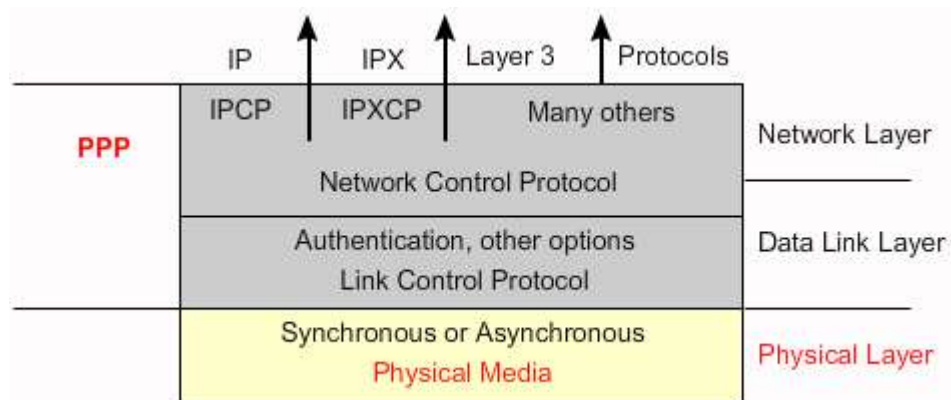
- **FCS.** The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

### Byte Stuffing

The similarity between PPP and HDLC ends at the frame format. PPP, as we discussed before, is a byte-oriented protocol totally different from HDLC. As a byte-oriented protocol, the flag in PPP is a byte and needs to be escaped whenever it appears in the data section of the frame. The escape byte is 01111101, which means that every time the flaglike pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag.

### PPP Stack

Although PPP is a data link layer protocol, PPP uses another set of other protocols to establish the link, authenticate the parties involved, and carry the network layer data. Three sets of protocols are defined to make PPP powerful: the Link Control Protocol (LCP), two Authentication Protocols (APs), and several Network Control Protocols (NCPs). At any moment, a PPP packet can carry data from one of these protocols in its data field. Note that there is one LCP, two APs, and several NCPs. Data may also come from several different network layers.



*Fig:PPP Layered Architecture*

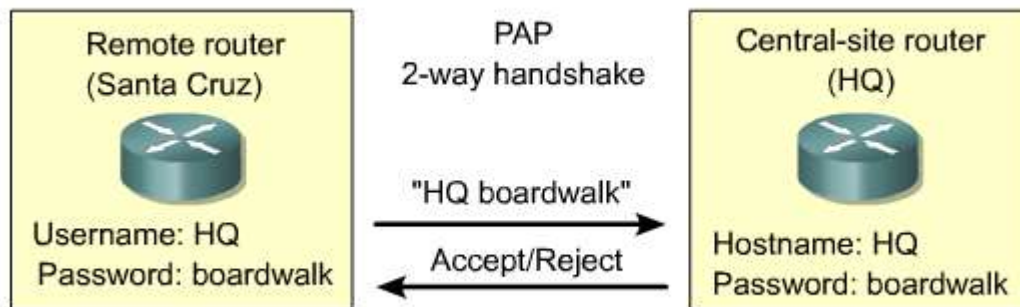
**The Link Control Protocol (LCP)** is responsible for establishing, maintaining, configuring, and terminating links. It also provides negotiation mechanisms to set options between the two endpoints. Both endpoints of the link must reach an agreement about the options before the link can be established. All LCP packets are carried in the payload field of the PPP frame with the protocol field set to C02 1 in hexadecimal .

### Authentication Protocols

Authentication plays a very important role in PPP because PPP is designed for use over dial-up links where verification of user identity is necessary. Authentication means validating the identity of a user who needs to access a set of resources. PPP has created two protocols for authentication: Password Authentication Protocol and Challenge Handshake Authentication Protocol. Note that these protocols are used during the authentication phase.

**PAP The Password Authentication Protocol (PAP)** is a simple authentication procedure with a two-step process:

1. The user who wants to access a system sends an authentication identification (usually the user name) and a password.
2. The system checks the validity of the identification and password and either accepts or denies connection.

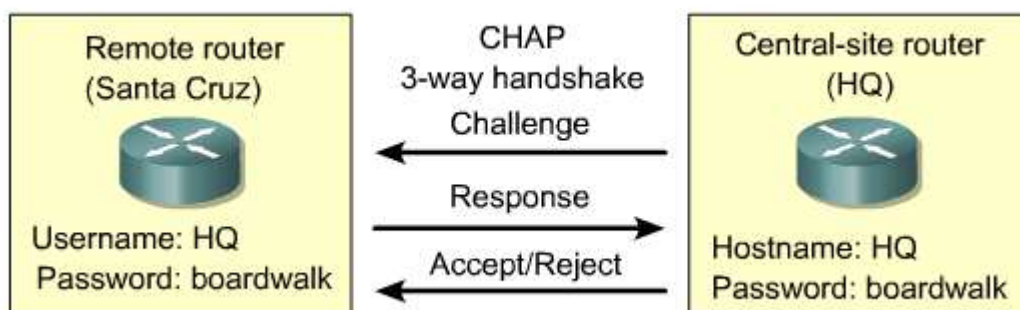


*Fig: PAP Authentication Protocol*

*Note: Passwords are sent in clear text in PAP.*

**CHAP The Challenge Handshake Authentication Protocol (CHAP)** is a three-way hand-shaking authentication protocol that provides greater security than PAP. In this method, the password is kept secret; it is never sent on-line.

1. The system sends the user a challenge packet containing a challenge value, usually a few bytes.
2. The user applies a predefined function that takes the challenge value and the user's own password and creates a result. The user sends the result in the response packet to the system.
3. The system does the same. It applies the same function to the password of the user (known to the system) and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied. CHAP is more secure than PAP, especially if the system continuously changes the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret.



*Fig: CHAP Authentication protocol*

### Network Control Protocols

PPP is a multiple-network layer protocol. It can carry a network layer data packet from protocols defined by the Internet, OSI, Xerox, DECnet, AppleTalk, Novel, and so on. To do this, PPP has defined a specific Network Control Protocol for each network protocol. For example, IPCP (Internet Protocol Control Protocol) configures the link for carrying IP data packets. Xerox CP does the same for the Xerox protocol data packets, and so on. Note that none of the NCP packets carry network layer data; they just configure the link at the network layer for the incoming data.

## SLIP: (SERIAL LINE INTERNET PROTOCOL):-

An industry standard protocol developed in 1984 for UNIX environments that supports TCP/IP networking over serial transmission lines. These serial lines are typically dial-up connections using a modem. Serial Line Internet Protocol (SLIP) can provide TCP/IP hosts with dial-up access to the Internet by using SLIP servers located at Internet service providers (ISPs).

The TCP/IP protocol family runs over a variety of network media: IEEE 802.3 (Ethernet) and 802.5 (a token ring) LAN's, X.25 lines, satellite links, and serial lines. There are standard encapsulations for IP packets defined for many of these networks, but there is no standard for serial lines. SLIP, Serial Line IP, is currently a de facto standard, commonly used for point-to-point serial connections running TCP/IP. It is not an Internet standard. The Serial Line Internet Protocol (SLIP) is a mostly obsolete encapsulation of the Internet Protocol designed to work over serial ports and modem connections. SLIP has been largely replaced by the Point-to-Point Protocol (PPP), which is better engineered, has more features and does not require its IP address configuration to be set before it is established.

The following are commonly perceived shortcomings in the existing SLIP protocol:

- **addressing:** Both computers in a SLIP link need to know each other's IP addresses for routing purposes. Also, when using SLIP for hosts to dial-up a router, the addressing scheme may be quite dynamic and the router may need to inform the dialing host of the host's IP address. SLIP currently provides no mechanism for hosts to communicate addressing information over a SLIP connection.
- **type identification:** SLIP has no type field. Thus, only one protocol can be run over a SLIP connection, so in a configuration of two DEC computers running both TCP/IP and DECnet, there is no hope of having TCP/IP and DECnet share one serial line between them while using SLIP. Thus, SLIP can support only one connection on the link at any time. While SLIP is "Serial Line IP", if a serial line connects two multi protocol computers, those computers should be able to use more than one protocol over the line.
- **error detection/correction:** Noisy phone lines will corrupt packets in transit. Because the line speed is probably quite low (likely 2400 baud), retransmitting a packet is very expensive. Error detection is not absolutely necessary at the SLIP level. It takes so long to retransmit a packet which was corrupted by line noise, it would be efficient if SLIP could provide some sort of simple error correction mechanism of its own.
- **compression:** Because dial-in lines are so slow (usually 2400 bps), packet compression would cause large improvements in a packet throughput.

# Chapter: 6 TCP/IP Reference Model, IP Addressing and Subnetting

## TCP/IP Model:

The U.S. Department of Defense (DOD) created the TCP/IP reference model because it wanted a network that could survive any conditions

### Application Layer:

The application layer handles high-level protocols, representation, encoding, and dialog control. The TCP/IP protocol suite combines all application related issues into one layer. It ensures that the data is properly packaged before it is passed on to the next layer. TCP/IP includes Internet and transport layer specifications such as IP and TCP as well as specifications for common applications. TCP/IP has protocols to support file transfer, e-mail, and remote login, in addition to the following:

- **File Transfer Protocol (FTP)** – FTP is a reliable, connection-oriented service that uses TCP to transfer files between systems that support FTP. It supports bi-directional binary file and ASCII file transfers.
- **Trivial File Transfer Protocol (TFTP)** – TFTP is a connectionless service that uses the User Datagram Protocol (UDP). TFTP is used on the router to transfer configuration files and Cisco IOS images, and to transfer files between systems that support TFTP. It is useful in some LANs because it operates faster than FTP in a stable environment.
- **Network File System (NFS)** – NFS is a distributed file system protocol suite developed by Sun Microsystems that allows file access to a remote storage device such as a hard disk across a network.
- **Simple Mail Transfer Protocol (SMTP)** – SMTP administers the transmission of e-mail over computer networks. It does not provide support for transmission of data other than plain text.
- **Telnet** – Telnet provides the capability to remotely access another computer. It enables a user to log into an Internet host and execute commands. A Telnet client is referred to as a local host. A Telnet server is referred to as a remote host.
- **Simple Network Management Protocol (SNMP)** – SNMP is a protocol that provides a way to monitor and control network devices. SNMP is also used to manage configurations, statistics, performance, and security.
- **Domain Name System (DNS)** – DNS is a system used on the Internet to translate domain names and publicly advertised network nodes into IP addresses.



*TCP/IP Model*

### Transport Layer:

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

- Creates packet from bytes stream received from the application layer.
- Uses port number to create process to process communication.



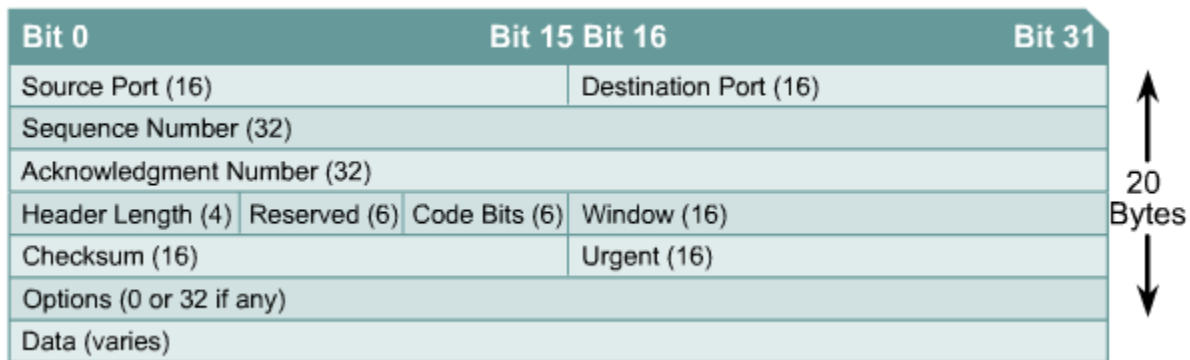
- Uses a sliding window protocol to achieve flow control.
- Uses acknowledgement packet, timeout and retransmission to achieve error control.

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

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

## TCP Header Format:

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



The following protocols use TCP:

- FTP
- HTTP
- SMTP
- Telnet

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

- **Source port** – Number of the port that sends data
- **Destination port** – Number of the port that receives data
- **Sequence number** – Number used to ensure the data arrives in the correct order
- **Acknowledgment number** – Next expected TCP octet
- **HLEN** – Number of 32-bit words in the header
- **Reserved** – Set to zero
- **Code bits** – Control functions, such as setup and termination of a session
- **Window** – Number of octets that the sender will accept
- **Checksum** – Calculated checksum of the header and data fields
- **Urgent pointer** – Indicates the end of the urgent data

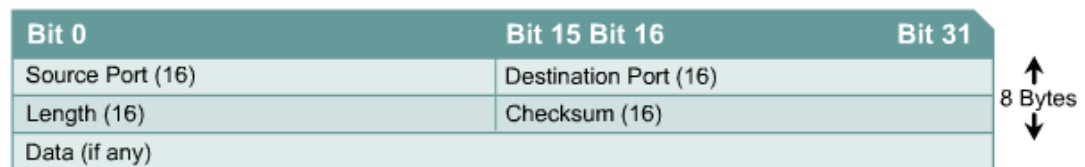
- **Option** – One option currently defined, maximum TCP segment size
- **Data** – Upper-layer protocol data

#### Code Bits or Flags (6 bits).

- URG: Urgent pointer field significant.
- ACK: Acknowledgment field significant.
- PSH: Push function.
- RST: Reset the connection.
- SYN: Synchronize the sequence numbers.
- FIN: No more data from sender.

## UDP (User Datagram Protocol):

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



**Fig: UDP Datagram**

UDP does not use windows or ACKs. Reliability is provided by application layer protocols. UDP is designed for applications that do not need to put sequences of segments together.

The following protocols use UDP:

- TFTP
- SNMP
- DHCP
- DNS

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

- **Source port** – Number of the port that sends data
- **Destination port** – Number of the port that receives data
- **Length** – Number of bytes in header and data
- **Checksum** – Calculated checksum of the header and data fields
- **Data** – Upper-layer protocol data

## TCP vs UDP:

S.no	TCP - Transmission Control Protocol	UDP - User Datagram Protocol
1	connection-oriented, reliable (virtual circuit)	connectionless, unreliable, does not check message delivery
2	Divides outgoing messages into segments	sends “datagrams”
3	reassembles messages at the destination	does not reassemble incoming messages
4	re-sends anything not received	Does-not acknowledge.

5	provides flow control	provides no flow control
6	more overhead than UDP (less efficient)	low overhead - faster than TCP
7	Examples:HTTP, NFS, SMTP	Eg. VOIP,DNS,TFTP

## Internet Layer:

The purpose of the Internet layer is to select the best path through the network for packets to travel. The main protocol that functions at this layer is IP. Best path determination and packet switching occur at this layer.

The following protocols operate at the TCP/IP Internet layer:

- IP provides connectionless, best-effort delivery routing of packets. IP is not concerned with the content of the packets but looks for a path to the destination.
- Internet Control Message Protocol (ICMP) provides control and messaging capabilities.
- Address Resolution Protocol (ARP) determines the data link layer address, or MAC address, for known IP addresses.
- Reverse Address Resolution Protocol (RARP) determines the IP address for a known MAC address.

### IP performs the following operations:

- Defines a packet and an addressing scheme
- Transfers data between the Internet layer and network access layer
- Routes packets to remote hosts

## Network Access Layer:

The network access layer allows an IP packet to make a physical link to the network media. It includes the LAN and WAN technology details and all the details contained in the OSI physical and data link layers.

Drivers for software applications, modem cards, and other devices operate at the network access layer. The network access layer defines the procedures used to interface with the network hardware and access the transmission medium. Modem protocol standards such as Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) provide network access through a modem connection. Many protocols are required to determine the hardware, software, and transmission-medium specifications at this layer. This can lead to confusion for users. Most of the recognizable protocols operate at the transport and Internet layers of the TCP/IP model.

Network access layer protocols also map IP addresses to physical hardware addresses and encapsulate IP packets into frames. The network access layer defines the physical media connection based on the hardware type and network interface.

## Comparison of OSI Model and TCP/IP Model:

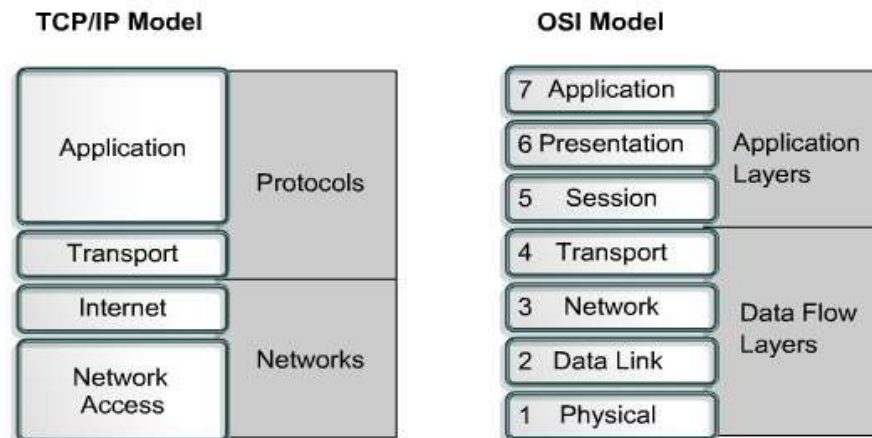
### The OSI and TCP/IP models have many similarities:

- Both have layers.
- Both have application layers, though they include different services.
- Both have comparable transport and network layers.
- Both use packet-switched instead of circuit-switched technology.
- Networking professionals need to know both models.

**Here are some differences of the OSI and TCP/IP models:**

- TCP/IP combines the OSI application, presentation, and session layers into its application layer.
- TCP/IP combines the OSI data link and physical layers into its network access layer.
- TCP/IP appears simpler because it has fewer layers.
- When the TCP/IP transport layer uses UDP it does not provide reliable delivery of packets. The transport layer in the OSI model always does.

The Internet was developed based on the standards of the TCP/IP protocols. The TCP/IP model gains credibility because of its protocols. The OSI model is not generally used to build networks. The OSI model is used as a guide to help students understand the communication process.



## IP Address:

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

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

## Ipv4 Header:

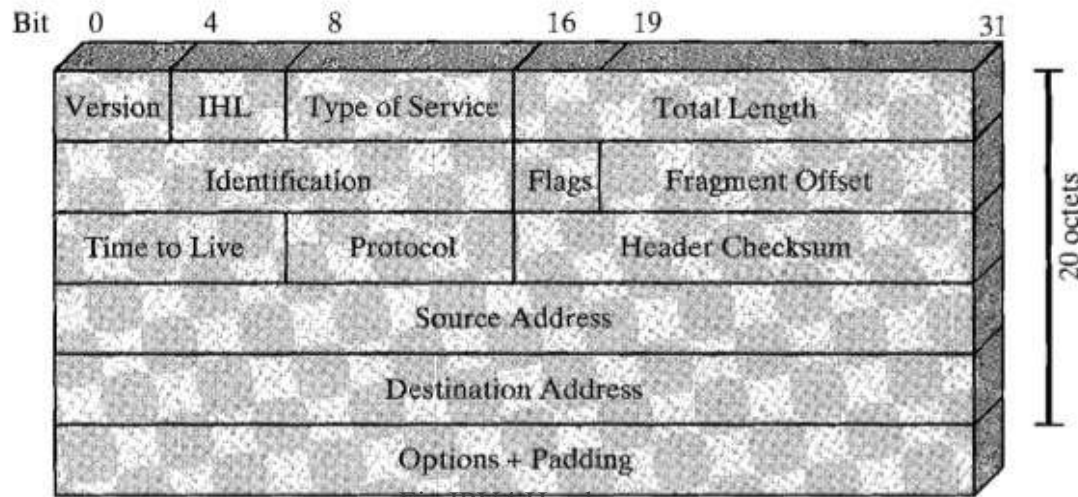


Fig:IPv4 Header

**Version:(4 bits):** Indicates the version number, to allow evolution of the protocol.

**Internet Header Length(IHL 4 bits):** Length of header in 32 bit words. The minimum value is five for a minimum header length of 20 octets.

### Type-of-Service :

The Type-of-Service field contains an 8-bit binary value that is used to determine the priority of each packet. This value enables a Quality-of-Service (QoS) mechanism to be applied to high priority packets, such as those carrying telephony voice data. The router processing the packets can be configured to decide which packet it is to forward first based on the Type-of-Service value.

**Total length:** total datagram length ,in octets.

**Identifier (16 bits):** A sequence number that, together with the source address, destination address, and user protocol, is intended to uniquely identify a datagram. Thus, the identifier should be unique for the datagram's source address, destination address, and user protocol for the time during which the datagram will remain in the internet.

**Fragment Offset :** A router may have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU. When fragmentation occurs, the IPv4 packet uses the Fragment Offset field and the MF flag in the IP header to reconstruct the packet when it arrives at the destination host. The fragment offset field identifies the order in which to place the packet fragment in the reconstruction.

**Flags(3 bits):** Only two of the bits are currently defined: MF(More Fragments) and DF(Don't Fragment):

**More Fragments flag (MF):**The More Fragments (MF) flag is a single bit in the Flag field used with the Fragment Offset for the fragmentation and reconstruction of packets. The More Fragments flag bit is set, it means that it is not the last fragment of a packet. When a receiving host sees a packet arrive with the MF = 1, it examines the Fragment Offset to see where this fragment is to be placed in the reconstructed packet. When a receiving host receives a frame with the MF = 0 and a non-zero value in the Fragment offset, it places that fragment as the last part of the reconstructed packet. An unfragmented packet has all zero fragmentation information (MF = 0, fragment offset =0).

**Don't Fragment flag (DF):**The Don't Fragment (DF) flag is a single bit in the Flag field that indicates that fragmentation of the packet is not allowed. If the Don't Fragment flag bit is set, then fragmentation of this packet is NOT permitted. If a router needs to fragment a packet to allow it to be passed downward to the Data Link layer but the DF bit is set to 1, then the router will discard this packet.

### **IP Destination Address**

The IP Destination Address field contains a 32-bit binary value that represents the packet destination Network layer host address.

### **IP Source Address**

The IP Source Address field contains a 32-bit binary value that represents the packet source Network layer host address.

### **Time-to-Live**

The Time-to-Live (TTL) is an 8-bit binary value that indicates the remaining "life" of the packet. The TTL value is decreased by at least one each time the packet is processed by a router (that is, each hop). When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow. This mechanism prevents packets that cannot reach their destination from being forwarded indefinitely between routers in a routing loop. If routing loops were permitted to continue, the network would become congested with data packets that will never reach their destination. Decrementing the TTL value at each hop ensures that it eventually becomes zero and that the packet with the expired TTL field will be dropped.

### **Protocol:**

This 8-bit binary value indicates the data payload type that the packet is carrying. The Protocol field enables the Network layer to pass the data to the appropriate upper-layer protocol.

Example values are:

01 ICMP

06 TCP

17 UDP

**Header checksum (16 bits):** An error-detecting code applied to the header only. Because some header fields may change during transit (e.g., time to live, segmentation-related fields), this is reverified and recomputed at each router. The checksum field is the 16-bit one's complement addition of all 16-bit words in the header. For purposes of computation, the checksum field is itself initialized to a value of zero .

**Options (variable).** Encodes the options requested by the sending user.

**Padding (variable).** Used to ensure that the datagram header is a multiple of 32 bits.

**Data (variable).** The data field must be an integer multiple of 8 bits. The maximum length of the datagram (data field plus header) is 65,535 octets.

### **IP addresses are divided into class:**

IP Address Class	First Octet Address Range	Used for:
Class A	0-127	Unicast (Very Large Networks)
Class B	128-191	Unicast (Medium to large network)

Class C	192-223	Unicast (Small Network)
Class D	224-239	Multicast
Class E	240-255	Reserved

## Class A Blocks

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

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

No of Class A Network:  $2^7$

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

## Class B Blocks

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

The first two bits of the first octet of a Class B address are always 10. The remaining six bits may be populated with either 1s or 0s. Therefore, the lowest number that can be represented with a Class B address is 10000000, decimal 128. The highest number that can be represented is 10111111, decimal 191. Any address that starts with a value in the range of 128 to 191 in the first octet is a Class B address.

No of Class B Network:  $2^{14}$

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

## Class C Blocks:

The class C address space was the most commonly available of the historic address classes. This address space was intended to provide addresses for small networks with a maximum of 254 hosts.

Class C address blocks used a /24 prefix. This meant that a class C network used only the last octet as host addresses with the three high-order octets used to indicate the network address.

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

No of Class C Network: 221

No. of Usable Host address per Network: 28-2

## Class D Blocks:

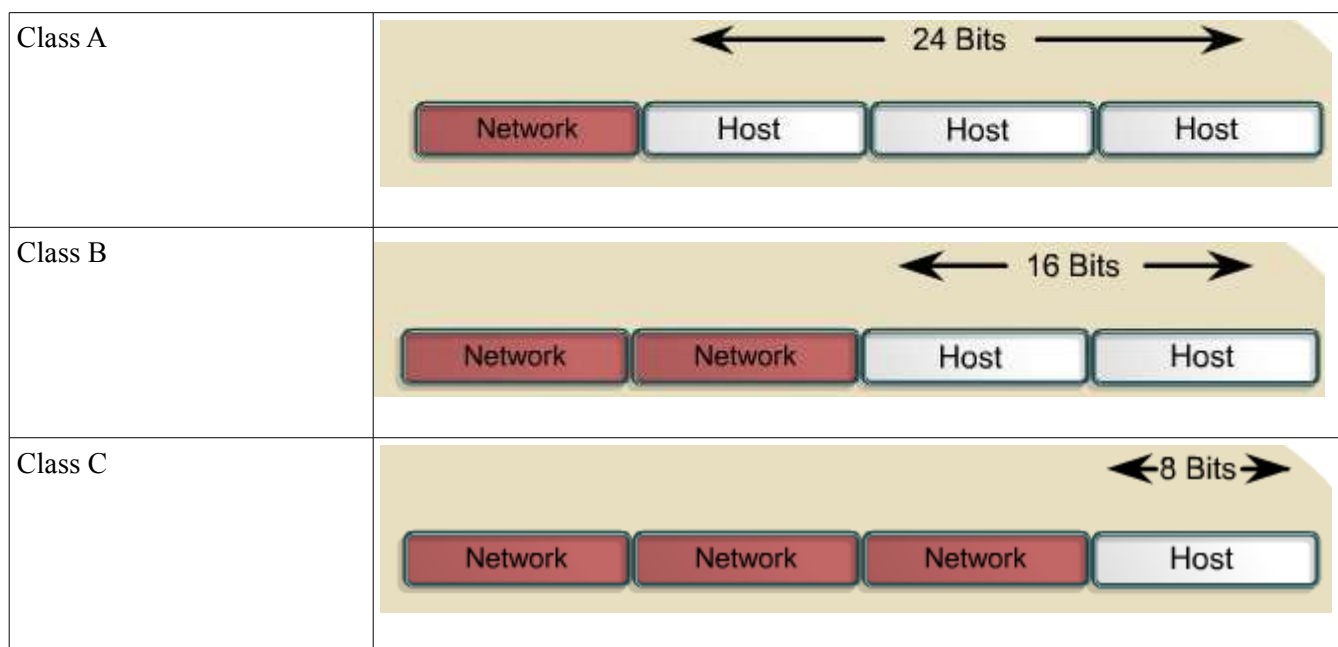
The Class D address class was created to enable multicasting in an IP address. A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses. Therefore, a single station can simultaneously transmit a single stream of data to multiple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

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

## Class E Block:

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

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



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

**Network address** - The address by which we refer to the network

**Broadcast address** - A special address used to send data to all hosts in the network

**Host addresses** - The addresses assigned to the end devices in the network



## Special Ipv4 addresses:

**Default Route:** we represent the IPv4 default route as 0.0.0.0. The default route is used as a "catch all" route when a more specific route is not available. The use of this address also reserves all addresses in the 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8) address block.

**Network and Broadcast Addresses:** As explained earlier, within each network the first and last addresses cannot be assigned to hosts. These are the network address and the broadcast address, respectively.

**Loopback:** One such reserved address is the IPv4 loopback address 127.0.0.1. The loopback is a special address that hosts use to direct traffic to themselves. Although only the single 127.0.0.1 address is used, addresses 127.0.0.0 to 127.255.255.255 are reserved. Any address within this block will loop back within the local host. No address within this block should ever appear on any network.

**Link-Local Addresses:** IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16) are designated as link-local addresses. These addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available. These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from a Dynamic Host Configuration Protocol (DHCP) server.

**TEST-NET Addresses :** The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0 /24) is set aside for teaching and learning purposes. These addresses can be used in documentation and network examples

**Network Prefixes:** An important question is: How do we know how many bits represent the network portion and how many bits represent the host portion? When we express an IPv4 network address, we add a prefix length to the network address. The prefix length is the number of bits in the address that gives us the network portion. For example, in 172.16.4.0 /24, the /24 is the prefix length - it tells us that the first 24 bits are the network address. This leaves the remaining 8 bits, the last octet, as the host portion.

## Private and Public IP addresses:

**Public IP addresses:** Public IP addresses are assigned by the InterNIC (Internet's Network Information Centre) and consists of class based network Ids or blocks of CIDR based addresses (called CIDR blocks) that are globally rout-able to the Internet and are unique.

**Private IP address:** An address that is used for internal networks. These addresses are not rout-able to the Internet.

*The private address blocks are:*

10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)

172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)

192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)

## Subnet Mask:

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

each bit position that represents the host portion.

The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

### **Default Subnet Mask:**

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

### **CIDR:**

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

### **How It Works**

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

### **How to Create Subnets**

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

### **How many bits to borrow?**

1. No of subnetwork =  $2^{BB}$
2. No. of usable hosts per subnetwork =  $2^{BR} - 2$

$TB = BR + BB$

TB=Total bits in host portion

BB=Bits borrowed

BR=Bits Remaining

### **Subnetting Class C Addresses**

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

Class C subnet masks can be the following:

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

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

All you need to do is answer five simple questions:

How many subnets does the chosen subnet mask produce?

How many valid hosts per subnet are available?

What are the valid subnets?

1. What's the broadcast address of each subnet?
2. What are the valid hosts in each subnet?

## **Subnetting Class C Address: 192.168.10.0/26**

255.255.255.192 (/26)

In this second example, we're going to subnet the network address 192.168.10.0 using the subnet mask 255.255.255.192.

192.168.10.0 = Network address

255.255.255.192 = Subnet mask

Now, let's answer the big five:

How many subnets? Since 192 is 2 bits on (11000000), the answer would be  $2^2 = 4$  subnets.

How many hosts per subnet? We have 6 host bits off (11000000), so the equation would be  $2^6 - 2 = 62$  hosts.

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

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

next subnet is 64, so the broadcast address for the zero subnet is 63.

What are the valid hosts? These are the numbers between the subnet and broadcast address.

The easiest way to find the hosts is to write out the subnet address and the broadcast address. This way, the valid hosts are obvious. The following table shows the 0, 64, 128, and 192 subnets, the valid host ranges of each, and the broadcast address of each subnet:

The subnets (do this first)	0	64	128	192
The broadcast address	63	127	191	255
Usable Host Range	1 – 62	65 – 126	129 – 190	193 - 254

## Subnetting Class B Address: 172.16.0.0/17

255.255.128.0 (/17)

172.16.0.0 = Network address

255.255.128.0 = Subnet mask

Subnets?  $2^1 = 2$  (same as Class C).

Hosts?  $2^{15} - 2 = 32,766$  (7 bits in the third octet, and 8 in the fourth).

Valid subnets?  $256 - 128 = 128$ . 0, 128. Remember that subnetting is performed in the third octet, so the subnet numbers are really 0.0 and 128.0, as shown in the next table.

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

Broadcast address for each subnet?

Valid hosts?

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

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

## Another Example Subnetting Class B address: 172.16.0.0/18

255.255.192.0 (/18)

172.16.0.0 = Network address

255.255.192.0 = Subnet mask

Subnets?  $2^2 = 4$ .

Hosts?  $2^{14} - 2 = 16,382$  (6 bits in the third octet, and 8 in the fourth).

Valid subnets?  $256 - 192 = 64$ . 0, 64, 128, 192. Remember that the subnetting is performed in the third octet, so the subnet numbers are really 0.0, 64.0, 128.0, and 192.0, as shown in the next table.

Broadcast address for each subnet?

Valid hosts?

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

Subnet	0.0	64.0	128.0	192.0	
Broadcast		63.255	127.255	191.255	255.255
First host		0.1	64.1	128.1	192.1
Last host		63.254	127.254	191.254	255.254

### **Another Example: 172.16.0.0/25**

#### **255.255.255.128 (/25)**

This is one of the hardest subnet masks you can play with. And worse, it actually is a really good subnet to use in production because it creates over 500 subnets with 126 hosts for each subnet—a nice mixture. So, don't skip over it!

172.16.0.0 = Network address

255.255.255.128 = Subnet mask

Subnets?  $2^9 = 512$ .

Hosts?  $2^7 - 2 = 126$ .

Valid subnets? Okay, now for the tricky part.  $256 - 255 = 1$ . 0, 1, 2, 3, etc. for the third octet. But you can't forget the one subnet bit used in the fourth octet. You actually get two subnets for each third octet value, hence the 512 subnets. For example, if the third octet is showing subnet 3, the two subnets would actually be 3.0 and 3.128.

Broadcast address for each subnet?

Valid hosts?

The following table shows how you can create subnets, valid hosts, and broadcast addresses using the Class B 255.255.255.128 subnet mask (the first eight subnets are shown, and then the last two subnets):

Subnet	0.0	0.128	1.0	1.128	2.0	2.128	3.0	3.128 ...	255.0	255.128
Broadcast	0.127	0.255	1.127	1.255	2.127	2.255	3.127	3.255 ...	255.127	255.255
First host	0.1	0.129	1.1	1.129	2.1	2.129	3.1	3.129 ...	255.1	255.129
Last host	0.126	0.254	1.126	1.254	2.126	2.254	3.126	3.254 ...	255.126	255.254

## Subnetting Class A network: 10.0.0.0/16

255.255.0.0 (/16)

Class A addresses use a default mask of 255.0.0.0, which leaves 22 bits for subnetting since you must leave 2 bits for host addressing. The 255.255.0.0 mask with a Class A address is using 8 subnet bits.

Subnets?  $2^8 = 256$ .

Hosts?  $2^{16} - 2 = 65,534$ .

Valid subnets? What is the interesting octet?  $256 - 255 = 1$ . 0, 1, 2, 3, etc. (all in the second octet). The subnets would be 10.0.0.0, 10.1.0.0, 10.2.0.0, 10.3.0.0, etc., up to 10.255.0.0.

Broadcast address for each subnet?

Valid hosts?

The following table shows the first two and last two subnets, valid host range, and broadcast addresses for the private Class A 10.0.0.0 network:

Subnet	10.0.0.0	10.1.0.0 ...	10.254.0.0	10.255.0.0
Broadcast	10.0.255.255	10.1.255.255 ...	10.254.255.255	10.255.255.255
First host	10.0.0.1	10.1.0.1 ...	10.254.0.1	10.255.0.1
Last host	10.0.255.254	10.1.255.254 ...	10.254.255.254	10.255.255.254

## IPV6:

### Features of IPV6:

<ul style="list-style-type: none"><li>• <b>Larger address space:</b><ul style="list-style-type: none"><li>- Global reachability and flexibility</li><li>- Aggregation</li><li>- Multihoming</li><li>- Autoconfiguration</li><li>- Plug and play</li><li>- End-to-end without NAT</li><li>- Renumbering</li></ul></li><li>• <b>Mobility and security:</b><ul style="list-style-type: none"><li>- Mobile IP RFC-compliant</li><li>- IPsec mandatory (or native) for IPv6</li></ul></li></ul>	<ul style="list-style-type: none"><li>• <b>Simple header:</b><ul style="list-style-type: none"><li>- Routing efficiency</li><li>- Performance and forwarding rate scalability</li><li>- No broadcasts</li><li>- No checksums</li><li>- Extension headers</li><li>- Flow labels</li></ul></li><li>• <b>Transition richness:</b><ul style="list-style-type: none"><li>- Dual stack</li><li>- 6to4 tunnels</li><li>- Translation</li></ul></li></ul>
--	---

- **Larger address space** Offers improved global reachability and flexibility; the aggregation of prefixes that are announced in routing tables; multihoming to several Internet service providers (ISPs) auto configuration that can include link-layer addresses in the address space; plug-and-play options; public-to private readdressing end to end without address translation; and simplified mechanisms for address renumbering and modification.

- **Simpler header:** Provides better routing efficiency; no broadcasts and thus no potential threat of broadcast storms; no requirement for processing checksums; simpler and more efficient extension header mechanisms; and flow labels for per-flow processing with no need to open the transport inner packet to identify the various traffic flows.
- **Mobility and security:** Ensures compliance with mobile IP and IPsec standards functionality; mobility is built in, so any IPv6 node can use it when necessary; and enables people to move around in networks with mobile network devices—with many having wireless connectivity.

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

IPsec is the IETF standard for IP network security, available for both IPv4 and IPv6. Although the functionalities are essentially identical in both environments, IPsec is mandatory in IPv6. IPsec is enabled on every IPv6 node and is available for use. The availability of IPsec on all nodes makes the IPv6 Internet more secure. IPsec also requires keys for each party, which implies a global key deployment and distribution.

- **Transition richness:** You can incorporate existing IPv4 capabilities in IPv6 in the following ways:
  - Configure a dual stack with both IPv4 and IPv6 on the interface of a network device.
  - Use the technique IPv6 over IPv4 (also called 6to4 tunneling), which uses an IPv4 tunnel to carry IPv6 traffic. This method (RFC 3056) replaces IPv4-compatible tunneling (RFC 2893). Cisco IOS Software Release 12.3(2)T (and later) also allows protocol translation (NAT-PT) between IPv6 and IPv4. This translation allows direct communication between hosts speaking different protocols.

## IPv4 VS IPv6

Bits	0	3	4	7	9	15	16	31
	Version		Header length		Type of service		Total length	
	Identification					Flags	Fragment offset	
	Time to live			Protocol		Header checksum		
	32-bit source address							
	32-bit destination address							
	Options						Padding	

Fig: IPV4 Header

An IPv4 header contains the following fields:

**version** The IP version number, 4.

**length** The length of the datagram header in 32-bit words.

**type of service** Contains five subfields that specify the precedence, delay, throughput, reliability, and cost desired for a packet. (The Internet does not guarantee this request.) This field is not widely used on the Internet.

**total length** The length of the datagram in bytes including the header, options, and the appended transport protocol segment or packet.

**Identification** An integer that identifies the datagram.

**Flags:** Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.

**fragment offset** The relative position of this fragment measured from the beginning of the original datagram in units of 8 bytes.

**time to live** How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever.

**Protocol** The high-level protocol type.

**header checksum** A number that is computed to ensure the integrity of the header values.

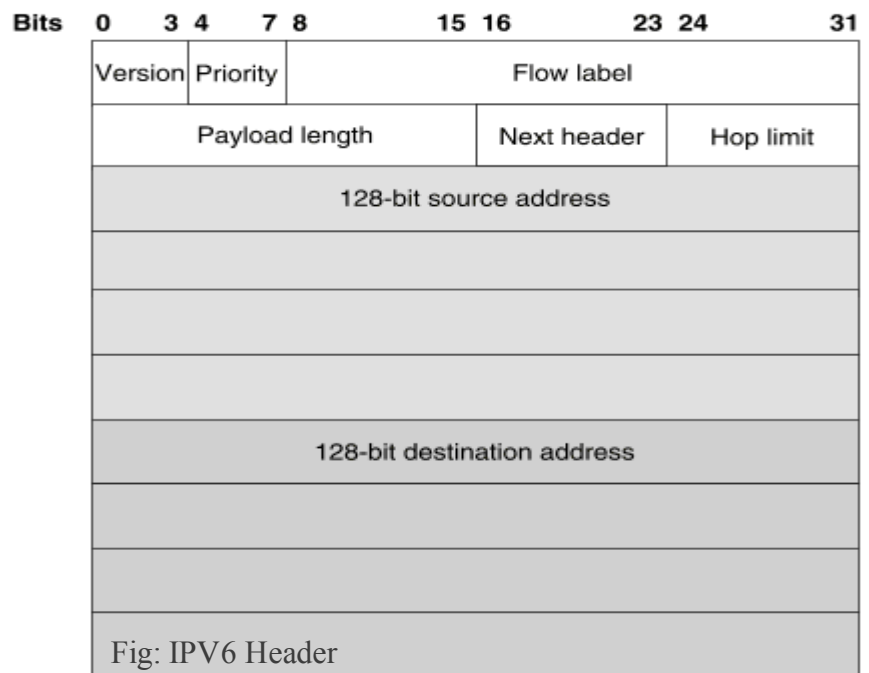
**source address** The 32-bit IPv4 address of the sending host.

**destination address** The 32-bit IPv4 address of the receiving host.

**Options** A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.

**Padding** Null bytes which are added to make the header length an integral multiple of 32 bytes as required by the header length field.

**IPv6 header:**



Specifically, IPv6 omits the following fields in its header.

- header length (the length is constant)
- identification
- flags



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

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

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

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

## IPV6 Addressing:

### Address Representation:

Represented by breaking 128 bit into Eight 16-bit segments (Each 4 Hex character each)

Each segment is written in Hexadecimal separated by colons.

Hex digit are not case sensitive.

#### Rule 1:

Drop leading zeros:

2001:0050:0000:0235:0ab4:3456:456b:e560

2001:050:0:235:ab4:3456:456b:e560

#### Rule2:

Successive fields of zeros can be represented as “::”, But double colon appear only once in the address.

FF01:0:0:0:0:0:1

FF01::1

*Note : An address parser identifies the number of missing zeros by separating the two parts and entering 0 until the 128 bits are complete. If two “::” notations are placed in the address, there is no way to identify the size of each block of zeros.*

### Ipv4 vs ipv6

IPV4	IPV6
1. source and destination addresses are 32 bits.)	1. Source and destination addresses are 128 bits.
2. ipv4 support small address space.	2. Supports a very large address space sufficeint for each and every people on earth.
3. ipv4 header includes checksum.	3. ipv6 header doesn't includes the checksum. (the upper-layer protocol or security extension header handles data integrity)
4. addresses are represented in dotted decimal format. (Eg. 192.168.5.1)	4. Addresses are represented in 16-bit segments Each segment is written in Hexadecimal separated by colons. (Eg. 2001:0050:020c:0235:0ab4:3456:456b:e560
5. Header includes options.	All optional data is moved to IPV6 extension header..
6. Broadcast address are used to send traffic to all	6. There is no IPV6 broadcast address. Instead a link

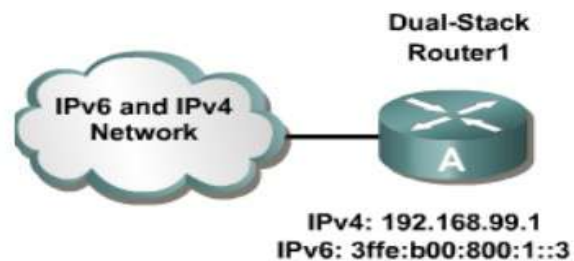
nodes on a subnet.	local scope all-nodes multicast address is used.
7. No identification of packet flow for QOS handling by router is present within the ipv4 header.	7. Packet flow identification for QOS handling by routers is present within the IPV6 header using the flow label field.
8. uses host address (A) resource records in the Domain name system(DNS) to map host names to ipv4 addresses.	8. Uses AAAA records in the DNS to map host names to ipv6 addresses.
9. Both routers and the sending host fragment packets.	9. Only the sending host fragments packets; routers do not.
10. ICMP Router Discovery is used to determine the IPv4 address of the best default gateway, and it is optional.	10. ICMPv6 Router Solicitation and Router Advertisement messages are used to determine the IP address of the best default gateway, and they are required.

## IPV6 Transition Mechanism:

1. Dual Stack
2. Tunneling Technique
3. Translation technique

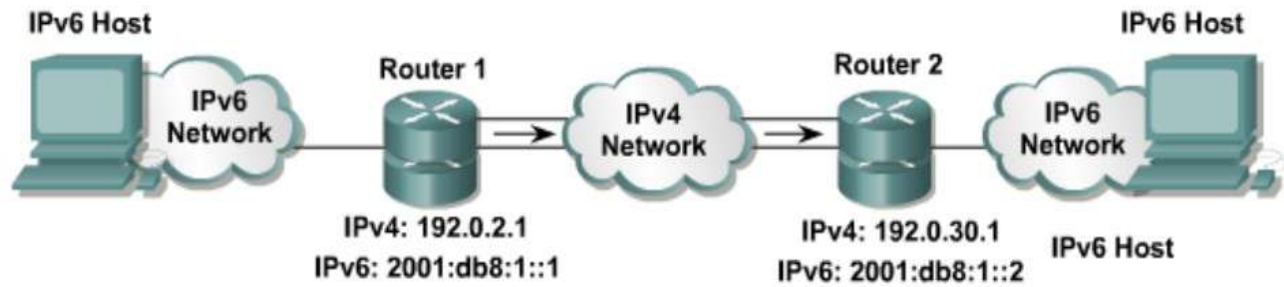
### Dual Stack:

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



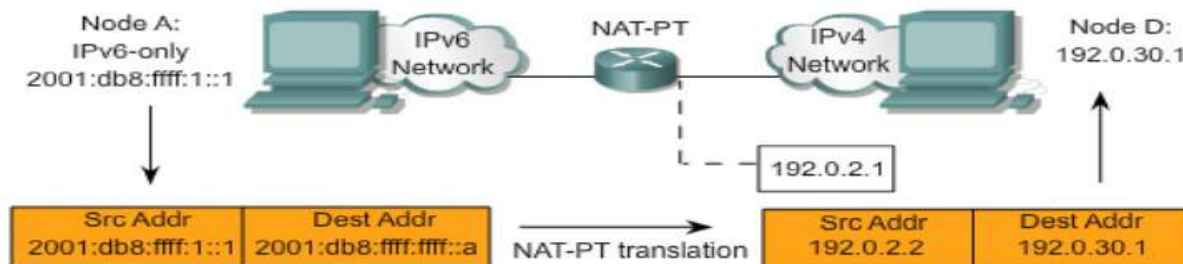
### Tunneling Technique

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



## NAT-Protocol Translation (NAT-PT)

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



## Chapter: 7 Network and Internet Layer

Network Layer and Design Issues; Virtual Circuit and Data grams Subject; Introduction of Routing – Shortest path Routing Algorithm, Flow Based Routing Algorithm. Distance Vector Routing Algorithm, Spanning Tree Routing; Congestion Control; Traffic Shaping and Leaky Bucket Algorithm.

### Design issues for the network layer.

The network layer has been designed with the following goals:

1. The services provided should be independent of the underlying technology. Users of the service need not be aware of the physical implementation of the network - for all they know, they're messages could be transported via carrier pigeon! This design goal has great importance when we consider the great variety of networks in operation. In the area of Public networks, networks in underdeveloped countries are nowhere near the technological prowess of those in the countries like the US or Ireland. The design of the layer must not disable us from connecting to networks of different technologies.
2. The transport layer (that is the host computer) should be shielded from the number, type and different topologies of the subnets he uses. That is, all the transport layer want is a communication link, it need not know how that link is made.
3. Finally, there is a need for some uniform addressing scheme for network addresses.

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

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

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

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

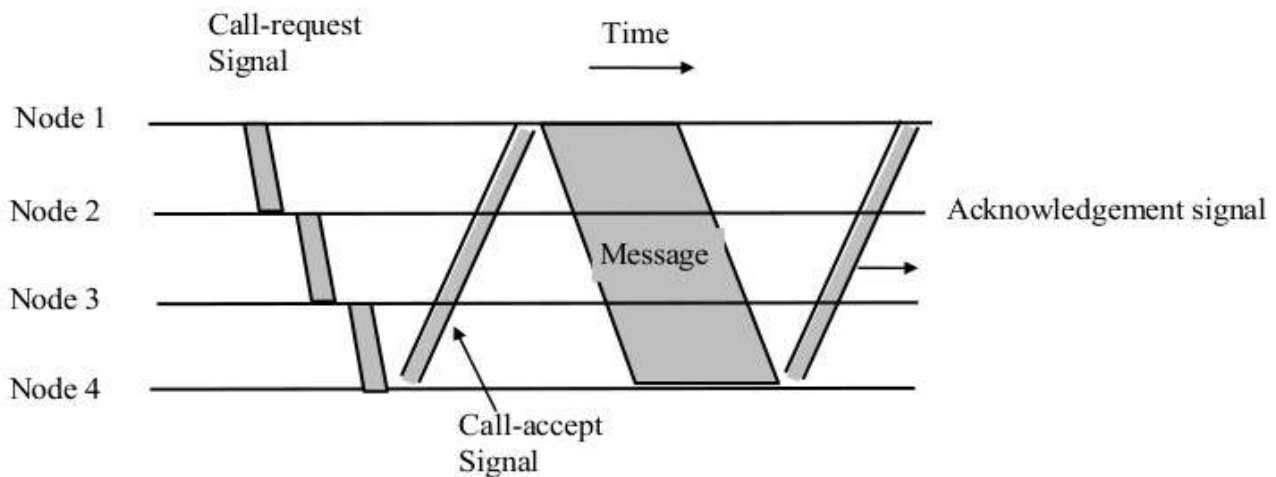
One would therefore think that the reliable nature of the connection oriented service would prompt people to choose it over the connectionless service - this is in fact not the case. One can never ensure that the network is 100% reliable, in fact for many applications we must assume that the network is not reliable at all. With this in mind, many applications perform their own error detection, flow and congestion control at a higher level in the protocol stack, that is, on their own machine, in the transport layer. So, if the sender and the receiver are going to engage in their own control mechanisms, why put this functionality into the network layer? This is the argument for the connectionless service: the network layer should provide a raw means of sending packets from a to b, and that is all. Proponents of this argument are quick to point out that the standard of our networks has increased greatly in the past years, that packets of information rarely ever do get lost, so much of the correction facilities in the network layer are redundant and serve only to complicate the layer and slow down transfer.

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

## Circuit Switching:

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

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



### *Circuit Switching*

#### **Examples: PSTN, PBX etc.**

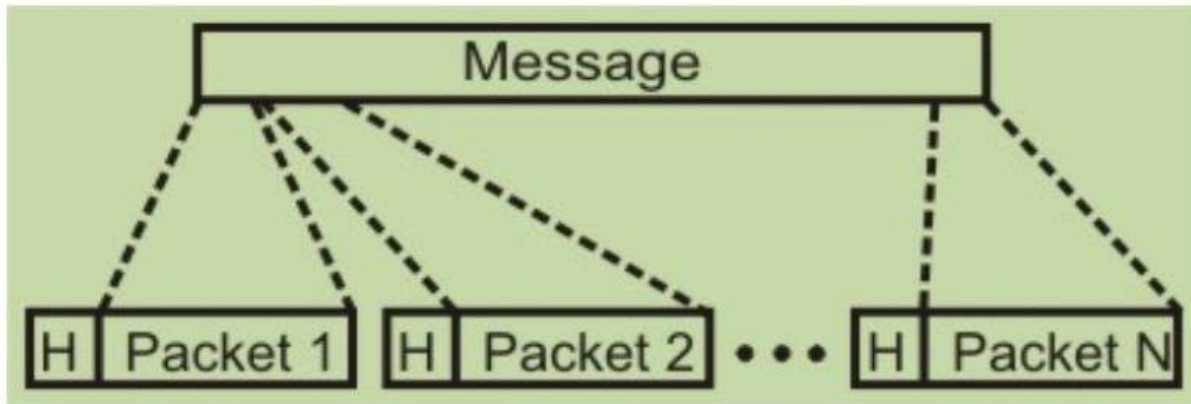
circuit switching telecommunication networks was originally designed to handle voice traffic, and the majority of the traffic on these networks continues to be voice. A key characteristics of the circuit switching is that resources within the network are dedicated to a particular call. For voice communication the resulting circuit will enjoy the high percentage of utilization because most of the time one party or the other is talking.

However, as the circuit-switching network began to be used increasingly for data connections, two shortcomings became apparent:

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

## Packet Switching:

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



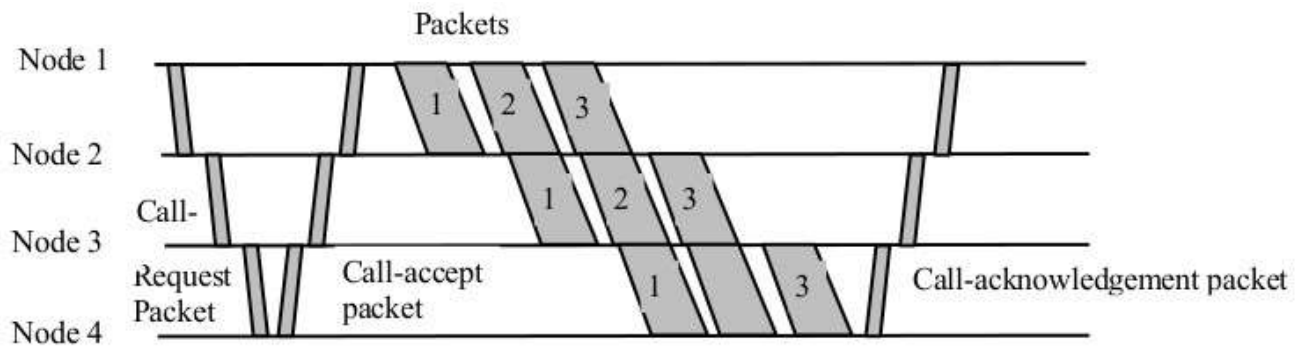
*A message is divided into a number of equal length short packets*

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

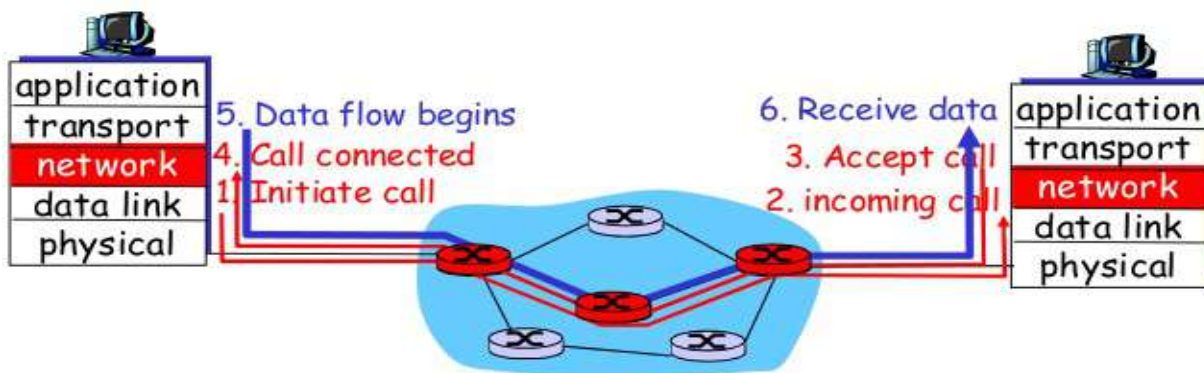
There are two basic approaches commonly used to packet Switching: **virtual circuit packet switching** and **datagram packet switching**. In virtual-circuit packet switching a virtual circuit is made before actual data is transmitted, but it is different from circuit switching in a sense that in circuit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

## Virtual Circuit:

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



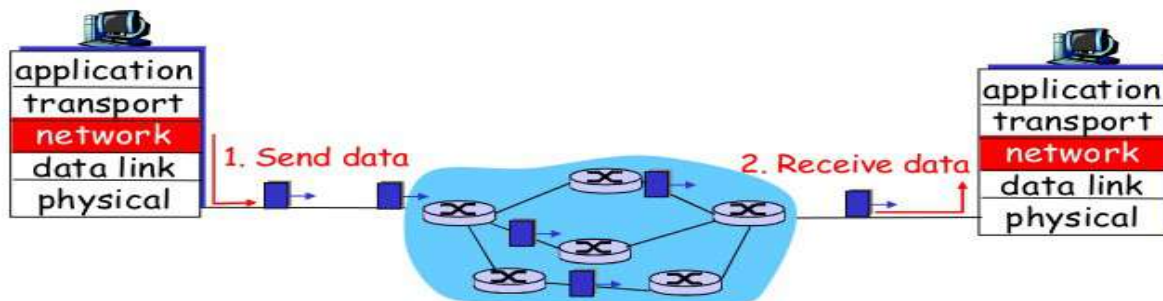
*Virtual circuit Packet Switching techniques*



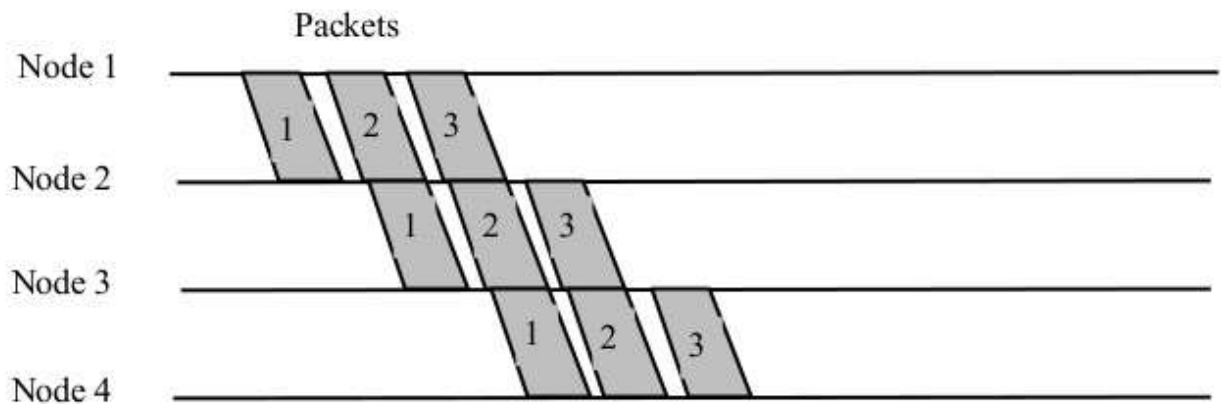
*Virtual Circuit*

## Datagram:

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



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



*Datagram Packet Switching*

### **Datagram Packet Switching Vs Virtual-circuit Packet Switching:**

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.

## **Router: (Introduction)**

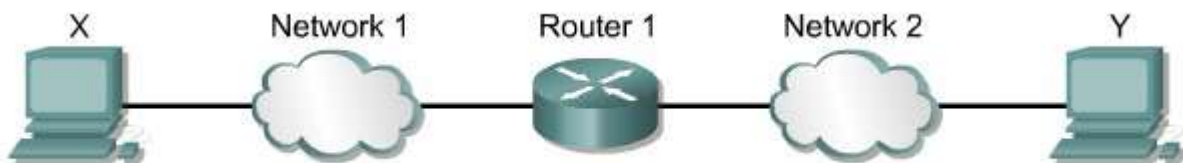
A Router is a computer, just like any other computer including a PC. Routers have many of the same hardware and software components that are found in other computers including:

- CPU
- RAM
- ROM
- Operating System

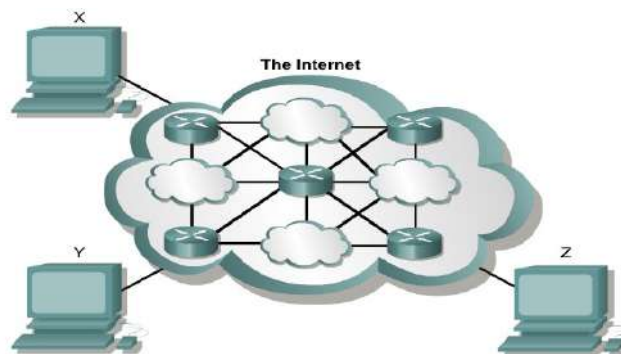




Router is the basic backbone for the Internet. The main function of the router is to connect two or more than two network and forwards the packet from one network to another. A router connects multiple networks. This means that it has multiple interfaces that each belong to a different IP network. When a router receives an IP packet on one interface, it determines which interface to use to forward the packet onto its destination. The interface that the router uses to forward the packet may be the network of the final destination of the packet (the network with the destination IP address of this packet), or it may be a network connected to another router that is used to reach the destination network.



*Router connects two network*



A router uses IP to forward packets from the source network to the destination network. The packets must include an identifier for both the source and destination networks. A router uses the IP address of the destination network to deliver a packet to the correct network. When the packet arrives at a router connected to the destination network, the router uses the IP address to locate the specific computer on the network.

# Routing and Routing Protocols:

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

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

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

## Static Routes:

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

## When to use static Routing:

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

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

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

## Connected Routes:

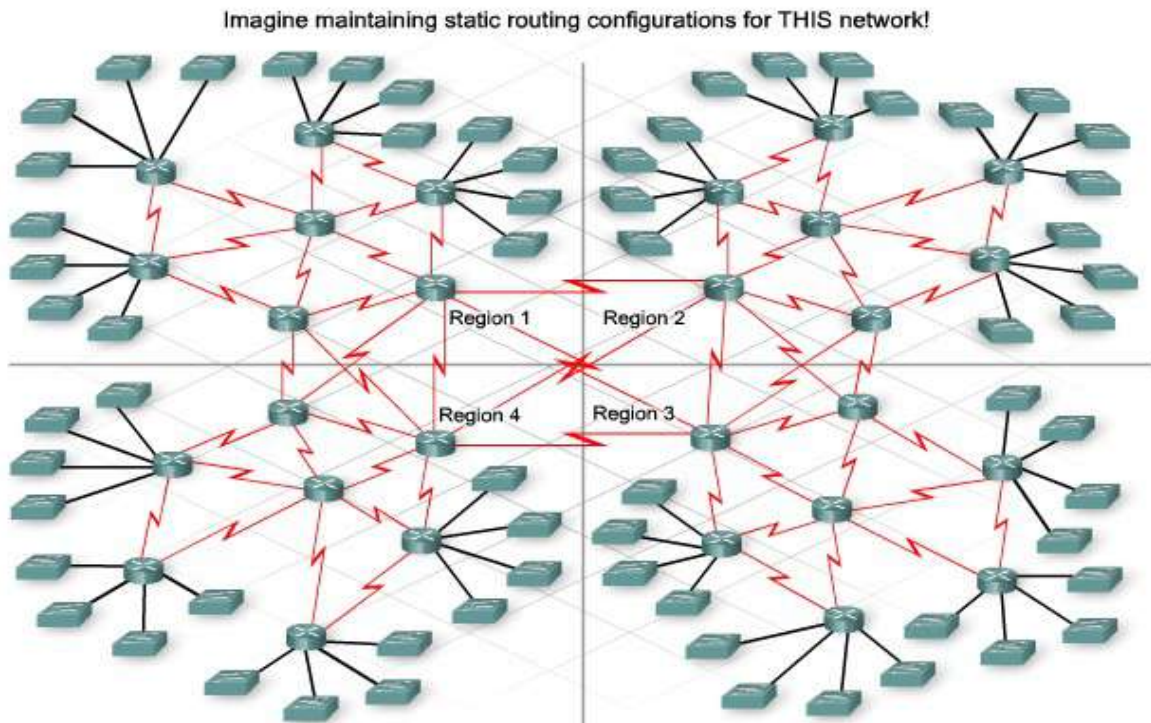
Those network that are directly connected to the Router are called connected routes and are not needed to configure on the router for routing. They are automatically routed by the Router.

## Dynamic Routes:

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

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

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



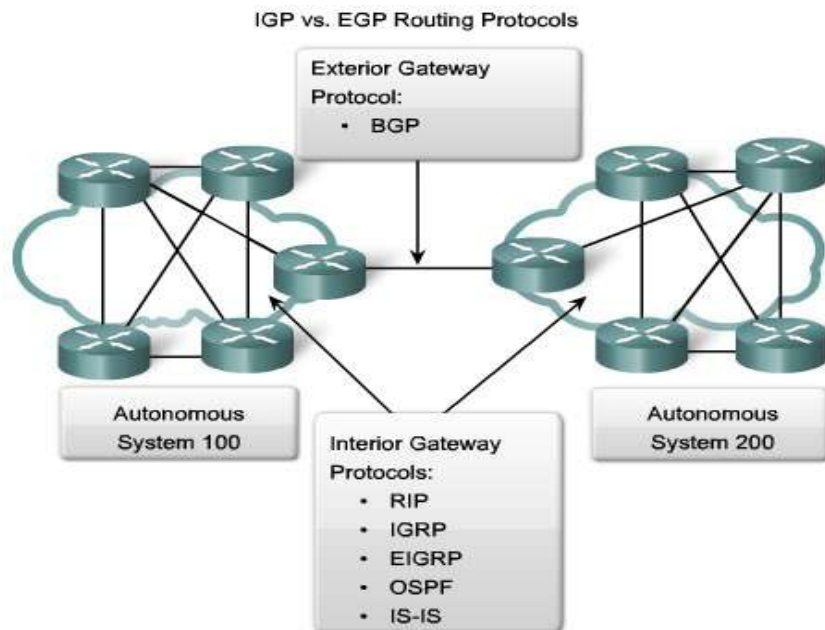
### Routing Protocol:

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

### Autonomous System:

An AS is a collection of networks under a common administration that share a common routing strategy. To the outside world, an AS is viewed as a single entity. The AS may be run by one or more operators while it presents a consistent view of routing to the external world.

The American Registry of Internet Numbers (ARIN), a service provider, or an administrator assigns a 16-bit identification number to each AS.



## Dynamic Routing Protocol:

1. Interior Gateway protocol (IGP)
  - I). Distance Vector Protocol
  - II). Link State Protocol
2. Exterior Gateway Protocol (EGP)

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

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

## Metric:

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

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

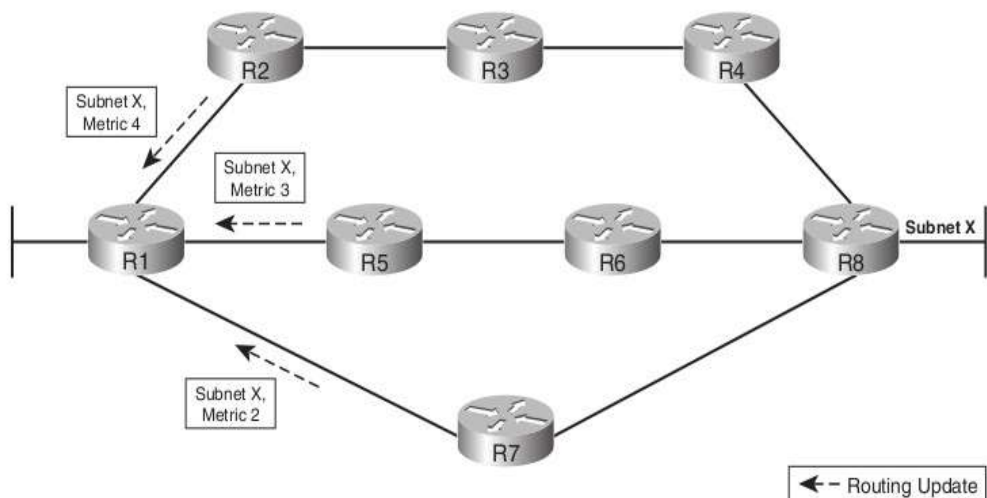
## Distance Vector Routing Algorithm:

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

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

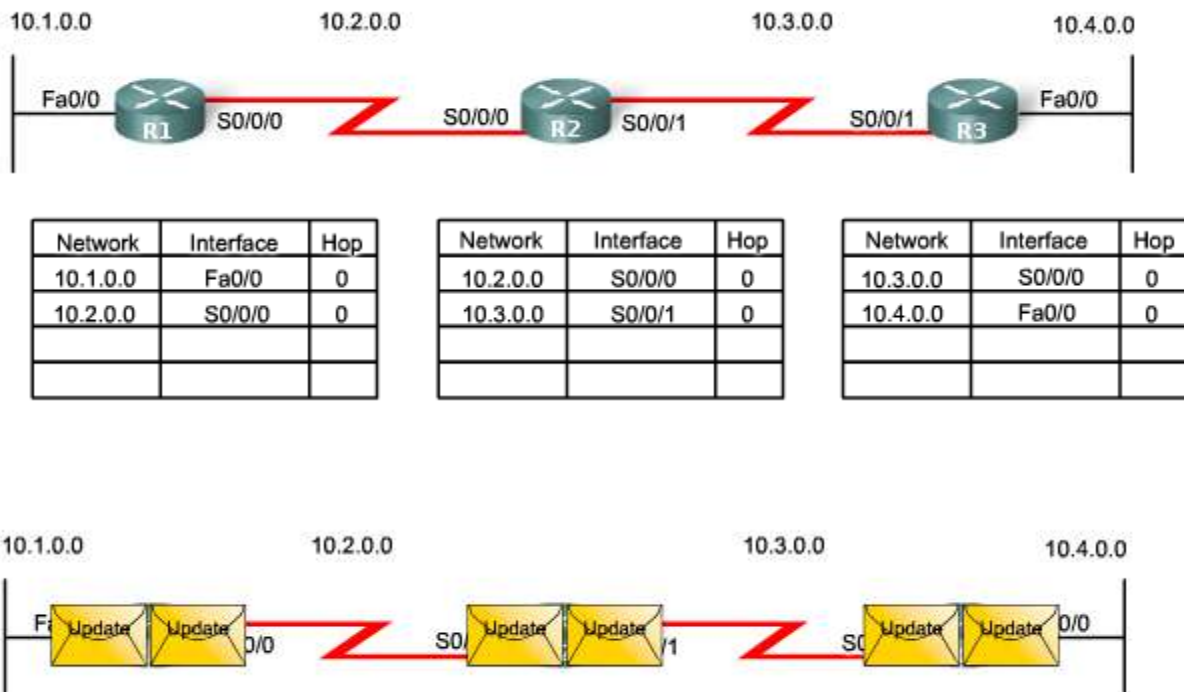
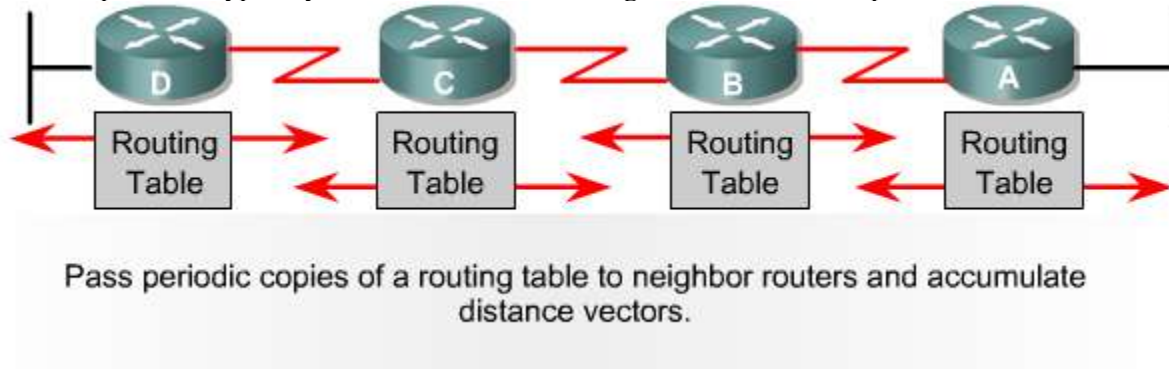
To show you more exactly what a distance vector protocol does, Figure shows a view of what a router learns with a distance vector routing protocol. The figure shows an internetwork in which R1 learns about three routes to reach subnet X:

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



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

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



### Initial Update:

#### R1

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

## R2

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

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

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

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

## R3

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

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

### Next Update:

#### R1

Sends an update about network 10.1.0.0 out the Serial 0/0/0 interface.

Sends an update about networks 10.2.0.0 and 10.3.0.0 out the FastEthernet0/0 interface.

Receives an update from R2 about network 10.4.0.0 with a metric of 2.

Stores network 10.4.0.0 in the routing table with a metric of 2.

Same update from R2 contains information about network 10.3.0.0 with a metric of 1. There is no change; therefore, the routing information remains the same.

#### R2

Sends an update about networks 10.3.0.0 and 10.4.0.0 out of Serial 0/0/0 interface.

Sends an update about networks 10.1.0.0 and 10.2.0.0 out of Serial 0/0/1 interface.

Receives an update from R1 about network 10.1.0.0. There is no change; therefore, the routing information remains the same.

Receives an update from R3 about network 10.4.0.0. There is no change; therefore, the routing information remains the same.

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

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

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



### R3

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

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

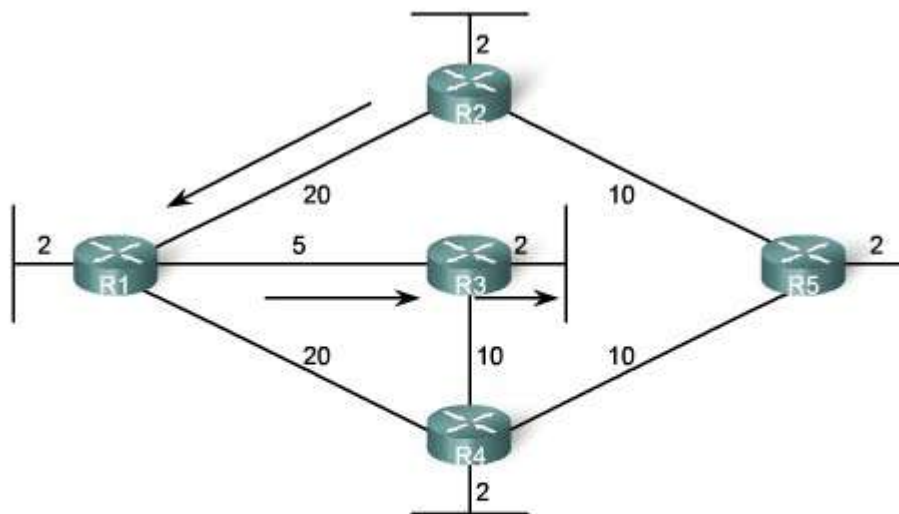
## Link State Routing Algorithm:

Also known as Shortest path Routing algorithm.

### Link states:

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

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



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

*Dijkstra's Shortest Path first algorithm*

So exactly how does a link-state routing protocol work? All routers will complete the following generic link-

state routing process to reach a state of convergence:

1. **Each router learns about its own links, its own directly connected networks.** This is done by detecting that an interface is in the up state.
2. **Each router is responsible for meeting its neighbors on directly connected networks.** link state routers do this by exchanging Hello packets with other link-state routers on directly connected networks.
3. **Each router builds a Link-State Packet (LSP) containing the state of each directly connected link.** This is done by recording all the pertinent information about each neighbor, including neighbor ID, link type, and bandwidth.
4. **Each router floods the LSP to all neighbors, who then store all LSPs received in a database.** Neighbors then flood the LSPs to their neighbors until all routers in the area have received the LSPs. Each router stores a copy of each LSP received from its neighbors in a local database.
5. **Each router uses the database to construct a complete map of the topology and computes the best path to each destination network.** Like having a road map, the router now has a complete map of all destinations in the topology and the routes to reach them. The SPF algorithm is used to construct the map of the topology and to determine the best path to each network.

## Advantages of Link state Routing protocol:

### Build the topological map:

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

### Faster Convergence:

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

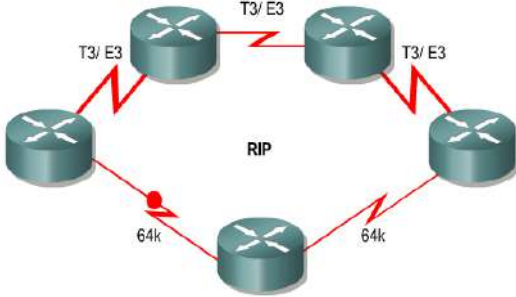
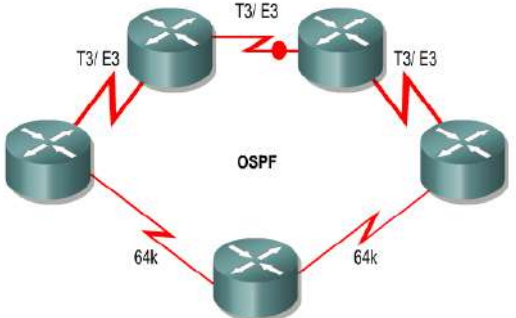
### Event Driven Updates:

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

## Distance vector vs. Link state:

Sno.	Distance Vector	Link State
1	Uses hop count as Metric.	Uses shortest path.
2	View the network from the perspective of neighbor.	Gets common view of entire network topology.
3	Has frequent and periodic updates	Has event triggered updates.
4	Slow convergence	Faster convergence



5	Susceptible to routing loops.	Not as susceptible to routing loops.
6	Easy to configure and administer.	Difficult to configure and administer.
7	Requires less memory and processing power of routers.	Requires more precessing power and memory than distance vector.
8	Consumes a lot of Bandwidth.	Consumes less BW than distance vector.
9	Passes copies of routing table to neighbor routers.	Passes link-state routing updates to other routers.
10	Eg. RIP 	Eg. OSPF 

### Flow based routing:

A flooding algorithm is an algorithm for distributing material to every part of a connected network. The name derives from the concept of inundation by a flood. Its implemented by the ospf:

### Advantages of Flooding

The main advantage of flooding the increased reliability provided by this routing method. Since the message will be sent at least once to every host it is almost guaranteed to reach its destination. In addition, the message will reach the host through the shortest possible path.

### Disadvantages of Flooding

There are several disadvantages with this approach to routing. It is very wasteful in terms of the networks total bandwidth. While a message may only have one destination it has to be sent to every host. This increases the maximum load placed upon the network.

Messages can also become duplicated in the network further increasing the load on the networks bandwidth as well as requiring an increase in processing complexity to disregard duplicate messages.

A variant of flooding called *selective flooding* partially addresses these issues by only sending packets to routers in the same direction.

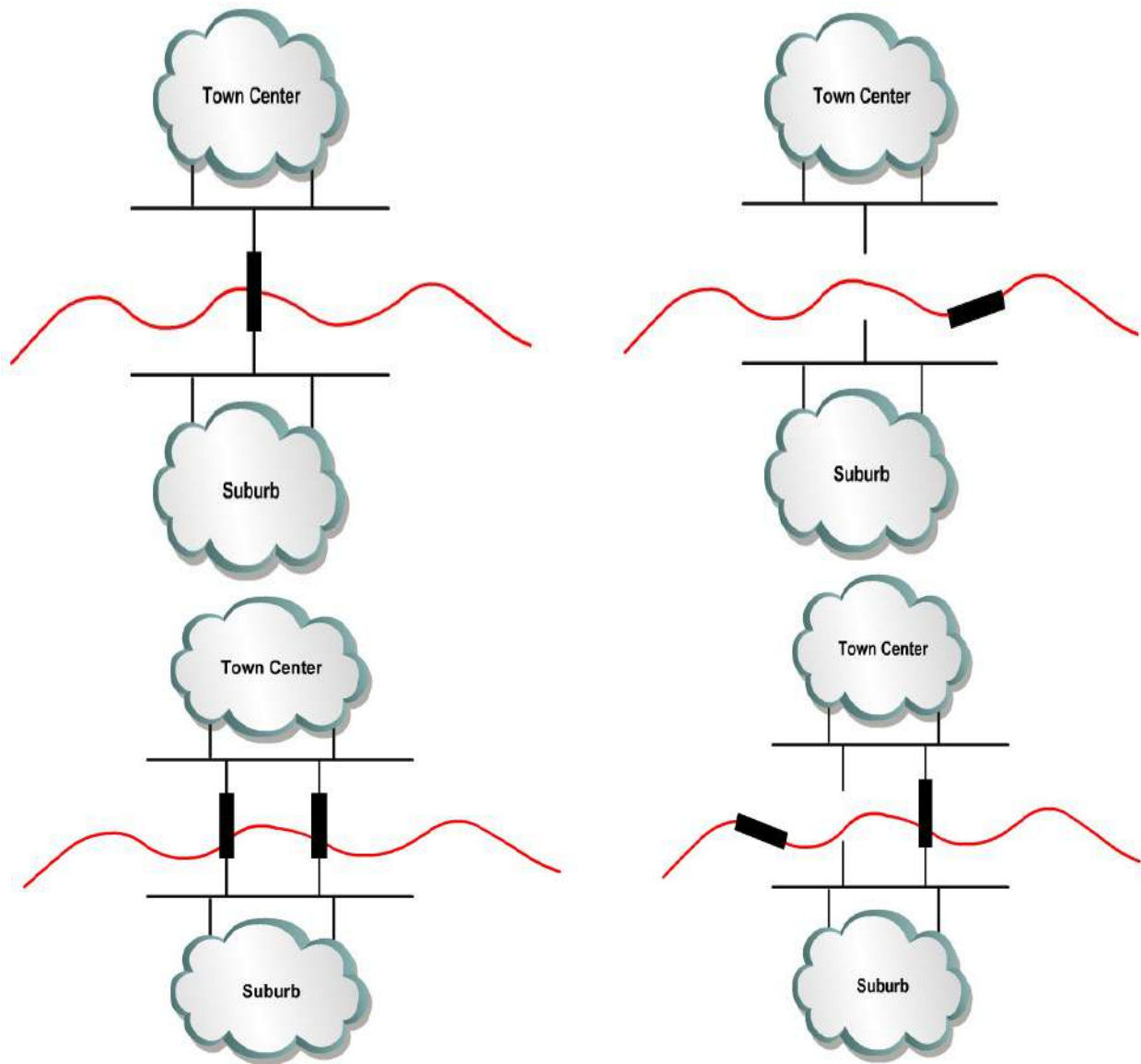
## Spanning Tree Protocol(STP)

### Need for Redundant Topology:

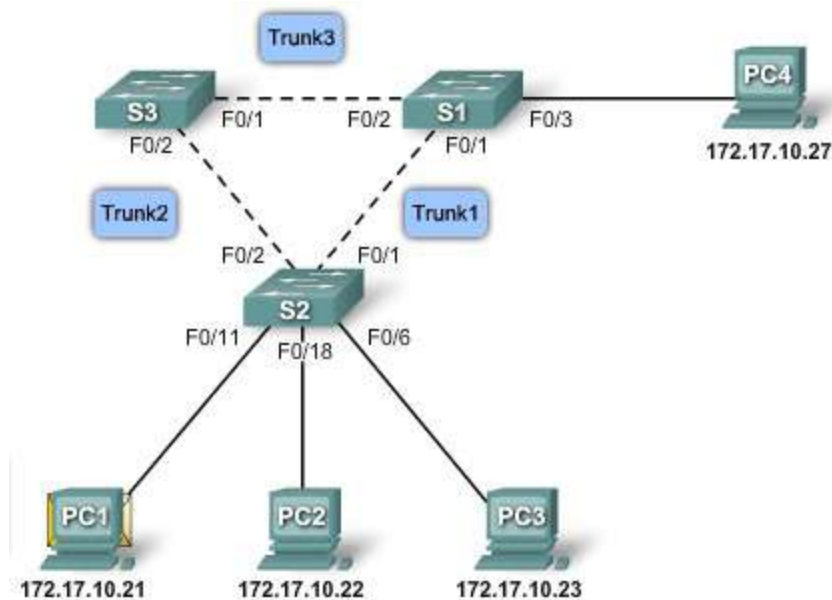
*The goal of redundant topologies is to eliminate network outages caused by a single point of failure. All networks need redundancy for enhanced reliability.*

A network of roads is a global example of a redundant topology. If one road is closed for repair, there is likely an alternate route to the destination. Consider a community separated by a river from the town center. If there is only one bridge across the river, there is only one way into town. The topology has no redundancy. If the bridge is flooded or damaged by an accident, travel to the town center across the bridge is impossible. A second bridge

across the river creates a redundant topology. The suburb is not cut off from the town center if one bridge is impassable.



## Issues with Redundancy:



*Redundant link*

## Layer 2 loops

Ethernet frames do not have a time to live (TTL) like IP packets traversing routers. As a result, if they are not terminated properly on a switched network, they continue to bounce from switch to switch endlessly or until a link is disrupted and breaks the loop.

## Broadcast storms

A broadcast storm occurs when there are so many broadcast frames caught in a Layer 2 loop that all available bandwidth is consumed. Consequently, no bandwidth is available for legitimate traffic, and the network becomes unavailable for data communication.

## Duplicate unicast frame:

Broadcast frames are not the only type of frames that are affected by loops. Unicast frames sent onto a looped network can result in duplicate frames arriving at the destination device.

## What is STP?

Redundancy increases the availability of the network topology by protecting the network from a single point of failure, such as a failed network cable or switch. When redundancy is introduced into a Layer 2 design, loops and duplicate frames can occur. Loops and duplicate frames can have severe consequences on a network. The **Spanning Tree Protocol (STP)** was developed to address these issues.

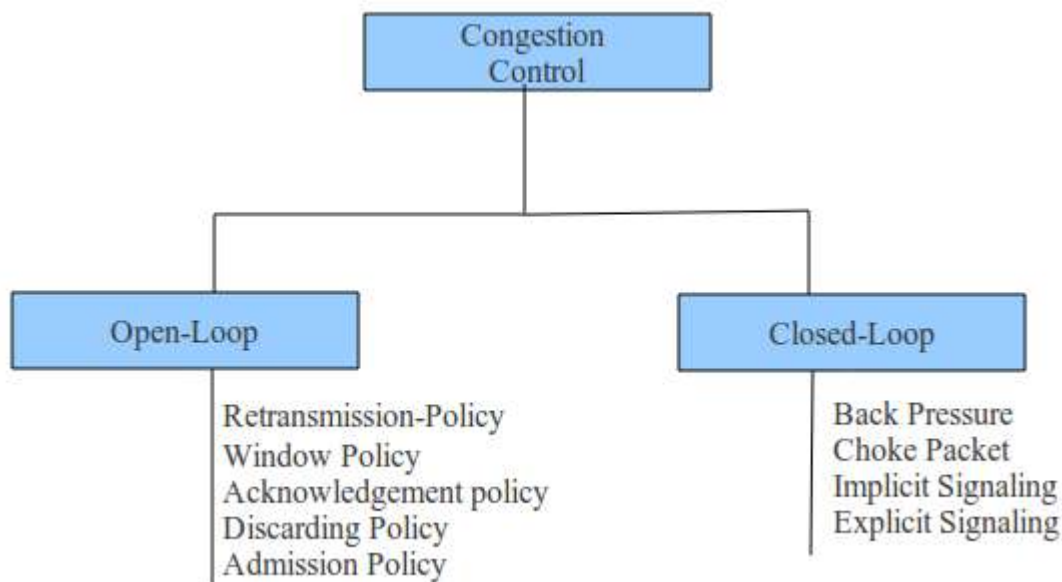
STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop. A port is considered blocked when network traffic is prevented from entering or leaving that port. This does not include bridge protocol data unit (BPDU) frames that are used by STP to prevent loops. You will learn more about STP BPDU frames later in the chapter. Blocking the redundant paths is critical to preventing loops on the network. The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops from occurring. If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

## Congestion control:

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

- When too many packets are pumped into the system, congestion occurs leading into degradation of performance.
- Congestion tends to feed upon itself and back up.
- Congestion shows lack of balance between various networking equipments.
- It is a global issue.

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



### Open Loop Congestion Control:

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

#### Retransmission Policy

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

## **Window Policy**

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

## **Acknowledgment Policy :**

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

## **Discarding Policy :**

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

## **Admission Policy :**

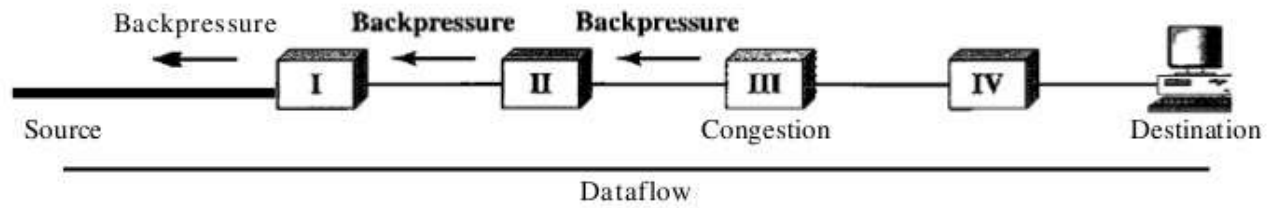
An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual- circuit connection if there is congestion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

## **Closed-Loop Congestion Control**

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

## **Back-pressure:**

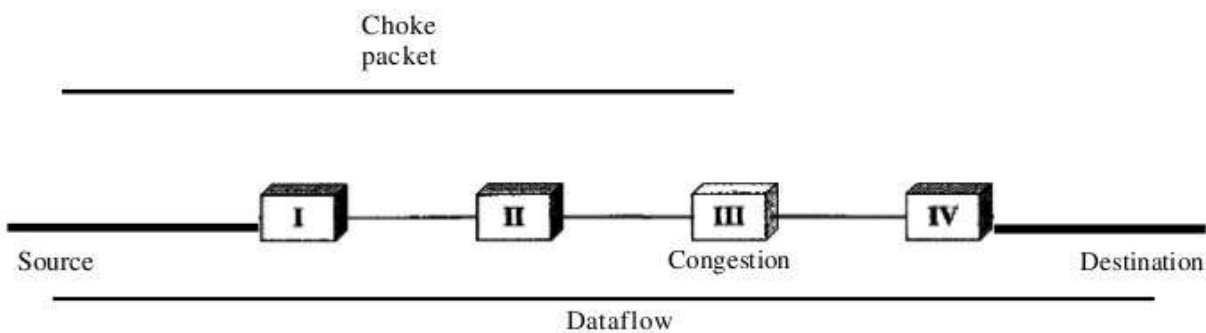
The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes. And so on.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



Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion. If so, node I informs the source of data to slow down. This, in time, alleviates the congestion. Note that the pressure on node III is moved backward to the source to remove the congestion. None of the virtual-circuit networks we studied in this book use backpressure. It was, however, implemented in the first virtual-circuit network, X.25. The technique cannot be implemented in a datagram network because in this type of network, a node (router) does not have the slightest knowledge of the upstream router.

## Choke Packet

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



## Implicit Signaling

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

## Explicit Signaling

The node that experiences congestion can explicitly send a signal to the source or destination. The explicit

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

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

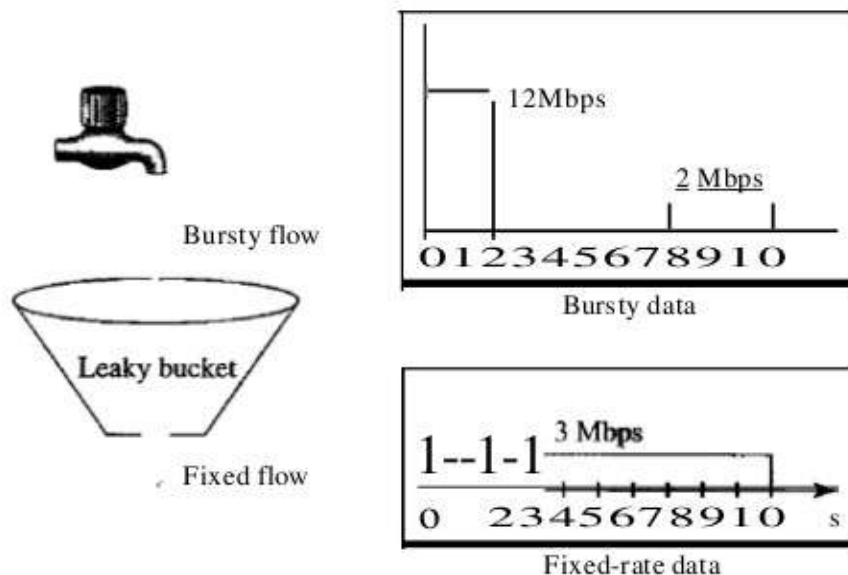
**Forward Signaling** A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

## Traffic Shaping

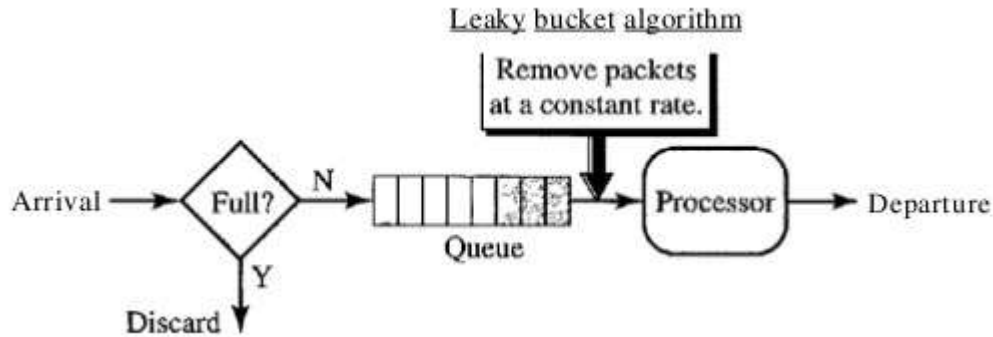
Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic: leaky bucket and token bucket.

### Leaky Bucket

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



In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In Figure 24.19 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. Without the leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host. We can also see that the leaky bucket may prevent congestion.



### *Leaky Bucket Implementation*

A simple leaky bucket implementation is shown in Figure 24.20. A FIFO queue holds the packets. If the traffic consists of fixed-size packets (e.g., cells in ATM networks), the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

The following is an algorithm for variable-length packets:

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.

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



## Chapter: 8 Network Servers and Protocols

HTTP, DHCP; SMTP, DNS, PROXY, FTP, POP and IMAP; Examples of Clients Servers Tools and Virtual private Networks.

### Hypertext Transfer Protocol HTTP:

A standard Internet protocol that specifies the client/server interaction processes between Web browsers such as Mozilla Firefox and Web servers such as Apache. It's the network protocol used to deliver virtually all files and other data (collectively called resources) on the World-Wide-Web, whether they are HTML files, image files, query results or anything else. Usually HTTP takes place through TCP/IP Sockets.

A Browser is an HTTP client because it sends requests to an HTTP server (Web Server), which then sends response back to the client. The standard and default port for the HTTP servers to listen is 80, though they can use any port.

#### What are Resources?

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

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

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

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

# HTTPS VS HTTP.

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

## DHCP(Dynamic Host Configuration Protocol)

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

### How It Works

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

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

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

#### 1. DHCPDISCOVER:

The client broadcasts a request for a DHCP server.

#### 2. DHCPOFFER:

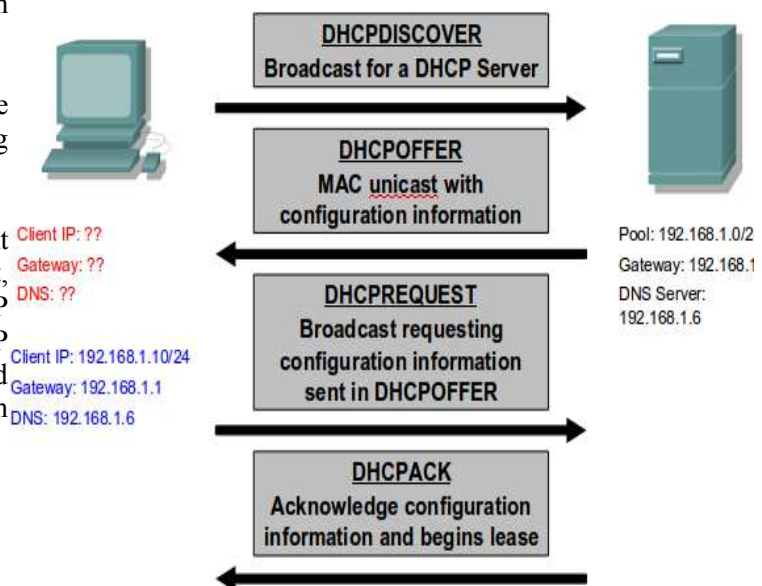
DHCP servers on the network offer an address to the client.

#### 3. DHCPREQUEST:

The client broadcasts a request to lease an address from one of the offering DHCP servers.

#### 4. DHCPACK:

The DHCP server that the client responds to acknowledges the client, assigns it any configured DHCP options, and updates its DHCP database. The client then initializes and binds its TCP/IP protocol stack and can begin network communication.





Ethernet Frame	IP	UDP	DHCP Request
SRC MAC: MAC A DST MAC: FF:FF:FF:FF:FF:FF	IP SRC: ? IP DST: 255.255.255.255	UDP 67	CIADDR: ?   GIADDR: ? Mask: ?   CHADDR: MAC A

MAC: Media Access Control Address  
 CIADDR: Client IP Address  
 GIADDR: Gateway IP Address  
 CHADDR: Client Hardware Address



Ethernet Frame	IP	UDP	DHCP Reply
SRC MAC: MAC Serv DST MAC: MAC A	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10   GIADDR: ? Mask: 255.255.255.0   CHADDR: MAC A

MAC: Media Access Control Address  
 CIADDR: Client IP Address  
 GIADDR: Gateway IP Address  
 CHADDR: Client Hardware Address

## Domain Name System (DNS):

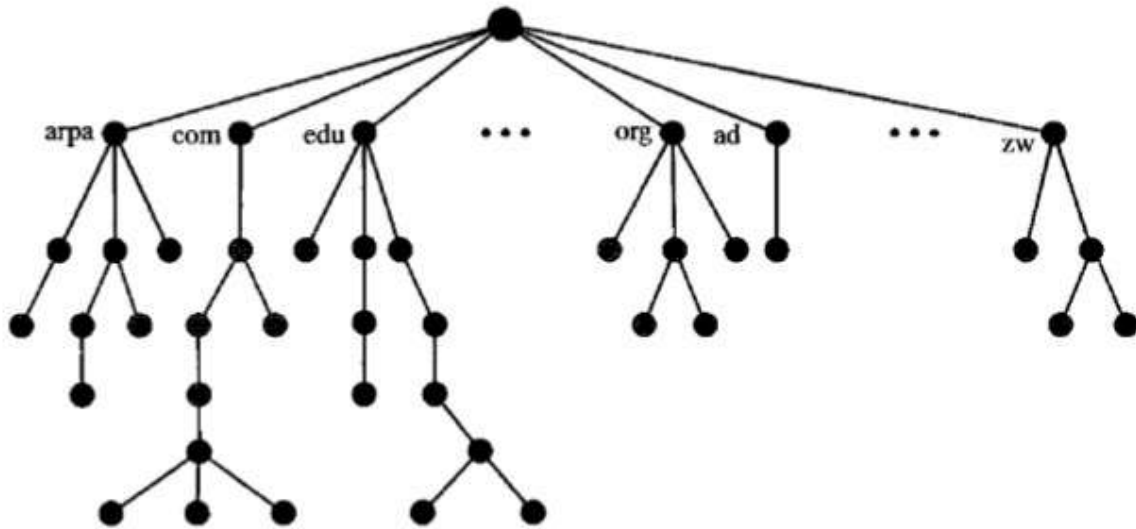
IP address are tough for human to remember and impossible to guess. Domain Name System are usually used to translate a hostname or Domain name (eg. nec.edu.np) into an IP address (eg. 202.37.94.177). Domain name comprise a hierarchy so that names are unique, yet easy to remember.

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

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

## Domain Name Space:

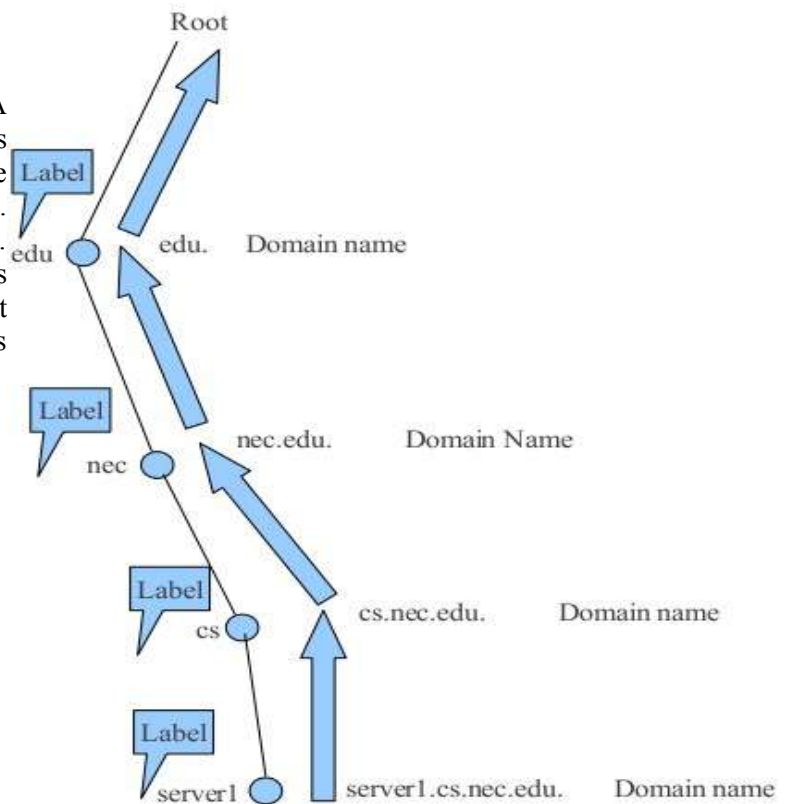
To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127 .



*Fig: Domain Name Space*

### Domain Name

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



*Fig: Domain Name and Labels*

### Fully Qualified Domain Name

If a label is terminated by a null string, it is called a fully qualified domain name (FQDN). An FQDN is a domain name that contains the full name of a host. It contains all labels, from the most specific to the most general, that uniquely define the name of the host. For example, the domain name `server1.cs.nec.edu.` is the FQDN of a computer named `server1` installed at the NEC Collete. A DNS server can only match an FQDN to an address. Note that the name must end with a null label, but because null means nothing, the label ends with a dot (.).

### Partially Qualified Domain Name

If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN). A PQDN starts from a node, but it does not reach the root. It is used when the name to be resolved belongs to the same site as the client. Here the resolver can supply the missing part, called the suffix, to create an FQDN. For example, if a user at the `nec.edu.` site wants to get the IP address of the challenger computer, he or she can define the partial name `server1`.

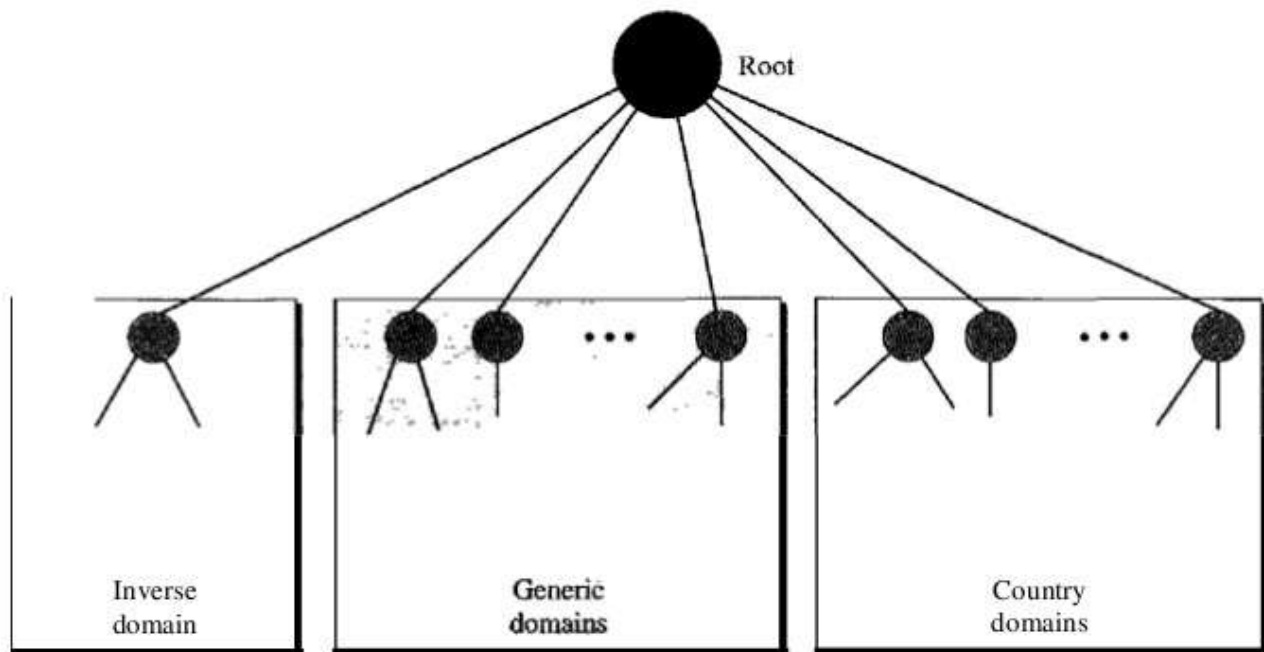
The DNS client adds the suffix `cs.nec.edu` before passing the address to the DNS server. The DNS client normally holds a list of suffixes. The following can be the list of suffixes at NEC College. The null suffix defines nothing. This suffix is added when the user defines an FQDN.

`cs.nec.edu`

`nec.edu`

`null`

### DNS in the Internet:



### Generic Domains

The generic domains define registered hosts according to their generic behavior. Each node in the tree defines a domain, which is an index to the domain name space database

<i>Label</i>	<i>Description</i>
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

Fig: Generic Domain Labels

## Country Domains

The country domains section uses two-character country abbreviations (e.g., np for Nepal and us for United States). Second labels can be organizational, or they can be more specific, national designations. The United States, for example, uses state abbreviations as a subdivision of us (e.g., ca.us.).

## Inverse Domain

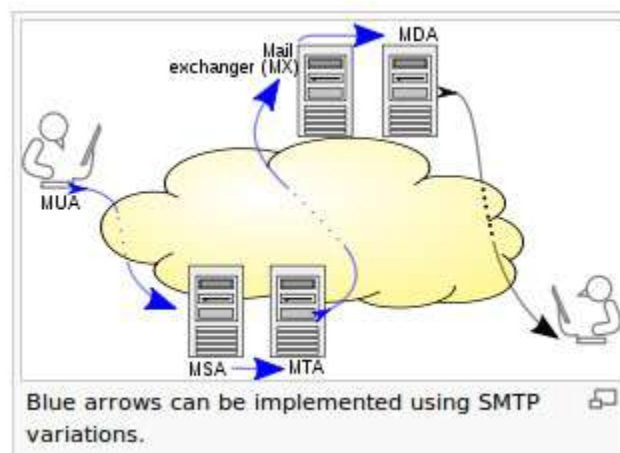
The inverse domain is used to map an address to a name. This may happen, for example, when a server has received a request from a client to do a task. This type of query is called an inverse or pointer (PTR) query. To handle a pointer query, the inverse domain is added to the domain name space with the first-level node called arpa (for historical reasons). The second level is also one single node named in-addr (for inverse address). The rest of the domain defines IP addresses.

# Simple Mail Transfer Protocol (SMTP)

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

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

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



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

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

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

Once the MX target accepts the incoming message, it hands it to a mail delivery agent (MDA) for local mail delivery. An MDA is able to save messages in the relevant mailbox format. Again, mail reception can be done using many computers or just one —the picture displays two nearby boxes in either case. An MDA may deliver

messages directly to storage, or forward them over a network using SMTP, or any other means, including the Local Mail Transfer Protocol (LMTP), a derivative of SMTP designed for this purpose.

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

## **IMAP:(Internet Mail Access Protocol)**

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

### **How It Works**

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

IMAP4 provides mechanisms for storing messages received by SMTP in a receptacle called a mailbox. An IMAP4 server stores messages received by each user until the user connects to download and read them using an IMAP4 client such as Evolution or Microsoft Outlook Express.

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

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

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

- **LIST:**  
Retrieves a list of folders in the client's mailbox
- **SELECT:**  
Selects a particular folder to access its messages
- **FETCH:**  
Retrieves individual messages
- **LOGOUT:**  
Ends the IMAP4 session



## Post Office Protocol version 3 (POP3)

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

### How It Works

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

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

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

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

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

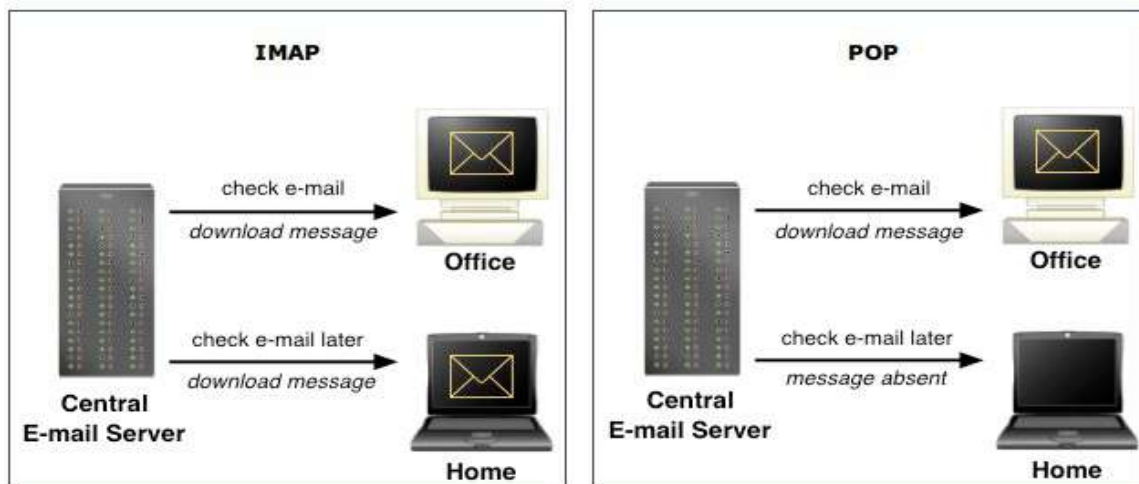
## IMAP VS POP:

### What's the difference?

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

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

POP does the opposite. Instead of just showing you what is in your inbox on the U's mail server, it checks the server for new messages, downloads all the new messages in your inbox onto your computer, and then deletes them from the server. This means that every time you use POP to view your new messages, they are no longer on the central mail server. Figure illustrates these concepts



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

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

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

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

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

Feature	POP3	IMAP
Where is protocol defined	RFC 1939	RFC 2060
TCP port used	110	143
Where is e-mail stored	User's PC	Server
Where is e-mail read	Off-line	On-line
Connect time required	Little	Much
Use of server resources	Minimal	Extensive
Multiple mailboxes	No	Yes
Who backs up mailboxes	User	ISP
Good for mobile users	No	Yes
User control over downloading	Little	Great
Partial message downloads	No	Yes
Are disk quotas a problem	No	Could be in time
Simple to implement	Yes	No
Widespread support	Yes	Growing

# Virtual Private Network (VPN)

The Internet is a worldwide, publicly accessible IP network. Due to its vast global proliferation, it has become a viable method of interconnecting remote sites. However, the fact that it is a public infrastructure has deterred most enterprises from adopting it as a viable remote access method for branch and SOHO sites.

A virtual private network (VPN) is a concept that describes how to create a private network over a public network infrastructure while maintaining confidentiality and security. VPNs use cryptographic tunneling protocols to provide sender authentication, message integrity, and confidentiality by protecting against packet sniffing. VPNs can be implemented at Layers 2, 3, and 4 of the Open Systems Interconnection (OSI) model.

Figure illustrates a typical VPN topology. Components required to establish a VPN include:

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

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

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

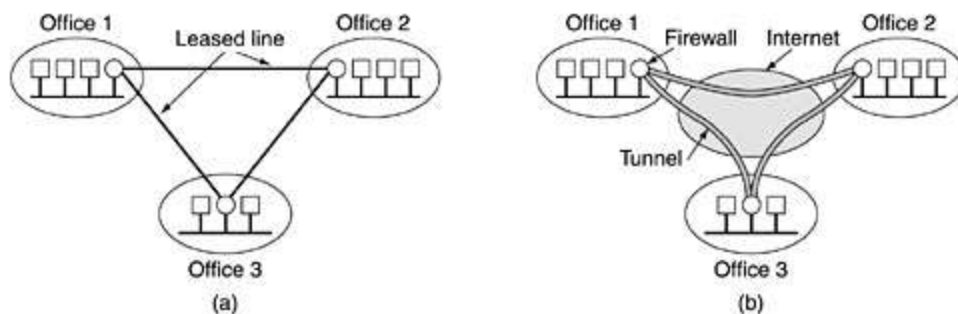
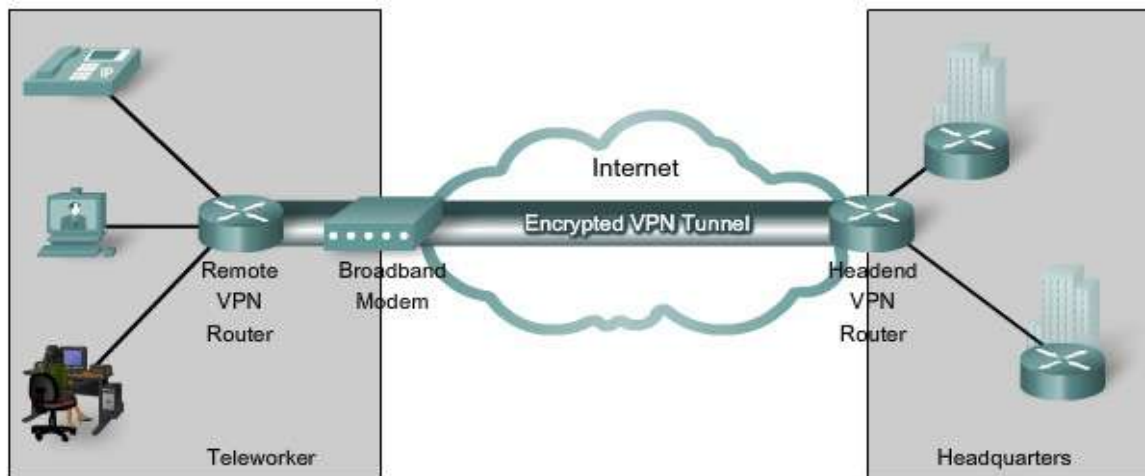


Fig:(a) A leased-line private network. (b) A virtual private network.

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

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

- Extend geographic connectivity
- Improve security
- Reduce operational costs versus traditional WAN
- Reduce transit time and transportation costs for remote users
- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide telecommuter support
- Provide broadband networking compatibility
- Provide faster ROI (return on investment) than traditional WAN

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

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

## IPSEC

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

*IPsec is an Internet Engineering Task Force (IETF) standard (RFC 2401-2412) that defines how a VPN can be created over IP networks.*

**IPsec provides the following essential security functions:**

**Data confidentiality:** IPsec ensures confidentiality by using encryption. Data encryption prevents third parties from reading the data, especially data that is transmitted over public networks or wireless networks. The IPsec sender can encrypt packets before transmitting the packets across a network and prevent anyone from hearing or viewing the communication (eavesdropping).

**Data integrity:** IPsec ensures that data arrives unchanged at the destination; that is, that the data is not manipulated at any point along the communication path. IPsec ensures data integrity by using hashes.

**Data origin authentication:** The IPsec receiver can authenticate the source of the IPsec packets. Authentication ensures that the connection is actually made with the desired communication partner.

**Anti-replay:** Anti-replay protection verifies that each packet is unique, not duplicated. IPsec packets are protected by comparing the sequence number of the received packets and a sliding window on the destination host, or security gateway. A packet whose sequence number is before the sliding window is considered late, or a duplicate. Late and duplicate packets are dropped.

## proxy server

A computer that can act on the behalf of other computers to request content from the Internet or an intranet. Proxy Server is placed between a user's machine and the Internet. It can act as a firewall to provide protection and as a cache area to speed up Web page display.

A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

**Proxy servers have two main purposes:**

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

## Types of Proxy:

### 1. Forward Proxy:

Forward proxies are proxies where the client server names the target server to connect to. Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).

The terms "forward proxy" and "forwarding proxy" are a general description of behavior (forwarding traffic) and thus ambiguous. Except for Reverse proxy

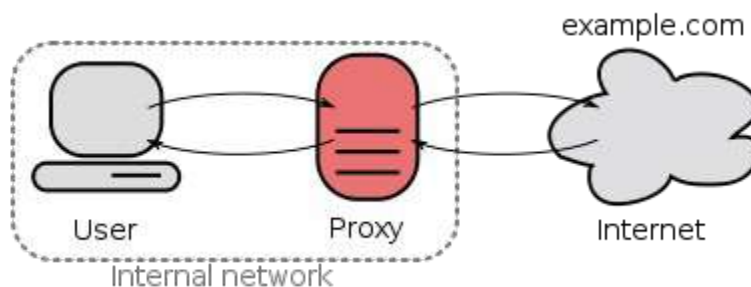


Fig:A forward proxy taking requests from an internal network and forwarding them to the Internet

### 2. Open Proxy:

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

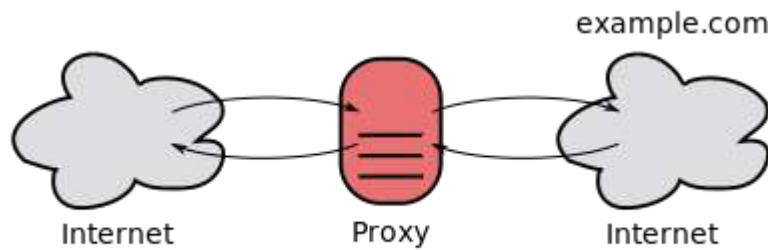


Fig: An open proxy forwarding requests from and to anywhere on the Internet.

### 3. Reverse Proxy:

A **reverse proxy** is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more origin servers which handle the request. The response is returned as if it came directly from the proxy server

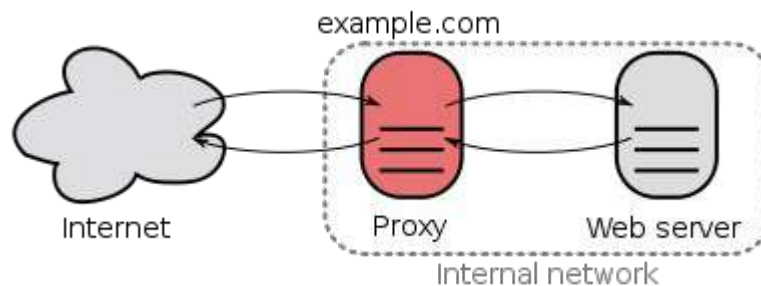


Fig: A reverse proxy taking requests from the Internet and forwarding them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network.

## File Transfer Protocol (FTP)

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

### How It Works

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

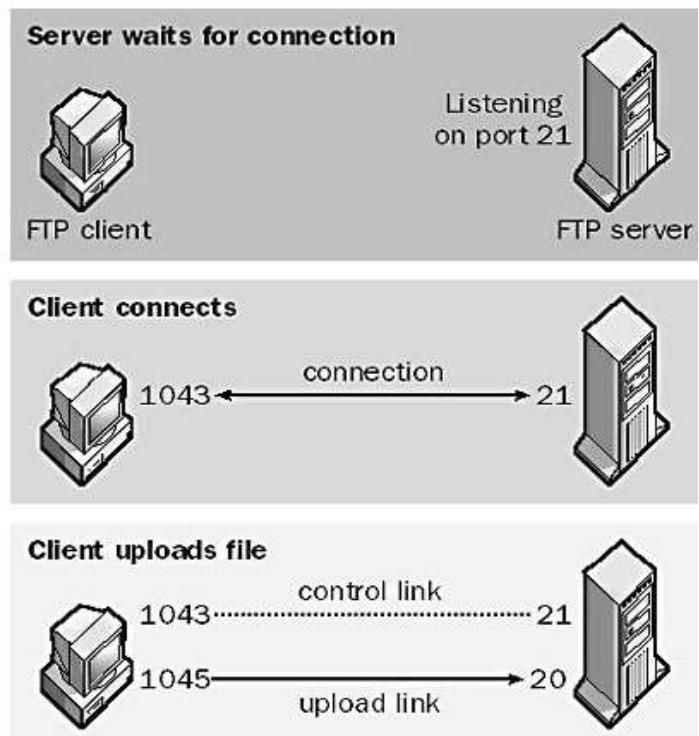
**While transferring Data over the network, two modes can be used:**

1. Ascii Mode
2. Binary Mode

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

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

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



## Chapter9: Network Management and Security:

Introduction to Network management, Internet Network – Management framework (SMI & HIB) & SNMP protocol; Data encryption, Data Encryption standard; Principles of Cryptography (Symmetric Key & public key Encryption). Integrity & Principles of cryptography (Symmetric Key & public key Encryption) Integrity & firewalls.

### Introduction to Network Management:

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

### Functions of Network Management System:

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

#### Configuration Management

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

#### Fault Management:

Falls on two categories.

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

#### Performance management:

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

#### Security Management

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

#### Accounting Management

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

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



# Simple Network Management Protocol(SNMP)

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

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

## Concept

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

## Managers and Agents

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

## An SNMP-managed network consists of three key components:

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

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

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

A **network management system (NMS)** executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

Management with SNMP is based on three basic ideas:

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

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

To do management tasks, SNMP uses two other protocols:

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

### **Role of SNMP**

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

### **Roles of SMI**

SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values. SMI does not define the number of objects an entity should manage or name the objects to be managed or define the association between the objects and their values.

The Structure of Management Information, version 2 (SMIv2) is a component for network management. Its functions are

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

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

### **Roles of MIB**

For each entity to be managed, this protocol must define the number of objects, name them according to the rules defined by SMI, and associate a type to each named object. *MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.*

Each agent has its own MIB2, which is a collection of all the objects that the manager can manage. The objects in MIB2 are categorized under 10 different groups: system, interface, address translation, ip, icmp, tcp, udp, egp, transmission, and snmp.

### **Analogy:**

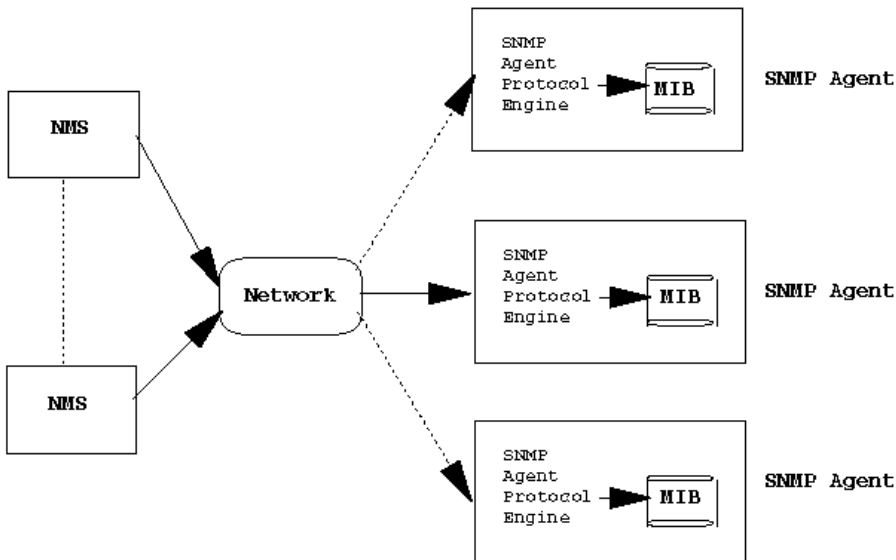
We can compare the task of network management to the task of writing a program.

- Both tasks need rules. In network management this is handled by SMI.
- Both tasks need variable declarations. In network management this is handled by MIB.
- Both tasks have actions performed by statements. In network management this is handled by SNMP.

## **Network Management Architectures**

Network management system contains two primary elements: a manager and agents. The Manager is the console through which the network administrator performs network management functions. Agents are the entities that interface to the actual device being managed. Bridges, Hubs, Routers or network servers are examples of managed devices that contain managed objects. These managed objects might be hardware, configuration parameters, performance statistics, and so on, that directly relate to the current operation of the device in question. These objects are arranged in what is known as a virtual information database, called a management information base, also called MIB. SNMP allows managers and agents to communicate for the purpose of accessing these objects.

## Architecture



### **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
  - Set variables in agents




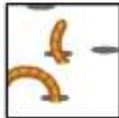
## **Computer security requirements and Attacks:**

Computer and network security address four requirements:

1. **Confidentiality:** Requires that data only be accessible by authorized parties. This types of access includes printing, displaying and other forms of disclosure of the data.
2. **Integrity:** Requires that data can be modified only by authorized users. Modification includes writing, changing, changing status, deleting and creating.
3. **Availability:** Requires that data are available to authorized parties.
4. **Authenticity:** Requires that host or service be able to verify the identity of a user.

## Types of Network Attacks

There are four primary classes of attacks.

1. **Reconnaissance** : Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, it precedes another type of attack. Reconnaissance is similar to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows.  Reconnaissance
2. **Access** : System access is the ability for an intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.  Access
3. **Denial of Service** : Denial of service (DoS) is when an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack involves simply running a hack or script. For these reasons, DoS attacks are the most feared.  Denial of Services
4. **Worms, Viruses, and Trojan Horses** : Malicious software can be inserted onto a host to damage or corrupt a system, replicate itself, or deny access to networks, systems, or services. Common names for this type of software are worms, viruses, and Trojan horses.  Worms, Viruses, and Trojan Horses

## Data Encryption/Decryption, Cryptography, Integrity & Firewalls:

### Cryptography

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

### Encryption and Decryption



## Plain-text and Cipher-text

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

## Cipher

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

## Key

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

## Alice, Bob, and Eve

In cryptography, it is customary to use three characters in an information exchange scenario; we use Alice, Bob, and Eve. Alice is the person who needs to send secure data. Bob is the recipient of the data. Eve is the person who somehow disturbs the communication between Alice and Bob by intercepting messages to uncover the data or by sending her own disguised messages. These three names represent computers or processes that actually send or receive data, or intercept or change data.

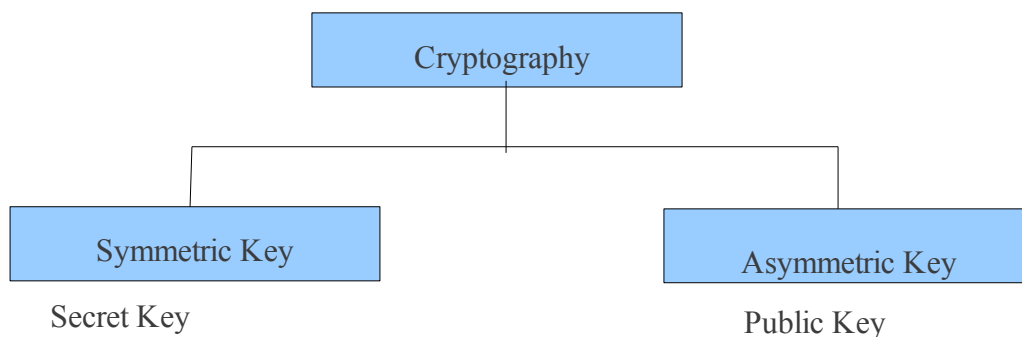
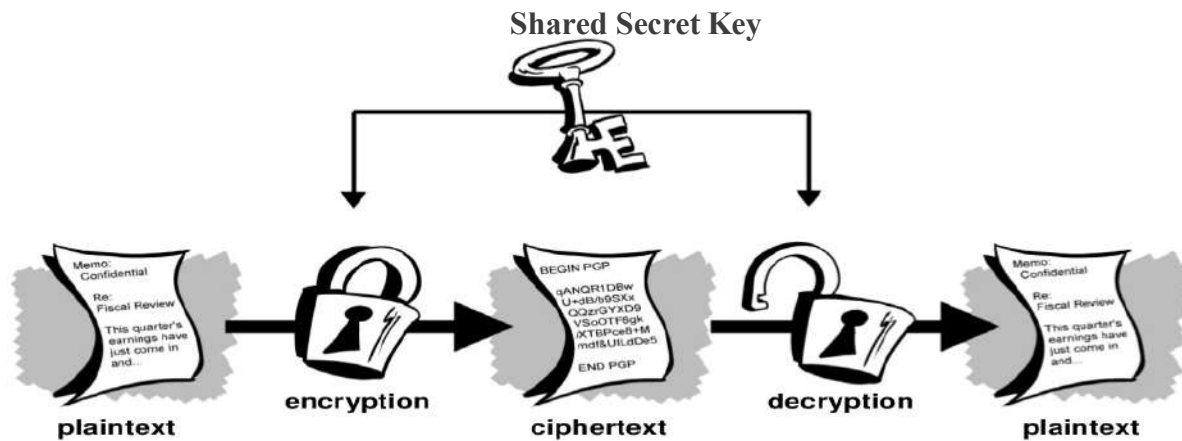


Fig:Categories of Cryptography

## Symmetric-key

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

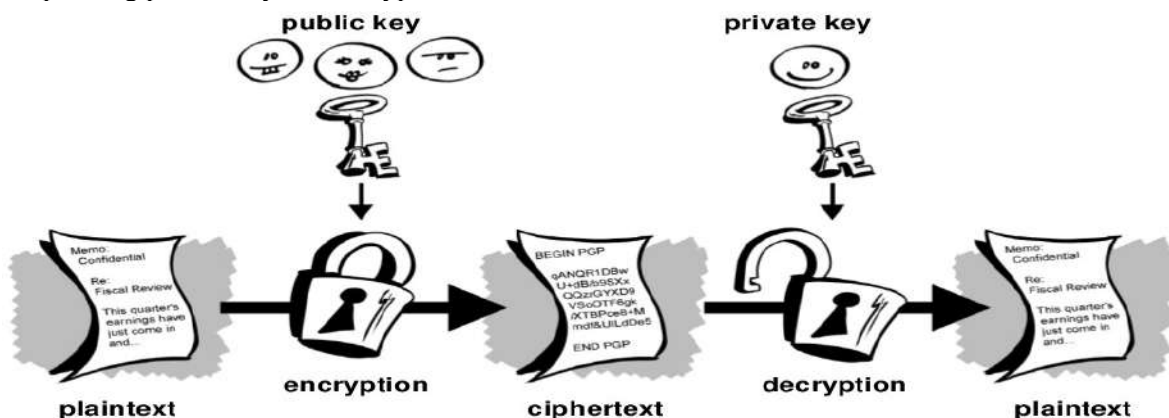


Conventional encryption has benefits. It is very fast. It is especially useful for encrypting data that is not going anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution.

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

## Asymmetric-Key Cryptography

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



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

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

the message because only Alice knows the Alice's private key.

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

### **Comparison**

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

### **Traditional Cipher used in Symmetric-key Cryptography:**

Two types:

1. Substitution cipher
2. Transposition cipher

### **Substitution cipher:**

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

For example, if we encode the word “SECRET” using Caesar’s key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet.

So starting with

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get

DEFGHIJKLMNOPQRSTUVWXYZABC

where D=A, E=B, F=C, and so on.

Using this scheme, the plaintext, “SECRET” encrypts as “VHFUHW.” To allow someone else to read the ciphertext, you tell them that the key is 3.

### **Transposition Ciphers**

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

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

Plaintext:      2 4 1 3

Ciphertext:    1 2 3 4

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

### **Encryption algorithm:**

The most commonly used symmetric encryption are block ciphers. A block cipher processes the plain text input in fixed size blocks and produces a block of cipher text of equal size for each palintext block.

The two most important symmetric algorithms, both of which are block ciphers, are  
Data Encryption Standard (DES)  
Advanced Encryption Standard (AES)

## DES (Data Encryption Standard):

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

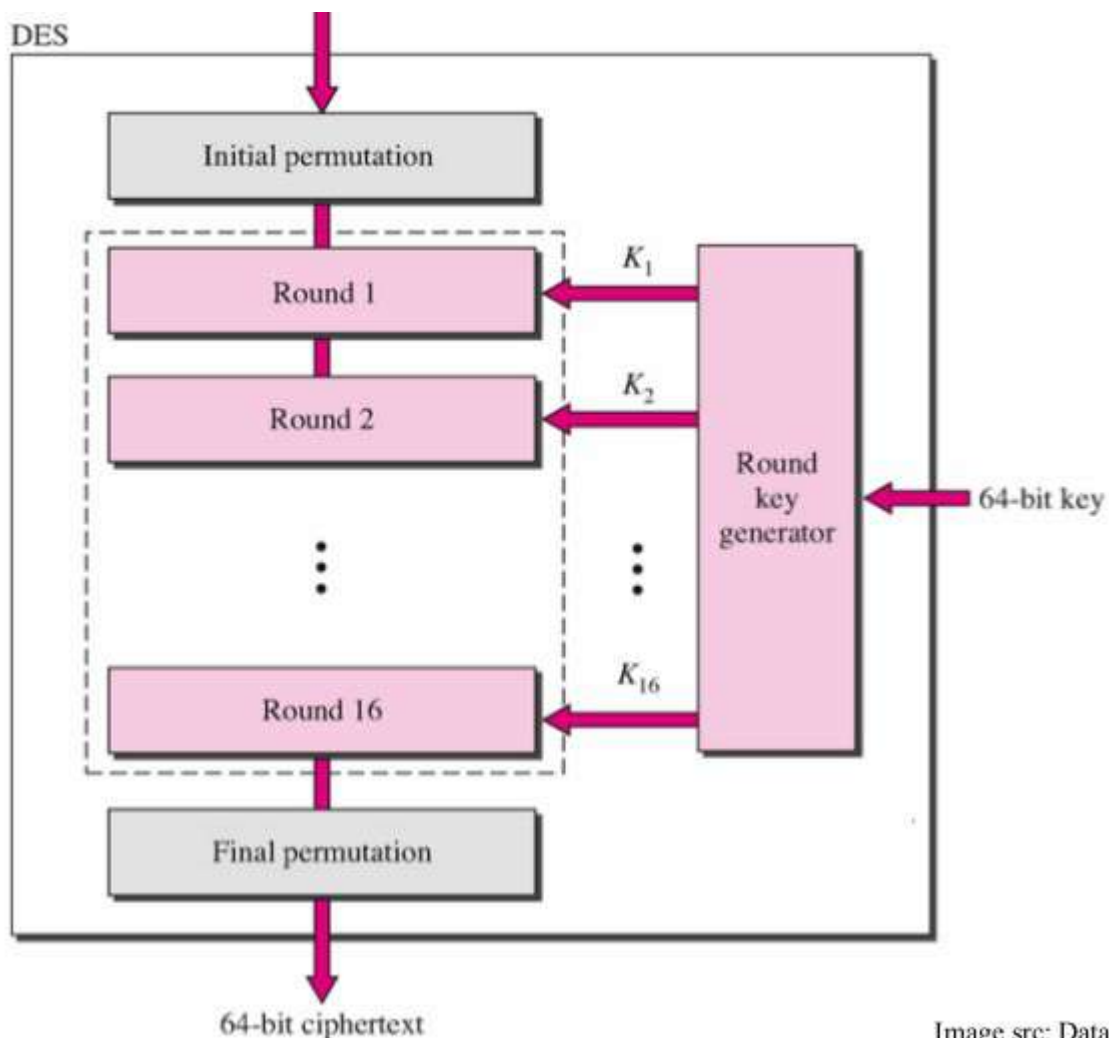
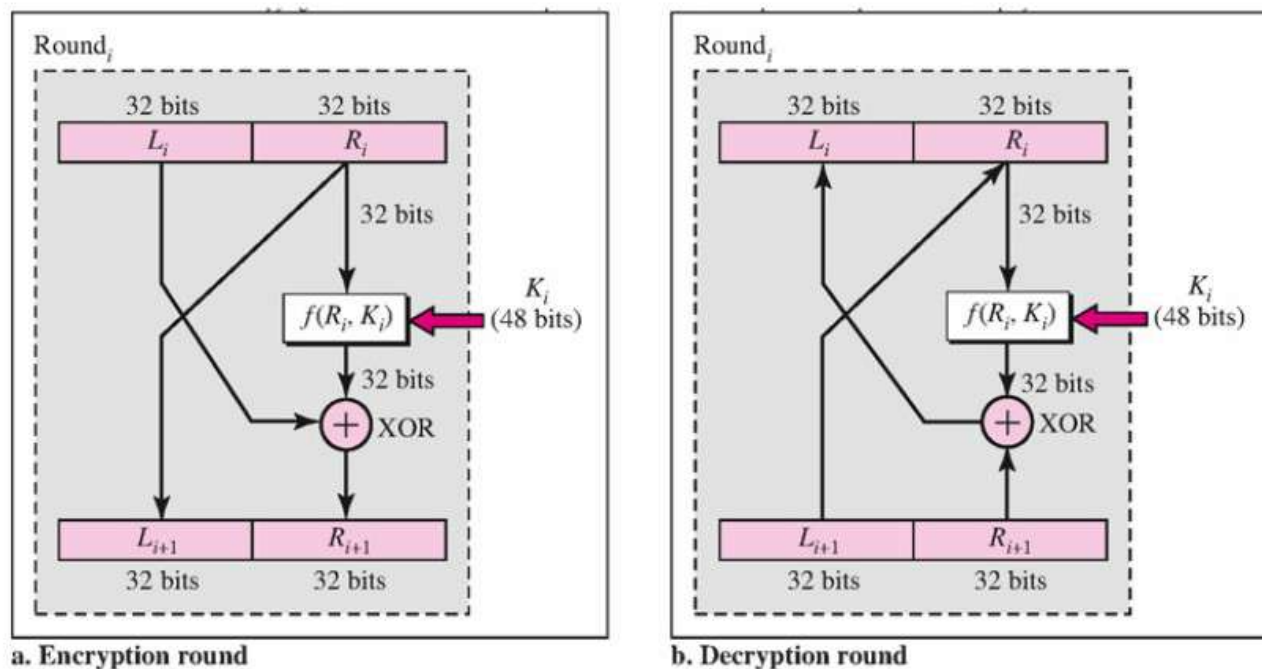


Image src: Dataf

DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated). Although the 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key. The initial and final permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64-bit input and permutes them according to predefined values. Each round of DES is a complex round cipher, as shown in Figure below. Note that the structure of the encryption round ciphers is different from that of the decryption one.





### Asymmetric Key Cryptography:

Some examples of public-key cryptosystems are :

Elgamal (named for its inventor, Taher Elgamal),

RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman),

Diffie-Hellman (named for its inventors),

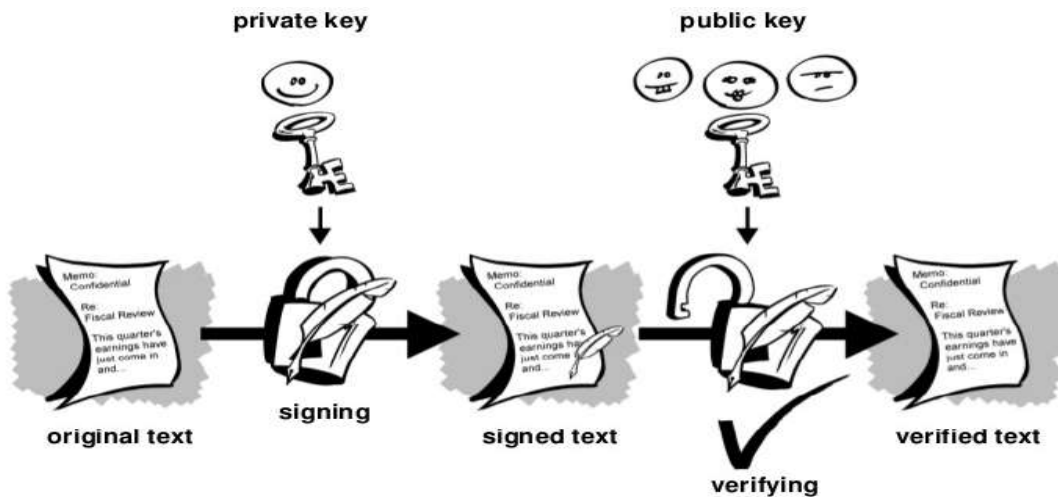
DSA ,the Digital Signature Algorithm (invented by David Kravitz).

## Digital signatures

A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more.

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as to the identity of the signer. Some people tend to use signatures more than they use encryption. For example, you may not care if anyone knows that you just deposited \$1000 in your account, but you do want to be darn sure it was the bank teller you were dealing with.

The basic manner in which digital signatures are created is illustrated in Figure . Instead of encrypting information using someone else's public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you.



### HASH Function:

Hash (also called a message digest):- A one-way hash function takes variable-length input — in this case, a message of any length, even thousands or millions of bits — and produces a fixed-length output; say, 160-bits. PGP uses a cryptographically strong hash function on the plaintext the user is signing. This generates a fixed-length data item known as a message digest.

A hash function generates a fixed-length output value based on an arbitrary-length input file, say 160 bits. To validate the integrity of a file, a recipient would calculate the hash value of that file and compare it to the hash value sent by the sender. Thus, the recipient can be assured that the sender had the file at the time he or she created the hash value. Examples of hash algorithms are MD5, SHA-1 and RIPE-MD-160.

Hashes are used in serving authentication and integrity goals of cryptography. A cryptographic hash can be described as  $f(\text{message}) = \text{hash}$ . A *hash function*  $H$  is a transformation that takes an input  $m$  and returns a fixed-size string, which is called the hash value  $h$  (that is,  $h = H(m)$ ).

## Firewall

Any system or device that allows safe network traffic to pass while restricting or denying unsafe traffic. Firewalls are usually dedicated machines running at the gateway point between your local network and the outside world, and are used to control who has access to your private corporate network from the outside—for example, over the Internet. More generally, a firewall is any system that controls communication between two networks. In today's networking environment in which corporate networks are connected to the Internet—inviting hackers to attempt unauthorized access to valuable business information—a corporate firewall is essential.

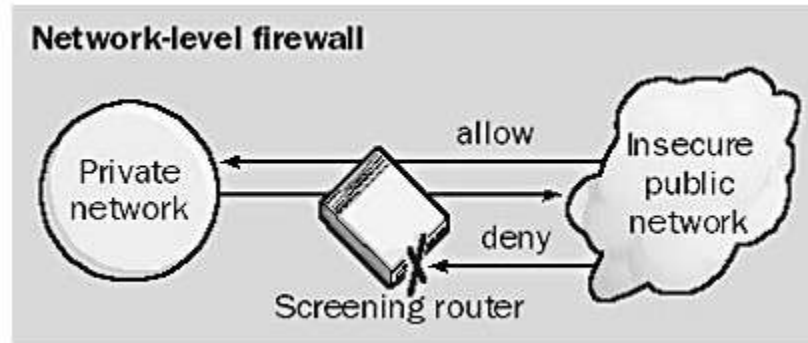
### Types of Firewall

#### Network Level Firewall:

The simple firewall is sometimes called a network-level firewall because it operates at the lower levels of the Open Systems Interconnection (OSI) reference model for networking. Network-level firewalls are transparent to

users and use routing technology to determine which packets are allowed to pass and which will be denied access to the private network. Network-level firewalls implemented solely on stand-alone routers are called packet-filtering routers or screening routers.

In its simplest form, a firewall is essentially a kind of router or computer with two network interface cards that filters incoming network packets. This device is often called a packet-filtering router. By comparing the source addresses of these packets with an access list specifying the firewall's security policy, the router determines whether to forward the packets to their intended destinations or stop them. The firewall can simply examine the IP address or domain name from which the packet was sent and determine whether to allow or deny the traffic. However, packet-filtering routers cannot be used to grant or deny access to networks on the basis of a user's credentials.



Packet-filtering routers can also be configured to block certain kinds of traffic while permitting others. Usually this is done by disabling or enabling different TCP/IP ports on the firewall system. For example, port 25 is usually left open to permit Simple Mail Transfer Protocol (SMTP) mail to travel between the private corporate network and the Internet, while other ports (such as port 23 for Telnet) might be disabled to prevent Internet users from accessing other services on corporate network servers. The difficulty with this approach is that the size of the access list for the firewall can become huge if a large number of domains or ports are blocked and a large number of exceptions are configured. Some ports are randomly assigned to certain services (such as remote procedure call services) on startup; it is more difficult to configure firewalls to control access to these ports.

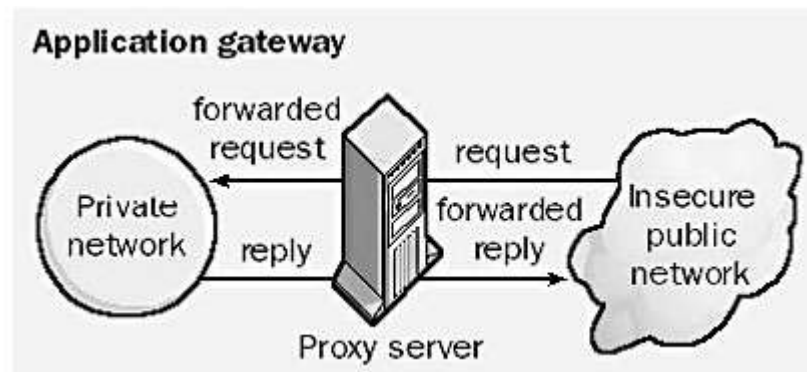
### **Circuit-level Firewall:**

Another type of firewall is a circuit-level gateway, which is usually a component of a proxy server. Circuit-level gateways essentially operate at a higher level of the OSI model protocol stack than network-level firewalls do. With a circuit-level firewall, connections with the private network are hidden from the remote user. The remote user connects with the firewall, and the firewall forms a separate connection with the network resource being accessed after changing the IP address of the packets being transmitted in either direction through the firewall. The result is a sort of virtual circuit between the remote user and the network resource. This is a safer configuration than a packet-filtering router because the external user never sees the IP address of the internal network in the packets he or she receives, only the IP address of the firewall. A popular protocol for circuit-level gateways is the SOCKS v5 protocol.

### **Application Level Firewall:**

Another more advanced type of firewall is the application-level firewall (or application gateway), which is also usually a component of a proxy server. Application gateways do not allow any packets to pass directly between the two networks they connect. Instead, proxy applications running on the firewall computer forward requests to services on the private network, and then forward responses to the originators on the unsecured public network.

Application gateways generally authenticate the credentials of a user before allowing access to the network, and they use auditing and logging mechanisms as part of their security policy. Application gateways generally require some configuration on the part of users to enable their client machines to function properly, but they are more atomic in their configurability than network-level firewalls. For example, if a File Transfer Protocol (FTP) proxy is configured on an application gateway, it can be configured to allow some FTP commands but deny others. You could also configure an SMTP proxy on an application gateway that would accept mail from the outside (without revealing internal e-mail addresses), and then forward the mail to the internal mail server. However, because of the additional processing overhead, application gateways have greater hardware requirements and are generally slower than network-level firewalls.



## Chapter 10 :Introduction to Socket Programming:

Client/ Server Computing:-Distributed Applications (Web Technology), Distributed processing (Three – Tier Architecture); Introduction to socket calls & operating system calls: TCP socket calls & UDP Socket calls.

### Client Server Computing:

A client is defined as a requester (request) of services and a server is defined as the provider (Response) of services. A single machine can be both a client and a server depending on the software configuration. Typically a client is an application that runs on a personal computer or workstation or server, and relies on a server to perform some operations. For example, an e-mail client (Outlook Express) is an application that enables you to send and receive e-mail.

On the other hand servers are computers-most of the time powerful ones- or processes, dedicated to managing disk drives (file servers), printers (print servers) or network traffic (network servers).

#### Properties of a server:

- Passive (Slave)
- Waiting for requests
- On requests serves them and send a reply

#### Properties of a client:

- Active (Master)
- Sending requests
- Waits until reply arrives

### Client-Server Architecture:

#### 2-Tier Architecture

2-tier architecture is used to describe client/server systems where the client requests resources and the server responds directly to the request, using its own resources. This means that the server does not call on another application in order to provide part of the service.

#### The main advantages of the 2-tier model are as follows:

- Productive: many advanced tools have special optimizations that mean less effort is required when working within the two-tier model.
- Better Re-use: Where application logic is placed solely on the server, it can be initiated from many client applications and tools.

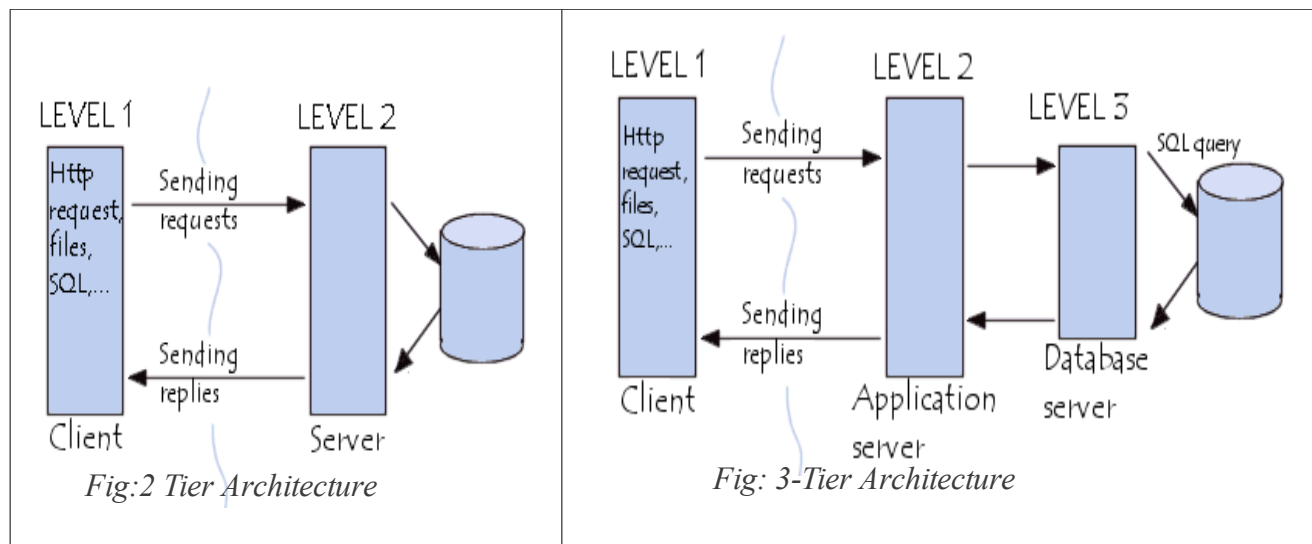
#### The main disadvantages of the 2-tier model are:

- Inability to partition application logic
- Lack of robust security
- Lack of scalability.

#### 3-Tier Architecture:

In 3-tier architecture, there is an intermediary level(Middle-ware), meaning the architecture is generally split up between:

1. **A client**, i.e. the computer, which requests the resources, equipped with a user interface (usually a web browser) for presentation purposes
2. **The application server** (also called **middleware**), whose task it is to provide the requested resources, but by calling on another server
3. **The data server**, which provides the application server with the data it requires.



The widespread use of the term 3-tier architecture also denotes the following architectures:

- Application sharing between a client, middleware and enterprise server
- Application sharing between a client, application server and enterprise database server.

**The benefits of the 3-Tier model are as follows:**

- **Scalability:** In this model the application servers (application logic) can be deployed on many machines. The database server no longer needs connections to every client. In stead it needs to be connected with a fewer amount of application servers.
- **Data Integrity:** Because of the fact that all database updates pass through the middle tier, the middle tier can ensure that only valid data is allowed to be updated in the database thus removing the risk of data corruption from fraud client applications.
- **Security:** Security is implemented in multiple levels thus making more difficult for a client to access unauthorized data, than it would be if security was placed only on the database. Business logic is implemented on a more secure central server, than if it was distributed across the network.
- **Reduced distribution:** Potential changes in the business logic can be centralized into one place.
- **Hidden Database structure:** The structure of the database is hidden from the caller, so a potential enhancement of the database application ( due to a new app. Release) will be transparent from him.

## Comparing both types of architecture

2-tier architecture is therefore a client-server architecture where the server is versatile, i.e. it is capable of directly responding to all of the client's resource requests.

In 3-tier architecture however, the server-level applications are remote from one another, i.e. each server is specialized with a certain task (for example: web server/database server). 3-tier architecture provides:

- A greater degree of flexibility
- Increased security, as security can be defined for each service, and at each level
- Increased performance, as tasks are shared between servers

## Multi-Tiered Architecture

In 3-tier architecture, each server (tier 2 and 3) performs a specialized task (a service). A server can therefore use services from other servers in order to provide its own service. As a result, 3-tier architecture is

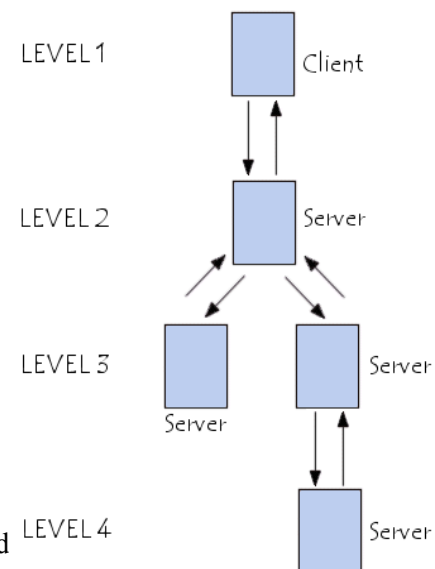


Fig: Multitier Architecture

potentially an n-tiered architecture

## Distributed processing:

The distribution of applications and business logic across multiple processing platforms. Distributed processing implies that processing will occur on more than one processor in order for a transaction to be completed. In other words, processing is distributed across two or more machines and the processes are most likely not running at the same time, i.e. each process performs part of an application in a sequence. Often the data used in a distributed processing environment is also distributed across platforms.

**Distributed computing** is a field of computer science that studies distributed systems. A **distributed system** consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. A computer program that runs in a distributed system is called a **distributed program**, and **distributed programming** is the process of writing such programs.

Distributed computing also refers to the use of distributed systems to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which is solved by one or more computers.

**Distributed Systems:-** A distributed application is designed to utilize the resources of multiple machines by separating the processing and functionality into components that can be deployed in a wide variety of physical configurations

Commonly implemented as N-Tier solutions, all distributed applications aim to achieve high performance, scalability, extensibility, maintainability, security, and re-usability.

*Distributed Application is a group of application made of distinct components running in separate runtime environments, usually on different platforms connected via a network.*

Distributed applications are able to concurrently serve multiple users and, depending on their design, make more optimal use of processing resources. Typical distributed applications are two-tier (client-server), three-tier (client-middleware-server), and multi-tier (client-multiple middleware-multiple servers).

## Socket Programming:

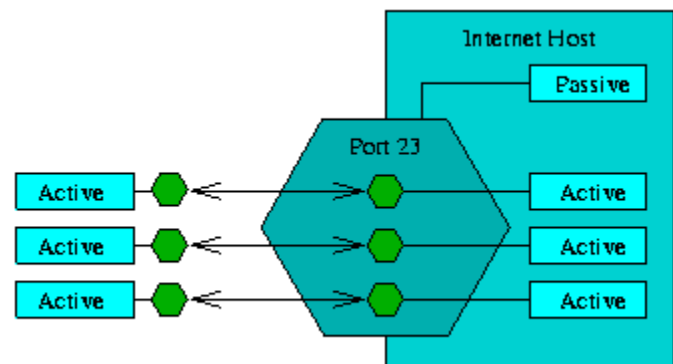
Introduction to socket calls & operating system calls: TCP socket calls & UDP Socket calls. Sockets are the combination of IP address plus corresponding TCP/UDP port numbers. For applications to work with TCP/IP, Application Program Interface (API) is required. *API serves as an interface between different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

Sockets come in two primary flavors. An active socket is connected to a remote active socket via an open data connection. Closing the connection destroys the active sockets at each endpoint. A passive socket is not connected, but rather awaits an incoming connection, which will spawn a new active socket.

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

--Sockets is the original networking interface, developed by UCB for their BSD-series UNIX operating systems.

Sockets are the combination of IP address plus



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

There are three types of sockets: stream, datagram, and raw, each of which represents a different type of communications service.

**Stream sockets** provide reliable, connection-based communications. In connection-based communications, the two processes must establish a logical connection with each other. A stream of bytes is then sent without errors or duplication and is received in the order in which it was sent. Stream sockets correspond to the TCP protocol in TCP/IP.

**Datagram sockets** communicate via discrete messages, called datagrams, which are sent as packets. Datagram sockets are connectionless; that is, the communicating processes do not have a logical connection with each other. The delivery of their data is unreliable. The datagrams can be lost or duplicated, or they may not arrive in the order in which they were sent. Datagram sockets correspond to the UDP protocol in TCP/IP.

**Raw sockets** provide direct access to the lower-layer protocols, for example, IP and the Internet Control Message Protocol (ICMP).

- **socket()** creates a new socket of a certain socket type, identified by an integer number, and allocates system resources to it.
- **bind()** is typically used on the server side, and associates a socket with a socket address structure, i.e. a specified local port number and IP address.
- **listen()** is used on the server side, and causes a bound TCP socket to enter listening state.
- **connect()** is used on the client side, and assigns a free local port number to a socket. In case of a TCP socket, it causes an attempt to establish a new TCP connection.
- **accept()** is used on the server side. It accepts a received incoming attempt to create a new TCP connection from the remote client, and creates a new socket associated with the socket address pair of this connection.
- **send() and recv(), or write() and read(), or recvfrom() and sendto()**, are used for sending and receiving data to/from a remote socket.
- **close()** causes the system to release resources allocated to a socket. In case of TCP, the connection is terminated.
- **gethostbyname() and gethostbyaddr()** are used to resolve host names and addresses.
- **select()** is used to prune a provided list of sockets for those that are ready to read, ready to write or have errors
- **poll()** is used to check on the state of a socket. The socket can be tested to see if it can be written to, read from or has errors.

<b>socket()</b>	create a socket
<b>bind()</b>	associate a socket with a network address
<b>connect()</b>	connect a socket to a remote network address
<b>listen()</b>	wait for incoming connection attempts
<b>accept()</b>	accept incoming connection attempts

The Berkeley socket interface is defined in several header files. The names and content of these files differ



slightly between implementations. In general, they include:

**<sys/socket.h>**

Core BSD socket functions and data structures.

**<netinet/in.h>**

AF\_INET and AF\_INET6 address families and their corresponding protocol families PF\_INET and PF\_INET6. Widely used on the Internet, these include IP addresses and TCP and UDP port numbers.

**<sys/un.h>**

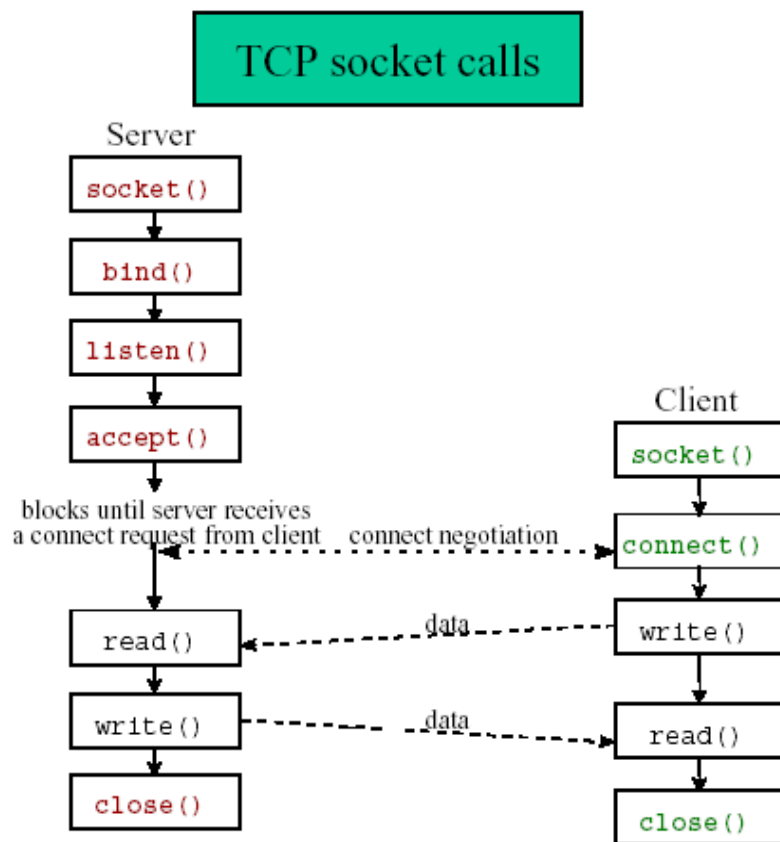
PF\_UNIX/PF\_LOCAL address family. Used for local communication between programs running on the same computer. Not used on networks.

**<arpa/inet.h>**

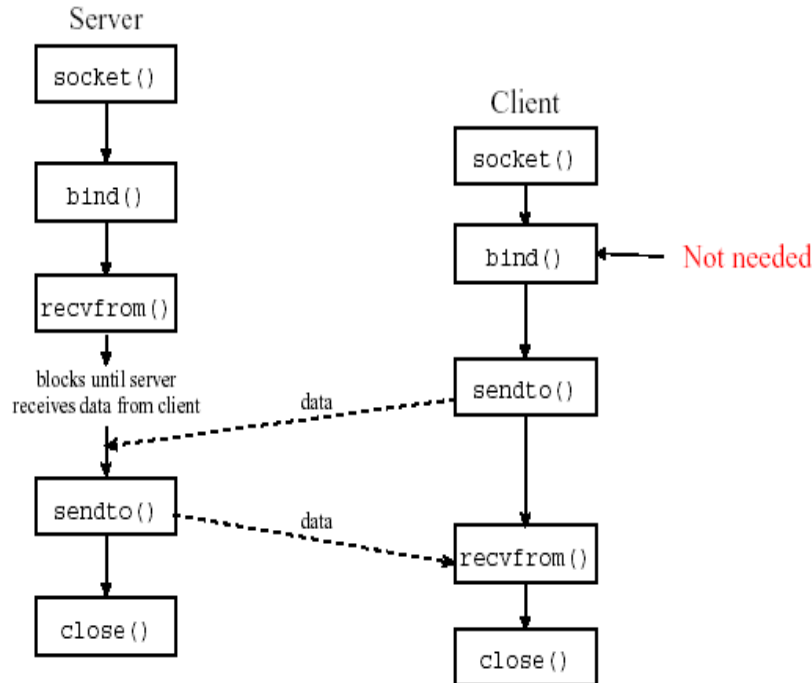
Functions for manipulating numeric IP addresses.

**<netdb.h>**

Functions for translating protocol names and host names into numeric addresses. Searches local data as well as DNS



## UDP socket calls



### NAME

*socket* - create an endpoint for communication

### SYNOPSIS

```
#include <sys/types.h>      /* See NOTES */
#include <sys/socket.h>
```

```
int socket(int domain, int type, int protocol);
```

### DESCRIPTION

The *domain* argument specifies a communication domain; this selects the protocol family which will be used for communication. These families are defined in `<sys/socket.h>`. some of the currently understood formats include:

Name	Purpose
<code>AF_UNIX, AF_LOCAL</code>	Local communication
<code>AF_INET</code>	IPv4 Internet protocols
<code>AF_INET6</code>	IPv6 Internet protocols

The *socket* has the indicated type, which specifies the communication semantics. Currently defined types are:

`SOCK_STREAM` Provides sequenced, reliable, two-way, connection-based byte streams. An out-of-band data transmission mechanism may be supported.

`SOCK_DGRAM` Supports datagrams (connectionless, unreliable messages of a fixed maximum length).

*SOCK\_RAW* Provides raw network protocol access.

*The protocol specifies a particular protocol to be used with the socket. Normally only a single protocol exists to support a particular socket type within a given protocol family, in which case protocol can be specified as 0. However, it is possible that many protocols may exist, in which case a particular protocol must be specified in this manner.*

#### *NAME*

*bind* - bind a name to a socket

#### *SYNOPSIS*

```
#include <sys/types.h>      /* See NOTES */
#include <sys/socket.h>
```

```
int bind(int sockfd, const struct sockaddr *addr, socklen_t addrlen);
```

#### *DESCRIPTION*

*When a socket is created with socket(2), it exists in a name space (address family) but has no address assigned to it. bind() assigns the address specified to by addr to the socket referred to by the file descriptor sockfd. addrlen specifies the size, in bytes, of the address structure pointed to by addr. Traditionally, this operation is called “assigning a name to a socket”.*

#### *NAME*

*listen* - listen for connections on a socket

#### *SYNOPSIS*

```
#include <sys/types.h>      /* See NOTES */
#include <sys/socket.h>
```

```
int listen(int sockfd, int backlog);
```

#### *DESCRIPTION*

*listen() marks the socket referred to by sockfd as a passive socket, that is, as a socket that will be used to accept incoming connection requests using accept.*