# محاضرات مادة شبكات الحاسوب

المرحلة الرابعة

مدرسة المادة

م. د. سميرة عامر عبدالقادر

# Computer Network

**Topologies in Computer**

Network topologies are categorized into the following basic types:

- bus
- ring
- star
- tree
- mesh

**Bus Topology**

Bus networks use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector.

**Ring Topology**

In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction. A failure in any cable or device breaks the loop and can take down the entire network.

**Star Topology**

Many home networks use the star topology. A star network features a central connection point called a "hub" that may be a hub, switch orrouter.

**Tree Topology**

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the "root" of a tree of devices.

**Mesh Topology**

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination.

**What is Computer n/w ?**

A computer network is a group of two or more computers connected to each electronically. This means that the computers can "talk" to each other and that every computer in the network can send information to the others.

**OSI reference model**

The ISO looked to create a simple model for networking. They took the approach of defining layers that rest in a stack formation, one layer upon the other. Each layer would have a specific function, and deal with a specific task. Much time was spent in creating their model called "**The ISO OSI Seven Layer Model for Networking**". In this model, they have 7 layers, and each layer has a special and specific function.

Ans:The Nyquist Limit can be disregarded as this is not a noiseless thus we use Shannon's result which says the maximum data rate of a noisy channel is $X=H\log_2(1+S/N)$ bps using $10\text{Log}_{10}\ S/N$ as our standard quality $2=\text{Log}_{10}\ S/N \rightarrow S/N=10^2 \rightarrow S/N=100$ $X=3000\text{Log}_2(1+100)$bps which gives X= 19,974.63 bps.

Computer networking is a great way of connecting the computers and sharing data with each other. There are many vendors that produce different hardware devices and software applications and without coordination among them there can be chaos, unmanaged communication and disturbance can be faced by the users. There should be some rules and regulations that all the vendors should adopt and produce the devices based on those communication standards.

The Open Systems Interconnect (OSI) model has seven layers. This article describes and explains them, beginning with the 'lowest' in the hierarchy (the physical) and proceeding to the 'highest' (the application). The layers are stacked this way:

- Application

- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

**PHYSICAL LAYER**

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
    - What signal state represents a binary 1
    - How the receiving station knows when a "bit-time" starts
    - How the receiving station delimits a frame
- Physical medium attachment, accommodating various possibilities in the medium:
    - Will an external transceiver (MAU) be used to connect to the medium?
    - How many pins do the connectors have and what is each pin used for?
- Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- Physical medium transmission: transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
    - What physical medium options can be used
    - How many volts/db should be used to represent a given signal state, using a given physical medium

**DATA LINK LAYER**

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

- Link establishment and termination: establishes and terminates the logical link between two nodes.
- Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
- Frame sequencing: transmits/receives frames sequentially.
- Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- Frame delimiting: creates and recognizes frame boundaries.
- Frame error checking: checks received frames for integrity.
- Media access management: determines when the node "has the right" to use the physical medium.

**NETWORK LAYER**

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

- Routing: routes frames among networks.

- Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
- Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

**TRANSPORT LAYER**

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.
The transport layer provides:

- Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
- Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
- Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.

**SESSION LAYER**
The session layer allows session establishment between processes running on different stations. It provides:

- Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

**PRESENTATION LAYER**

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

**APPLICATION LAYER**
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)
- Network virtual terminals

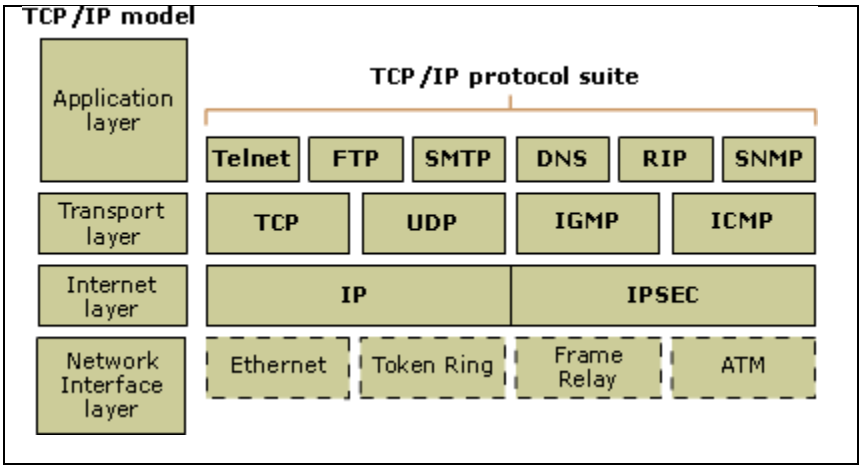
**Compare UDP & TCP ?**

| | TCP | UDP |
|---|---|---|
| **Error Checking:** | TCP does error checking | UDP does not have an option for error checking. |
| **Header Size:** | TCP header size is 20 bytes | UDP Header size is 8 bytes. |
| **Usage:** | TCP is used in case of non-time critical applications. | UDP is used for games or applications that require fast transmission of data. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients. |
| **Function:** | As a message makes its way across the internet from one computer to another. This is connection based. | UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of therelationship. |
| **Acronym for:** | Transmission Control Protocol | User Datagram Protocol or Universal Datagram Protocol |
| **Weight:** | TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control. | UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP. |
| **Streaming of data:** | Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries. | Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent. |
| **Speed of transfer:** | The speed for TCP in comparison with UDP is slower. | UDP is faster because there is no error-checking for packets. |
| **Examples:** | HTTP, HTTPs, FTP, SMTP Telnet etc... | DNS, DHCP, TFTP, SNMP, RIP, VOIP etc... |
| **Data Reliability:** | There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent. | There is no guarantee that the messages or packets sent would reach at all. |
| **Connection Reliable:** | Two way Connection reliable | one way Connection Reliable |
| **Ordering:** | TCP rearranges data packets inthe order specified. | UDP does not order packets. If ordering is required, it has to be managed by the application layer. |

**The TCP/IP model :**

TCP/IP is based on a four-layer reference model. All protocols that belong to the TCP/IP protocol suite are located in the top three layers of this model.

As shown in the following illustration, each layer of the TCP/IP model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model proposed by the International Standards Organization (ISO).




The types of services performed and protocols used at each layer within the TCP/IP model are described in more detail in the following table.

| Layer | Description | Protocols |
|---|---|---|
| Application | Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network. | HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, other application protocols |
| Transport | Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data. | TCP, UDP, RTP |
| Internet | Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams. | IP, ICMP, ARP, RARP |
| Network interface | Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire. | Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35 |

**Computer networks are classified into**

- personal area network
- local area network
- metropolitan area network
- wide area network
- internetwork

according to their scale.

**1.PERSONAL AREA NETWORK**-The interprocessor distance is 1 meter and the processors are located within a square meter.

**2.LOCAL AREA NETWORK(LAN)-**The interprocessor distance is 10 meters to 1 kilometer and the processors are located in a room or a building or a campus.

**3.METROPOLITAN AREA NETWORK(MAN)-**The interprocessor distance is 10 kilometers and the processors are located in a city.

**4.WIDE AREA NETWORKS(WAN)-**The interprocessor distance is from 100 kilometers to 1000 kilometers and the processors are located in a country or a continent.

**5.INTERNETWORKS-**The interprocessor distance is 10,000 kilometers and a popular example is the INTERNET.

**Comparison between OSI and TCP/IP model**

| Sr.No. | OSI | TCP/IP |
|---|---|---|
| **1.** | he OSI model originally distinguishes between service,interval and protocols. | The TCP/IP model doesnt clearly distinguish between service,interval and protocol. |
| **2.** | The OSI model is a reference model. | The TCP/IP model is an implementation of the OSI model. |
| **3.** | In OSI model,the protocols came after the model was described. | In TCP/TP model,the protocols came first,and the model was really just a description of the existing protocols. |
| **4.** | In OSI model,the protocols are better hidden. | In TCP/IP model ,the protocols are not hidden. |
| **5.** | The OSI model has 7 layers. | The TCP/IP model has only 4 layers. |
| **6.** | The OSI model supports both connectionless and connection-oriented communication in the network layer,but only connection -oriented communication in transport layer. | The TCP/IP model supports both connectionless and connection-oriented communication in the transport layer.,giving users the choice |

| OSI | TCP/IP |
|---|---|
| **Application Layer** | **Application Layer** |
| **Presentation Layer** | |
| **Session Layer** | |
| **Transport Layer** | **Internet Layer** |
| **Network Layer** | **Network Layer** |
| **Data link Layer** | **Host to Network Layer** |
| **Physical Layer** | |

**Difference between unacknowledged connection less services and acknowledged connection less services**

Unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledged. Most LAN's use this service.

Acknowledged connectionless service in this service there are no logical connections used but each frame sent individually acknowledged. In this way the sender knows whether a frame has arrived correctly. It is useful on wireless systems

**Transmission media**

The means through which data is transformed from one place to another is called transmission or communication media. There are two categories of transmission media used in computer communications.

- **BOUNDED/GUIDED MEDIA**
- **UNBOUNDED/UNGUIDED MEDIA**

1. **BOUNDED MEDIA:**

Bounded media are the physical links through which signals are confined to narrow path. These are also called guide media. Bounded media are made up o a external conductor (Usually Copper) bounded by jacket material. Bounded media are great for LABS because they offer high speed, good security and low cast. However, some time they cannot be used due distance communication. Three common types of bounded media are used of the data transmission. These are

- Coaxial Cable
- Twisted Pairs Cable
- Fiber Optics Cable

I. **COAXIAL CABLE:**

- Coaxial cable is very common & widely used commutation media. For example TV wire is usually coaxial.
- Coaxial cable gets its name because it contains two conductors that are parallel to each other. The center conductor in the cable is usually copper. The copper can be either a solid wire or stranded martial.

**II. TWISTED PAIR CABLE**

The most popular network cabling is Twisted pair. It is light weight, easy to install, inexpensive and support many different types of network. It also supports the speed of **100 mps.**

**III. FIBER OPTICS**

Fiber optic cable uses electrical signals to transmit data. It uses light. In fiber optic cable light only moves in one direction for two way communication to take place a second connection must be made between the two devices.

**2. UNBOUNDED MEDIA**

Unbounded / Unguided media or wireless media doesn't use any physical connectors between the two devices communicating. Usually the transmission is send through the atmosphere but sometime it can be just across the rule. Wireless media is used when a physical obstruction or distance blocks are used with normal cable media. The three types of wireless media are:

- RADIO WAVES
- MICRO WAVES
- INFRARED WAVES

**I. RADIO WAVES**

It has frequency between **10 K Hz** to **1 G Hz.** Radio waves has the following types.

1. Short waves
2. VHF (Very High Frequency)
3. UHF (Ultra High Frequency)

**II. MICRO WAVES**

Micro waves travels at high frequency than radio waves and provide through put as a wireless network media. Micro wave transmission requires the sender to be inside of the receiver.

Following are the types of Micro waves.

1. · Terrestrial Micro waves
2. · Satellite Micro waves

### III. INFRARED

Infrared frequencies are just below visible light. These high frequencies allow high sped data transmission. This technology is similar to the use of a remote control for a TV. Infrared transmission can be affected by objects obstructing sender or receiver. These transmissions fall into two categories.

1. Point to point
2. Broadcast

**What is modem? null modem?**

A **modem** (**mo**dulator-**dem**odulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analog signals, from driven diodes to radio. Modems, as devices that can either initiate or terminate telecommunications. A modem connection is never an end in itself. Users make modem connections in order to access the Internet or other online services, or to perform a function by emulating some other equipment such as a standalone fax machine, video telephone, or voice telephone. This fact may bring into access considerations other applications that by themselves may not be considered telecommunications.

**Null modem** is a communication method to connect two DTEs (computer, terminal, printer etc.) directly using an RS-232 serial cable. The RS-232 standard is asymmetrical as to the definitions of the two ends of the communications link so it assumes that one end is a DTE and the other is a DCE e.g. a modem. With a null modem connection the transmit and receive lines are cross linked. Depending on the purpose, sometimes also one or more handshake lines are cross linked. Several wiring layouts are in use because the null modem connection is not covered by a standard.

Types of null modem

**No hardware handshaking**

The simplest type of serial cable has no hardware handshaking. This cable has only the data and signal ground wires connected. All of the other pins have no connection.

**Loop back handshaking**

Because of the compatibility issues and potential problems with a simple null modem cable, a solution was developed to trick the software into thinking there was handshaking available.

**Partial handshaking**

In this cable the flow control lines are still looped back to the device. However, they are done so in a way that still permits *Request To Send*(RTS) and *Clear To Send* (CTS) flow control but has no actual functionality.

**Full handshaking**

This cable is incompatible with the previous types of cables' hardware flow control, due to a crossing of its RTS/CTS pins. It also supports software flow control.

**Virtual null modem**

A virtual null modem is a communication method to connect two computer applications directly using a virtual serial port. Unlike a null modem cable, a virtual null modem is a software solution which emulates a hardware null modem within the computer.

**Applications**

- The original application of a null modem was to connect two teletype terminals directly without using modems.
- Null modems are commonly used for file transfer between computers, or remote operation.
- The popularity and availability of faster information exchange systems such as Ethernet made the use of null-modem cables less common.
- This can also provide a serial console through which the in-kernel debugger can be dropped to in case of kernel panics.

**Frame**

In computer networking and telecommunication, a **frame** is a digital data transmission unit or data packet that includes frame synchronization, i.e. a sequence of bits or symbols making it possible for the receiver to detect the beginning and end of the packet in the stream of symbols or bits.

**Main goals of n/w design :**

- **Improve network security**. Improving or redesigning the security of an organization's network is an example of a technical goal.
- **Improve network performance**. Improving performance through the implementation of a new network or the upgrade of an existing network is another common example of a technical goal.
- **Increase network availability**. Increasing network availability is a technical goal usually achieved through the implementation of network redundancy features.
- **Streamline network management**. The redesign of network management processes in another example of a technical goal.
- **Increase network scalability**. Over time, the network requirements for an organization will change

**What is piggybacking ?**

**Piggybacking on Internet access** is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge. It is a legally and ethically controversial practice, with laws that vary by jurisdiction around the world. While completely outlawed or regulated in some places, it is permitted in others.

**Sub layers of Data link layer.**

1.Logical link control(LLC)

Protocols : SDLC, NetBIOS, NetWare

2.Media access Control (MAC)

Protocols : CSMA/CA, Slotted-ALOHA, CDMA, OFDMA

**What is HDLC ? List the features. Explain various response modes and station type.**

**Protocol Overall Description:**

Layer 2 of the OSI model is the data link layer. One of the most common layer 2 protocols is the HDLC

protocol. In fact, many other common layer 2 protocols are heavily based on HDLC, particularly its framing structure: namely, SDLC, SS#7, LAPB ,LAPD and ADCCP .
HDLC uses zero insertion/deletion process (commonly known as bit stuffing) to ensure that the bit pattern of the delimiter flag does not occur in the fields between flags. The HDLC frame is synchronous and therefore relies on the physical layer to provide method of clocking and synchronizing the transmission and reception of frames.
The HDLC protocol is defined by ISO for use on both point-to-point and multipoint (multidrop) data links. It supports full duplex transparent-mode operation and is now extensively used in both multipoint and computer networks.

**HDLC Features**

The main features of HDLC are divided into various aspects

- The modes for operation
- Stations
- Configuration
- Frames and Structures
- The subsets of HDLC

**HDLC Stations**

- The HDLC has three levels of stations, the primary station, secondary station and the combined station.
- The primary station is responsible for controlling all the other secondary stations for a network that uses the HDLC protocol. The primary station also takes care of the error control aspect and organizes the data flow on the links.
- The secondary station is controlled by the primary station and is activated when the primary station sends a request.
- The combined station controls the links and overlooks the primary and the secondary stations functions. The combined stations have complete control over the links and do not need the authorization of any other station.
- These stations are further dependant on the configuration types and basically follow three different types of configuration.

HDLC has three operational modes:

**Normal Response Mode** (NRM) - Normal Response Mode is used in unbalanced configurations. In this mode, slave stations (or secondary) can only transmit when specially instructed by the master (primary station). The link may be point-to-point or multipoint. In the latter case only one primary station is allowed.

**Asynchronous Response Mode (**ARM) - Asynchronous Response Mode: This mode is used in unbalanced configurations. [unbalanced configurations]. It allows a secondary station to initiate a transmission without receiving permission from the primary station . This mode is normally used with point-to-point configurations and full duplex links and allows the secondary station to send frames asynchronously with respect to the primary station)

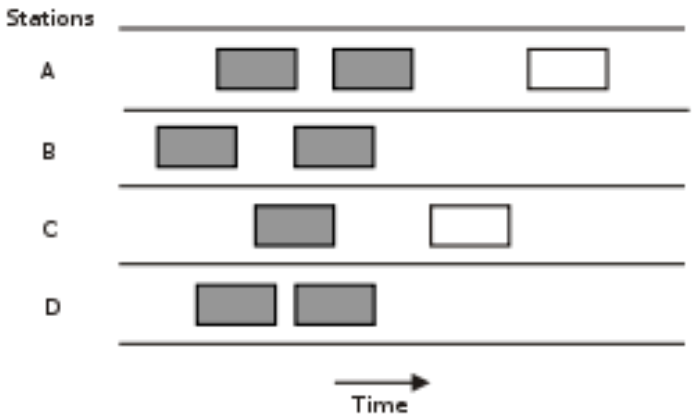
**Asynchronous Balanced Mode** (ABM) - The Asynchronous Balanced Mode (ABM), is used mainly on full duplex point-to-point links for computer to computer communications and for connections between a computer and a packed switched data network, in this case each station has an equal status and performs the role of both primary and secondary functions. This mode is used in the protocol set known as X.25.

**Pure ALOHA and Slotted ALOHA.**

ALOHA is a medium access protocol that was originally designed for ground based radio broadcasting however it is applicable to any system in which uncoordinated users are competing for the use of a shared channel. Pure ALOHA and slotted ALOHA are the two versions of ALOHA.

**Pure Aloha Protocol**

With Pure Aloha, stations are allowed access to the channel whenever they have data to transmit. Because the threat of data collision exists, each station must either monitor its transmission on the rebroadcast or await an acknowledgment from the destination station. By comparing the transmitted packet with the received packet or by the lack of an acknowledgement, the transmitting station can determine the success of the transmitted packet. If the transmission was unsuccessful it is resent after a random amount of time to reduce the probability of re-collision.




**Advantages:**

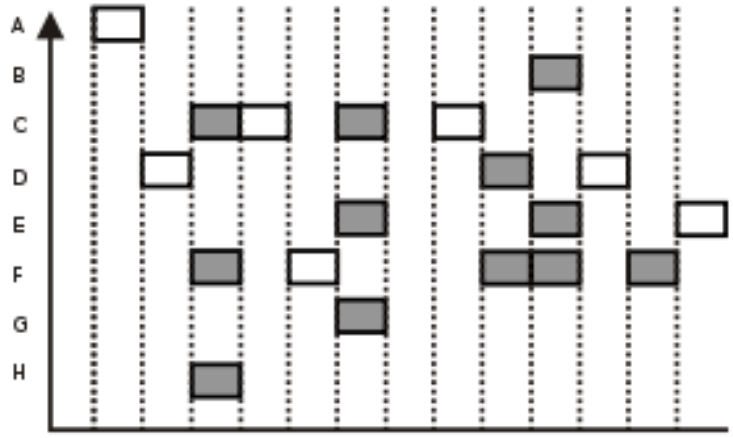
· Superior to fixed assignment when there is a large number of bursty stations.
· Adapts to varying number of stations.

**Disadvantages:**

· Theoretically proven throughput maximum of 18.4%.
· Requires queueing buffers for retransmission of packets

**Slotted Aloha Protocol**

By making a small restriction in the transmission freedom of the individual stations, the throughput of the Aloha protocol can be doubled. Assuming constant length packets, transmission time is broken into slots equivalent to the transmission time of a single packet. Stations are only allowed to transmit at slot boundaries. When packets collide they will overlap completely instead of partially. This has the effect of doubling the efficiency of the Aloha protocol and has come to be known as Slotted Aloha.




Slotted ALOHA protocol (shaded slots indicate collision)

**Advantages:**
· Doubles the efficiency of Aloha.
· Adaptable to a changing station population.
**Disadvantages:**
· Theoretically proven throughput maximum of 36.8%.
· Requires queueing buffers for retransmission of packets.

**Ethernet with frame format**

Ethernet is the most widely-installed local area network ( LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox from an earlier specification called Alohanet and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs.

Ethernet was originally developed to run on a long coaxial cable that connected all the computers on the network. This type of network topology is called a bus. When one station transmitted data, all the other stations heard it. Ethernet was designed assuming that all stations would hear these broadcasts to the segment of wire used to connect them. This is where the terms 'wire segment' and 'broadcast domain' come from. A broadcast domain includes all the wire and computers that can hear each other whenever one of the computers is transmitting. A wire segment is the piece of wire used to connect two devices.

**IEEE 803.2 / 802.2**

<table>
<tr><td>7 bytes</td><td>1 byte</td><td>2 or 6 bytes</td><td>2 or 6 bytes</td><td>2 bytes</td><td colspan="4">4-1500 bytes</td><td>4 bytes</td></tr>
<tr><td rowspan="2">Preamble</td><td rowspan="2">Start Frame Delimiter</td><td rowspan="2">Dest. MAC address</td><td rowspan="2">Source MAC address</td><td rowspan="2">Length</td><td colspan="4">(Data / Pad)</td><td rowspan="2">FCS</td></tr>
<tr><td>DSAP</td><td>SSAP</td><td>CTRL</td><td>NLI</td></tr>
</table>

**Preamble**
This is a stream of bits used to allow the transmitter and receiver to synchronize their communication. The preamble is an alternating pattern of binary 56 ones and zeroes. The preamble is immediately followed by the Start Frame Delimiter.

**Start Frame Delimiter**
This is always 10101011 and is used to indicate the beginning of the frameinformation.

**Destination MAC**
This is the MAC address of the machine receiving data. When a network interface card (NIC) is listening to the wire is checking this field for it's own MAC address.

**Source MAC**
This is the MAC address of the machine transmitting data.

**Length**
This is the length of the entire Ethernet frame in bytes. Although this field can hold any value between 0 and 65,534, it is rarely larger than 1500 as that is usually the maximum transmission frame size for most serial connections. Ethernet networks tend to use serial devices to access the Internet.

**Data/Padding** (a.k.a. Payload)
The data is inserted here. This is where the IP header and data is placed if you are running IP over Ethernet. This field contains IPX information if you are running IPX/SPX (Novell). Contained within the data/padding section of an IEEE 803.2 frameare four specific fields:

DSAP - Destination Service Access Point
SSAP - Source Service Access Poiont
CTRL - Control bits for Ethernet communication
NLI - Network Layer Interface.

**FCS**
This field contains the Frame Check Sequence (FCS) which is calculated using a Cyclic Redundancy Check (CRC). The FCS allows Ethernet to detect errors in the Ethernetframe and reject the frame if it appears damaged.

**What is bit stuffing?**

Bit stuffing is the insertion of one or more bits into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

**Protocols used in signaling channel of the mobile phones**

The protocol used in mobile phones is GSM.

**GSM**

- GSM stands for **G**lobal **S**ystem for **M**obile Communication and is an open, digital cellular technology used for transmitting mobile voice and data services.
- The GSM emerged from the idea of cell-based mobile radio systems at Bell Laboratories in the early 1970s.
- The GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.
- The GSM standard is the most widely accepted standard and is implemented globally.
- The GSM is a circuit-switched system that divides each 200kHz channel into eight 25kHz time-slots. GSM operates in the 900MHz and 1.8GHz bands in Europe and the 1.9GHz and 850MHz bands in the US.
- The GSM is owning a market share of more than 70 percent of the world's digital cellular subscribers.

**Why GSM?**

The GSM study group aimed to provide the followings through the GSM:

- Improved spectrum efficiency.
- International roaming.
- Low-cost mobile sets and base stations (BSs)
- High-quality speech
- Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services.
- Support for new services.

**GSM network areas:**

In a GSM network, the following areas are defined:

- **Cell:** Cell is the basic service area: one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.
- **Location Area:** A group of cells form a Location Area. This is the area that is paged when a subscriber gets an incoming call. Each Location Area is assigned a Location Area Identity (LAI). Each Location Area is served by one or more BSCs.
- **MSC/VLR Service Area:** The area covered by one MSC is called the MSC/VLR service area.
- **PLMN:** The area covered by one network operator is called PLMN. A PLMN can contain one or more MSCs.

**What is the purpse of Jam signal in CSMA/CD ?**

**Collision**

A condition where two devices detect that the network is idle and end up trying to send packets at exactly the same time. (within 1 round-trip delay) Since only one device can transmit at a time, both devices must back off and attempt to retransmit again.

CSMA/CD is designed to handle collisions with a re-transmit. The retransmission algorithm requires each device to wait a random amount of time, so the two are very likely to retry at different times, and thus the second one will sense that the network is busy and wait until the packet is finished. If the two devices retry at the same time (or almost the same time) they will collide again, and the process repeats until either the packet finally makes it onto the network without collisions, or 16 consecutive collision occur and the packet is aborted.

**Jam**

This is part of the CSMA/CD algorithm, that tells all stations that a collision has occurred, and to hold off transmitting for a short time, called the back off time, which is a random number. When a workstation detects a collision during transmission of a frame - none of the other stations are aware that the collision has occurred. So the station transmits a 32 to 48-bit jam signal so all other stations will see the collision also. When a repeater detects a collision on one port, it puts out a jam on all other ports, causing a collision to occur on those lines that are transmitting, and causing any non-transmitting stations to wait to transmit.

Interestingly enough, the actual format of jam is unspecified in the 802.3 specifications. Most manufacturers have used alternating 1s and 0s as jam, which is displayed as 0x5 (0101) or 0xA (1010) depending on when the jam is captured in the data stream.

**Retransmission**

When a collision is detected, the station sends a jam signal and then waits for a random backoff time, and then retransmits the frame. It will retry n attempts, where n is a user-defined number. If all attempts fail, it will report this to the LLC layer, which will then decide whether to retry another n times, or report that the link is down.

**How error detected & corrected in network ?**

Error detection and correction or error control are techniques that enable reliable delivery of digital data over unreliable communication channels. Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Error detection techniques allow detecting such errors, while error correction enables reconstruction of the original data.
The general definitions of the terms are as follows:

- Error detection is the detection of errors caused by noise or other impairments during transmission from the transmitter to the receiver.
- Error correction is the detection of errors and reconstruction of the original, error-free data.

**Error Detection Techniques :**

- **Repetition codes**

A **repetition code** is a coding scheme that repeats the bits across a channel to achieve error-free communication. Given a stream of data to be transmitted, the data is divided into blocks of bits. Each block is transmitted some predetermined number of times

- **Parity bits**

A **parity bit** is a bit that is added to a group of source bits to ensure that the number of set bits (i.e., bits with value 1) in the outcome is even or odd. It is a very simple scheme that can be used to detect single or any other odd number (i.e., three, five, etc.) of errors in the output. An even number of flipped bits will make the parity bit appear correct even though the data is erroneous.

- **Checksums**

A **checksum** of a message is a modular arithmetic sum of message code words of a fixed word length (e.g., byte values). The sum may be negated by means of a one's-complement prior to transmission to detect errors resulting in all-zero messages.

- **Cyclic redundancy checks (CRCs)**

A cyclic redundancy check (CRC) is a single-burst-error-detecting cyclic code and non-secure hash function designed to detect accidental changes to digital data in computer networks. It is characterized by specification of a so-called generator polynomial, which is used as thedivisor in a polynomial long division over a finite field, taking the input data as the dividend, and where the remainder becomes the result.

- **Cryptographic hash functions**

A cryptographic hash function can provide strong assurances about data integrity, provided that changes of the data are only .Any modification to the data will likely be detected through a mismatching hash value.

- **Error-correcting codes**

Any error-correcting code can be used for error detection. A code with minimum Hamming distance, d, can detect up to d-1 errors in a code word. Using minimum-distance-based error-correcting codes for error detection can be suitable if a strict limit on the minimum number of errors to be detected is desired.

**Error Correction Techniques:**

- **Automatic repeat request**

Automatic Repeat reQuest (ARQ) is an error control method for data transmission that makes use of error-detection codes, acknowledgment and/or negative acknowledgment messages, and timeouts to achieve reliable data transmission. An acknowledgment is a message sent by the receiver to indicate that it has correctly received a data frame.

- **Error-correcting code**

An error-correcting code (ECC) or forward error correction (FEC) code is a system of adding redundant data, or parity data, to a message, such that it can be recovered by a receiver even when a number of errors were introduced, either during the process of transmission, or on storage

- **Hybrid schemes**

Hybrid ARQ is a combination of ARQ and forward error correction. There are two basic approaches:

- Messages are always transmitted with FEC parity data. A receiver decodes a message using the parity information, and requests retransmission using ARQ only if the parity data was not sufficient for successful decoding.
- Messages are transmitted without parity data. If a receiver detects an error, it requests FEC information from the transmitter using ARQ, and uses it to reconstruct the original message.

**Give mathematical derivation to sketch out efficiency of pure ALOHA & slotted ALOHA . draw a graph between system throughput and offered load.**

**Ans:** Suppose N stations have packets to send

- meach transmits in slot with probability p
- mprob. successful transmission S is:
- by single node:

  $S= p (1-p)^{(N-1)}$
- by any of N nodes

  $S = Prob (only one transmits) = N p (1-p)^{(N-1)}$

**Pure ALOHA**

The value of p (p*) that maximizes the efficiency of ALOHA is:

E(p) =Np(1 - p)2(N-1)

E'(p) =N(1 - p) 2N-2 – Np2(N-1)(1 - p) 2(N-3)

= N(1-p) 2(N-3) ((1 - p)-p2(N- 1))

E'(p) = 0 => p* = 1/(2N-1)

Using this value, the max efficiency of ALOHA is;

lim (N-> infinity) E(p*)= ½ * 1/e =1/2e

**Slotted ALOHA**

The value of p (p*) that maximises the efficiency of slotted ALOHA is:

E(p) =Np(1 - p)N-1

E'(p) =N(1 - p) N-1- Np(N-1)(1 - p) N-2

= N(1-p) N-2((1 - p)-p(N- 1))

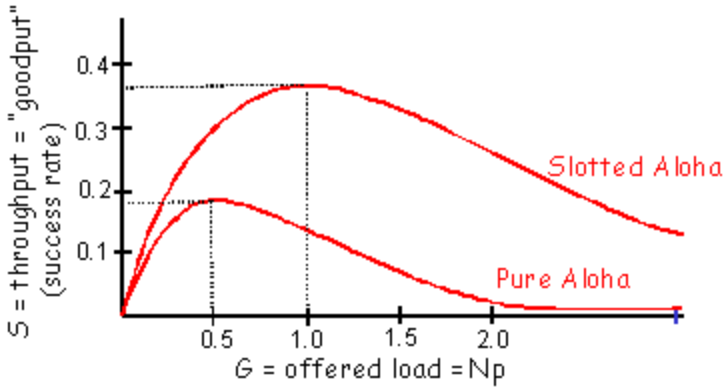
E'(p) = 0 => p* = 1/N

Using this value, the max efficiency of slotted ALOHA is;

E(p*)=N 1/N(1-1/N) N-1= (1-1/N) N-1= (1-1/N) N/(1-1/N)

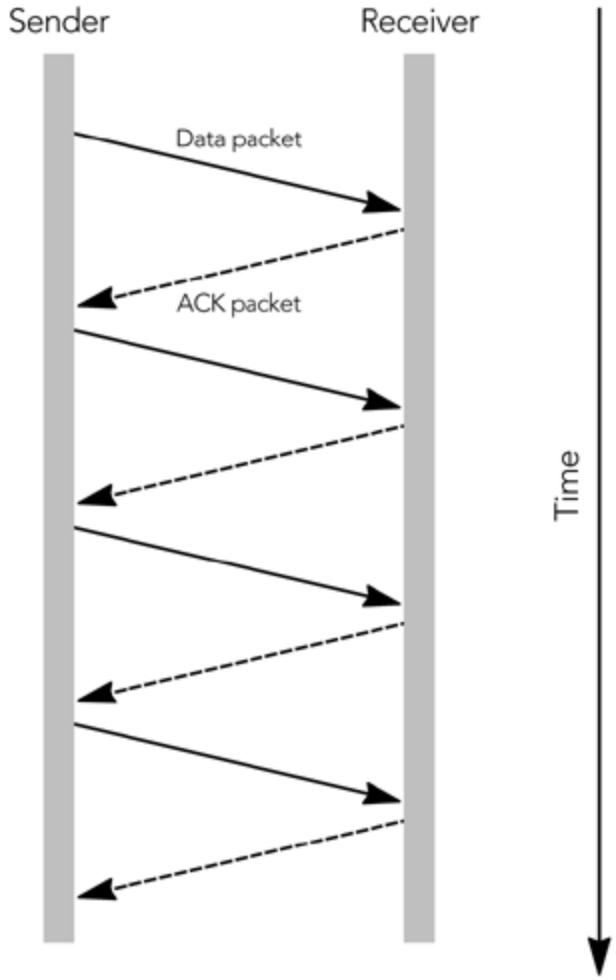
lim (N-> infinity) (1-1/N) = 1 lim (N-> infinity) (1-1/N) N = 1/e

Thus: lim (N-> infinity) E(p*)= 1/e




**Stop and wait Protocol :**

- Stop-and-wait is a method used in telecommunications to send information between two connected devices.
- It ensures that information is not lost due to dropped packets and that packets are received in the correct order.
- It is the simplest kind of automatic repeat-request (ARQ) method. A stop-and-wait ARQ sender sends one frame at a time; it is a special case of the general sliding window protocol with both transmit and receive window sizes equal to 1.
- After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal. After receiving a good frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again.




**Sliding Window Protocol :**

Sliding window algorithms are a method of flow control for network data transfers.
TCP uses a sliding window algorithm, which allows a sender to have more than one unacknowledged packet "in flight" at a time, which improves network throughput.

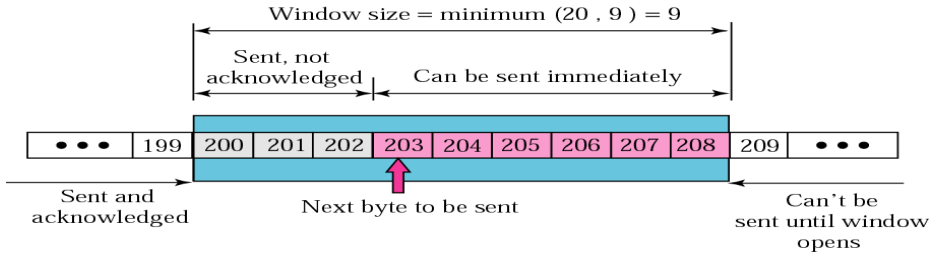
Key concepts of the Sliding Window

- Both the sender and receiver maintain a finite size buffer to hold outgoing and incoming packets from the other side.
- Every packet sent by the sender, must be acknowledged by the receiver. The sender maintains a timer for every packet sent, and any packet unacknowledged in a certain time, is resent.
- The sender may send a whole window of packets before receiving an acknowledgement for the first packet in the window.
  This results in higher transfer rates, as the sender may send multiple packets without waiting for each packet's acknowledgement.
- The Receiver advertises a window size that tells the sender how much data it can receive, in order for the sender not to fill up the receivers buffers.

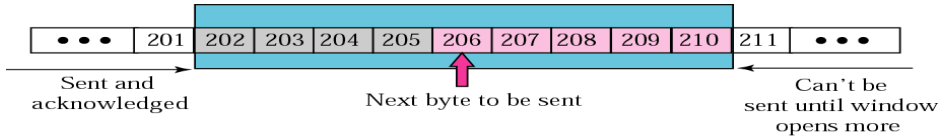
Example

Figure shows an unrealistic example of a sliding window. The sender has sent bytes up to 202. We assume that cwnd is 20 (in reality this value is thousands of bytes). The receiver has sent an

acknowledgment number of 200 with an rwnd of 9 bytes (in reality this value is thousands of bytes). The size of the sender window is the minimum of rwnd and cwnd or 9 bytes. Bytes 200 to 202 are sent, but not acknowledged. Bytes 203 to 208 can be sent without worrying about acknowledgment. Bytes 209 and above cannot be sent.

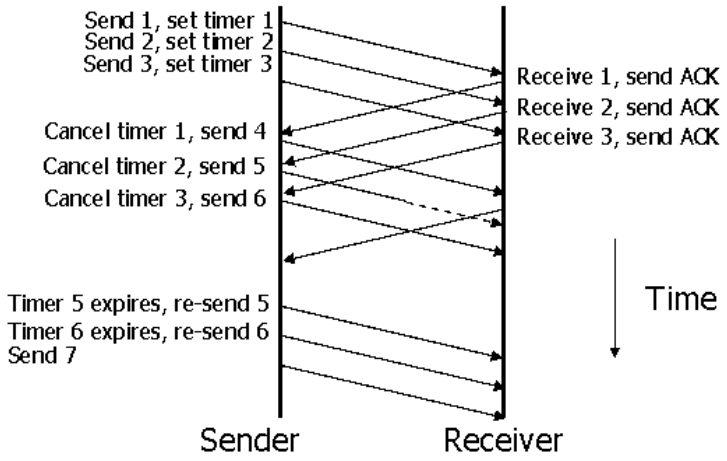



In Figure the server receives a packet with an acknowledgment value of 202 and an rwnd of 9. The host has already sent bytes 203, 204, and 205. The value of cwnd is still 20. Show the new window.




**Go Back-N :**

Go-Back-N ARQ is a specific instance of the Automatic Repeat-reQuest (ARQ) Protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an ACK packet from the receiver.
The receiver process keeps track of sequence number of the next frame it expects to receive, and sends that number with every ACK it sends. The receiver will ignore any frame that does not have the exact sequence number it expects -- whether that frame is a "past" duplicate of a frame it has already ACK'ed, or whether that frame is a "future" frame past the lost packet it is waiting for. Once the sender has sent all of the frames in its window, it will detect that all of the frames since the first lost frame are outstanding, and will go back to sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.




**Ad-hoc network :**

"Ad Hoc" is actually a Latin phrase that means "for this purpose." It is often used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station.
For example, if you need to transfer a file to your friend's laptop, you might create an ad hoc network between your computer and his laptop to transfer the file. This may be done using an Ethernet crossover cable, or the computers' wireless cards to communicate with each other. If you need to share files with more than one computer, you could set up a mutli-hop ad hoc network, which can transfer data over multiple nodes.
Basically, an ad hoc network is a temporary network connection created for a specific purpose (such as transferring data from one computer to another). If the network is set up for a longer period of time, it is just a plain old local area network (LAN).

**Virtual circuit and Datagram**

Datagram :
a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.

Virtual ckt :
In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is aconnection oriented communication service that is delivered by means of packet mode communication. After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

**Adaptive and Non adaptive algorithm**

Adaptive Algorithm :
An adaptive algorithm is an algorithm that changes its behavior based on the resources available. For example, stable partition, using no additional memory is O(n lg n) but given O(n) memory, it can be O(n) in time.

Non adaptive 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.

**Responsibility of network layer**
following responsibilities,

- Routing: routes frames among networks.
- Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information

**Algorithm of congestion control**

In any network when there is too much the data traffic at a node that the network slows down or starts loosing data, it is known as network congestion. It degrades quality of service and also can lead to delays, lost data.

Congestion Control Algorithm:
Summing the relative delay measurements over a period of data flow gives us an indication of the level of queuing at the bottleneck. If the sum of relative delays over an interval was 0, we would know that no additional congestion or queuing was present in the network at the end of the interval with respect to the beginning. Likewise, if we were to sum from the beginning of a session, and at any point if the summation was equal to zero, we would know that all of the data was contained in the links and not in the network queues. The congestion control algorithm of TCP-Santa Cruz operates by summing the relative delays from the beginning of a session, and then updating the measurements at intervals equal to the amount of time to transmit a windowful of data and receive the corresponding ACKs. The relative delay sum is then translated into the equivalent number of packets (queued at the bottleneck) represented by the sum of relative delays. In other words, the algorithm attempts to maintain the following condition:

$Nt_i = n$

Where

$Nt_{i=} Nt_{i-1}+Mw_{i+1}$

and $N_{ti}$ is the total number of packets queued at the bottleneck from the beginning of the connection until $t_i$; $n$ is the desired number of packets, per session, to be queued at the bottleneck; $M_{Wi-1}$ is the additional amount of queuing introduced over the previous window $W_{i-1}$; and $N_{t1} = M_{W0}$.

**Flooding**

Every incoming packet is sent out on every other link by every router.
Super simple to implement, but generates lots of redundant packets. Interesting to note that all routes are discovered, including the optimal one, so this is robust and high performance (best path is found without being known ahead of time). Good when topology changes frequently (USENET example).
Some means of controlling the expansion of packets is needed. Could try to ensure that each router only floods any given packet once.

Could try to be a little more selective about what is forwarded and where.

**Flow-based**
Similar in spirit to minimum distance, but takes traffic flow into consideration.

The key here is to be able to characterize the nature of the traffic flows over time. You might be able to do this if you know a lot about how the network is used (traffic arrival rates and packet lengths). From the known average amount of traffic and the average length of a packet you can compute the mean packet delays using queuing theory. Flow-based routing then seeks to find a routing table to minimize the average packet delay through the subnet.

**Distance Vector**
Also known as Belman-Ford or Ford-Fulkerson. Used in the original ARPANET, and in the Internet as RIP.
The heart of this algorithm is the routing table maintained by each host. The table has an entry for every other router in the subnet, with two pieces of information: the link to take to get to the router, and the estimated distance from the router. For a router A with two outgoing links L1, L2, and a total of four routers in the network, the routing table might look like this:

| router | distance | link |
|---|---|---|
| B | 5 | L1 |
| C | 7 | L1 |
| D | 2 | L2 |

Neighboring nodes in the subnet exchange their tables periodically to update each other on the state of the subnet (which makes this a dynamic algorithm). If a neighbor claims to have a path to a node which is shorter than your path, you start using that neighbor as the route to that node. Notice that you don't actually know the route the neighbor thinks is shorter - you trust his estimate and start sending frames that way.

You can think of this as forming an approximation of the global state of the subnet from local information only (exchange with neighbors). Unfortunately it has problems (it's only an approximation, after all). Good news (a link comes up, a new router is available, a router or link are made faster) propogate very quickly through the whole subnet (in the worst case it takes a number of exchanges equal to the longest path for everyone to know the good news).

Bad news is not spread reliably. Neighbors only slowly increase their path length to a dead node, and the condition of being dead (infinite distance) is reached by counting to infinity one at a time. Various means of fixing this have been tried, but none are foolproof.

**Link State**

Widely used today, replaced Distance Vector in the ARPANET. Link State improves the convergence of Distance Vector by having everybody share their idea of the state of the net with everybody else (more information is available to nodes, so better routing tables can be constructed).

The basic outline is

1. discover your neighbors
2. measure delay to your neighbors

3. bundle all the information about your neighbors together
4. send this information to all other routers in the subnet
5. compute the shortest path to every router with the information you receive

Neighbor discovery
: Send an HELLO packet out. Receiving routers respond with their addresses, which must be globally unique.

Measure delay
: Time the round-trip for an ECHO packet, divide by two. Question arises: do you include time spent waiting in the router (i.e. load factor of the router) when measuring round-trip ECHO packet time or not?

Bundle your info
: Put information for all your neighbors together, along with your own id, a sequence number and an age.

Distribute your info
: Ideally, every router would get every other routers data simultaneously. This can't happen, so in effect you have different parts of the subnet with different ideas of the topology of the net at the same time. Changes ripple through the system, but routers that are widely spread can be using very different routing tables at the same time. This could result in loops, unreachable hosts, other types of problems.

Compute shortest path tree
: Using an algorithm like Dijkstra's, and with a complete set of information packets from other routers, every router can locally compute a shortest path to every other router. The memory to store the data is proportional to k * n, for n routers each with k neighbors. Time to compute can also be large.
Bad data (from routers in error, e.g.) will corrupt the computation.

**Hierarchical**

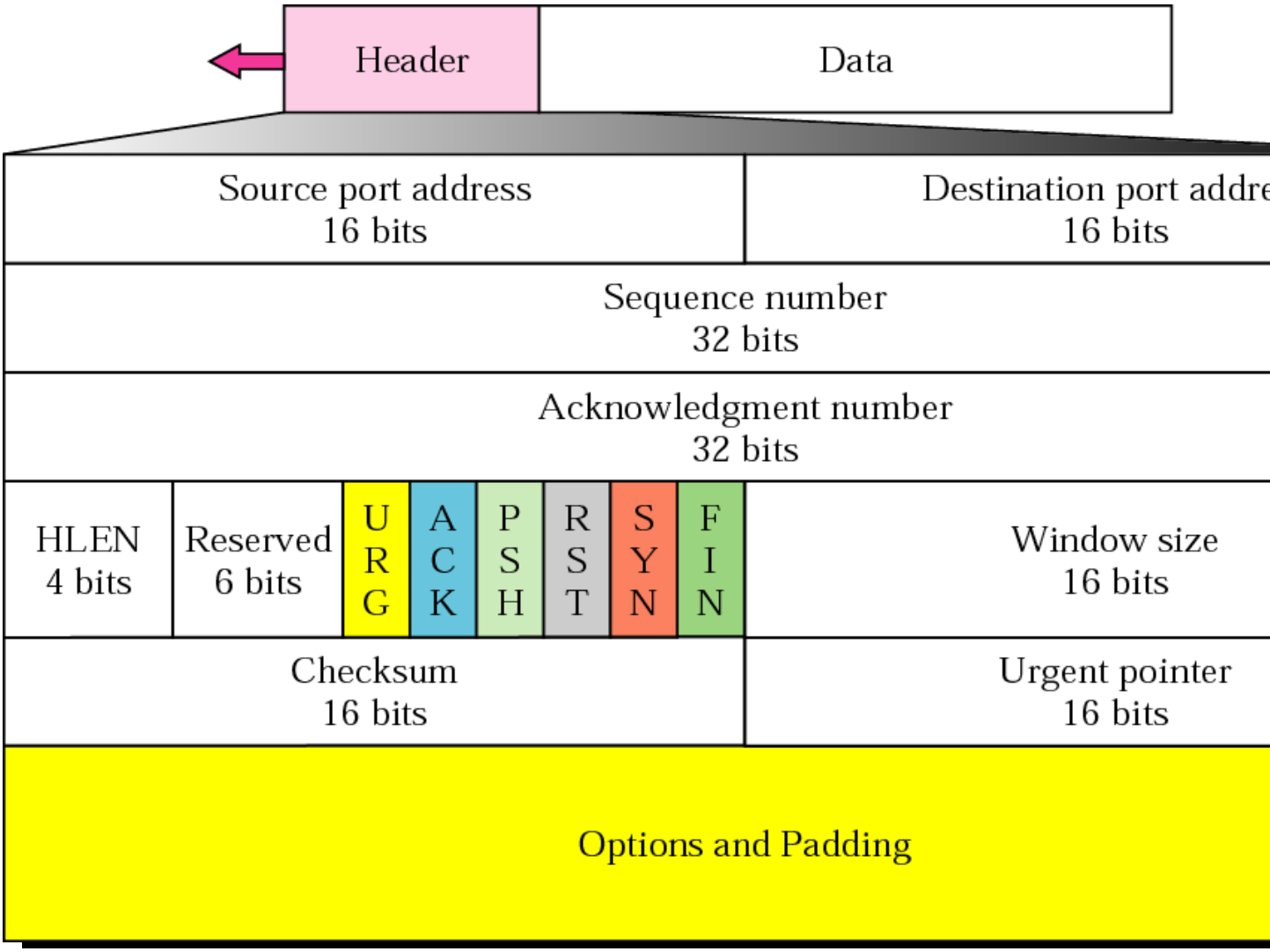
When your subnet is large then the routing tables become unwieldy. Too much memory to store them, too much time to search them, too much time to compute them. When something is too large, people form a hiearchy to deal with it.
The idea is to replace N different routing table entries to N different individual routers with a single entry for a cluster of N routers. You can apply many different levels of hierarchy.

**Precautions**

In order to keep your files safe, you should always have backups. Copy the most important documents you have on flash drives or external hard drives. The more copies you have of crucial data the better. Purchasing an additional HDD or two only puts you behind budget by $50, which still sounds better than a rudimentary data restore process.
Note that sometimes even your flash drive backups will fail. If this has happened to you, then you might want to check out this site on flash data recovery. It has a lot of tips and tools to get your data back working for you.
There are times when you can't be wise enough and there are files you've yet to duplicate, or you simply want to avoid possible disk failures, just for good measure. It makes perfect sense to deal with laptops gently, as any physical shock affects the life-span of your HDDs immensely. Other than trying not to drop the notebook there is one thing you can do; try picking a laptop or HDD protected against drops. These units throw the head into a safe position if they detect the computer is in free-fall(through G-sensors) state. Macbooks sport this feature out of the box, so do business class Lenovo models. Try choosing one of them. There are certain inherent problems with the technology, which lets you predict a likely failure after a given number of work hours, so make sure you are familiar with the MTBF(mean time between failures) value assigned to the particular model you use and replace it before its time has come.
Oddly enough problems with data often occur when you are formatting your computer's hard drive. Formatting is supposed to clean the drive and make it work quicker, but it often leads to problems such as erasing valuable data. This site ondata recovery after format might be of help to you, if you are in that situation.

**TCP & UDP header format.**

**TCP**




Source Port: 16 bits,The source port number.

Destination Port: 16 bits,The destination port number.

Sequence Number: 32 bits,The sequence number of the first data octet in this segment (except when SYN is present). If SYN is present the sequence number is the initial sequence number (ISN) and the first data octet is ISN+1.

Acknowledgment Number: 32 bits, If the ACK control bit is set this field contains the value of the next sequence number the sender of the segment is expecting to receive. Once a connection is established this is always sent.

Data Offset: 4 bits, The number of 32 bit words in the TCP Header. This indicates where the data begins. The TCP header (even one including options) is integral number of 32 bits long.

Reserved: 6 bits, Reserved for future use. Must be zero.

Control Bits: 6 bits (from left to right):
URG: Urgent Pointer field significant
ACK: Acknowledgment field significant
PSH: Push Function

RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: No more data from sender

Window: 16 bits
The number of data octets beginning with the one indicated in the acknowledgment field which the sender of this segment is willing to accept.

Checksum: 16 bits
The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header and text. If a segment contains an odd number of header and text octets to check summed, the last octet is padded on the right with zeros to form a 16 bit word for checksum purposes. The pad is not transmitted as part of the segment. While computing the checksum, the checksum field itself is replaced with zeros.

Urgent Pointer: 16 bits
This field communicates the current value of the urgent pointer as a positive offset from the sequence number in this segment. The urgent pointer points to the sequence number of the octet following the urgent data. This field is only be interpreted in segments with the URG control bit set.

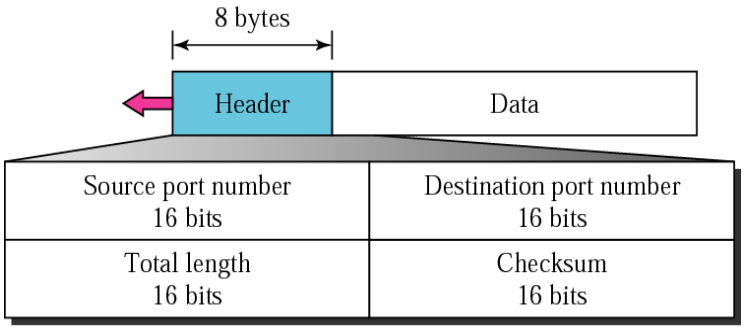
Options: variable
Options may occupy space at the end of the TCP header and are a multiple of 8 bits in length. All options are included in the

checksum. An option may begin on any octet boundary. There are two cases for the format of an option:

Case 1: A single octet of option-kind.
Case 2: An octet of option-length, and the actual option-data octets.

Padding: variable
The TCP header padding is used to ensure that the TCP header ends and data begins on a 32 bit boundary.The padding is composed of zeros.

**UDP**




**Source Port.** 16 bits.
The port number of the sender. Cleared to zero if not used.

**Destination Port.** 16 bits.
The port this packet is addressed to.

**Length.** 16 bits.
The length in bytes of the UDP header and the encapsulated data. The minimum value for this field is 8.

**Checksum.** 16 bits.
Computed as the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded as needed with zero bytes at the end to make a multiple of two bytes.

**Q 9. What is traffic shaping ?How it is done.**
**Ans:** Traffic shaping, also known as "packet shaping," is the practice of regulating network data transfer to assure a certain level of performance, quality of service (QoS) or return on investment (ROI). The practice involves delaying the flow of packets that have been designated as less important or less desired than those of prioritized traffic streams. Regulating the flow of packets into a network is known as "bandwidth throttling." Regulation of the flow of packets out of a network is known as "rate limiting."
Benefits
When lots of traffic flows past a packet bottleneck (logical or physical) the benefits of traffic shaping are:

- Less jitter.
- Reduced packet loss.
- Lower latency.

It is done as

- Other important factors may include the available video compression, frame rate, resolutions, two-way audio capability, motion detection, installation configurations, object detection, and anti-tampering features. Because the person observing a robotic webcam through the website can interact with it — panning, tilting, and zooming — the experience is quite different than watching a static webcam.
- Many models today include such features as an end piece that includes a retractable foot rest, or storage pockets that are ideal for remote controls and magazines. For anyone who wants seating options that can be utilized in different configurations, has a high level of comfort, and is easy to transport, sectional couches are well worth consideration

**DISTANCE VECTOR**
Distance
Distance is the cost of reaching a destination, usually based on the number of hosts the path passes through, or the total of all the administrative metrics assigned to the links in the path.
Vector
From the standpoint of routing protocols, the vector is the interface traffic will be forwarded out in order to reach an given destination network along a route or path selected by the routing protocol as the best path to the destination network.
Distance vector protocols use a distance calculation plus an outgoing network interface (a vector) to choose the *best path* to a destination network. The network protocol (IPX, SPX, IP, Appletalk, DECnet etc.) will forward data using the best paths selected.
**Common distance vector routing protocols include:**

- Appletalk RTMP
- IPX RIP
- IP RIP
- IGRP

**Advantages of Distance Vector Protocols**

Well Supported

Protocols such as RIP have been around a long time and most, if not all devices that perform routing will understand RIP.

| Sr.No. | Distance Vector Routing Algorithm | Link state routing algorithm |
|---|---|---|
| 1 | Entire routing table is sent as an update | Updates are incremental & enitire routing table is not sent as update |
| 2 | Distance vector protocol send periodic update at every 30 or 90 second | Updates are triggered not periodic |
| 3 | Update are broadcasted | Updates are multicasted |
| 4 | Updates are sent to directly connected neighbor only | Update are sent to entire network & to just directly connected neighbor .Updates are carry SPF tree information & SPF cost Calculation information of entire topology |
| 5 | Routers don't have end to end visibility of entire network. | Routers have visibility of entire network of that area only. |
| 6 | It is proned to routing loops | No routing loops |
| 7 | Distance vector routing protocol has slow convergance due to periodic update. | Convergance is fast because of triggered updates. |
| 8 | Eg. **RIP ,IGRP , BGP** . | Eg. : **OSPF , IS-IS** |

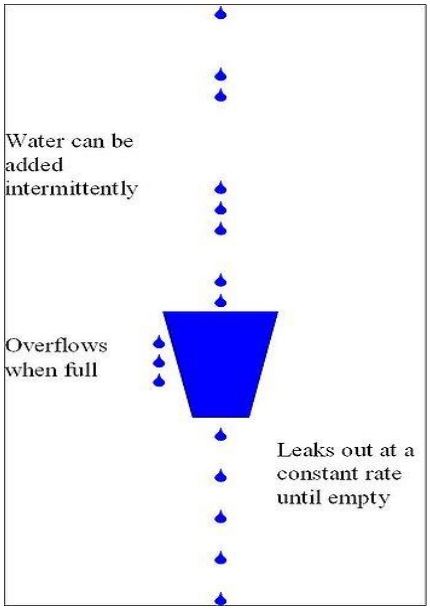
**Leaky bucket Algorithm.**

The leaky bucket is an algorithm used in packet switched computer networks and telecommunications networks to check that data transmissions conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). The leaky bucket algorithm is also used in leaky bucket counters, e.g. to detect when the average or peak rate of random or stochastic events orstochastic processes exceed defined limits.

The Leaky Bucket Algorithm is based on an analogy of a bucket that has a hole in the bottom through which any water it contains will leak away at a constant rate, until or unless it is empty. Water can be added intermittently, i.e. in bursts, but if too much is added at once, or it is added at too high an average rate, the water will exceed the capacity of the bucket, which will overflow.

There are actually two different methods of applying this analogy described in the literature. These give what appear to be two different algorithms, both of which are referred to as the leaky bucket algorithm. This has resulted in confusion about what the leaky bucket algorithm is and what its properties are.

In one version,the analogue of the bucket is a counter or variable, separate from the flow of traffic, and is used only to check that traffic conforms to the limits, i.e. the analogue of the water is brought to the bucket by the traffic and added to it so that the level of water in the bucket indicates conformance to the rate and burstiness limits. This version is referred to here as the leaky bucket as a meter. In the second version the traffic passes through a queue that is the analogue of the bucket, i.e. the traffic is the analogue of the water passing through the bucket. This version is referred to here as the leaky bucket as a queue. The leaky bucket as a meter is equivalent to (a mirror image of) the token bucket algorithm, and given the same parameters will see the same traffic as conforming or nonconforming. The leaky bucket as a queue can be seen as a special case of the leaky bucket as a meter



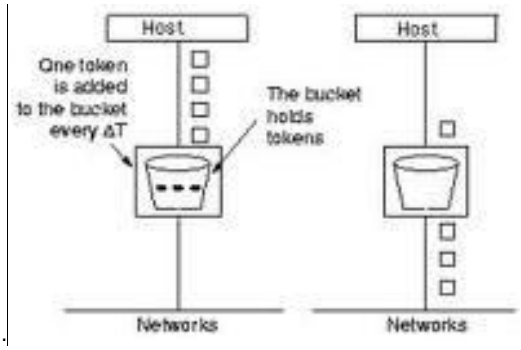

**Token bucket Algorithm.**

The algorithm can be conceptually understood as follows:

- A token is added to the bucket every 1 / r seconds.
- The bucket can hold at the most b tokens. If a token arrives when the bucket is full, it is discarded.
- When a packet (network layer PDU) of n bytes arrives, ntokens are removed from the bucket, and the packet is sent to the network.
- If fewer than n tokens are available, no tokens are removed from the bucket, and the packet is considered to be non-conformant.

The algorithm allows bursts of up to b bytes, but over the long run the output of conformant packets is limited to the constant rate, r. Non-conformant packets can be treated in various ways:

- They may be dropped.
- They may be enqueued for subsequent transmission when sufficient tokens have accumulated in the bucket.
- They may be transmitted, but marked as being non-conformant, possibly to be dropped subsequently if the network is overloaded.




**How the algorithm works**

The algorithm is based on a concept of credit. We begin with an amount of credits calculated from the values specified with the --limit and --limit- burst. This amount of credits we start with is also the maximum credit we can have. We also calculate a cost that every packet that pass needs to pay. The only way to get new credit is to wait, that means that only time can give us new credit. It use the jiffies counter because it's more efficient

than using a real clock on every packet. It's thus impossible to give new credits every time, we must have a checkpoint. This checkpoint is the jiffy counter which is incremented HZ times per second. As stated above,

**Application layer protocol .**

This is the actual internet service or access that we follow to get work or services done through the internet. Millions of people across the world access the internet everyday. The root of the internet lie in the academia and much research I think is still being carried out. Since the internet was opened up to commerce in the early 1990's, many new facilities have arisen. Also with the advent of the world wide web, business has seized the opportunity to use the internet for communication, marketing, advertising and selling of different products.

- **FTP** - File Transfer Protocol allows file transfer between two computers with login required. ile Transfer Protocol (FTP) is a standard network protocol used to copy a file from one host to another over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server.[1] FTP users may authenticate themselves using a clear-text sign-in protocol but can connect anonymously if the server is configured to allow it.
- **TFTP** - Trivial File Transfer Protocol allows file transfer between two computers with no login required. It is limited, and is intended for diskless stations. Trivial File Transfer Protocol (TFTP) is a file transfer protocol known for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user.
- **NFS** - Network File System is a protocol that allows UNIX and Linux systems remotely mount each other's file systems. 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
- **SNMP** - Simple Network Management Protocol is used to manage all types of network elements based on various data sent and received. 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.
- **SMTP** - Simple Mail Transfer Protoco l is used to transport mail. Simple Mail Transport Protocol is used on the internet, it is not a transport layer protocol but is an application layer protocol. Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks. SMTP was first defined by RFC 821 (1982, eventually declared STD 10),[1] and last updated by RFC 5321 (2008)[2] which includes theextended SMTP (ESMTP) additions, and is the protocol in widespread use today. SMTP is specified for outgoing mail transport and uses TCP port 25.
- **HTTP** - Hypertext Transfer Protocol is used to transport HTML pages from web servers to web browsers. The protocol used to communicate between web servers and web browser software clients.
- **DHCP** - Dynamic host configuration protocol is a method of assigning and controlling the IP addresses of computers on a given network. It is a server based service that automatically assigns IP numbers when a computer boots. This way the IP address of a computer does not need to be assigned manually. This makes changing networks easier to manage. DHCP can perform all the functions of BOOTP.
- **BGP** - Border Gateway Protocol. When two systems are using BGP, they establish a TCP connection, then send each other their BGP routing tables. BGP uses distance vectoring. It detects failures by sending periodic keep alive messages to its neighbors every 30 seconds. It exchanges information about reachable networks with other BGP systems including the full path of systems that are between them. Described by RFC 1267, 1268, and 1497.

- **RIP** - Routing Information Protocol is used to dynamically update router tables on WANs or the internet. A distance-vector algorithm is used to calculate the best route for a packet. RFC 1058, 1388 (RIP2).
- **OSPF** - Open Shortest Path First dynamic routing protocol. A link state protocol rather than a distance vector protocol. It tests the status of its link to each of its neighbors and sends the acquired information to them.
- **Telnet** is used to remotely open a session on another computer. It relies on TCP for transport and is defined by RFC854. Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

**How Compression done**

When you have a file containing text, there can be repetitive single words, word combinations and phrases that use up storage space unproductively. Or there can be media such as high tech graphical images in it whose data information occupies too much space. To reduce this inefficiency electronically, you can compress the document.

Compression is done by using compression algorithms (formulae) that rearrange and reorganize data information so that it can be stored more economically. By encoding information, data can be stored using fewer bits. This is done by using a compression/decompression program that alters the structure of the data temporarily for transporting, reformatting, archiving, saving, etc.

Compression, when at work, reduces information by using different and more efficient ways of representing the information. Methods may include simply removing space characters, using a single character to identify a string of repeated characters, or substituting smaller bit sequences for recurring characters. Some compression algorithms delete information altogether to achieve a smaller file size. Depending on the algorithm used, files can be adequately or greatly reduced from its original size.

**Techniques of Compression**

**Lossless Compression** is a type of compression that can reduce files without a loss of information in the process. The original file can be recreated exactly when uncompressed. To achieve this, algorithms create reference points (substitution characters) for things such as textual patterns, store them in a catalogue and send them along with the smaller encoded file. When uncompressed, the file is "re-generated" by using those documented reference points to re-substitute the original information.

Lossless compression is ideal for documents containing text and numerical data where any loss of textual information can't be tolerated. ZIP compression, for instance, is a Lossless compression that detects patterns and replaces them with a single character. Another example, LZW compression (Abraham Lempel, Jakob Ziv and Terry Welch-creators of LZW), works best for files containing lots of repetitive data.

**Lossy Compression,** on the other hand, reduces the size of a file by eliminating bits of information. It permanently deletes any unnecessary data. This compression is usually used with images, audio and graphics where a loss of quality is affordable. However, the original file can't be retained.

For instance, in an image containing a green landscape with a blue sky, all the different and slight shades of blue and green are eliminated with compression. The essential nature of the data isn't lost-the essential colours are still there. One popular example of Lossy compression is JPEG compression (Joint Photographic Experts Group) that is suitable for grayscale or colour images.

**Role of application layer in OSI model**

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)
- Network virtual terminals

**Difference between routers and gateway**

Routers send data to a specific location based on a address for the network segment. The benefit is the ability for a router to search routing tables and find the shortest path to the destination. The downside to routers is that they are protocol dependent and therefore can only route data between network segments using the same protocol. Today this is a moot because everyone uses TCP/IP and has an open architecture. This is why, for example, data can be sent between a Windows NT network and a Netware network.

Here's how a router works: When it receives a packet and sees a MAC address (hardware address) that is not on the local segment, it strips away the MAC address, looks at the IP address (software address), searches its routing table, and then sends the packet based on the IP address to the router that's connected to the segment that contains that address.

Gateways are network points that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.
All gateways are routers, but not all routers are gateways.

Routers "route" traffic from one network to another. They can be used to connect different IP ranges/segments of larger networks together. Commonly used in wide area networks, and larger networks with multiple IP ranges spread out...such as campus networks, large enterprise companies that are spread out across several buildings, etc. You may have a building where all the pcs are 10.50.1.xxx, and another building where all the pcs are 10.50.2.xxx, and another building where all the pcs are 10.50.3.xxx. Each building would have a router that connects the building to the central part of the network..where one big router takes connections from all the other buildings (like a star-hub layout)..and makes one big network out of it...and also gives everyone internet access.

Gateways usually refer to a router that performs the job of connecting the network to the internet. It's still a router, because it's connecting one network (the private network) to another network (the internet). When you talk about home grade broadband routers, or SOHO/SMB routers..they're usually running "gateway

mode" by default. You can take many consumer grade routers and configure them into "router" mode..and use them in larger networks such as described in the above paragraph. In the web administration you'll commonly find a configuration section for this.

**Gateway**

A gateway is a network point that acts as an entrance to another network. On the Internet, anode or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within

In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and afirewall server. A gateway is often associated with both arouter, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

**Routers**

A router is used to route data packets between two networks. It reads the information in each packet to tell where it is going. If it is destined for an immediate network it has access to, it will strip the outer packet, readdress the packet to the proper ethernet address, and transmit it on that network. If it is destined for another network and must be sent to another router, it will re-package the outer packet to be received by the next router and send it to the next router. The section on routing explains the theory behind this and how routing tables are used to help determine packet destinations. Routing occurs at the network layer of the OSI model. They can connect networks with different architectures such as Token Ring and Ethernet. Although they can transform information at the data link level, routers cannot transform information from one data format such as TCP/IP to another such as IPX/SPX. Routers do not send broadcast packets or corrupted packets. If the routing table does not indicate the proper address of a packet, the packet is discarded.

**Bridge**

A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets. Bridges can be programmed to reject packets from particular networks. Bridging occurs at the data link layer of the OSI model, which means the bridge cannot read IP addresses, but only the outermost hardware address of the packet. In our case the bridge can read the ethernet data which gives the hardware address of the destination address, not the IP address. Bridges forward all broadcast messages. Only a special bridge called a translation bridge will allow two networks of different architectures to be connected. Bridges do not normally allow connection of networks with different architectures. The hardware address is also called the MAC (media access control) address. To determine the network segment a MAC address belongs to, bridges use one of:

- Transparent Bridging - They build a table of addresses (bridging table) as they receive packets. If the address is not in the bridging table, the packet is forwarded to all segments other than the one it came from. This type of bridge is used on ethernet networks.
- Source route bridging - The source computer provides path information inside the packet. This is used on Token Ring networks.

**Repeater**

A repeater connects two segments of your network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. When talking about, ethernet topology, you are probably talking about using a hub as a repeater. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.

**Switch**

In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. In the

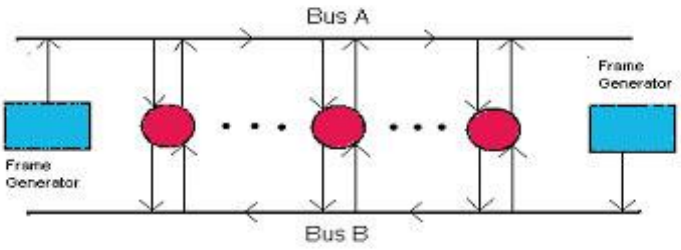
traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties. On an Ethernet local area network (LAN), a switch determines from the physical device (Media Access Control or MAC) address in each incoming message framewhich output port to forward it to and out of. In a wide area packet-switched network such as the Internet, a switch determines from the IP address in each packet which output port to use for the next part of its trip to the intended destination.
In the Open Systems Interconnection (OSI) communications model, a switch performs theLayer 2 or Data-link layer function. That is, it simply looks at each packet or data unit and determines from a physical address (the "MAC address") which device a data unit is intended for and switches it out toward that device. However, in wide area networks such as the Internet, the destination address requires a look-up in a routing table by a device known as a router. Some newer switches also perform routing functions (Layer 3 or the Network layer functions in OSI) and are sometimes called IP switches.

**Hub**
A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
A passive hub serves simply as a conduit for the data, enabling it to go from one device (or segment) to another. So-called intelligent hubs include additional features that enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub. Intelligent hubs are also called manageable hubs.
A third type of hub, called a switching hub, actually reads the destination address of each packet and then forwards the packet to the correct port.

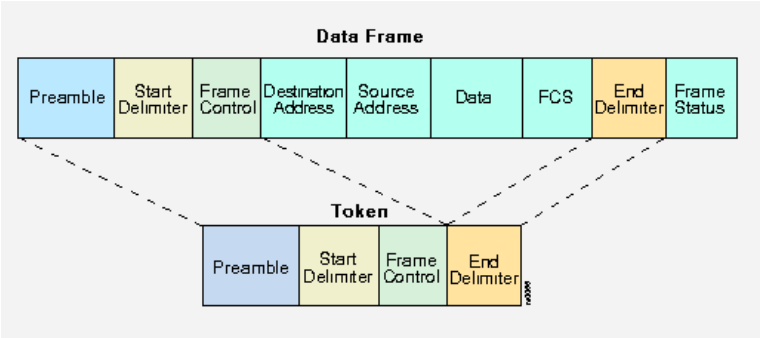
**Patch panel**
A patch panel is a mounted hardware unit containing an assembly of port locations in a communications or other electronic or electrical system. In a network, a patch panel serves as a sort of static switchboard, using cables to interconnect computers within the area of a local area network (LAN) and to the outside for connection to the Internet or other wide area network (WAN). A patch panel uses a sort of jumper cable called a patch cord to create each interconnection.

**Architecture of DQDB.**

DQDB: Distributed Queue Dual Bus Defined in IEEE 802.6
Data Over Cable Service Interface Distributed Queue Dual Bus (DQDB) is a Data-link layer communication protocol for Metropolitan Area Networks (MANs), specified in the IEEE 802.6 standard, designed for use in MANs. DQDB is designed for data as well as voice and video transmission based on cell switching technology (similar to ATM). DQDB, which permits multiple systems to interconnect using two unidirectional logical buses, is an open standard that is designed for compatibility with carrier transmission standards such as SMDS, which is based on the DQDB standards.
For a MAN to be effective it requires a system that can function across long, i°city-widei± distances of several miles, have a low susceptibility to error, adapt to the number of nodes attached and have variable bandwidth distribution. Using DQDB, networks can be thirty miles long and function in the range of 34 Mbps to 155 Mbps. The data rate fluctuates due to many hosts sharing a dual bus as well as the location of a single host in relation to the frame generator, but there are schemes to compensate for this problem making DQDB function reliably and fairly for all hosts.
The DQDB is composed of a two bus lines with stations attached to both and a frame generator at the end of each bus. The buses run in parallel in such a fashion as to allow the frames generated to travel across the stations in opposite directions.
**the basic DQDB architecture:**




**FDDI Frame Format.**
The following figure shows the frame format of an FDDI data frame and token:




FDDI Frame Fields

**Preamble** -- A unique sequence that prepares each station for an upcoming frame.

**Start Delimiter** -- Indicates the beginning of a frame by employing a signaling pattern that differentiates it from the rest of the frame.

**Frame Control** -- Indicates the size of the address fields, whether the frame contains asynchronous or synchronous data, and other control information.

**Destination Address** -- Contains a unicast (singular), multicast (group), or broadcast (every station) address. As with Ethernet and Token Ring addresses, FDDI destination addresses are 6 bytes long.

**Source Address** -- Identifies the single station that sent the frame. As with Ethernet and Token Ring addresses, FDDI source addresses are 6 bytes long.

**Data** -- Contains either information destined for an upper-layer protocol or control information.

**Frame Check Sequence** (FCS) -- Filled by source station with a calculated cyclic redundancy check (CRC) value dependent on frame contents (as with Token Ring and Ethernet). The destination address recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.

**End Delimiter** -- Contains nondata symbols that indicate the end of the frame.

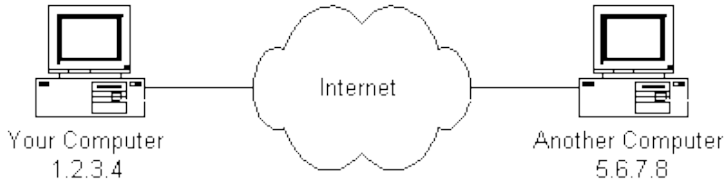
**Frame Status** -- Allows the source station to determine if an error occurred and if the frame was recognized and copied by a receiving station.

**Working of internet.**

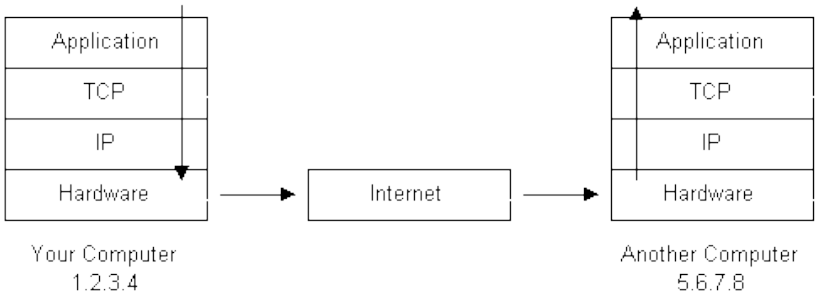
The **Internet** is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is anetwork of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertextdocuments of the World Wide Web (WWW) and the infrastructure to supportelectronic mail.

Because the Internet is a global network of computers each computer connected to the Internet **must** have a unique address. Internet addresses are in the form **nnn.nnn.nnn.nnn** where nnn must be a number from 0 - 255. This address is known as an IP address. (IP stands for Internet Protocol; more on this later.)

The picture below illustrates two computers connected to the Internet; your computer with IP address 1.2.3.4 and another computer with IP address 5.6.7.8. The Internet is represented as an abstract object in-between. (As this paper progresses, the Internet portion of Diagram 1 will be explained and redrawn several times as the details of the Internet are exposed.)




If you connect to the Internet through an Internet Service Provider (ISP), you are usually assigned a temporary IP address for the duration of your dial-in session. If you connect to the Internet from a local area network (LAN) your computer might have a permanent IP address or it might obtain a temporary one from a DHCP (Dynamic Host Configuration Protocol) server. In any case, if you are connected to the Internet, your computer has a unique IP address.




1. The message would start at the top of the protocol stack on your computer and work it's way downward.
2. If the message to be sent is long, each stack layer that the message passes through may break the message up into smaller chunks of data. This is because data sent over the Internet (and most computer networks) are sent in manageable chunks. On the Internet, these chunks of data are known as **packets**.

3. The packets would go through the Application Layer and continue to the TCP layer. Each packet is assigned a **port number**. Ports will be explained later, but suffice to say that many programs may be using the TCP/IP stack and sending messages. We need to know which program on the destination computer needs to receive the message because it will be listening on a specific port.
4. After going through the TCP layer, the packets proceed to the IP layer. This is where each packet receives it's destination address, 5.6.7.8.
5. Now that our message packets have a port number and an IP address, they are ready to be sent over the Internet. The hardware layer takes care of turning our packets containing the alphabetic text of our message into electronic signals and transmitting them over the phone line.
6. On the other end of the phone line your ISP has a direct connection to the Internet. The ISPs **router** examines the destination address in each packet and determines where to send it. Often, the packet's next stop is another router. More on routers and Internet infrastructure later.
7. Eventually, the packets reach computer 5.6.7.8. Here, the packets start at the bottom of the destination computer's TCP/IP stack and work upwards.
8. As the packets go upwards through the stack, all routing data that the sending computer's stack added (such as IP address and port number) is stripped from the packets.
9. When the data reaches the top of the stack, the packets have been re-assembled into their original form, "Hello computer 5.6.7.8!"

**IEEE 802.4 lan standard.**

Token bus is a network implementing the token ring protocol over a "virtual ring" on a coaxial cable. A token is passed around the network nodes and only the node possessing the token may transmit. If a node doesn't have anything to send, the token is passed on to the next node on the virtual ring. Each node must know the address of its neighbour in the ring, so a special protocol is needed to notify the other nodes of connections to, and disconnections from, the ring.

Token bus was standardized by IEEE standard 802.4. It is mainly used for industrial applications. Token bus was used by GM (General Motors) for their Manufacturing Automation Protocol (MAP) standardization effort. This is an application of the concepts used in token ring networks. The main difference is that the endpoints of the bus do not meet to form a physical ring. The IEEE 802.4 Working Group is disbanded. In order to guarantee the packet delay and transmission in Token bus protocol, a modified Token bus was proposed in Manufacturing Automation Systems and flexible manufacturing system (FMS)