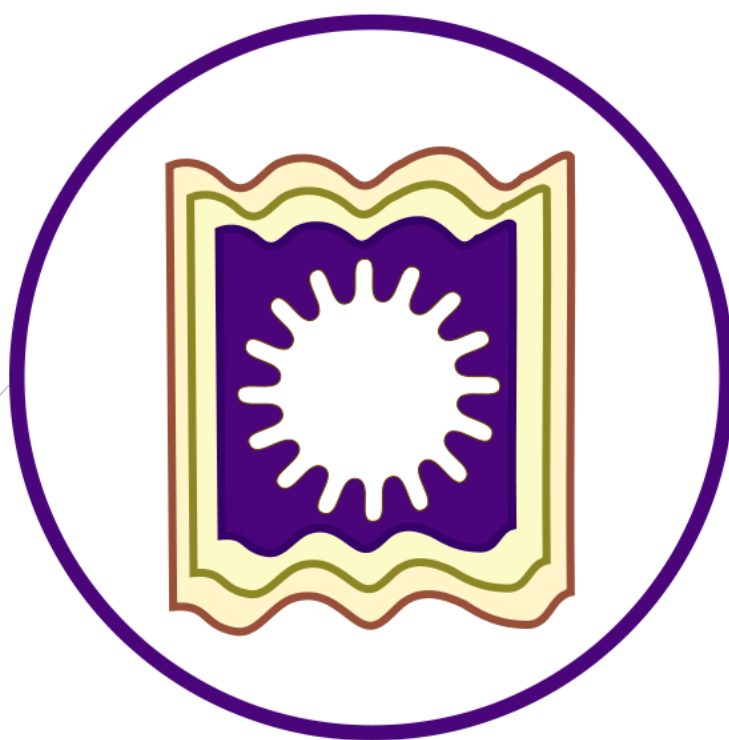


6/3/2014

COMPUTER NETWORKS

CSE-2012 B.Sc. (Honours) Question Solution



S M TALHA JUBAED

DEPT. OF COMPUTER SCIENCE & ENGINEERING (CSE)

UNIVERSITY OF RAJSHAHI (RU)

HOTLINE# +088-01911-088 706

Question-01: Differentiating between circuit switching and packet switching. 4 Marks CSE-2012

Difference Between circuit switching and packet switching:

Following are some important difference between circuit switching and packet switching:

Circuit switching	Packet Switching
Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the communication session. The circuit functions as if the nodes were physically connected as with an electrical circuit.	Packet switching is a digital networking communications method that groups all transmitted data – regardless of content, type, or structure – into suitably sized blocks, called packets.
In circuit switching, the whole message is sent from the source to the destination without being divided into packets.	In packet switching, the message is first divided into manageable packets at the source before being transmitted. The whole message is sent from the source to the destination after being divided into packets. The packets are assembled at the destination.
The circuit switching was never implemented at the network layer; it is mostly used at the physical layer.	The packet switching is implemented at the network layer.
Circuit switching is old and expensive, and it is what PSTN uses.	Packet switching is modern and relatively less expensive.
The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the communication session.	Packet switching shares available network bandwidth between multiple communication sessions.
Circuit switching can be relatively inefficient because capacity is guaranteed on connections which are set up but are not in continuous use, but rather momentarily. However, unused capacity guaranteed to a connection cannot be used by other connections on the same network.	Packet switching can be relatively efficient because capacity is guaranteed on connections which are shared by multiple communication sessions and are in continuous use.
Circuit switching networks require a circuit to be established. The circuit functions as if the nodes were physically connected as with an electrical circuit.	Packet switching networks do not require a circuit to be established and allow many pairs of nodes to communicate concurrently over the same channel.
In circuit switching, network links are dedicated to one communication session at a time, guarantees the quality of service.	In packet switching, instead of being dedicated to one communication session at a time, network links are shared by packets from multiple competing communication sessions, resulting in the loss of the quality of service guarantees that are provided by circuit switching.
In circuit switching, the bit delay is constant during a connection.	In packet switching, packet queues may cause varying and potentially indefinitely long packet transfer delays.
While circuit switching is commonly used for connecting voice circuits, the concept of a dedicated path persisting between two communicating parties or nodes can be extended to signal content other than voice. Its advantage is that it provides for continuous transfer without the overhead associated with packets making	Packet switching is used to optimize the use of the channel capacity available in digital telecommunication networks such as computer networks, to minimize the transmission latency (the time it takes for data to pass across the network), and to increase robustness of communication.

maximal use of available bandwidth for that communication.	
No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.	Performance can be degraded by competing users because it is not protected from use by other users.
Examples of circuit-switched networks: <ol style="list-style-type: none"> 1. The defining example of a circuit-switched network is the early analog telephone network 2. Public switched telephone network (PSTN) 3. ISDN B-channel 4. Circuit Switched Data (CSD) and High-Speed Circuit-Switched Data (HSCSD) service in cellular systems such as GSM 5. Datakit 6. X.21 (Used in the German DATEX-L and Scandinavian DATEX circuit switched data network) 7. Optical mesh network 	The best-known use of packet switching is the Internet and most local area networks. X.25 is a notable use of packet switching in that, despite being based on packet switching methods, it provided virtual circuits to the user. In 1978, X.25 provided the first international and commercial packet switching network, the International Packet Switched Service (IPSS).

Question-02: Briefly describe different types of channel access methods. 6 Marks CSE-2012

Different types of channel access methods:

In telecommunications and computer networks, a channel access method or multiple access method allows several terminals connected to the same multi-point transmission medium to transmit over it and to share its capacity.

Circuit mode and channelization channel access methods:

The following are common circuit mode and channelization channel access methods:

- ***Frequency-division multiple access (FDMA)***, based on frequency-division multiplexing (FDM)
 - Wavelength division multiple access (WDMA)
 - Orthogonal frequency-division multiple access (OFDMA), based on Orthogonal frequency-division multiplexing (OFDM)
 - Single-carrier FDMA (SC-FDMA), a.k.a. linearly-precoded OFDMA (LP-OFDMA), based on single-carrier frequency-domain-equalization (SC-FDE).
- ***Time-division multiple access (TDMA)***, based on time-division multiplexing (TDM)
 - Multi-Frequency Time Division Multiple Access (MF-TDMA)
- ***Code division multiple access (CDMA)***, a.k.a. Spread spectrum multiple access (SSMA)
 - Direct-sequence CDMA (DS-CDMA), based on Direct-sequence spread spectrum (DSSS)
 - Frequency-hopping CDMA (FH-CDMA), based on Frequency-hopping spread spectrum (FHSS)
 - Orthogonal frequency-hopping multiple access (OFHMA)
 - Multi-carrier code division multiple access (MC-CDMA)
- ***Space division multiple access (SDMA)***

Packet mode methods:

The following are examples of packet mode channel access methods:

- ***Contention based random multiple access methods***
 - Aloha
 - Slotted Aloha

- Multiple Access with Collision Avoidance (MACA)
- Multiple Access with Collision Avoidance for Wireless (MACAW)
- Carrier sense multiple access (CSMA)
- Carrier sense multiple access with collision detection (CSMA/CD) - suitable for wired networks
- Carrier sense multiple access with collision avoidance (CSMA/CA) - suitable for wireless networks
 - Distributed Coordination Function (DCF)
- Carrier sense multiple access with collision avoidance and Resolution using Priorities (CSMA/CARP)
- Carrier Sense Multiple Access/Bitwise Arbitration (CSMA/BA) Based on constructive interference (CAN-bus)
- ***Token passing:***
 - Token ring
 - Token bus
- ***Polling***
- ***Resource reservation (scheduled) packet-mode protocols***
 - Dynamic Time Division Multiple Access (Dynamic TDMA)
 - Packet reservation multiple access (PRMA)
 - Reservation ALOHA (R-ALOHA)

Pure ALOHA:

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between frames from different stations.

It is obvious that we need to resend the frames that have been destroyed during transmission. The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.

Slotted ALOHA:

In slotted ALOHA we divide the time into slots of T_{fr} s and force the station to send only at the beginning of the time slot. Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to T_{fr} .

Carrier sense multiple access (CSMA)

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. **Carrier sense multiple access (CSMA)** requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle “sense before transmit” or “listen before talk.” CSMA can reduce the possibility of collision, but it cannot eliminate it.

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

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision. In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again. For CSMA/CD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission. This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time T_{fr} must be at least two times the maximum propagation time T_p .

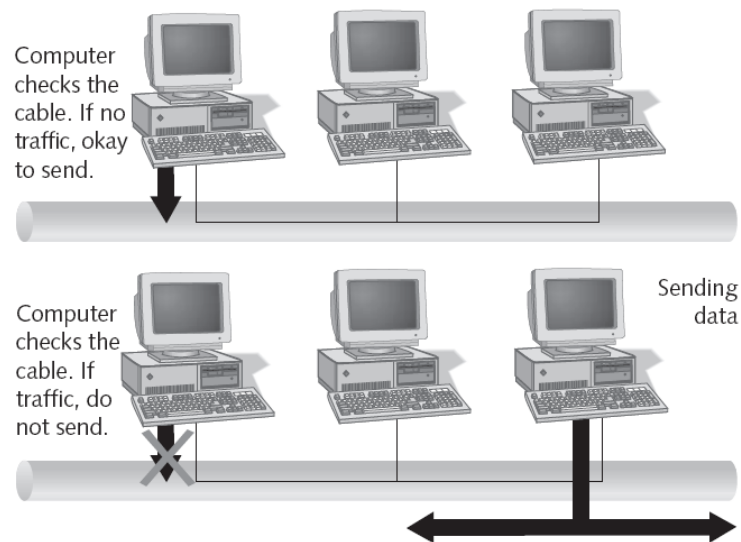


Figure 7-1 With CSMA/CD, computers check for cable traffic

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

The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station. In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.

We need to avoid collisions on wireless networks because they cannot be detected. Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network. Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments.

Reservation

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval. If there are N stations in the system, there are exactly N reservation minislots in the reservation frame. Each minislot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own minislot. The stations that have made reservations can send their data frames after the reservation frame.

Polling

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session.

If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

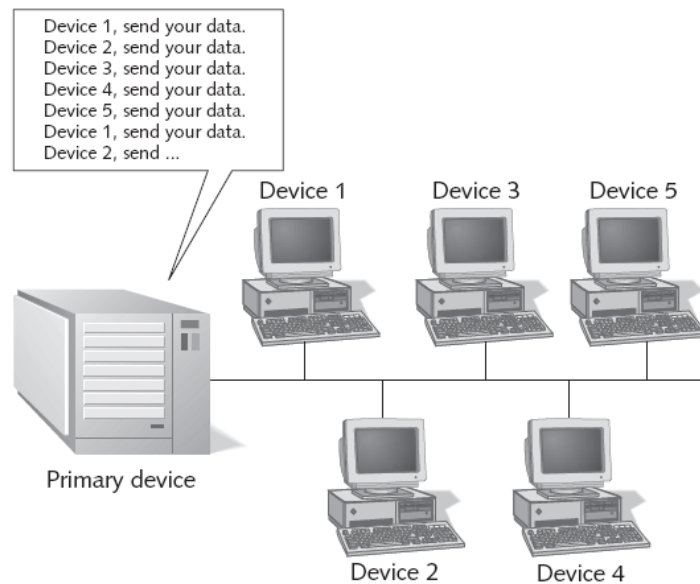


Figure 7-3 The primary device controls polling

Token Passing:

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station.

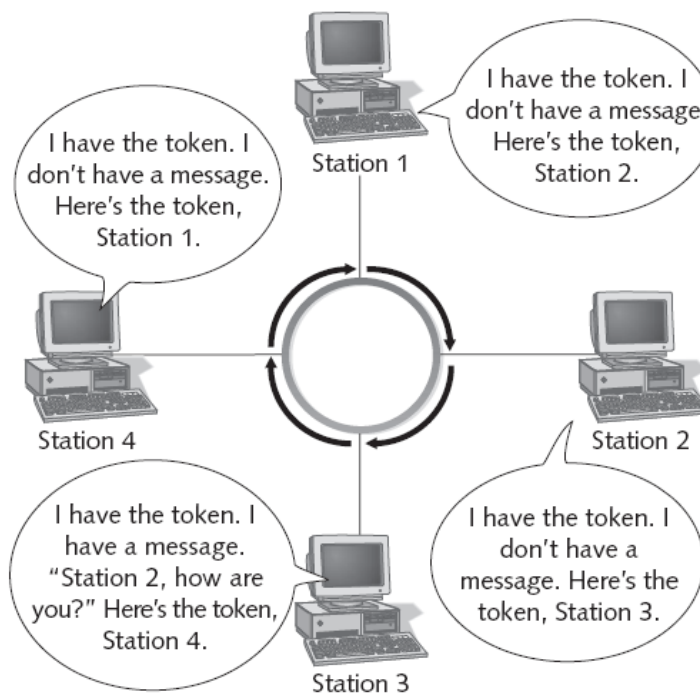


Figure 7-2 Communications in a token-passing network

Frequency-Division Multiple Access (FDMA)

In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands. In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands.

Time-Division Multiple Access (TDMA)

In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in its assigned time slot. In TDMA, the bandwidth is just one channel that is timeshared between different stations.

Code-Division Multiple Access (CDMA)

Code-division multiple access (CDMA) was conceived several decades ago. Recent advances in electronic technology have finally made its implementation possible. CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link. It differs from TDMA because all stations can send data simultaneously; there is no timesharing. In CDMA, one channel carries all transmissions simultaneously.

বিশেষ নির্দেশনাঃ এই প্রশ্নের উত্তর অন্যভাবেও করা যেতে পারে। পাওয়ার পয়েন্ট স্লাইডে ৫ টি প্রধান এক্সেস মেথডের কথা উল্লেখ আছে বিধায়, পরীক্ষায় ৫ টি প্রধান এক্সেস মেথড সম্পর্কে লিখলেও চলবে। উপরে যেসকল এক্সেস মেথড উল্লেখ করা হয়েছে, সেগুলো বইয়ের ধারাবাহিকতায় লেখা। স্লাইড অনুযায়ী লিখলে, এই প্রশ্নের উত্তর বেশ সংক্ষেপে লেখা সম্ভবঃ

Major Access Methods

Channel access is handled at the MAC sublayer of the Data Link layer in the OSI model.

- Five major types of channel access
 1. Contention
 2. Switching
 3. Token passing
 4. Demand priority
 5. Polling

Contention:

- In early networks based on **contention**, computers sent data whenever they had data to send
- As networks grow, outgoing messages collide more frequently, must be sent again, and then collide again
- To organize contention-based networks, two carrier access methods were created
 - CSMA/CD
 - CSMA/CA

Switching:

- **Switching:** nodes are interconnected through a switch, which controls access to the media
 - Contention occurs only when multiple senders ask to reach the same receiver simultaneously or when the simultaneous transmission requests exceed the switch's capability to handle multiple connections
- Advantages: fairer, centralized management (enables QoS), switch can have connection ports that operate at different speeds
- Disadvantage: higher cost

Token Passing

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring.

The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station.

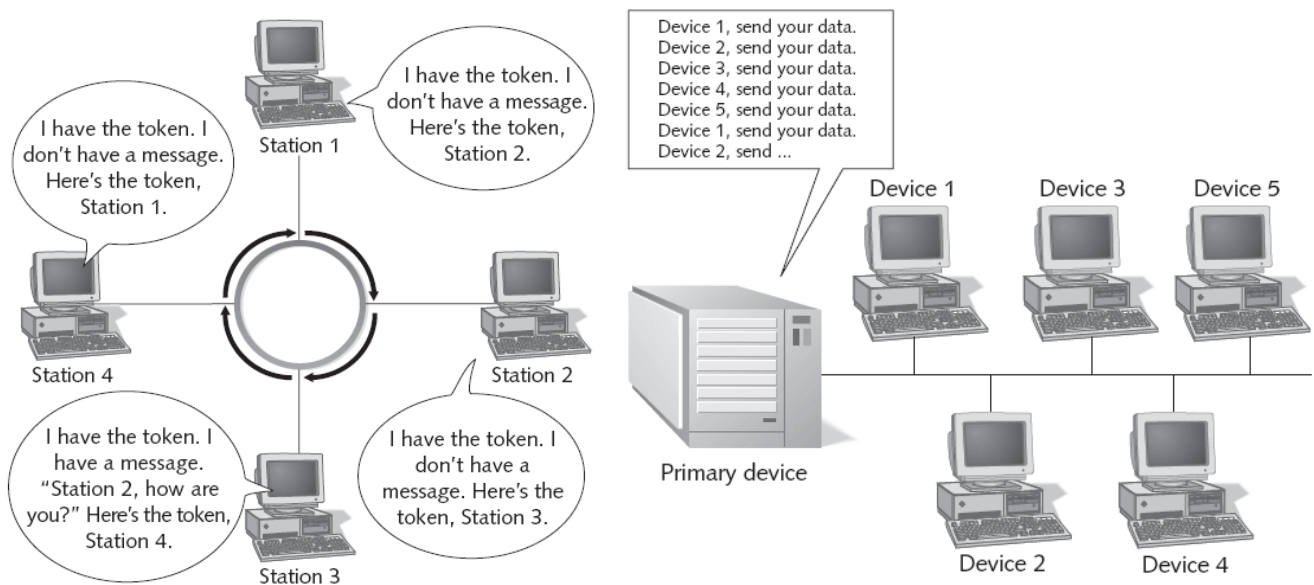


Figure 7-2 Communications in a token-passing network Figure 7-3 The primary device controls polling

Demand Priority

- **Demand priority:** channel access method used solely by the 100VG-AnyLAN 100 Mbps Ethernet standard (IEEE 802.12)
 - 100VG-AnyLAN runs on a star bus topology
 - Intelligent hubs control access to the network
 - Hub searches all connections in a round-robin fashion
 - When an end node has data to send, it transmits a **demand signal** to the hub
 - The hub then sends an acknowledgement that the computer can start transmitting its data
 - The major disadvantage of demand priority is price

Polling

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session.

If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

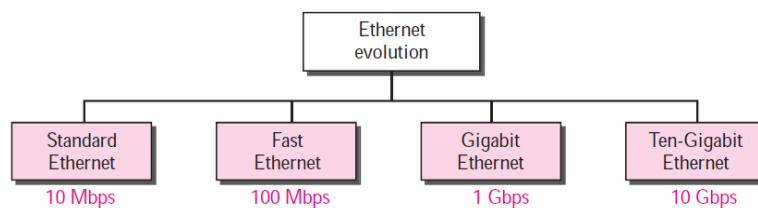
Question-03: What is Ethernet? Briefly describe technical specification of 10 Base T, 100 Base T and Gigabit Ethernet standard. 6 Marks CSE-2012

Ethernet:

A local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus. Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet. The LAN market has seen several technologies. Ethernet is one of them.

Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and Ten-Gigabit Ethernet (10 Gbps), as shown in Figure 3.6.

Figure 3.6 *Ethernet evolution through four generations*



10 Base T:

Access Method: CSMA/CD

The IEEE 802.3 standard defines carrier sense multiple access with collision detection (CSMA/CD) as the access method for traditional Ethernet. Stations on a traditional Ethernet can be connected together using a physical bus or star topology, but the logical topology is always a bus. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle “sense before transmit” or “listen before talk.” CSMA can reduce the possibility of collision, but it cannot eliminate it.

Minimum Frame Size

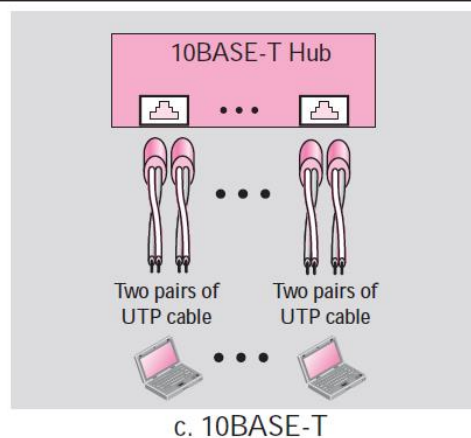
For CSMA/CD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission. This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time T_{fr} must be at least two times the maximum propagation time T_p .

Implementation

The Standard Ethernet defined several implementations, but only four of them became popular during '80s. Table 3.1 shows a summary of Standard Ethernet implementations. In the nomenclature 10Base-X, the number defines the data rate (10 Mbps), the term Base means baseband (digital) signal, and X approximately defines either the maximum size of the cable in 100 meters (for example 5 for 500 or 2 for 185 meters) or the type of the cable, T for unshielded twisted pair cable (UTP) and F for fiber-optic i.e. 10 base T Ethernet is implemented with UTP cable and data rate is 10 Mbps.

Table 7-7 10BaseT Ethernet summary

Category	Summary
IEEE specification	802.3
Advantages	Very inexpensive; easy to install and troubleshoot
Disadvantages	Small maximum cable segment length
Topology	Star
Cable type	Category 3 or higher UTP, but typically Cat 5e or 6 today
Channel access method	CSMA/CD
Transceiver location	On NIC
Maximum cable segment length	100 m (328 ft.)
Minimum distance between devices	N/A
Maximum number of segments	1024
Maximum devices per segment	2
Maximum devices per network	1024
Transmission speed	10 Mbps



c. 10BASE-T

Figure: Implementation of 10 Base-T Standard Ethernet

100 Base T:

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is Backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

MAC Sublayer

A main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched. However, a decision was made to drop the bus topologies and keep only the star topology. For the star topology, there are two choices: half duplex and full duplex. In the half-duplex approach, the stations are connected via a hub; in the full-duplex approach, the connection is made via a switch with buffers at each port. The access method is the same (CSMA/CD) for the half-duplex approach; for full-duplex Fast Ethernet, there is no need for CSMA/CD. However, the implementations keep CSMA/CD for backward compatibility with Standard Ethernet.

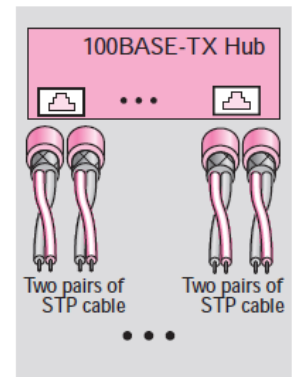
Autonegotiation:

A new feature added to Fast Ethernet is called autonegotiation. It allows a station or a hub a range of capabilities. Autonegotiation allows two devices to negotiate the mode or data rate of operation. It was designed particularly for the following purposes:

- ❑ To allow incompatible devices to connect to one another. For example, a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity (but can work at a lower rate).
- ❑ To allow one device to have multiple capabilities.
- ❑ To allow a station to check a hub's capabilities.

Implementation

Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire. The two-wire implementation can be either shielded twisted pair, STP (100Base-TX) or fiber-optic cable (100Base-FX). The four-wire implementation is designed only for unshielded twist pair, UTP (100Base-T4) i.e. 100 base T Ethernet is implemented with UTP cables and data rate is 100 Mbps.



a. 100BASE-TX

Figure: Implementation of 100 Base TX

Gigabit Ethernet:

The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support autonegotiation as defined in Fast Ethernet.

MAC Sublayer

A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched. However, to achieve a data rate of 1 Gbps, this was no longer possible. Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex. Almost all implementations of Gigabit Ethernet follow the full-duplex approach. However, we briefly discuss the half-duplex approach to show that Gigabit Ethernet can be compatible with the previous generations.

Full-Duplex Mode In full-duplex mode, there is a central switch connected to all computers or other switches. In this mode, each switch has buffers for each input port in which data are stored until they are transmitted. There is no collision in this mode. This means that CSMA/CD is not used. Lack of collision implies that the maximum length of the cable is determined by the signal attenuation in the cable, not by the collision detection process. In the full-duplex mode of Gigabit Ethernet, there is no collision; the maximum length of the cable is determined by the signal attenuation in the cable.

Half-Duplex Mode Gigabit Ethernet can also be used in half-duplex mode, although it is rare. In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half-duplex approach uses CSMA/CD. However, as we saw before, the maximum length of the network in this approach is totally dependent on the minimum frame size. Three solutions have been defined: traditional, carrier extension, and frame bursting.

❑ **Traditional.** In the traditional approach, we keep the minimum length of the frame as in traditional Ethernet (512 bits). However, because the length of a bit is 1/100 shorter in Gigabit Ethernet than in 10-Mbps Ethernet, the maximum length of the network is 25 m. This length may be suitable if all the stations are in one room, but it may not even be long enough to connect the computers in one single office.

❑ **Carrier Extension.** To allow for a longer network, we increase the minimum frame length. The **carrier extension** approach defines the minimum length of a frame as 512 bytes (4096 bits). This means that the

minimum length is 8 times longer. This method forces a station to add extension bits (padding) to any frame that is less than 4096 bits. In this way, the maximum length of the network can be increased 8 times to a length of 200 m. This allows a length of 100 m from the hub to the station.

❑ **Frame Bursting.** Carrier extension is very inefficient if we have a series of short frames to send; each frame carries redundant data. To improve efficiency, **frame bursting** was proposed. Instead of adding an extension to each frame, multiple frames are sent. However, to make these multiple frames look like one frame, padding is added between the frames (the same as that used for the carrier extension method) so that the channel is not idle. In other words, the method deceives other stations into thinking that a very large frame has been transmitted.

Table 7-9 1000BaseT Ethernet summary

Category	Summary
IEEE specification	802.3ab
Advantages	Fast; supports full-duplex communications
Disadvantages	High cost; short-haul cable segments only
Topology	Star
Cable type	Four-pair, balanced Category 5 cable; 100-ohm impedance
Channel access method	CSMA/CD or switching
Transceiver location	On NIC
Maximum cable segment length	Half-duplex: 100 m (328 ft.) Full-duplex: 100 m (328 ft.)
Maximum number of segments	1024
Maximum devices per segment	2
Maximum devices per network	1024
Transmission speed	1000 Mbps; 2000 Mbps in full-duplex mode

Implementation

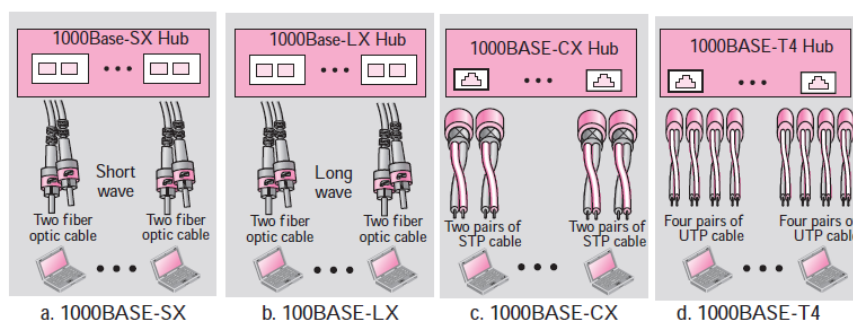
Table 3.3 is a summary of the Gigabit Ethernet implementations.

Table 3.3 Summary of Gigabit Ethernet implementations

Characteristics	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T4
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m

Figure 3.12 shows the simplified diagrams for Gigabit Ethernet.

Figure 3.12 Gigabit Ethernet implementation



বিশেষ নির্দেশনাঃ উপরের প্রশ্নটি সংক্ষেপে চার্ট আকারে উত্তর করা যেতে পারে। এখানে বিস্তারিত আকারে দেওয়া হয়েছে, একই সাথে চার্ট আকারে দেখান হয়েছে। চার্ট আকারে সংক্ষেপে লিখলেও পরীক্ষায় পূর্ণ মার্কস পাওয়া যাবে। চার্ট আকারে মুখস্থ করলে, মনে রাখতে বেশ সুবিধা হবে। তবে, বিস্তারিত অংশসমূহ পড়া জরুরী, কারণ পরীক্ষায় ফাস্ট ইথারনেট লিংবা গিগাবিট ইথারনেট সম্পর্কে আলাদাভাবে প্রশ্ন আসতে পারে, যা শুধু চার্ট আকারে পড়ে পরীক্ষায় লেখা সম্ভব নয়।

Question-04: What is Collision? How collision is managed in the transmission channel. 4 Marks CSE-2012

Collision:

The event that occurs when two transmitters send at the same time on a channel designed for only one transmission at a time is called collision. When collision is occurred, data will be destroyed or changed.

How collision is managed in the transmission channel:

Question-05: What are the functions of ARP and RARP? How ARP works? 5 Marks CSE-2012

Functions of ARP:

Before the IP protocol can deliver a packet from a source host to the destination host, it needs to know how to deliver it to the next hop first. An IP packet can consult its routing table to find the IP address of the next hop. But since IP uses the services of the data link layer, it needs to know the physical address of the next hop. This can be done using Address Resolution Protocol (ARP).

Functions of RARP:

At the beginning of the Internet era, a protocol called Reverse Address Resolution Protocol (RARP) was designed to provide the IP address for a booted computer. RARP was actually a version of ARP. ARP maps an IP address to a physical address: RARP maps a physical address to an IP address. However, RARP is deprecated today for two reasons. First, RARP used the broadcast service of the data link layer, which means that a RARP server must be present in each network. Second, RARP can provide only the IP address of the computer, but a computer today needs all four pieces of information i.e. The IP address of the computer, The subnet mask of the computer, The IP address of a router, The IP address of a name server.

How ARP works:

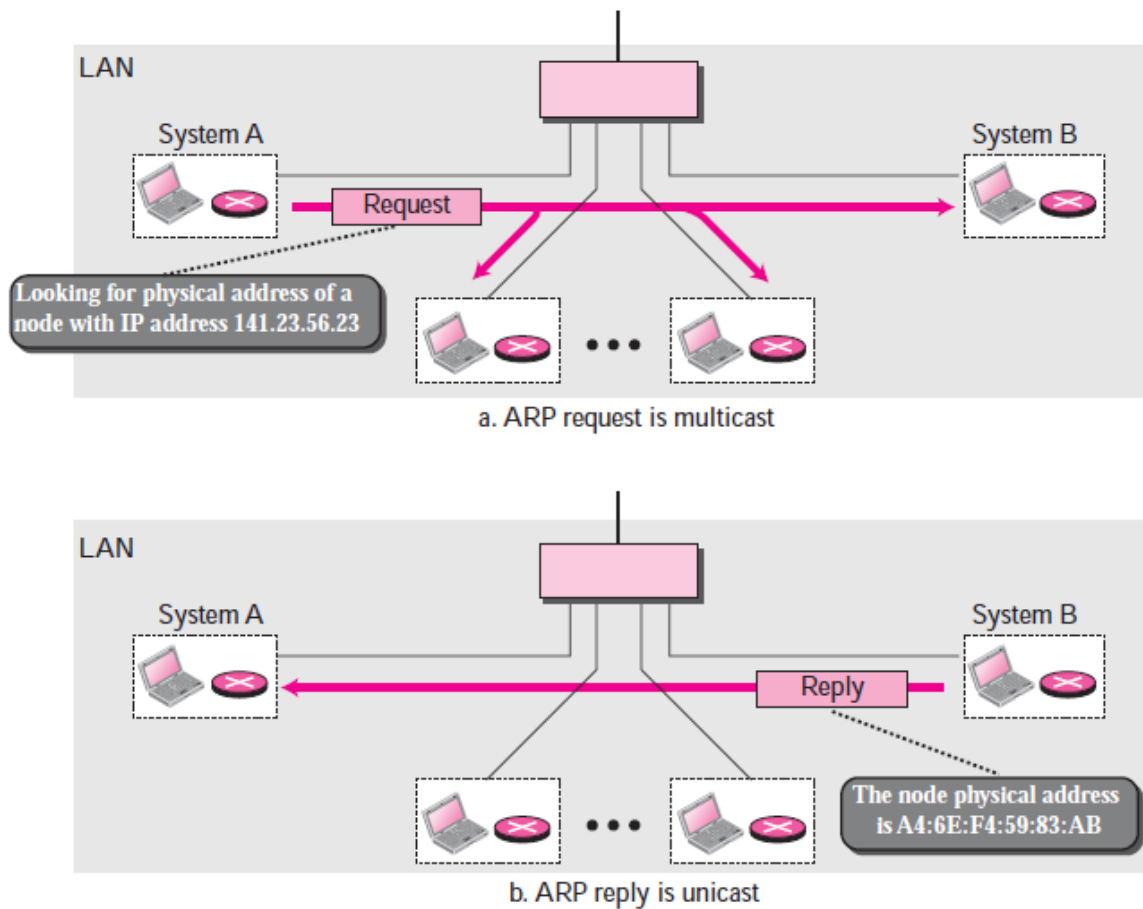
ARP associates an IP address with its physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address that is usually imprinted on the NIC. Anytime a host, or a router, needs to find the physical address of another host or router on its network, it sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network (see Figure 8.2).

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

In Figure 8.2a, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address 141.23.56.23. System A needs to pass the packet to its data link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of 141.23.56.23. This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure 8.2b. System B sends an ARP reply packet that includes its

physical address. Now system A can send all the packets it has for this destination using the physical address it received.

Figure 8.2 *ARP operation*



বিশেষ নির্দেশনাঃ ARP কিভাবে কাজ করে, এই অংশের উত্তর নিচের মতো করেও সাজানো যেতে পারেঃ

Operation

Let us see how ARP functions on a typical internet. These are seven steps involved in an ARP process:

1. The sender knows the IP address of the target. We will see how the sender obtains this shortly.
2. IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with 0s.
3. The message is passed to the data link layer where it is encapsulated in a frame using the physical address of the sender as the source address and the physical broadcast address as the destination address.
4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes the IP address.
5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.
6. The sender receives the reply message. It now knows the physical address of the target machine.
7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

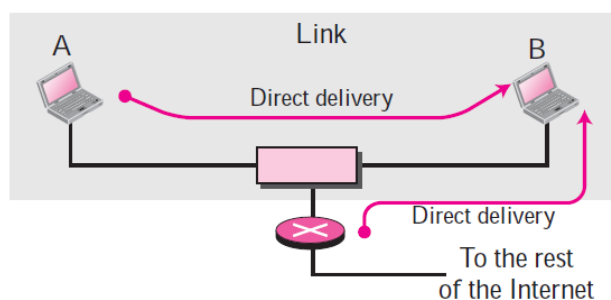
Question-06: What are meant by direct packet delivery and packet forwarding? Give example. 4 Marks CSE-2012

Direct packet delivery:

Delivery refers to the way a packet is handled by the underlying networks under the control of the network layer. The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet. The delivery of a packet to its final destination is accomplished using two different methods of delivery: direct and indirect.

In a direct delivery, the final destination of the packet is a host connected to the same physical network as the deliverer. Direct delivery occurs when the source and destination of the packet are located on the same physical network or if the delivery is between the last router and the destination host (see Figure 6.1).

Figure 6.1 *Direct delivery*



The sender can easily determine if the delivery is direct. It can extract the network address of the destination (using the mask) and compare this address with the addresses of the networks to which it is connected. If a match is found, the delivery is direct. In direct delivery, the sender uses the destination IP address to find the destination physical address. The IP software then gives the destination IP address with the destination physical address to the data link layer for actual delivery. This process is called mapping the IP address to the physical address. Although this mapping can be done by finding a match in a table, a protocol called Address Resolution Protocol (ARP) dynamically maps an IP address to the corresponding physical address.

Packet forwarding:

Forwarding refers to the way a packet is delivered to the next station. Forwarding means to place the packet in its route to its destination. There are two trends in forwarding: forwarding based on destination address of the packet and forwarding based on the label attached to the packet.

The first searches a routing table to forward a packet; the second uses the label as an index to a switching table to forward a packet.

□ There are several methods in destination-address-based forwarding including host-specific method, next-hop method, network-specific method, and the default method.

□ In destination-address-based forwarding, the routing table for classful forwarding can have three columns. The routing table for classless addressing needs at least four columns. Address aggregation simplifies the forwarding process in classless addressing. Longest mask matching is required in classless addressing.

□ In label-based forwarding, a switching table is used instead of a routing table. The Multi-Protocol Label Switching (MPLS) is the standard approved by IETF, which adds a pseudo layer to the TCP/IP protocol suite by encapsulating the IP packet in an MPLS packet.

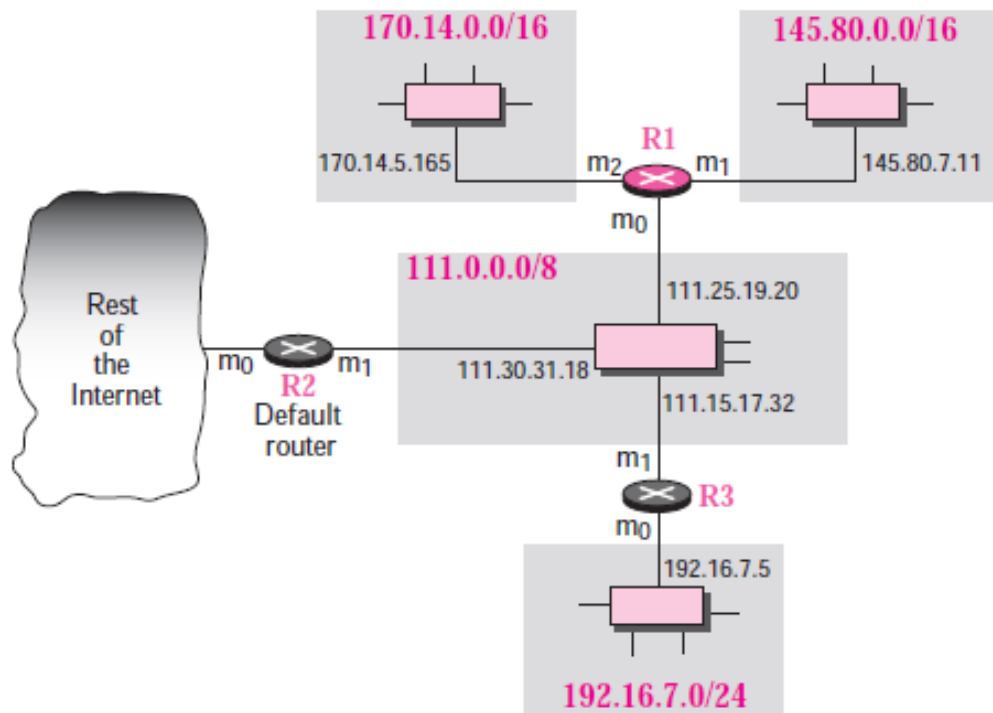
Since the Internet today is made of a combination of links (networks), forwarding means to deliver the packet to the next hop (which can be the final destination or the intermediate connecting device). Although

the IP protocol was originally designed as a connectionless protocol, today the tendency is to use IP as a connection-oriented protocol. When IP is used as a connectionless protocol, forwarding is based on the destination address of the IP datagram; when the IP is used as a connection-oriented protocol, forwarding is based on the label attached to an IP datagram.

Example

Router R1 in Figure 6.8 receives a packet with destination address 167.24.160.5. How the packet is forwarded is described below:

Figure 6.8 Configuration for routing, Example 1



The destination address in binary is 10100111 00011000 10100000 00000101. A copy of the address is shifted 28 bits to the right. The result is 00000000 00000000 00000000 00001010 or 10. The class is B. The network address can be found by masking off 16 bits of the destination address, the result is 167.24.0.0. The table for Class B is searched. No matching network address is found. The packet needs to be forwarded to the default router (the network is somewhere else in the Internet). The next-hop address 111.30.31.18 and the interface number m0 are passed to ARP.

Question-07: Briefly describe a simplified forwarding module for the class full IP addresses with subnetting. 5 Marks CSE-2012

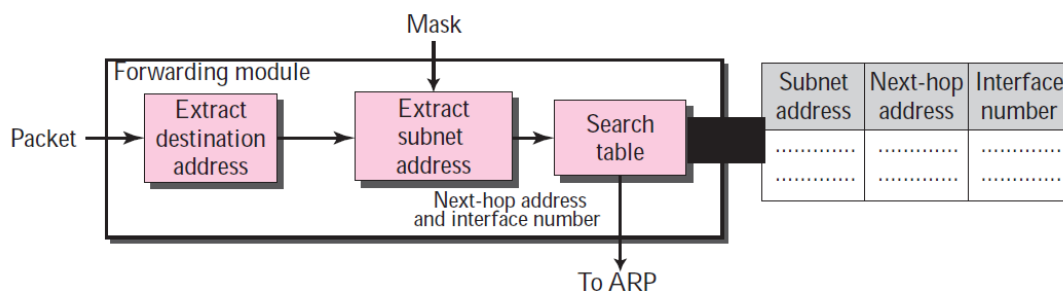
Forwarding with Classful Addressing with Subnetting

The existence of a default mask in a classful address makes the forwarding process simple. In classful addressing, subnetting happens inside the organization. The routers that handle subnetting are either at the border of the organization site or inside the site boundary. If the organization is using variable-length subnetting, we need several tables; otherwise, we need only one table. Figure 6.10 shows a simplified module for fixed-length subnetting.

1. The module extracts the destination address of the packet.
2. If the destination address matches any of the host-specific addresses in the table, the next-hop and the interface number is extracted from the table.
3. The destination address and the mask are used to extract the subnet address.
4. The table is searched using the subnet address to find the next-hop address and the interface number. If no match is found, the default is used.

5. The next-hop address and the interface number are given to ARP.

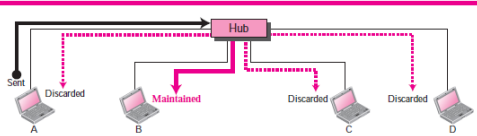
Figure 6.10 Simplified forwarding module in classful address with subnetting



Question-08: Differentiate among hub and router. 6 Marks CSE-2012

Difference among hub, switch and router:

Following are some important difference among hub, switch and router:

Hub	Router
A repeater or Hub is a device that operates only in the physical layer.	A router is a three-layer (physical, data link, and network) device.
A repeater receives a signal and, before it becomes too weak or corrupted, regenerates and retimes the original bit pattern. The repeater then sends the refreshed signal.	It operates in the physical, data link, and network layers.
In a star topology, a repeater is a multiport device, often called a hub, that can be used to serve as the connecting point and at the same time function as a repeater.	As a physical layer device, it regenerates the signal it receives. As a data link layer device, the router checks the physical addresses (source and destination) contained in the packet. As a network layer device, a router checks the network layer addresses (addresses in the IP layer).
Figure 3.41 shows the role of a repeater or a hub in a switched LAN. Figure 3.41 Repeater or hub	Bridges change collision domains, but routers limit broadcast domains.
	
a hub does not have a filtering capability; it does not have the intelligence to find from which port the frame should be sent out. A repeater forwards every bit; it has no filtering capability.	A router can connect LANs together; a router can connect WANs together; and a router can connect LANs and WANs together.
A hub or a repeater is a physical-layer device. They do not have any data-link address and they do not check the data-link address of the received frame.	A router is an internetworking device; it connects independent networks together to form an internetwork. According to this definition, two networks (LANs or WANs) connected by a router become an internetwork or an internet.
A repeater or a bridge connects segments of a LAN.	A router connects independent LANs or WANs to create an internetwork (internet).
	A router has a physical and logical (IP) address for each of its interfaces.
	A router acts only on those packets in which the physical destination address matches the address of the interface at which the packet arrives.

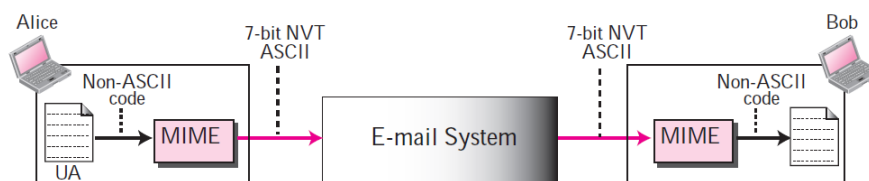
	A router changes the physical address of the packet (both source and destination) when it forwards the packet.
--	--

Question-09: What is MIME? Why it is used? 4 Marks CSE-2012

Multipurpose Internet Mail Extensions (MIME):

Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail. MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client MTA to be sent through the Internet. The message at the receiving site is transformed back to the original data. We can think of MIME as a set of software functions that transforms non-ASCII data to ASCII data and vice versa, as shown in Figure 23.15.

Figure 23.15 MIME



Why it is used:

Electronic mail has a simple structure. Its simplicity, however, comes with a price. It can send messages only in NVT 7-bit ASCII format. In other words, it has some limitations. It cannot be used for languages other than English (such as French, German, Hebrew, Russian, Chinese, and Japanese). Also, it cannot be used to send binary files or video or audio data.

MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client MTA to be sent through the Internet. The message at the receiving site is transformed back to the original data. We use MIME as a set of software functions that transforms non-ASCII data to ASCII data and vice versa.

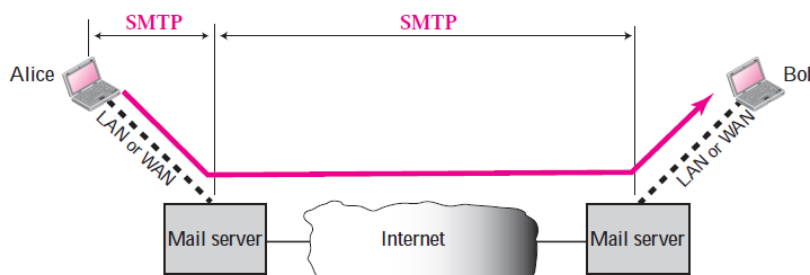
Question-10: Describe the working principle of SMTP protocol. 4 Marks CSE-2012

Working principle of SMTP protocol:

When both sender and receiver are connected to the mail server via a LAN or a WAN, we need two UAs, two pairs of MTAs (client and server), and a pair of MAAs (client and server). This is the most common situation today.

The actual mail transfer is done through message transfer agents (MTAs). To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA. **The formal protocol that defines the MTA client and server in the Internet is called Simple Mail Transfer Protocol (SMTP).** Two pairs of MTA client-server programs are used in the most common situation (fourth scenario). Figure 23.8 shows the range of the SMTP protocol in this scenario.

Figure 23.8 SMTP range



SMTP is used two times, between the sender and the sender's mail server and between the two mail servers. Another protocol is needed between the mail server and the receiver. SMTP simply defines how commands and responses must be sent back and forth. Each network is free to choose a software package for implementation.

SMTP uses commands and responses to transfer messages between an MTA client and an MTA server (see Figure 23.9). Each command or reply is terminated by a two-character (carriage return and line feed) end-of-line token. Commands are sent from the client to the server. The format of a command is shown below:

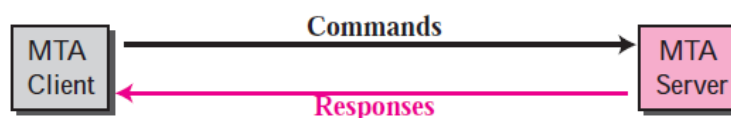
Keyword: argument(s)

It consists of a keyword followed by zero or more arguments. SMTP defines 14 commands such as HELO, MAIL FROM, RCPT TO, DATA, QUIT, RSET, VRFY, NOOP, TURN, EXPN, HELP, SEND FROM, SMOL FROM, SMAL FROM.

Responses are sent from the server to the client. A response is a three-digit code that may be followed by additional textual information. Some of the responses are:

- 211 System status or help reply
- 214 Help message
- 220 Service ready
- 221 Service closing transmission channel
- 250 Request command completed
- 251 User not local; the message will be forwarded

Figure 23.9 *Commands and responses*



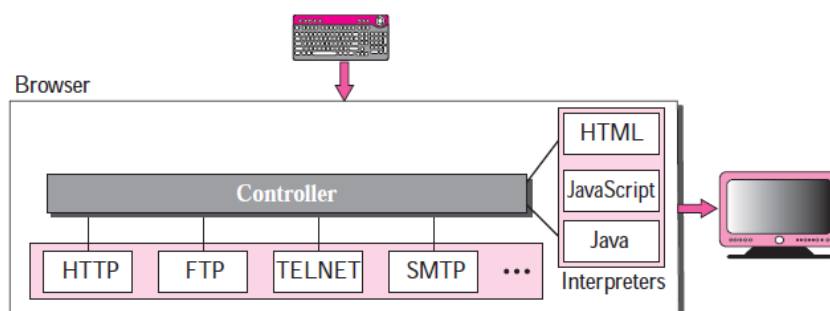
The process of transferring a mail message occurs in three phases: connection establishment, mail transfer, and connection termination. After a client has made a TCP connection to the well-known port 25, the SMTP server starts the connection phase. This phase involves THREE steps. After connection has been established between the SMTP client and server, a single message between a sender and one or more recipients can be exchanged. This phase involves eight steps. After the message is transferred successfully, the client terminates the connection. This phase involves two steps.

Question-11: Draw the architecture of a browser. 4 Marks CSE-2012

Architecture of a browser:

A variety of vendors offer commercial browsers that interpret and display a Web document, and all of them use nearly the same architecture. Each browser usually consists of three parts: a controller, client protocol, and interpreters. (see Figure 22.3).

Figure 22.3 *Browser*



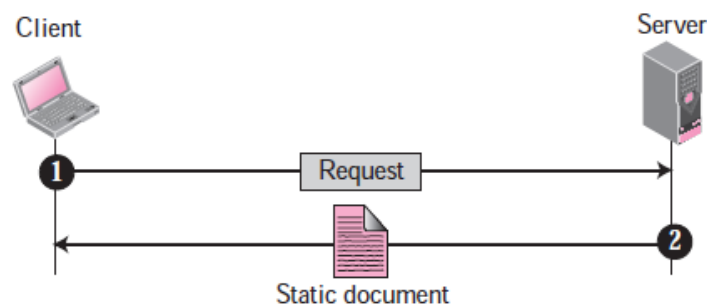
The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols such as FTP, or TELNET, or HTTP. The interpreter can be HTML, Java, or JavaScript, depending on the type of document.

Question-12: What do you mean by static document, dynamic document and active document? 4 Marks CSE-2012

Static Document:

Static documents are fixed-content documents that are created and stored in a server. The client can get a copy of the document only. In other words, the contents of the file are determined when the file is created, not when it is used. Of course, the contents in the server can be changed, but the user cannot change them. When a client accesses the document, a copy of the document is sent. The user can then use a browsing program to display the document (see Figure 22.5).

Figure 22.5 *Static document*



Static documents are prepared using one of the several languages: Hypertext Markup Language (HTML), Extensible Markup Language (XML), Extensible Style Language (XSL), and Extended Hypertext Markup Language (XHTML).

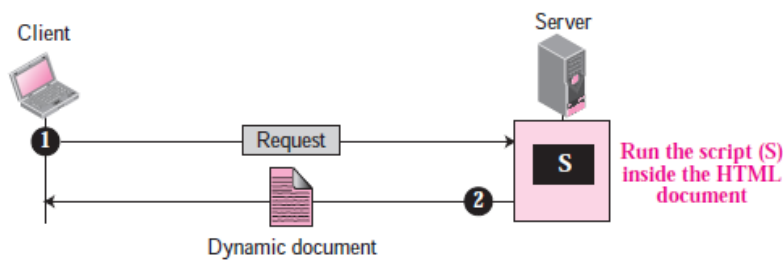
Dynamic Documents

A dynamic document is created by a Web server whenever a browser requests the document. When a request arrives, the Web server runs an application program or a script that creates the dynamic document. The server returns the output of the program or script as a response to the browser that requested the document. Because a fresh document is created for each request, the contents of a dynamic document may vary from one request to another. A very simple example of a dynamic document is the retrieval of the time and date from a server. Time and date are kinds of information that are dynamic in that they change from moment to moment. The client can ask the server to run a program such as the date program in UNIX and send the result of the program to the client. Dynamic documents are sometimes referred to as server-site dynamic documents.

The Common Gateway Interface (CGI) is a technology that creates and handles dynamic documents. CGI is a set of standards that defines how a dynamic document is written, how data are input to the program, and how the output result is used. The problem with CGI technology is the inefficiency that results if part of the dynamic document that is to be created is fixed and not changing from request to request.

The solution is to create a file containing the fixed part of the document using HTML and embed a script, a source code, that can be run by the server. Figure 22.7 shows the idea.

Figure 22.7 *Dynamic document using server-site script*



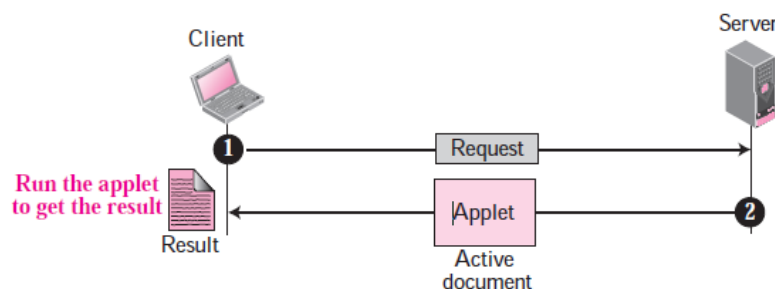
A few technologies have been involved in creating dynamic documents using scripts. Among the most common are **Hypertext Preprocessor (PHP)**, which uses the Perl language; **Java Server Pages (JSP)**, which uses the Java language for scripting; **Active Server Pages (ASP)**, a Microsoft product, which uses Visual Basic language for scripting; and **ColdFusion**, which embeds SQL database queries in the HTML document.

Active Documents

For many applications, we need a program or a script to be run at the client site. These are called **active documents**. For example, suppose we want to run a program that creates animated graphics on the screen or a program that interacts with the user. The program definitely needs to be run at the client site where the animation or interaction takes place. When a browser requests an active document, the server sends a copy of the document or a script. The document is then run at the client (browser) site. **Active documents** are sometimes referred to as **client-site dynamic documents**.

One way to create an active document is to use **Java applets**. JavaScript is also used to create an active document.

Figure 22.8 *Active document using Java applet*



Question-13: Write about TELNET and Remote-Login. 4 Marks CSE-2012

TELNET:

TELNET is an abbreviation for TERminal NETwork. It is the standard TCP/IP protocol for virtual terminal service as proposed by ISO. TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system. TELNET is a general-purpose client-server application program that allows a user to log on to a remote machine, giving the user access to the remote system. When a user accesses a remote system via the TELNET process, this is comparable to a time-sharing environment. A terminal driver correctly interprets the keystrokes on the local terminal or terminal emulator. This may not occur between a terminal and a remote terminal driver.

□ TELNET uses the Network Virtual Terminal (NVT) system to encode characters on the local system. On the server machine, NVT decodes the characters to a form acceptable to the remote machine. NVT uses a set of characters for data and a set of characters for control.

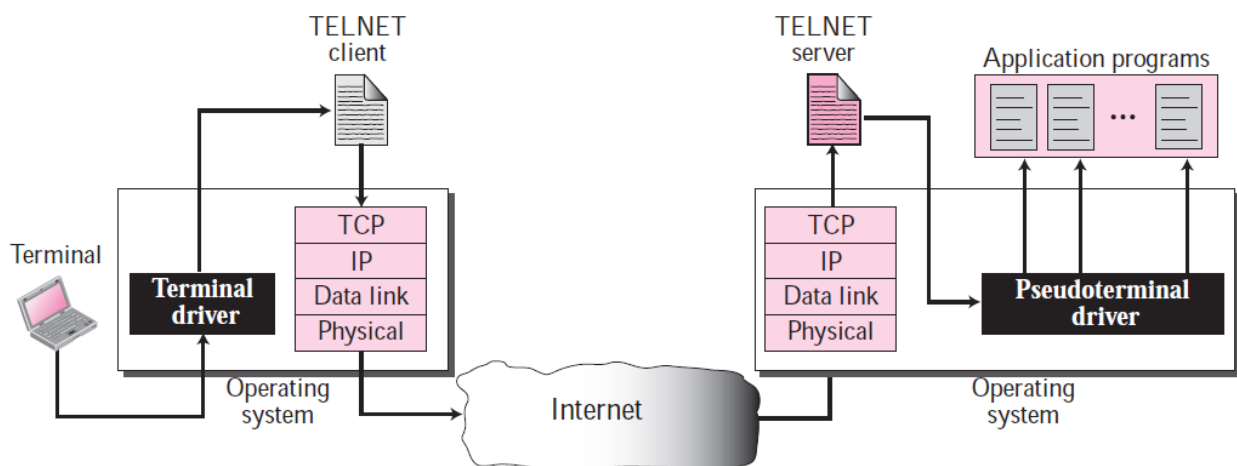
❑ Options are features that enhance the TELNET process. TELNET allows negotiation to set transfer conditions between the client and server before and during the use of the service. Some options can only be enabled by the server, some only by the client, and some by both. An option is enabled or disabled through an offer or a request. An option that needs additional information requires the use of suboption characters.

❑ A TELNET implementation operates in the default, character, or line mode. In the default mode, the client sends one line at a time to the server and waits for the go ahead (GA) character before a new line from the user can be accepted. In the character mode, the client sends one character at a time to the server. In the line mode, the client sends one line at a time to the server, one after the other, without the need for an intervening GA character.

Remote Login:

When a user wants to access an application program or utility located on a remote machine, he or she performs **remote login**. Here the TELNET client and server programs come into use. The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them. The characters are sent to the TELNET client, which transforms the characters to a universal character set called Network Virtual Terminal (NVT) characters and delivers them to the local TCP/IP stack (see Figure 20.2).

Figure 20.2 *Remote login*



The commands or text, in NVT form, travel through the Internet and arrive at the TCP/IP stack at the remote machine. Here the characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer. However, the characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server: It is designed to receive characters from a terminal driver. The solution is to add a piece of software called a *pseudoterminal driver*, which pretends that the characters are coming from a terminal. The operating system then passes the characters to the appropriate application program.