(Please write your Roll No. immediately) ROLL NO. --------------------------

END TERM EXAMINATION (MODELQUESTION PAPER WITH SOLUTION)

FORTH SEMESTER [B.TECH] MAY-JUNE 2014

Paper Code: ETME 212	***Subject: LAN and Networking***
Time: 3 Hours	***Maximum Marks: 75***

Note: Q. no.1 is compulsory. Attempt one question from each unit.

Q1. (a) What is the difference between baseband and broadband? (2.5*10)
(b)What is the difference between TCP and UDP?
(c)Compare UTP and STP cable.
(d)Why OSI model called "Open System Interconnection"?
(e) For n devices in a network, what is the number of cable links required for a mesh and ring topology?
(f)Define the term Connection-oriented communication and Connection –less communication.
(g)Define protocols and what are key elements of protocol?
(h) Explain the concept of layered task of networking.
(i) What is MAC address?
(j) What is difference between physical and logical topology?

UNIT-I

Q2. (a) What are the different types of transmission impairments? (4.5)
(b) Define Masking. What is the difference between boundary level masking and non-boundary level masking? (3)
(c) Distinguish between adaptive and non adaptive routing algorithms. (5)

Q3. (a) What is an IP address? Discuss the class field in IP address. (4.5)
(b)What is the difference between service point address, logical address and physical address? (3)
(c)What is difference between Distance Vector Routing Protocols and Link State Routing Protocols. (5)

UNIT-II

Q4. (a) Compare TCP/IP and OSI reference model. (5)
(b) Explain broadcast network, point to point network and Multipoint networks. (5)
(c) Differentiate between amplifier and repeater. (2.5)

Q5. (a)Give advantages and disadvantages of mesh, and bus topologies. (4.5)

(b) Explain Internet, extranets, and intranets. (4)

(c) Name four factors needed for a secure network. (4)

UNIT-III

Q6. (a) A company is granted a site address 201.70.64.0. The company needs six subnets. Design the subnets. (6.5)

(b) Explain difference between mono-alphabetic cipher and poly-alphabetic cipher with example. (6)

Q7. (a) Explain IEEE 802.3 frame format. (4)

(b) Explain comparison of virtual-circuit and datagram networks. (4)

(c) What is VLAN? What are advantages of using VLANs? (4.5)

UNIT-IV

Q8. (a)Explain different types of computer networks. (6.5)

(b) Explain function of token ring. (6)

Q9. (a)Explain function of token bus. (4)

(b)What is the advantage of token passing protocol over CSMA/CD protocol? (3.5)

(c) What are the drawbacks of token ring topology? (3)

(d)What role the active token monitor performs? (2)

ANSWERS

1(a): In Baseband, data is sent as digital signals through the media as a single channel that uses the entire bandwidth of the media. Baseband communication is bi-directional, which means that the same channel can be used to send and receive signals. In Baseband, frequency-division multiplexing is not possible.

Broadband sends information in the form of an analog signal. Each transmission is assigned to a portion of the bandwidth; hence multiple transmissions are possible at the same time. Broadband communication is unidirectional, so in order to send and receive, two pathways are needed. This can be accomplished either by assigning a frequency for sending and assigning a frequency for receiving along the same cable or by using two cables, one for sending and one for receiving. In broadband frequency-division multiplexing is possible.

(b) Difference between Transmission Control Protocol (TCP) and User Datagram Protocol (UDP):

Transmission Control Protocol (TCP)

1) Transmission Control Protocol (TCP) is a connection oriented protocol, which means the devices should open a connection before transmitting data and should close the connection gracefully after transmitting the data.
2) Transmission Control Protocol (TCP) assures reliable delivery of data to the destination.
3) Transmission Control Protocol (TCP) protocol provides extensive error checking mechanisms such as flow control and acknowledgment of data.
4) Sequencing of data is a feature of Transmission Control Protocol (TCP).
5) Delivery of data is guaranteed if you are using Transmission Control Protocol (TCP).
6) Transmission Control Protocol (TCP) is comparatively slow because of these extensive error checking mechanisms
7) Multiplexing and Demultiplexing is possible in Transmission Control Protocol (TCP) using TCP port numbers.
8) Retransmission of lost packets is possible in Transmission Control Protocol (TCP).

User Datagram Protocol (UDP)

1) User Datagram Protocol (UDP) is Datagram oriented protocol with no overhead for opening a connection (using three-way handshake), maintaining a connection, and closing (terminating) a connection.
2) User Datagram Protocol (UDP) is efficient for broadcast/multicast type of network transmission.
3) User Datagram Protocol (UDP) has only the basic error checking mechanism using checksums.
4) There is no sequencing of data in User Datagram Protocol (UDP).

5) The delivery of data cannot be guaranteed in User Datagram Protocol (UDP).
6) User Datagram Protocol (UDP) is faster, simpler and more efficient than TCP. However, User Datagram Protocol (UDP) it is less robust then TCP
7) Multiplexing and Demultiplexing is possible in User Datagram Protocol (UDP) using UDP port numbers.
8) There is no retransmission of lost packets in User Datagram Protocol (UDP).

(c)

- STP cables are shielded while UTP cables are unshielded
- STP cables are more immune to interference and noise than UTP cables
- STP cables are better at maximizing bandwidth compared to UTP cables
- STP cable cost more per meter compared to UTP cables
- STP cables are heavier per meter compared to UTP cables
- UTP cables are more prevalent in *(Small office/home office)* SOHO networks while STP is used in more high-end applications.

(d) OSI stands for open system interconnection model which defines the networking frameworks. It is called open system because it was intended to be used by all vendors. The OSI standard was meant to improve networking.

(e) Mesh topology: n (n-1)/2
Ring topology: n

(f) Connection-oriented communication includes the steps of setting up a call from one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call. However, the network connecting the computers is a packet switched network, unlike the phone system's circuit switched network. Connectionless service is typically provided by the TCP.

Connectionless communication is just packet switching where no call establishment and release occur. A message is broken into packets, and each packet is transferred separately. Moreover, the packets can travel different route to the destination since there is no connection. Connectionless service is typically provided by the UDP (User Datagram Protocol).

(g) A protocol can be defined as a set of rules determining the format and transmission of data or a set of rules that governs data communication. A protocol defines what is going to be communicated. The key elements of protocol are syntax, semantics and timing.

(h) The main objective of a computer network is to be able to transfer the data from sender to receiver. This task can be done by breaking it into small sub tasks, each of which is well defined. Each subtask will have its own process or processes to do and will take specific inputs and give specific outputs to the subtask before or after it. In more technical terms we can call these sub tasks as layers. In general, every task or job can be done by dividing it into sub task or layers.

(i) It is the 48 bit hardware address of LAN card. MAC address is usually stored in ROM on the network adapter card and it is unique.

(j) A physical topology describes how devices are physically cabled together. A logical topology describes how devices communicate across the physical topology.

UNIT-I

2(a): TRANSMISSION IMPAIRMENT

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.

Attenuation

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

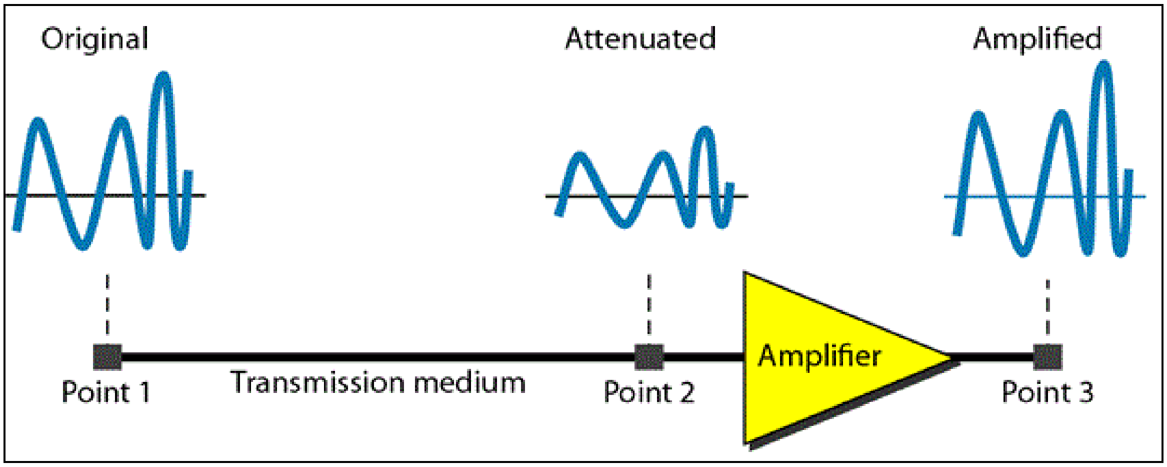


Fig. 2 (a): Attenuation

Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.

In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same.

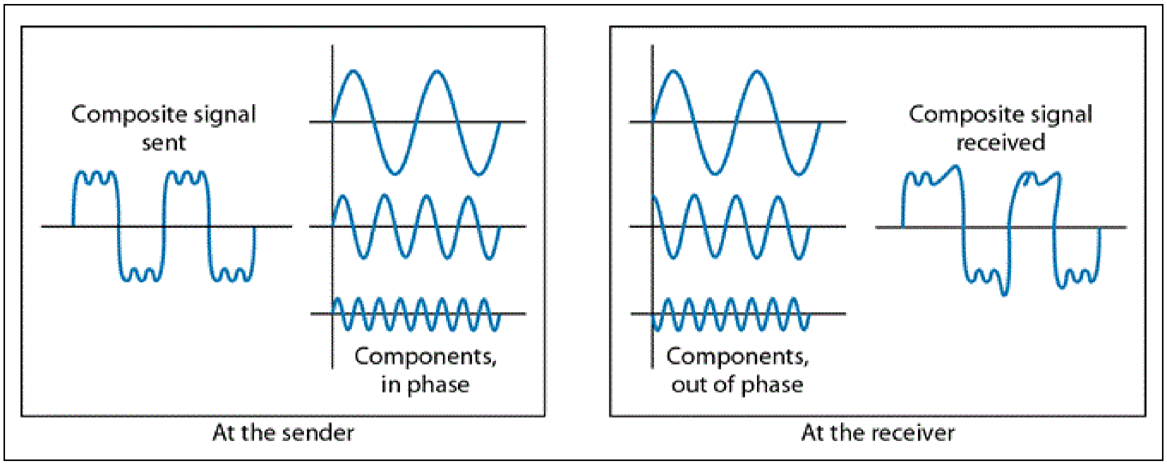


Fig. 2 (b): Distortion

Noise

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna. Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

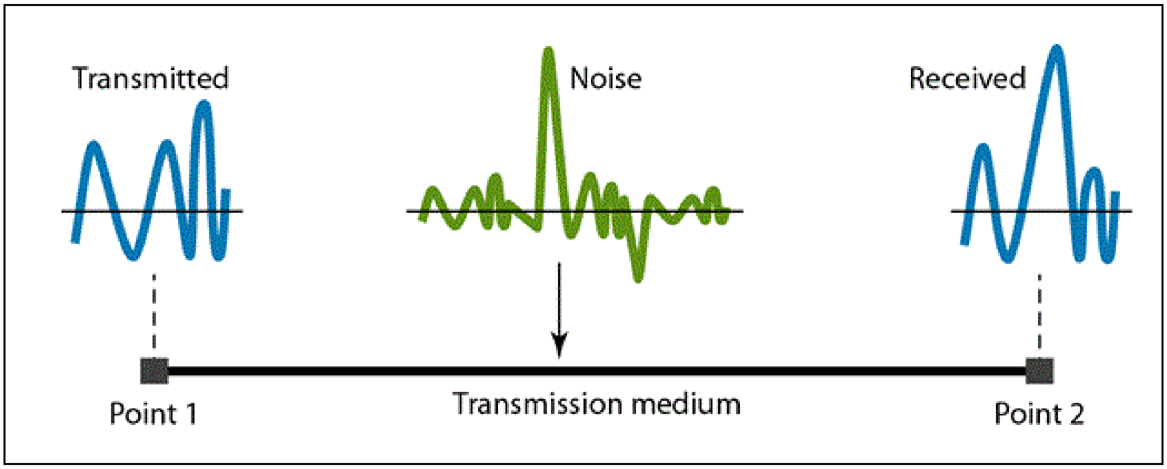


Fig. 2 (b): Noise

(b) Masking is a process that extracts the address of the physical network from an IP address.
Boundary level Masking: If the masking is at the boundary level, the mask numbers are either 255 or 0, finding the sub network address is very easy.

Non Boundary level Masking: If the masking is not at the boundary level, the mask numbers are not just 255 or 0, finding the sub network address involves using the bitwise AND operators.

(c) Non adaptive Routing:
Once a pathway to a destination has been selected the router sends all packets for that destination along that one route. The routing decisions are not based on the condition or topology of the networks.

Adaptive Routing:
Router may select a new route for each packet (even packets belonging to the same transmission) The routing decisions are based on the condition or topology of the networks.

3(a):
An IP address is a 32 - bit address that uniquely and universally define the connection of a host or a router to the Internet. The sender must know the IP address of the destination computer before sending a packet.
If the address is given in binary notation, the first few bits can tell us the class of the address.
Class A - 0
Class B - 10
Class C - 110
Class D - 1110
Class E - 1111

When the address is given in dotted decimal notation, then look at the first byte to determine the class of the address.
Class A - 0 to 127
Class B – 128 to 191
Class C – 192 to 223
Class D – 224 to 239
Class E – 240 to 255

(b)

Service point addressing	**Logical addressing**	**Physical addressing**
The transport layer header includes a type of address called a service point address	If a packet passes the network boundary we need another addressing to differentiate the	If the frames are to be distributed to different systems on the network, the

or port address, which makes a data delivery from a specific process on one computer to a specific process on another computer.	source and destination systems. The network layer adds a header, which indicate the logical address of the sender and receiver.	data link layer adds the header, which defines the source machine's address and the destination machine's address.

(c) Difference between Distance Vector Routing Protocol and Link State Routing Protocol:

Distance Vector Routing

- Entire routing table is sent as an update
- Distance vector protocol send periodic update at every 30 or 90 second
- Update are broadcasted
- Updates are sent to directly connected neighbor only
- Routers don't have end to end visibility of entire network.
- Distance vector routing protocol network may have patch in network carrying wrong information
- It is proned to routing loops
- Routing loop avoidance Mechanism used are as below :

1>Max Hop Count
2> Split horizon
3> Route poisoning
4> Hold down Timer

- Distance vector routing protocol has slow convergence due to periodic update. Eg. **RIP**

Link State Routing

- Updates are incremental & entire routing table is not sent as update
- Updates are triggered not periodic
- Updates are multicasted
- Update are sent to entire network & to just directly connected neighbor
- Updates are carry SPF tree information & SPF cost Calculation information of entire topology
- Routers have visibility of entire network of that area only.
- No routing loops
- Convergence is fast because of triggered updates.
- Eg. : **OSPF**

4(a):

OSI Model	TCP/IP Model
OSI stands for Open System Interconnection	TCP/IP stands for Transmission Control

because it allows any two different systems to communicate regardless of their architecture.	Protocol/Internet Protocol. It is named after these protocols, being part of this model.
OSI model has seven layers.	TCP/IP has four layers.
This model provides clear distinction between services, interfaces and protocols	It does not clearly distinguish between services, interfaces & protocols.
In this model, Protocols do not fit well into the model.	TCP and IP protocols fit well in the model.
Session & Presentation layers are present in this layer.	There is no session & presentation layer in this model.
OSI model supports both connection oriented & connectionless in network layer but connection oriented communication in transport layer.	TCP/IP supports only connectionless comm. In network layer but supports both in transport layer.

(b) Broadcast Network: A computer network which has a single communication channel. A packet sent by one computer is received by all the others computers on the network. In telecommunication and information theory, broadcasting refers to a method of transferring a message to all recipients simultaneously. Broadcasting can be performed as a high level operation in a program, for example broadcasting Message Passing Interface, or it may be a low level networking operation, for example broadcasting on Ethernet.

Point to Point Network: A simple Point to Point Network is a permanent link between two endpoints. A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

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

(c) A repeater is an electronic device that receives a signal and retransmits it at a higher level or higher power. A repeater does not amplify the signal it regenerates the signal. An amplifier is a device for increasing the power of a signal by increasing the amplitude of electrical signals.

5(a): Advantages and Disadvantages of Bus Topology

Advantages:

1. It is easy to set up, handle, and implement.
2. It is best-suited for small networks.
3. It costs very less.

Disadvantages:

1. The cable length is limited. This limits the number of network nodes that can be connected.
2. This network topology can perform well only for a limited number of nodes. When the number of devices connected to the bus increases, the efficiency decreases.
3. It is suitable for networks with low traffic. High traffic increases load on the bus, and the network efficiency drops.
4. It is heavily dependent on the central bus. A fault in the bus leads to network failure.
5. It is not easy to isolate faults in the network nodes.
6. Each device on the network "sees" all the data being transmitted, thus posing a security risk.

Advantages and Disadvantages of Mesh Topology

Advantages:

1. The arrangement of the network nodes is such that it is possible to transmit data from one node to many other nodes at the same time.

2. The failure of a single node does not cause the entire network to fail as there are alternate paths for data transmission.

3. It can handle heavy traffic, as there are dedicated paths between any two network nodes.

4. Point-to-point contact between every pair of nodes, makes it easy to identify faults.

Disadvantages:

1.The arrangement wherein every network node is connected to every other node of the network, many connections serve no major purpose. This leads to redundancy of many network connections.

2. A lot of cabling is required. Thus, the costs incurred in setup and maintenance are high.

3. Owing to its complexity, the administration of a mesh network is difficult.

(b) Intranet is shared content accessed by members within a single organization.

Extranet is shared content accessed by groups through cross-enterprise boundaries.

Internet is global communication accessed through the Web.

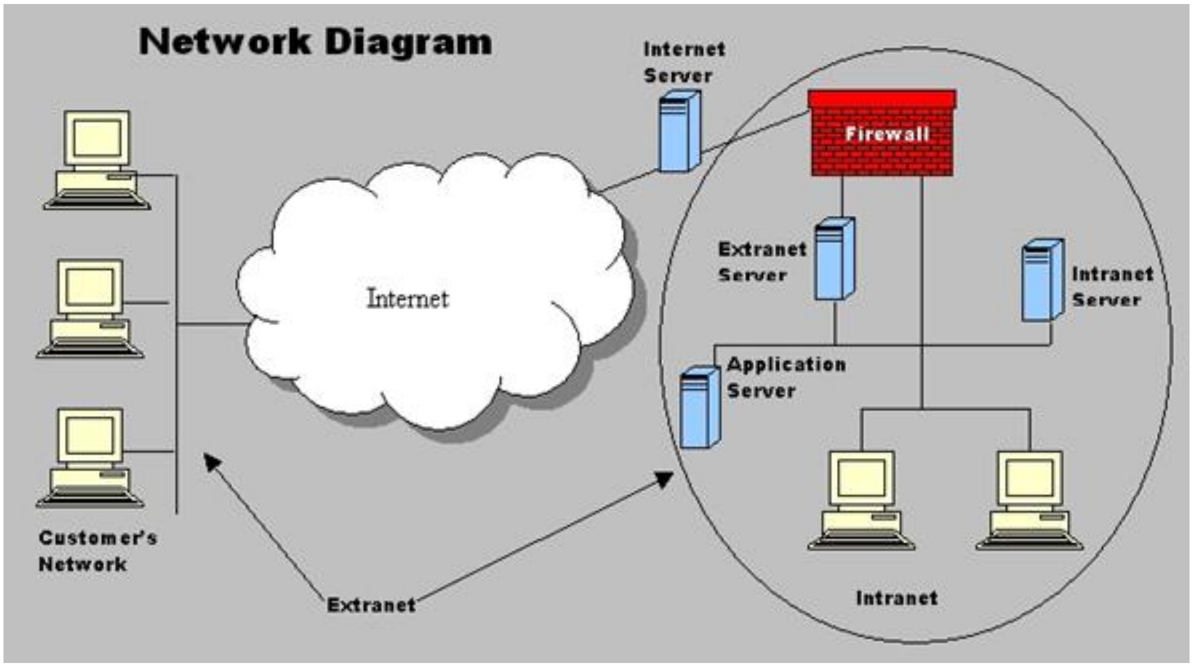


Fig. 5(a): Network Diagram

The Internet, extranets, and intranets all rely on the same TCP/IP technologies. However, they are different in terms of the levels of access they allow to various users inside and outside the organization and the size of the network. An intranet allows for restricted access to only members of an organization; an extranet expands that access by allowing non-members such as suppliers and customers to use company resources. The difference between the Internet and extranets is that while the extranet allows limited access to non-members of an organization, the Internet generally allows everyone to access all network resources.

(C) Privacy: The sender and the receiver expect confidentiality.

Authentication: The receiver is sure of the sender’s identity and that an imposter has not sent the message.

Integrity: The data must arrive at the receiver exactly as it was sent.

Non-Reputation: The receiver must able to prove that a received message came from a specific sender

6(a): This is a class C network. Therefore, the default mask is 255.255.255.0

As we need 6 subnets, we need three extra 1's. Hence, the subnet mask is 255.255.255.224
In a binary form the subnet mask is

11111111.11111111.11111111	**111**	00000

3 extra 1s

In order to have six subnets, we can have 6 different combinations of the 3- extra 1s as shown in table 1.

Table 1

Combination	**Subnet Number**
000	Subnet 1
001	Subnet 2
010	Subnet 3
011	Subnet 4
100	Subnet 5
101	Subnet 6

Therefore, the various addresses of 6 subnets are as shown in table 2.

Table 2

Subnet N0.	**Addresses**
1	201.70.64.0 to 201.70.64.31
2	201.70.64.32 to 201.70.64.63
3	201.70.64.64 to 201.70.64.95
4	201.70.64.96 to 201.70.64.127
5	201.70.64.128 to 201.70.64.159
6	201.70.64.160 to 201.70.64.191

(b)Difference between mono-alphabetic cipher and poly-alphabetic cipher:

In a mono-alphabetic cipher, the same substitution rule is used at every character position in the plaintext message. In a poly-alphabetic cipher, on the other hand, the substitution rule changes continuously from one character position to the next in the plain- text according to the elements of the encryption key.

Example of a substitution cipher: CAESAR CIPHER

In this example each character of a message is replaced by a character three position down in the alphabet.

Plaintext: are you ready

Cipher text: DUH BRX UHDGB

Example of Poly-alphabetic cipher

The Vigenere cipher is an example of a poly-alphabetic cipher.

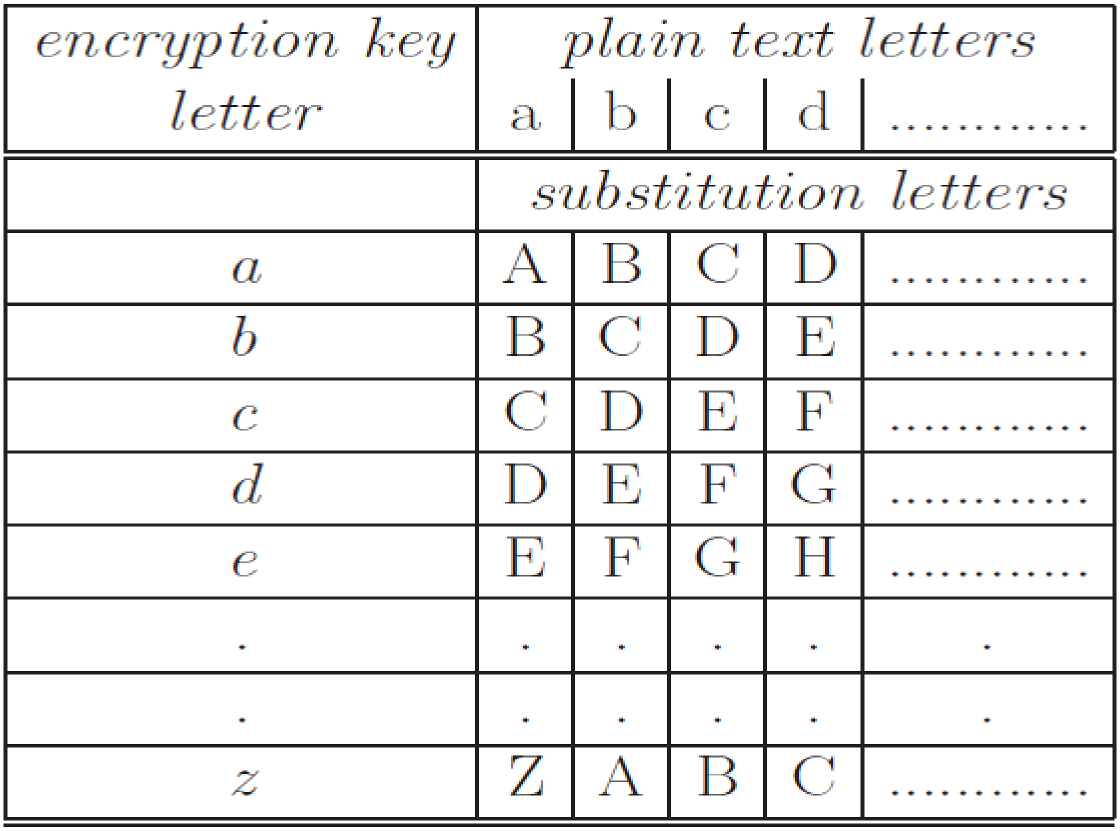
key: abracadabraabracadabraabracadabraab

plaintext: canyoumeetmeatmidnightihavethegoods

ciphertext: CBEYQUPEFKMEBK....

Since, in general, the encryption key will be shorter than the message to be encrypted, for the Vigenere cipher the key is repeated, as mentioned previously and as illustrated in the above example where the key is the string “abracadabra”.

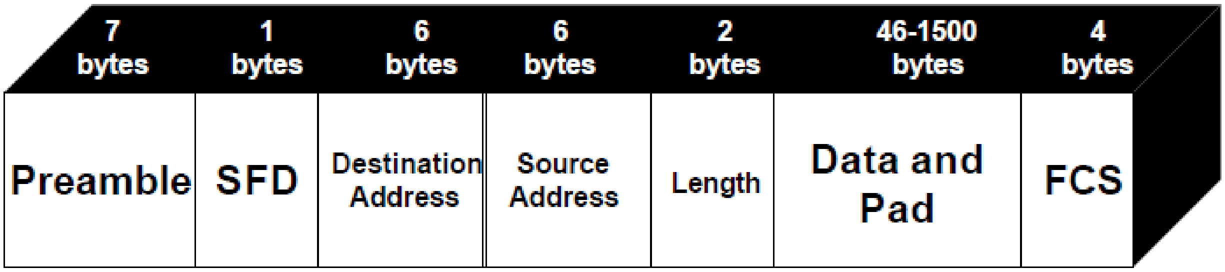
TABLE3: VIGENERE TABLE



encryption key letter	*plain text letters*				
	a	b	c	d	....
	substitution letters				
a	A	B	C	D	....
b	B	C	D	E	....
c	C	D	E	F	....
d	D	E	F	G	....
e	E	F	G	H	....
.	.	.	.	.	.
.	.	.	.	.	.
z	Z	A	B	C	....

7(a): IEEE 802.3 Frame Format

The IEEE standard was adopted in 1985. The 802.3 frame format is below:



7 bytes	1 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
Preamble	SFD	Destination Address	Source Address	Length	Data and Pad	FCS

The Preamble of the frame (the first 7 bytes) indicates the start of a new frame and establishes synchronization conditions between devices.

The Start Frame Delimiter (SFD) has the same 10101011-bit sequence found at the end of the preamble. Both formats use the same number of bytes to perform the synchronization of the signals.

The Destination and Source Addresses can be either 2 or 6 bytes. Whether 2 or 6 bytes are used, all devices within the same network must use the same format. IEEE protocols specify that a 10Mbs network must use 6 bytes. The 2 byte length is obsolete.

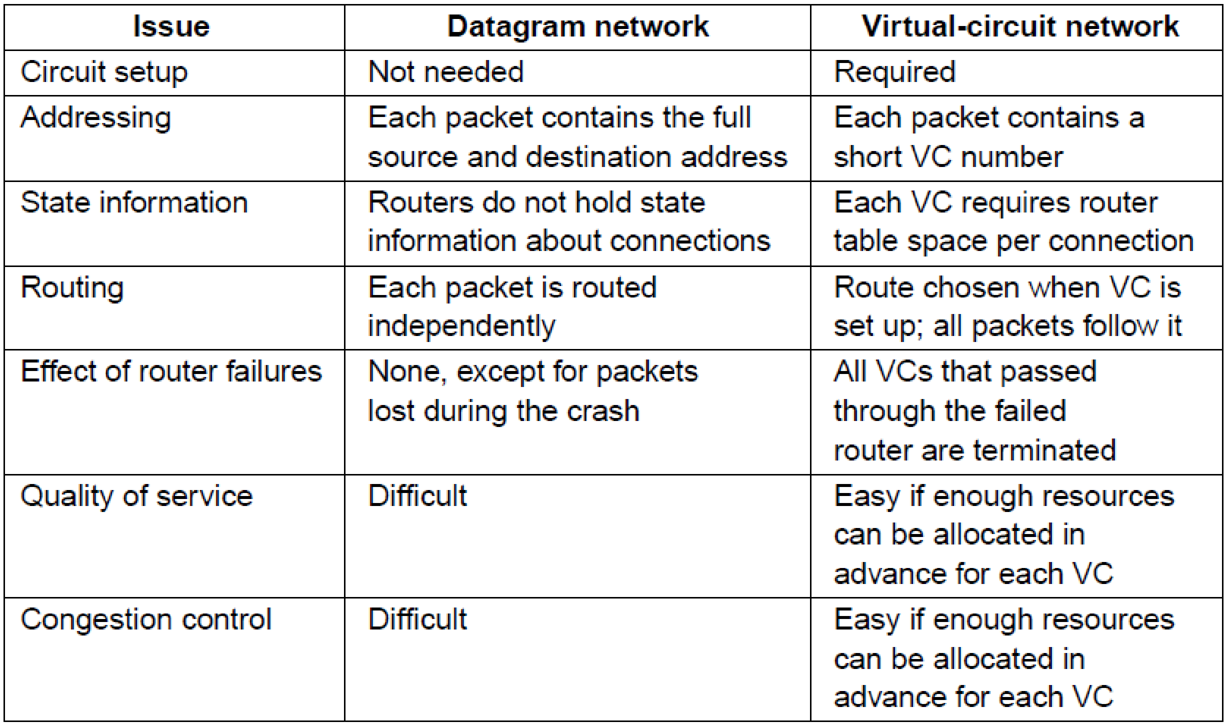
The Length field indicates the number of bytes in the data field. If the data field is less than the required 46 bytes, a pad field is added to the data frame. The bytes added for padding purposes are usually zeros.

The data field contains the data to be transmitted from device to device.

The Frame Check Sequence (FCS) field is used as an error detection function. The error detection function is a calculation completed by both the source and destination devices. If the calculations do not match, an error is then generated.

(b)

Table 3: Comparison of Virtual-Circuit and Datagram Networks



Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

(c) A Virtual Local Area Network is a group of devices that function as a single Local Area Network segment (broadcast domain). The devices that make up a particular VLAN may be widely separated, both by geography and location in the network. The creation of VLANs allows users located in separate areas or connected to separate ports to belong to a single VLAN group. Users that are assigned to such a group will send and receive broadcast and multicast traffic as though they were all connected to a single network segment. VLAN aware switches isolate broadcast and multicast traffic received from VLAN groups, keeping broadcasts from stations in a VLAN confined to that VLAN. When stations are assigned to a VLAN, the performance of their network connection is not changed. Stations connected to switched ports do not sacrifice the performance of the dedicated switched link to participate in the VLAN. As a VLAN is not a physical location, but a membership, the network switches determine VLAN membership by associating a VLAN with a particular port.

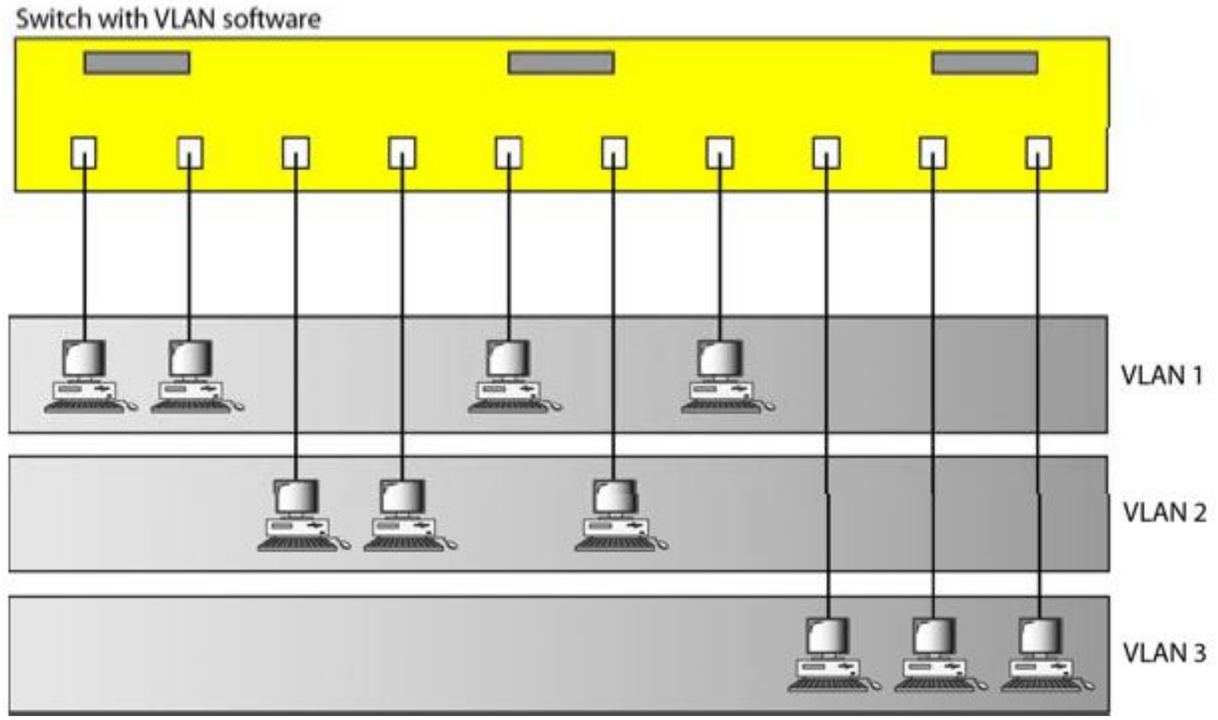


Fig.: A switch using VLAN software

VLAN characteristics:

- Any station can be logically moved to another VLAN
- All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN
- peoples in different buildings (LAN) could be in the same workgroup
- it groups stations belonging to one or more physical LANs into broadcast domains
- Stations in a VLAN communicate with one another as though they belonged to a physical segment.
- VLANs create broadcast domains.

Advantages of using VLANs:

Performance: Routers that forward data in software become a bottleneck as LAN data rates increase. Doing away with the routers removes this bottleneck.

Formation of virtual workgroups: Because workstations can be moved from one VLAN to another just by changing the configuration on switches, it is relatively easy to put all the people working together on a particular project all into a single VLAN. They can then more easily share files and resources with each other. To be honest, though, virtual workgroups sound like a good idea in theory, but often do not work well in practice. It turns out that users are usually more interested in accessing company-wide resources (file servers, printers, etc.) than files on each others' PCs.

Greater flexibility: If users move their desks, or just move around the place with their laptops, then, if the VLANs are set up the right way, they can plug their PC in at the new location, and still be within the same VLAN. This is much harder when a network is physically divided up by routers.

Ease of partitioning off resources: If there are servers or other equipment to which the network administrator wishes to limit access, then they can be put off into their own VLAN. Then users in other VLANs can be given access selectively.

8(a): A computer network is an interconnection of various computer systems located at different places. In computer network two or more computers are linked together with a medium and data communication devices for the purpose of communicating data and sharing resources. The computer that provides resources to other computers on a network is known as server. In the network the individual computers, which access shared network resources, are known as workstations or nodes.

Computer Networks may be classified on the basis of geographical area in two broad categories.

1. Local Area Network (LAN)

2. Wide Area Network (WAN)

I. Local Area Network:

Networks used to interconnect computers in a single room, rooms within a building or buildings on one site are called Local Area Network (LAN). LAN transmits data with a speed of several megabits per second (106 bits per second). The transmission medium is normally coaxial cables. LAN links computers, i.e., software and hardware, in the same area for the purpose of sharing information. Usually LAN links computers within a limited geographical area because they must be connected by a cable, which is quite expensive. People working in LAN get more capabilities in data processing, work processing and other information exchange compared to stand-alone computers. Because of this information exchange most of the business and government organizations are using LAN.

Major Characteristics of LAN are as follows:

- *Every computer has the potential to communicate with any other computers of the network*
- *High degree of interconnection between computers*
- *Easy physical connection of computers in a network*
- *Inexpensive medium of data transmission*
- *High data transmission rate*

Advantages of LAN are as follows:

- The reliability of network is high because the failure of one computer in the network does not effect the functioning for other computers.
- Addition of new computer to network is easy.
- High rate of data transmission is possible.
- Peripheral devices like magnetic disk and printer can be shared by other computers.

Disadvantages of LAN is

If the communication line fails, the entire network system breaks down.

Use of LAN

Followings are the major areas where LAN is normally used

- File transfers and Access
- Word and text processing
- Electronic message handling
- Remote database access
- Personal computing
- Digital voice transmission and storage

II. Wide Area Network:

The term Wide Area Network (WAN) is used to describe a computer network spanning a regional, national or global area. For example, for a large company the head quarters might be at Delhi and Regional branches at Bombay, Madras, Bangalore and Calcutta. Here regional centers are connected to head quarters through WAN. The distance between computers connected to WAN is larger. Therefore the transmission medium used is normally telephone lines, microwaves and satellite links.

Characteristics of WAN are as follows:

a. *Communication Facility:* For a big company spanning over different parts of the country the employees can save long distance phone calls and it overcomes the time lag in overseas communications. Computer conferencing is another use of WAN where users communicate with each other through their computer system.

b. *Remote Data Entry:* Remote data entry is possible in WAN. It means sitting at any location you can enter data, update data and query other information of any computer attached to the WAN but located in other cities. For example, suppose you are sitting at Madras and want to see some data of a computer located at Delhi, you can do it through WAN.

c. *Centralized Information:* In modern computerized environment you will find that big organizations go for centralized data storage. This means if the organization is spread over many cities, they keep their important business data in a single place. As the data are generated at different sites, WAN permits collection of this data from different sites and save at a single site.

Examples of WAN are as follows:

a. *Ethernet:* Ethernet developed by Xerox Corporation is a famous example of WAN. This network uses coaxial cables for data transmission. Special integrated circuit chips called controllers are used to connect equipment to the cable.

b. *Arpanet:* The Arpanet is another example of WAN. It was developed at Advanced Research Projects Agency of U. S. Department. This Network connects more than 40 universities and institutions throughout USA and Europe.

Difference between LAN and WAN are as follows:

- LAN is restricted to limited geographical area of few kilometers. But WAN covers great distance and operate nationwide or even worldwide.
- In LAN, the computer terminals and peripheral devices are connected with wires and coaxial cables. In WAN there is no physical connection. Communication is done through telephone lines and satellite links.

- Cost of data transmission in LAN is less because the transmission medium is owned by a single organization. In case of WAN the cost of data transmission is very high because the transmission medium used is hired either telephone lines or satellite links.
- The speed of data transmission is much higher in LAN than in WAN. The transmission speed in LAN varies from 0.1 to 100 megabits per second. In case of WAN the speed ranges from 1800 to 9600 bits per second (bps).
- Few data transmission errors occur in LAN compared to WAN. It is because in LAN the distance covered is negligible.

III. Hybrid Networks:

Between the LAN and WAN structures, you will find hybrid networks such as campus area networks (CANs) and metropolitan area networks (MANs). In addition, a new form of network type is emerging called home area networks (HANs). The need to access corporate Web sites has created two classifications known as intranets and extranets. The following sections introduce these networks.

a. Campus Area Networks (CANs): A campus area network (CAN) follows the same principles as a local area network, only on a larger and more diversified scale. With a CAN, different campus offices and organizations can be linked together. For example, in a typical university setting, accounts office might be linked to a registrar's office. In this manner, once a student has paid his or her tuition fees in the accounts section, this information is transmitted to the registrar's system so the student can enroll for classes. Some university departments or organizations might be linked to the CAN even though they already have their own separate LANs.

b. Metropolitan Area Networks (MANs): The metropolitan area network (MAN) is a large-scale network that connects multiple corporate LANs together. MANs usually are not owned by a single organization; their communication devices and equipment arc usually maintained by a group or single network provider that sells its networking services to corporate customers. MANs often take the role of a high-speed network that allows for the sharing of regional resources. MANs also can provide a shared connection to other networks using a WAN link.

c. Home Area Networks (HANs): A home area network (HAN) is a network contained within a user’s home connects a person’s digital devices, from multiple computers and their peripheral devices, such as a printer, to telephones, VCRs, DVDs, televisions, video games, between LANs, MANs. Home security systems, “smart” appliances, fax machines, and other digital devices that are wired into the network.

d. Intranets and Extranets: Much of the technology available on the Internet is also available for private network use. The company’s internal version of the Internet is called an intranet. An intranet uses the same Web server software that gives the public access to Web sites over the Internet. The major difference is that an intranet usually limits access to employees and selected contractors having ongoing business with the company.

(b) Token Ring Operation:

Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks. If early token release is supported, a new token can be released immediately after a frame transmission is complete. The information frame circulates around the ring until it reaches the intended destination station, which copies the information for further processing. The information frame makes a round trip and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination station in error-free form. Then the sending station inserts a new free token on the ring, if it has finished transmission of its packets. Unlike CSMA/CD networks (such as Ethernet), token-passing networks are deterministic, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting. Token Ring networks are ideal for applications in which delay must be predictable and robust network operation is important.

9(a): Functions of a Token Bus

It is the technique in which the station on bus or tree forms a logical ring that is the stations are assigned positions in an ordered sequence, with the last number of the sequence followed by the first one as shown in Fig. Each station knows the identity of the station following it and preceding it.

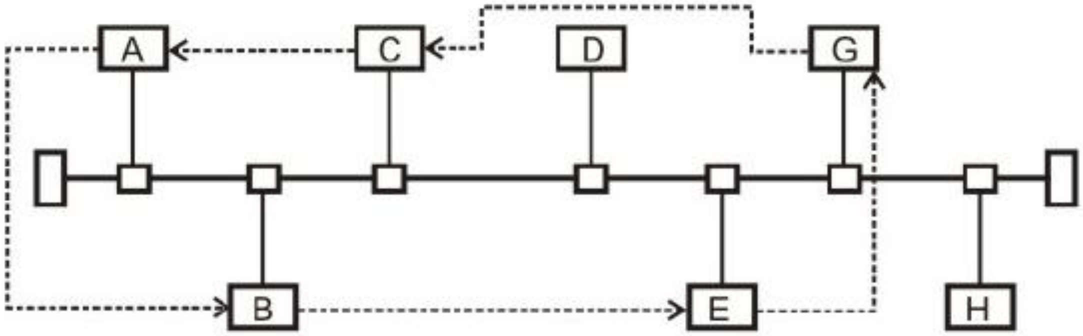


Fig.9 (a): Token Bus

A control packet known as a Token regulates the right to access. When a station receives the token, it is granted control to the media for a specified time, during which it may transmit one or more packets and may poll stations and receive responses when the station is done, or if its time has expired then it passes token to next station in logical sequence. Hence, steady phase consists of alternate phases of token passing and data transfer.

(b)Advantage of token passing protocol over CSMA/CD protocol:

The CSMA/CD is not a deterministic protocol. A packet may be delivered after many (up to 15) collisions leading to long variable delay. An unfortunate packet may not get delivered at all. This feature makes CSMA/CD protocol unsuitable for real-time applications. On the other hand, token passing protocol is a deterministic approach, which allows a packet to be delivered within a known time frame. It also allows priority to be assigned to packets. These are the two key advantages of token passing protocol over CSMA/CD protocol.

(c) Token ring protocol cannot work if a link or a station fails. So, it is vulnerable to link and station failure.

(d) Token ring is maintained with the help of active token monitor. Any one of the stations has the capability to act as active token monitor, but at a particular instant only one acts as active token monitor. It monitors various error situations such as multiple token, orphan packet, etc, and takes appropriate action to come out of the error situation.