Q 2 (a) Briefly describe the following terms for the nature of standardization required at each layer – Protocol specification, Service definition and Addressing.

Answer Page Number 36 of Text Book

Q 2 (b) Differentiate between circuit switching and packet switching.

Answer Page Number 14 of Text Book

Q 2 (c) Briefly state any two applications that have been standardized to operate on the top of TCP.

Answer Page Number 32 of Text Book

Q 3 (a) What do you understand by Bandwidth of a channel? State the characteristics of a channel.

Answer Page Number 78 of Text Book

Q 3 (b) Differentiate between guided and unguided media.

Answer Page Number 90-91 of Text Book

Q 4 (a) Explain parity check and Cyclic Redundancy check method of error detection.

Answer Page Number 173-174 of Text Book

Q 4 (b) How audio stream and Video stream digital data transmitted over the communication network?

Answer

This results from transferring types of data from:

• Audio streams (which is different from pre-recorded audio files)

• Video Streams

The source of stream-oriented digital data is usually analog signals that need to be sampled at a rate that is at least twice (two times) the bandwidth of the signal and then quantized at a specific number of bits per sample giving a total amount of *x* bits per second of data. Therefore, stream-oriented data is usually measured in terms of bit rates (or number of bits of data per second

For real-time applications, data must be delivered with a maximum delay of around 250 ms per

path (to insure reasonable audio or video two-way interaction). For such applications, if the data bit rate is *R s* bits/s and the communication system can

transfer a maximum rate of *R* bits/s, then to have real-time transfer of data, we must have

$R \geq Rs$

If real-time transfer of data is not required, then this type of data can be thought of as block oriented data where data can be transferred at a slower rate than it is actually generated

Q 5 (a) What is multiplexing? Why it is used? Briefly mention three types of multiplexing techniques.

Answer Page Number 224-225 of Text Book

Q 5 (b) Describe Stop –and- wait ARQ used for error control. Show how this algorithm perform in the case of lost frame.

Answer

Automatic Repeat Request (ARQ)

The ARQ protocol is responsible for verifying that all frames that are transmitted from a source machine reach the destination machine, and if some frames are received in error or they get lost completely, the source machine is requested to repeat the transmission of these frames again. There are three forms of
the ARQ:

1. Stop-and-Wait

From its name, the transmitter stops transmitting after a complete frame has been sent and waits for a response from the receiving machine to confirm the correct reception of the frame. This ARQ method can be described as the following:

1. The source machine starts transmitting a new frame.

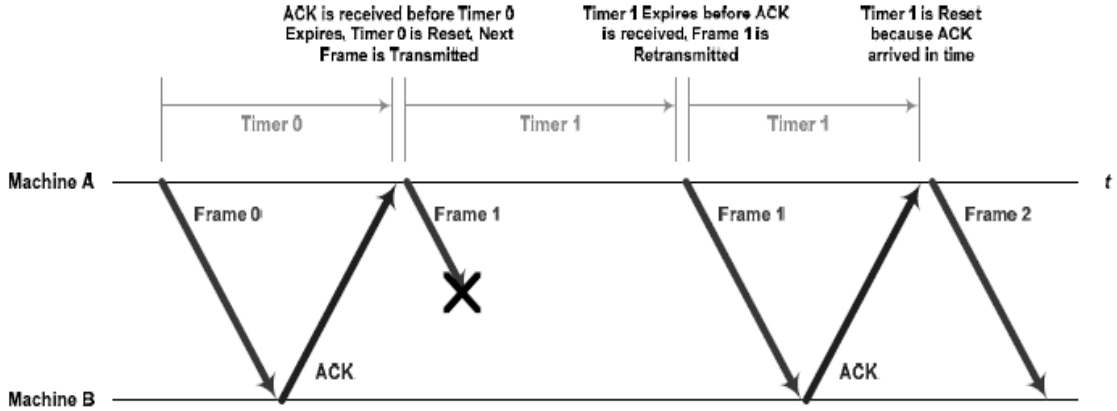
2. After transmitting the frame, a timer that expires after the expected time of the arrival of the
ACK is started (if the transmitting machine expects an ACK response after x seconds, a timer
with duration slightly more than x is set).

3. Once the frame reaches the destination machine, the destination machine responds with an
ACK message indicating the reception of an error-free frame.

4. Once the ACK message is received by the source machine, Step 1 is repeated.

There are several issues that must be considered with the Stop-and-Wait ARQ method. These include the possibility of late or lost frames, and the possibility of late or lost ACK messages. Consider for example the communication link shown below, where we have

the Data-Link Layer of Machine A wanting to send a series of frames to the Data-Link-Layer of Machine B. We will assume that data is transmitted from Machine A to Machine B only in this direction and ACK frames in the other direction (but an extension to this situation for information going in the opposite direction is also possible), and we will assume that the Error Detection algorithm used is strong enough to detect ALL errors



Q 6 (a) What do you mean by routing in packet-switching network? Why is it sometimes called an optimization problem? Explain any *two* basic routing algorithms.

Answer

(a) Routing

Routing is the task of selecting a path for the transport of packets across the network, and is one of the most important functions of the network layer. Routing is generally viewed as an optimization problem with the objective of choosing an optimal path according to certain criteria:

- Transmission cost (measured in terms of tied up network resources)
- Transmission delay (measured as the delay involved in delivering each packet).
- Throughput (measured as the total number of packets delivered per unit of time).

The overall cost depends on all these three, and an optimal route is one that minimizes the overall cost.

The cost of a route is the sum of the cost of its links.

In **flooding**, every possible path between the source and the destination station are exercised. Each node, upon receiving a packet, forwards copies of it to all its neighboring nodes (except the one from which it received the packet). Flooding is a highly robust technique since it offers the best chance of at least one packet copy reaching the destination. Its major disadvantage, however, is that it quickly congests the network. To avoid packets being indefinitely copied, each packet is assigned a limited lifetime which when expired will cause it to be destroyed (see Section 4.3.1). Because of its limitations, use of flooding is confined to specialized applications that

require very high levels of robustness (e.g., military networks). Flooding is only suited to the datagram approach.

Dynamic routing attempts to overcome the limitations of static routing by taking network variations into account when selecting a route. Each node maintains a route directory which describes the cost associated with reaching any other node via a neighboring node.

The nodes periodically calculate estimates for the costs of the links to their neighboring nodes according to the statistical data that they have collected (queue lengths, packet delays, traffic load, etc.), and share these estimates with other nodes. This enables the nodes to update their route directories in an objective manner so that they reflect the current state of the network.
To select a route between two stations, dynamic routing employs a graph optimization algorithm to find an optimal (or close to optimal) path as described earlier in this section.

The advantage of dynamic routing is its potential to improve performance and reduce congestion by choosing more optimal routes. Its disadvantage is its inherent complexity. Nevertheless, dynamic routing algorithms enjoy widespread use because they have proved to be generally more effective than other algorithms. Like static routing, dynamic routing can be used with both the datagram and the virtual circuit approach.

Dynamic route directory for node 'd' in Fig

	To						
	a	b	c	d	e	f	g
From d	b	b	c	-	e	f	e
Cost	7	7	4	0	6	8	6

Q 6 (b) What are the various methods to avoid congestion in networks?

Answer

The best way to deal with congestion is to avoid it. This is facilitated by putting in place measures that prevent buffer overflow. These measures include the following:

□□*Reducing the load on a node by disposing packets*. As mentioned in earlier sections, packet disposal can be guided by a *lifetime* indicator which is eroded by the nodes that handle the packet. More blatant ways of disposing packets may also be employed. For example, a node that receives a packet for which it

has almost no buffer space may destroy it immediately.

- *Reducing the traffic destined for a heavily-utilized link.* Nodes can monitor the traffic on their outgoing links and ask the source host to reduce the transmission rate when they feel that a link is approaching its capacity. The request can be put to the source host using a special packet.
- *Imposing a limit on the total number of packets in the network*. This approach requires some means of keeping a count of the packets in the network. Furthermore, the nodes will have to communicate to ensure that the count is kept up-to-date. Although, this approach ensures that the network cannot be overloaded with too many packets, it does not prevent an individual node from being overloaded.

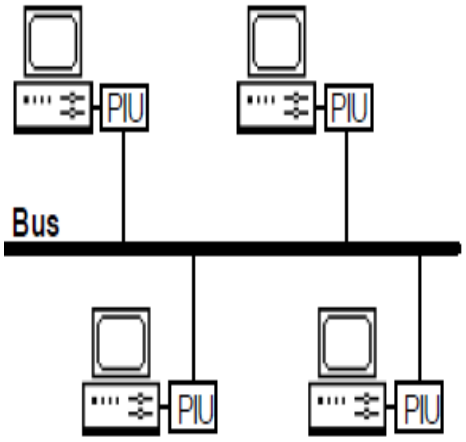
Q 7 (a) What are the basic topologies used in LAN? Describe LAN protocol architecture.

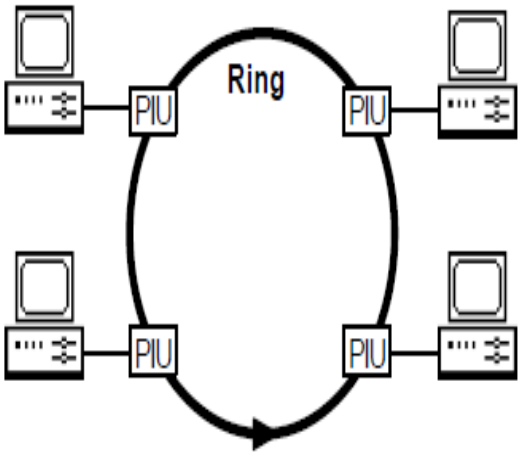
Answer

There are two general categories of LAN topologies: bus and ring (see Figure 9.94).

The **bus** topology uses a broadcast technique, hence only one station at a time can send messages and all other station listen to the message. A listening station examines the recipient address of the message and if it matches its own address, copies the message; otherwise, it ignores the message.

The **ring** topology uses a closed, point-to-point-connected loop of stations. Data flows in one direction only, from one station to the next. As with the bus topology, transmission is restricted to one user at a time. When a station gains control and sends a message, the message is sent to the next station in the ring. Each receiving station in the ring examines the recipient address of the message and if it matches its own address, copies the message. The message is passed around the ring until it reaches the originator which removes the message by not sending it to the next station.





Protocol Architecture

The role of the physical layer is the same as in the OSI model. It includes the connectors used
for connecting the PIU to the LAN and the signaling circuitry provided by the PIU. (The next section describes the transmission methods employed by this layer.)
The OSI data link layer is broken into two sublayers. The **Media Access Control** (MAC) layer is responsible for implementing a specific LAN access protocol, like the ones described earlier. This layer is therefore highly dependent on the type of the LAN. Its aim is to hide hardware and access protocol dependencies from the next layer. As we will see shortly, a number of MAC standards have been devised, one for each popular type of access protocol.
The **Logical Link Control** (LLC) layer provides data link services independent of the specific MAC protocol involved. LLC is a subset of HDLC and is largely compatible with the data link layer of OSI-compatible WANs. LLC is only concerned with providing Link Service Access Points (LSAPs). All other normal data link functions (i.e., link management, frame management, and error handling) are handled by the MAC layer.

LANs are not provided with a network layer (or any other higher layer) because such a layer would be largely redundant. Because the stations are directly connected, there is no need for switching or routing. In effect, the service provided by the LLC is equivalent to the OSI network layer service.

OSI Layer	LAN Layer	Purpose
higher layers	*undefined*	Application dependent.
Data Link	Logical Link Control	Provides generic data link services to higher layers.
	Media Access Control	Implements the protocol for accessing the LAN.
Physical	Physical	Transmission of data bits over the channel.

Q 7 (b) Write a short note on CSMA/CD. Describe CSMA/CD frame structure

Answer
The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol is specified by the IEEE 802.3 and ISO 8802.3 standards. CSMA/CD is based on the widely-publicized and well-adopted Ethernet specification, and offers data rates in order of 10 mbps using the baseband or the broadband technique.
.
The general structure of a CSMA/CD MAC frame is shown in Figure. It consists of a *Data* field (which is an LLC PDU) with a header and a trailer added at either end. The header provides synchronization, addressing, and length information.

The trailer provides a CRC-style *Frame Check Sequence* (*FCS*). CSMA/CD imposes a minimum frame size which in turn translates to a minimum data field size. Should the data field be shorter than required, it is padded with enough octets to achieve the required minimum.

CSMA/CD MAC frame structure.

Field	Description
Preamble	Special bit pattern for synchronization purposes.
Start Delimiter	Marks the beginning of frame.
Addresses	Source and destination addresses.
Length	Denotes the length of the LLC data unit in octets.
Data	Actual user data (i.e., LLC PDU).
Padding	Appended to the LLC data unit to ensure minimum length.
FCS	Frame Check Sequence.

Q 8 (a) Explain connection-oriented and connectionless internet-working.

Answer

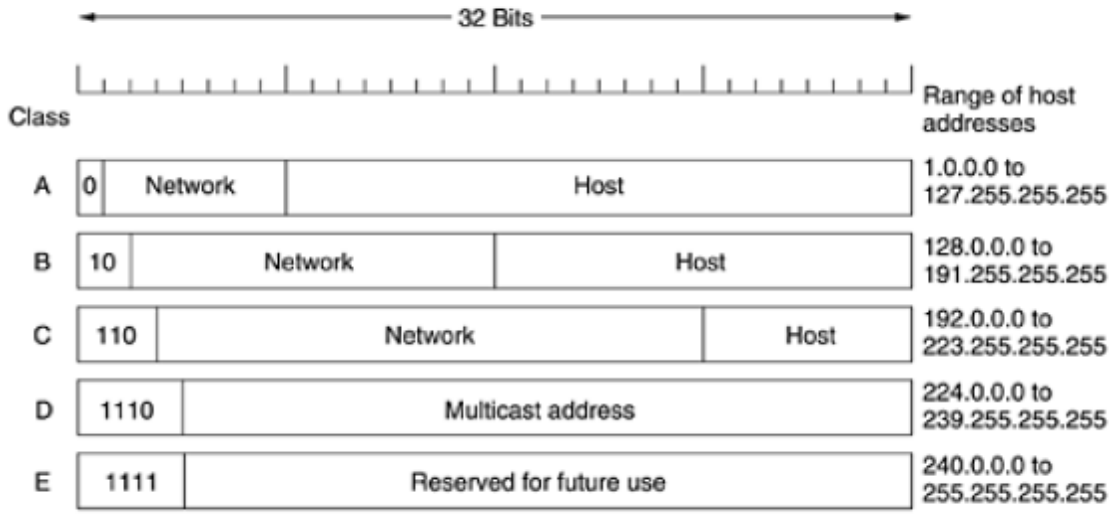
Q 8 (b) What is meant by dotted decimal notation used in network addressing?

Answer

Every host and router on the Internet has an IP address, which encodes its network number and host number. The combination is unique: in principle, no two machines on the Internet have the same IP address. All IP addresses are 32 bits long and are used in the *Source address* and *Destination address* fields of IP packets. It is important to note that an IP address does not actually refer to a host. It really refers to a network interface, so if a host is on two networks, it must have two IP addresses. However, in practice, most hosts are on one network and thus have one IP address.

The class A, B, C, and D formats allow for up to 128 networks with 16 million hosts each, 16,384 networks with up to 64K hosts, and 2 million networks (e.g., LANs) with up to 256 hosts each (although a few of these are special). Also supported is multicast, in which a datagram is directed to multiple hosts. Addresses beginning with 1111 are reserved for future

use. Over 500,000 networks are now connected to the Internet, and the number grows every
year. Network numbers are managed by a nonprofit corporation called **ICANN** (**Internet Corporation for Assigned Names and Numbers**) to avoid conflicts. In turn, ICANN has
delegated parts of the address space to various regional authorities, which then dole out IP
addresses to ISPs and other companies.
Network addresses, which are 32-bit numbers, are usually written in **dotted decimal notation**. In this format, each of the 4 bytes is written in decimal, from 0 to 255. For example, the 32-bit hexadecimal address C0290614 is written as 192.41.6.20. The lowest IP
address is 0.0.0.0 and the highest is 255.255.255.255.



Q 9 (a) Explain briefly any *four* common routing protocols used in Internetworking.

Answer
(a) Interior

u RIP
u OSPF
Exterior
u EGP
u BGP

ATM

u PNNI

RIP
n Distance vector
n Cost metric is hop count
n Infinity = 16
n Exchange distance vectors every 30 s
n Split horizon
n Useful for small subnets
u easy to install

OSPF
n Link-state
n Uses areas to route packets hierarchically within AS
n Complex
u LSP databases to be protected
n Uses designated routers to reduce number of endpoints

EGP
n Original exterior gateway protocol
n Distance-vector
n Costs are either 128 (reachable) or 255 (unreachable) =>
reachability protocol => backbone must be loop free (why?)
n Allows administrators to pick neighbors to peer with
n Allows backdoors (by setting backdoor cost < 128)

BGP
n Path-vector
u distance vector annotated with entire path
u also with policy attributes
u guaranteed loop-free
n Can use non-tree backbone topologies
n Uses TCP to disseminate DVs
u reliable
u but subject to TCP flow control
n Policies are complex to set up

PNNI
n Link-state
n Many levels of hierarchy
n Switch controllers at each level form a peer group
n Group has a group leader
n Leaders are members of the next higher level group
n Leaders summarize information about group to tell higher level
peers
n All records received by leader are flooded to lower level

n LSPs can be annotated with per-link QoS metrics
n Switch controller uses this to compute source routes for callsetup packets

Q 9 (b) In the early days of the ARPANET, e-mail consisted exclusively of text messages written in English and expressed in ASCII. But now a day you can send audio, images etc. through E-mail. How this is made possible?

Answer Page Number 712-715 of Text Book

Text Book

Data and Computer Communications, Eight Edition (2007), William Stallings, Pearson Education Low Price Edition