FIRST TERM EXAMINATION [FEB. 2017]
SIXTH SEMESTER [B.TECH]
DATA COMMUNICATION AND NETWORKS
[ETEC–310]

Time : 1.5 Hrs. **M.M. : 30**

Note: Q. No. 1 is compulsory. Attempt any two more Questions from the rest.

Q.1. (a) What is the difference between guided and unguided media? **(2)**

Ans. Guided media are more commonly known as wired media, or those media in which electrical or optical signals are transmitted through a cables or wires. Unguided media are more commonly known as wireless media, in which electromagnetic signals are sent through space with no direction. Both types of media can be used for long-distance and short-distance communication.

Guided transmission media:

1. Twisted pair cable 2. Co-axial cable 3. Fiber-optic cable

Unguided transmission media:

1. Infrared 2. Microwaves 3. Satellite.

Q.1. (b) What is the relationship between services and protocols? Explain. **(2)**

Ans. Protocol is the special set of rules that end points in a telecommunication connection use when they communicate. In other words Protocol is an agreed-upon format for transmitting data between two devices. The protocol determines the following: the type of error checking to be used data compression method, if any how the sending device will indicate that it has finished sending a message how the receiving device will indicate that it has received a message Service is a program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level.

A service is a program on the computer that provides a function for your software, such at the NetBIOS service that connects windows workgroup machines, or the DHCP Client that acquires a network address for your computer when you connect to the internet. A protocol is a language the computer uses to exchange information. For example, TCP/IP is used to negotiate connection and transfer data over the Internet, and HTTP is a protocol that handles transferring data between WWW servers, and clients.

Q.1. (c) What is bit stuffing. **(2)**

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

For example, the timing or bit rate of T-carrier system signals is constantly synchronized between any terminal device and an adjacent repeater or between any two repeaters. The synchronization is achieved by detecting the transition in polarity for 1 bits in the data stream. (T-1 signalling uses bipolar signaling, where each successive bit with a value of 1 is represented by voltage with a reverse polarity from the previous bit. Bits with a value of 0 are represented by a no-voltage time slot.) If more than 15 bits in a row are sent with a 0 value, this “lull” in 1 bits that the system depends on for synchronization may be long enough for two end points to become out of synchronization. To handle this situation (the sequence of more than 15 0 bits), the signal is “stuffed” with a short, unique bit pattern (which includes some 1 bits) that is recognized as a synchronization pattern. The receiving end removes the stuffed bits and restores the bit stream to its original sequence.

In another example of bit stuffing, a standard HDLC packet begins and ends with 01111110. To make sure this sequence doesn't appear again before the end of the packet, a 0 is inserted after every five consecutive 1s.

Bit stuffing is defined by some to include bit padding, which is the addition of bits to a tranmission to make the transmission unit conform to a standard size, but is distinct from bit robbing, a type of in-band signaling.

Q.1. (d) What kind of error is undetectable by checksum. (2)

Ans. At least three types of error cannot be detected by the current checksum calculation. First, if two data items are swapped during transmission, the sum and the checksum values will not change. Second, if the value of one data item is increased (intentionally or maliciously) and the value of another one is decreased (intentionally or maliciously) the same amount, the sum and the checksum cannot detect these changes. Third, if one or more data items is changed in such a way that the change is a multiple of 216 – 1, the sum or the checksum cannot detect the changes.

Q.1. (e) Which layer is responsible for: (2)

- **Dialogue Control** • **Compression**
- **Translations** • **Flow control**

Ans. Session layer,Presentation layer, Presentation layer, Data link and transport layer.

Q.2. (a) Explain the channel allocation problem. (5)

Ans. We have a limited resource transmission spectrum, that must be shared by several users. Unlike wired communications which benefits from isolation provided by cables, wireless users within close proximity of one another can cause significant interference to one another. To address this issue, the concept of cellular communications was introduced around in 1968 by researchers at AT and T Bell Labs. The basic concept being that a given geography is divided into polygons called cells.

Each cell is allocated a portion of the total frequency spectrum. As users move into a given cell, they are then permitted to utilize the channel allocated to that cell.

Channel-allocation schemes follow one of two types of strategy:

1. Fixed: FCA, fixed channel allocation: manually assigned by the network operator

2. Dynamic:

1. DCA, dynamic channel allocation

2. DFS, dynamic frequency selection

3. Spread spectrum .

In Fixed Channel Allocation or Fixed Channel Assignment (FCA) each cell is given a predetermined set of frequency channels. FCA requires manual frequency planning, which is an arduous task in TDMA and FDMA based systems, since such systems are highly sensitive to co-channel interference from nearby cells that are reusing the same channel. Another drawback with TDMA and FDMA systems with FCA is that the number of channels in the cell remains constant irrespective of the number of customers in that cell. This results in traffic congestion and some calls being lost when traffic gets heavy in some cells, and idle capacity in other cells.

Dynamic Frequency Selection (DFS) may be applied in wireless networks with several adjacent non-centrally controlled access points. The access points automatically select frequency channels with low interference levels. DFS is supported by the IEEE

802.11h wireless local area network standard. DFS is also mandated in the 5470-5725 MHz U-NII band for radar avoidance.

Q.2. (b) A channel has a bandwidth of 8 kHz, what is channel capacity if signal to noise ratio being 31. For same channel capacity, if signal to noise ratio is increased to 61, then, what will be the new channel bandwidth? **(5)**

Ans. According to Shannon theorem-

$C = B*LOG_2\ (1+S/N)$

$C = 8000*LOG_2(1+31)$

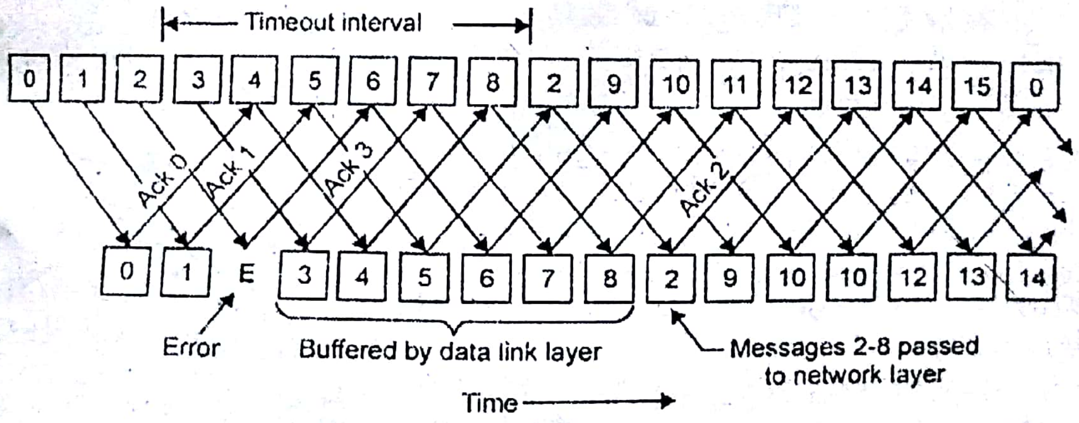
$= 40$ Kbps

(ii) $40000 = B*LOG_2(1+61)$

$B = 6.7$ KHz.

Q.3. (a) What is the difference between Selective Repeat and Go-back N ARQ. **(5)**

Ans. Selective Repeat is part of the automatic repeat request (ARQ). With selective repeat, the sender sends a number of frames specified by a window size even without the need to wait for individual ACK from the receiver as in Go-Back-N ARQ. The receiver may selectively reject a single frame, which may be retransmitted alone. this contrasts with other forms of ARQ, which must send every frame from that point again. The receiver accepts out-of-order frames and buffers them. The sender individually retransmits frames that have timed out.



Deciding factors are bandwidth, complexity of protocol, types of links (noisy and noisy less), window size, sorting, searching, storing.

Q.3. (b) Show that the hamming code can correct one bit error in the following case.

Transmitted code is 11101 and the code received at the receiver is 110010100. Specify which bit has an error and correct it. **(5)**

Ans. Transmitted code : 11101

received code : 110010100

we know that 2pow r > n+r+1

where n = code word of length n and r = parity bits

so

if r =4

then 2 power 4 > 5+4+1

2power 4= 10

for

(1) first parity check on the given code (11101) we will check even parity on bit place 1,3,5,7,9; then the corresponding value will be 1 so the result after first parity bit will be

1 _ 1 _ 1 1 0 _ 1

(2) second parity check on the given code (11101) we will check even parity on bit place 2,3,6,7,10,11, then the corresponding value will be 0 so the result after first parity bit will be

10 1 _ 1 1 0 _ 1

(3) fourth parity check on the given code (11101) we will check even parity on bit place 4,5,6,7,12,13,14 then the corresponding value will be 1 so the result after first parity bit will be

10 1 0 1 1 0 _ 1

(4) eighth parity check on the given code (11101) we will check even parity on bit place 8,15,24,31,40; then the corresponding value will be 1 so the result after first parity bit will be

10 1 0 1 1 0 0 1

this the code revived at receiver end but according to the question then received code is 110010100

if there is 1 bit error then the change will be in any bit in the corresponding received code (10 1 0 1 1 0 0 1) but there are multiple bit error, so this is the case of worst bit error in with multiple bit are changed.

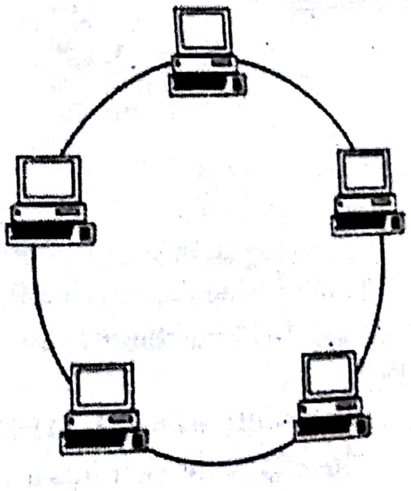
Also Refer Q.3(*b*) of First Term 2016.

Q.4. Write a short note on: **(2.5)**

(a) Ring Topology

Ans. A ring topology is a network configuration in which device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a ring network.

Ring Topology



In a ring network, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a unidirectional ring network. Others permit data to move in either direction, called bidirectional.

The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected.

Ring topologies may be used in either local area networks (LANs) or wide area networks (WANs).

(2.5)

Q.4. (b) Circuit Switching Networks.

Ans. Circuit switching is a switching method in which a dedicated communication path in physical form between two stations within a network is established, maintained and terminated for each communication session. It has basically three phases as circuit establishment, data transfer and circuit disconnect.

Once the connection is established, the data transfer is transparent. The main feature of such a connection is that it provides a fixed data rate channel and both subscribers must operate at this rate. It is considered inefficient compared to packet switching because channel capacity is completely dedicated for duration of connection. If there is no data at any moment of time, channel capacity goes wasted. Moreover, setting up of connection takes time.

Circuit switching has two types of transmissions.

Datagram transmissions - Datagram transmissions have individually addressed frames.

Data-stream transmissions - Data-stream transmissions have a stream of data for which address checking occurs only once. The routing in circuit switching may have either static routing or dynamic routing. In case of static routing, this methodology uses the same approach all the time while dynamic routing allows alternate routing depending on traffic.

Q.4. (c) Piggybacking **(2.5)**

Ans. Definition: Piggybacking, in a wireless communications context, is the unauthorized access of a wireless LAN. Piggybacking is sometimes referred to as "Wi-Fi squatting."

The usual purpose of piggybacking is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network. Furthermore, a network that is vulnerable to piggybacking for network access is equally vulnerable when the purpose is data theft, dissemination of viruses, or some other illicit activity.

It's quite simple to access an unsecured wireless network: All you have to do is get into the range of a Wi-Fi hotspot's signal and select your chosen network from the options presented. However, unauthorized network access, even to free Wi-Fi, may be illegal. People have been fined for accessing hot spots from outside businesses, such as coffee shops, that provide free Wi-Fi for customers' use.

To protect your network from piggybacking, ensure that encryption is enabled for your router. Use Wireless Encryption Protocol (WEP) if that's your only option, but if possible use Wireless Protected Access (WPA) or WPA2. Use a strong password for your encryption key, consisting of at least 14 characters and mixing letters and numbers.

Q.4. (d) Cable Modem **(2.5)**

Ans. A cable modem is a hardware device that allows your computer to communicate with an Internet Service Provider over a landline connection. It converts an analog signal to a digital signal for the purpose of granting access to broadband Internet. A cable modem works by connecting a coaxial cable to a jack in the wall and then a Cat5 (Ethernet) cord from the modem to a computer or a network router. Network routers are used to share your Internet connection between multiple computers.

The picture is an example of a traditional stand alone cable modem from Motorola, there are also all in one modems that have a modem and router built into one box. If your modem only has one coaxial cable connection and one Cat5 connection, your modem is a stand alone modem and needs a router to share the connection.

Cable offers a significant speed increase in Internet performance when compared to a dial-upconnection and is one of the fastest broadband solutions

Q.4. (e) Virtual Circuits **(2.5)**

Ans. A virtual circuit is a circuit or path between points in a network that appears to be a discrete, physical path but is actually a managed pool of circuit resources from which specific circuits are allocated as needed to meet traffic requirements.

A permanent virtual circuit (PVC) is a virtual circuit that is permanently available to the user just as though it were a dedicated or leased line continuously reserved for that user. A switched virtual circuit (SVC) is a virtual circuit in which a connection session is set up for a user only for the duration of a connection. PVCs are an important feature of frame relay networks and SVCs are proposed for later inclusion.