Computer Networks

Assignment-1

Name:: Naman Garg
Roll no:: B032
Class:: `Btech CS B

Q.1 How Information travels over from our computer to the Internet?

1. The Internet works by chopping data into chunks called packets. Each packet then moves through the network in a series of hops.
2. Wireless Router
A router connects networks together. Routers operate at the networking level of the TCP/IP protocol stack.
On Home networks the router is responsible for connecting the home network to the Internet and provides several important networking services like:
DHCP
DNS
3. Modem
This converts digital signals into analogue signals that are suitable for sending over a telephone line. It is usually built into the Internet/broadband router and not normally purchased as a separate component.
4. Each packet hops to a local Internet service provider (ISP), a company that offers access to the network -An ISP (Internet service provider) is a company that provides individuals and other companies' access to the Internet and other related services such as Web site building and virtual hosting.
5. The next hop delivers the packet to a long-haul provider
6. These providers use the Border Gateway Protocol to find a route across the many individual networks that together form the Internet.
Border Gateway Protocol (BGP) is the routing protocol for the Internet.
7.This journey often takes several more hops, which are plotted out one by one as the data packet moves across the Internet.
For the system to work properly, the BGP information shared among routers cannot contain lies or errors that might cause a packet to go off track – or get lost altogether.
8. Recipient's ISP
The information reaches to the recipient's ISP after which the information has travelled successfully over the internet and received by the user.
9. The final hop takes a packet to the recipient, which re-assembles all of the packets into a coherent message. A separate message goes back through the network confirming successful delivery.

Q.2 Give details as follows for OSI reference model:

Layer Name	What does the layer do?	Protocols at this layer	Hardware used at this layer
Application Layer	It provides a set of interfaces for applications to obtain access to networked services as well as access to network services that support applications directly. This layer also provides application access security checking and information validation. The Application Layer provides the following functions- 1 File Transfer, Access and Management (FTAM): Provides handling services in the network. This includes the movement of files between different systems, reading, writing and deletion of remote files, and management of remote file storage. 2 Virtual Terminal (VT): Provides services to access applications in different remote computer systems through stimulating a real terminal. 3 Electronic Mail and Messaging Handling (MHS): Facilitates the electronic exchange of documents. 4 Directory Services (DS): Provides services with the ability to match names with addressing information.	• Remote login to hosts: Telnet • File transfer: File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) • Electronic mail transport: Simple Mail Transfer Protocol (SMTP) • Networking support: Domain Name System (DNS) • Host initialization: BOOTP • Remote host management: Simple Network Management Protocol (SNMP), Common Management Information Protocol over TCP (CMOT)	Gateways, Firewalls, all end devices like PC's, Phones, Servers, Load Balancers.

	5 Common management Information Protocol (CMIP): Provides services for network management.		
Presentation Layer	The presentation layer is responsible for the format of the data transferred during network communications. This layer is concerned with the syntax and semantics of the information transmitted. The presentation layer	• Apple Filing Protocol (AFP) • Independent Computing Architecture (ICA), the Citrix system core protocol	Gateways, Firewalls, PC's, Load Balancers.
	provides common communication services such as encryption, text compression, and reformatting. The presentation layer is also concerned with other aspects of information representation. Data compression can be used to reduce the number of bits that have to be transmitted. Cryptography is frequently required. for privacy and authentication.	• Lightweight Presentation Protocol (LPP) • NetWare Core Protocol (NCP) • Network Data Representation (NDR) • Telnet (a remote terminal access protocol) • Tox, • Representation (XDR) • X.25 Packet Assembler/Disassembler Protocol (PAD)	
Session Layer	The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e., a semi-permanent dialogue. Communication sessions consist of requests and responses that occur between applications. The session	• PPTP, • RPC, • RTCP, • SMPP, • SCP, • SOCKS, • ZIP, • SDP, • ADSP, • ASP	Gateways, Firewalls, PC's, Load Balancers.

	layer of the OSI model is responsible for session checkpointing and recovery. It allows information of different streams, perhaps originating from different sources, to be properly combined or synchronized. Authentication, Authorization, Session restoration (checkpointing and recovery) are basic services it provides.	• H.245, • ISO-SP, • iSNS, • L2F, • L2TP, • NetBIOS, • PAP	
Transport Layer	The basic function of the transport layer is to accept data from the session layer, split it up into smaller units, pass it to the network layer, and ensure that the bits delivered are	• SCTP, • SPX, • SST, • TCP, • UDP, • UDP-Lite,	Gateways, Firewalls, Load Balancers.
	the same as the bits transmitted without modification, loss or duplication. The transport layer is also responsible for Error control. It provides services such as connection-oriented communication, reliability, flow control, and multiplexing. The transport layer might multiplex several transport connections onto the same network to reduce costs.	• µTP, • ATP, • CUDP, • DCCP, • FCP, • IL, • MPTCP, • RDP, • RUDP,	
Network Layer	The network layer is a portion of online communications that allows for the connection and transfer of data packets between different devices or networks. Logical connection setup, data forwarding, routing	• CLNS, • DDP, • EGP, • EIGRP, • ICMP, • IGMP, • IPsec,	Routers, Brouters, 3-layer switches.

	controlling the operation of a sub-net, congestion control and accounting and delivery error reporting are the network layer's primary responsibilities. Layer 3 can be either able to support connection-oriented or connectionless networks (but not both of them at the same time).	• IPv4/IPv6, • IPX, • OSPF, • PIM, • RIP, • WireGuard.	
Data link Layer	The data link layer is used for the encoding, decoding and logical organization of data bits. Data packets are framed and addressed by this layer, which has two sublayers. The data link layer's first sublayer is the media access control (MAC) layer. It is used for source and destination addresses. The MAC layer allows the data link layer to provide the best data transmission vehicle and manage data flow control.	Ethernet, Token Ring, and ARCnet are examples of LAN data link protocols. If communication extends beyond the LAN onto the Internet, the network might use other data link protocols, such as Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP).	Bridges, Modems, Network cards, 2-layer switches.

	The data link layer's second sublayer is the logical link control. It manages error checking and data flow over a network. Error detection and error checking is performed in this layer using frames.		
Physical Layer	The physical layer is aimed at consolidating the hardware requirements of a network to enable the successful transmission of data. Network	Examples of protocols that use physical layers include: Digital Subscriber Line.	Copper Cables, Fiber Cables, Wireless,

	engineers can define different bit-transmission mechanisms for the physical layer level, including the shapes and types of connectors, cables, and frequencies for each physical medium.	Integrated Services Digital Network. Infrared Data Association. Universal Serial Bus (USB.) Bluetooth. Controller Area Network. Ethernet.	Hubs, Repeaters.

Q.3 What is framing? Discuss the different framing techniques with the help of a suitable example.

Ans.

In the physical layer, data transmission involves synchronised transmission of bits from the source to the destination. The data link layer packs these bits into frames.

Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames make flow control and error control more efficient.

Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.

This is known as Framing.

Framing Techniques:

Framing can be of two types,

1.fixed sized framing

2.variable sized framing.

Fixed-sized Framing -

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example − ATM cells.

Variable – Sized Framing -

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

It is used in local area networks.

Two ways to define frame delimiters in variable sized framing are −

- **Length Field** − Here, a length field is used that determines the size of the frame. It is used in Ethernet (IEEE 802.3).
- **End Delimiter** − Here, a pattern is used as a delimiter to determine the size of frame. It is used in Token Rings. If the pattern occurs in the message, then two approaches are used to avoid the situation −
    - **Byte – Stuffing** − A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.
    - **Bit – Stuffing** − A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.

Q.4 What is meant encoding in Physical Layer? Discuss the various encoding techniques with proper illustration.

Encoding :

The bits in the encapsulated data link layer frame need to be grouped, or encoded, into patterns recognized by Layer 1 devices. After transmission, the receiving Layer

1 device decodes patterns and hands the frame up to the data link layer. It also does control information to indicate the start and end of frames.

Encoding is a method of converting a stream of data bits into a predefined code.

1- To provide a predictable pattern that can be recognized by both the sender and the received.

2- To distinguish data bits from control bits and provide better media error detection.

3- To provide codes for control purposes such as identifying the beginning and end of a frame.

Encoding is grouping of bits prior to being presented to the media.

- To improve the efficiency at higher speed data transmission
- To detect errors.
- To represent more data across the media, by transmitting

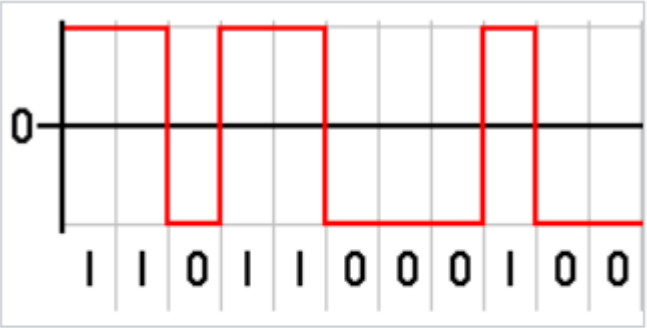
fewer bits. The stream of signals being transmitted needs to start in such a way that the receiver recognizes the beginning and end of the frame.

It uses two different voltage levels (one positive and one negative) as the signal elements for the two binary digits.

1. Non Return to Zero NRZ

NRZ Codes has 1 for High voltage level and 0 for Low voltage level. The main behavior of NRZ codes is that the voltage level remains constant during bit interval. The end or start of a bit will not be indicated and it will maintain the same voltage state, if the value of the previous bit and the value of the present bit are same. The following figure explains the concept of NRZ coding.

If the above example is considered, as there is a long sequence of constant voltage level and the clock synchronization may be lost due to the absence of bit interval, it becomes difficult for the receiver to differentiate between 0 and 1.



The binary signal is encoded using rectangular pulse-amplitude modulation with polar NRZ(L), or polar non-return-to-zero-level code

There are two variations in NRZ namely −

a. NRZ - L NRZ–LEVELNRZ–LEVEL

There is a change in the polarity of the signal, only when the incoming signal changes from 1 to 0 or from 0 to 1. It is the same as NRZ, however, the first bit of the input signal should have a change of polarity.

b. NRZ - I NRZ–INVERTEDNRZ–INVERTED

If a 1 occurs at the incoming signal, then there occurs a transition at the beginning of the bit interval. For a 0 at the incoming signal, there is no transition at the beginning of the bit interval.

NRZ codes has a disadvantage that the synchronization of the transmitter clock with the receiver clock gets completely disturbed, when there is a string of 1s and 0s. Hence, a separate clock line needs to be provided.

2. Bi-phase Encoding

The signal level is checked twice for every bit time, both initially and in the middle. Hence, the clock rate is double the data transfer rate and thus the modulation rate is also doubled. The clock is taken from the signal itself. The bandwidth required for this coding is greater. There are two types of Bi-phase Encoding.

- Bi-phase Manchester
- Differential Manchester

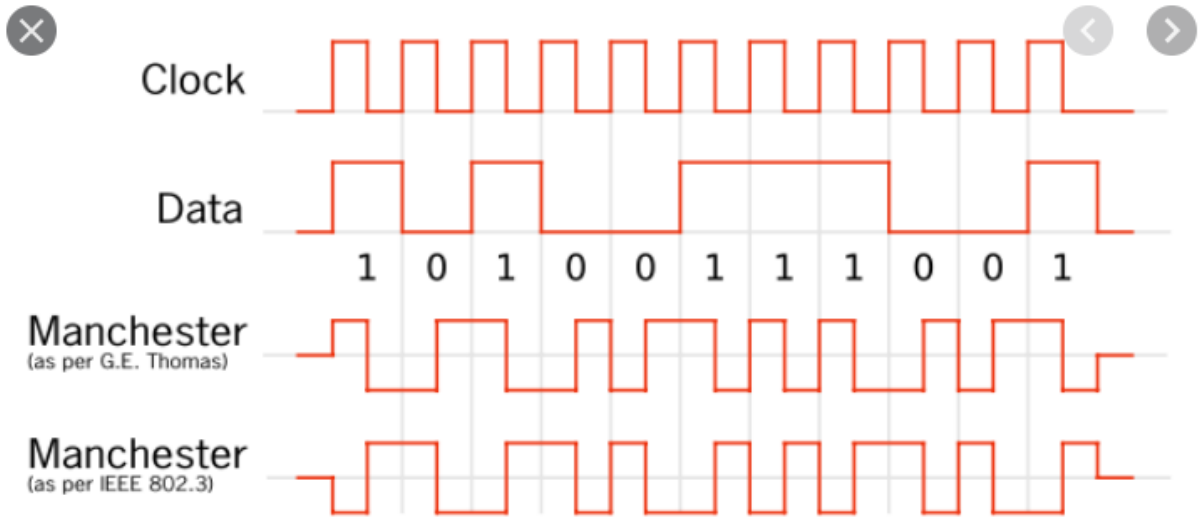
a. Bi-phase Manchester

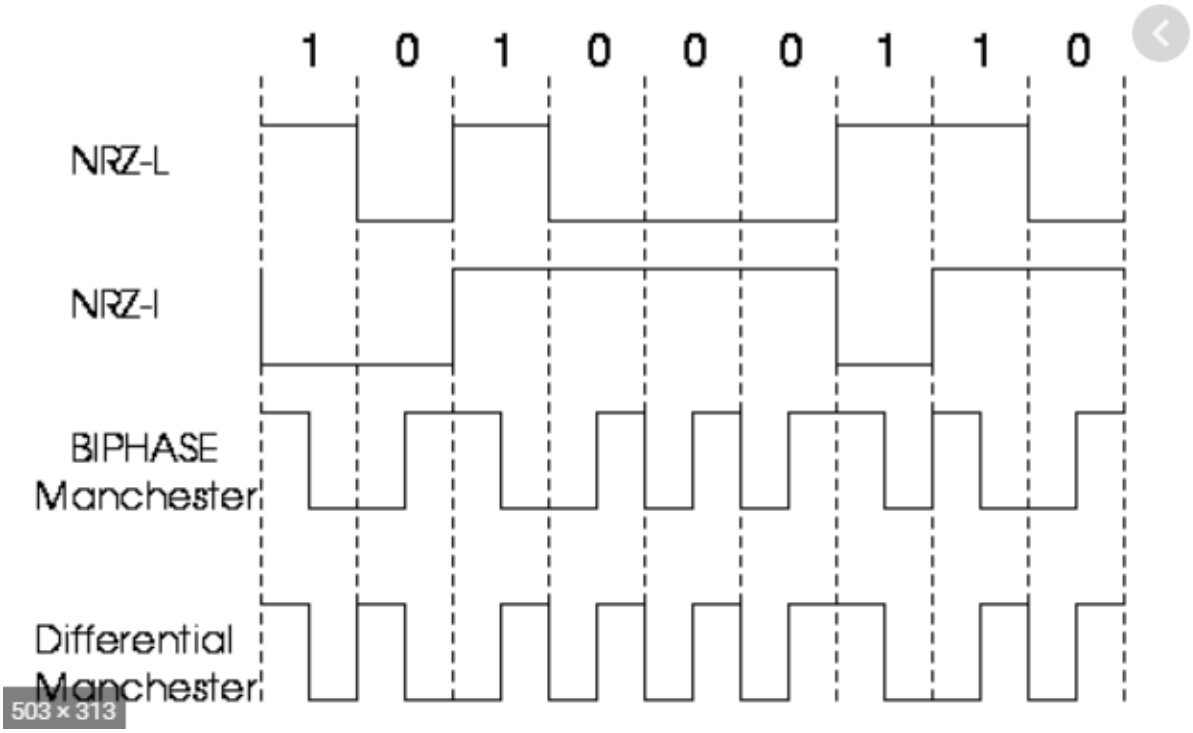
In this type of coding, the transition is done at the middle of the bit-interval. The transition for the resultant pulse is from High to Low in the middle of the interval, for the input bit 1. While the transition is from Low to High for the input bit 0.

b. Differential Manchester

In this type of coding, there always occurs a transition in the middle of the bit interval. If there occurs a transition at the beginning of the bit interval, then the input bit is 0. If no transition occurs at the beginning of the bit interval, then the input bit is 1.

The following figure illustrates the waveforms of NRZ-L, NRZ-I, Bi-phase Manchester and Differential Manchester coding for different digital inputs.





Block Coding

Among the types of block coding, the famous ones are 4B/5B encoding and 8B/6T encoding. The number of bits are processed in different manners, in both of these processes.

8B/6T Encoding

We have used two voltage levels to send a single bit over a single signal. But if we use more than 3 voltage levels, we can send more bits per signal. For example, if 6 voltage levels are used to represent 8 bits on a single signal, then such encoding is termed as 8B/6T encoding. Hence in this method, we have as many as 729 3636 combinations for signal and 256 2828 combinations for bits.

These are the techniques mostly used for converting digital data into digital signals by compressing or coding them for reliable transmission of data.

4B/5B Encoding

In Manchester encoding, to send the data, the clocks with double speed is required rather than NRZ coding. Here, as the name implies, 4 bits of code is mapped with 5 bits, with a minimum number of 1 bits in the group.

The clock synchronization problem in NRZ-I encoding is avoided by assigning an equivalent word of 5 bits in the place of each block of 4 consecutive bits. These 5-bit words are predetermined in a dictionary. The basic idea of selecting a 5-bit code is that, it should have one leading 0 and it should have no more than two trailing 0s. Hence, these words are chosen such that two transactions take place per block of bits.