NOORUL ISLAM COLLEGE OF ENGINEERING
Department of Software Engineering
XCS 353 – Computer Networks
2 Marks Q & A

UNIT – I

1. List out the various error detecting algorithm?
   - CRC(Cyclic Redundancy check)
   - Two dimensional parity
   - Check sum

2. What is ARQ?

The general strategy of using acknowledgements and timeouts to implement reliable delivery is called automatic repeat request (ARQ).

3. What is the key idea of Stop & Wait Protocol?

After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame. If the acknowledgement does not arrive after a certain period of time, the sender time out and retransmits the original frame.

4. What is CSMA/CD?

CSMA/CD stands for Carrier Sense Multiple Access with Collision Detect. Ethernet is a multiple access network (shared link) and the carrier sense means that all the nodes can distinguish between an idle and busy link. collision detect means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered with a frame transmitted by another node.

5. Write short notes on Ethernet.

Carrier Sense Multiple Access with Collision Detect. Ethernet is a multiple access network (shared link) and the carrier sense means that all the nodes can distinguish between an idle and busy link. collision detect means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered with a frame transmitted by another node.

6. What is transceiver?

Transceiver is a small device directly attached to the tap and detects when the line is idle and drives the signal when the host is transmitting.

7. What is Repeater?

Repeater propagate the signal from one segment to another

8. What is a Hub?

Hub (MultiWay Repeater) propagates the signal onto a number of segments, possibly with different types of cable.

9. Write short notes on Ethernet address?

Ethernet host in the world has a unique address. The address belongs to the adaptor, not the host; it is usually burned into ROM. it has six hexa decimal numbers separated by colons. Example 8:0:2b:e4:b1:2.

10. Differentiate between Service interface and Peer-to-Peer interface.

Service interface communicate between object in the same network system.

Peer-to-peer interface communicate between object in different systems.

11. Write short notes on promiscuous mode.

In promiscuous mode it delivers all received frames to the host, but this is not the normal mode.

12. Why Ethernet is called 1 persistent protocol?

Ethernet is said to be a 1 persistent protocol because an adaptor with a frame to send transmits with probability 1 whenever a busy line goes idle.

13. What is an exponential back off?

Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again. This strategy of doubling the delay interval between each transmission attempt is a general technique known as exponential back off.

14. What are the advantages of Ethernet?

- Easy to admin and maintain
- No switch, Router and configuration table
- Easy to add a new Host
- Inexpensive one

15. Write short notes on Token Ring.

A number of stations connected by transmission links in a ring topology. Information flows in one direction along the ring from source to destination and back to source. Medium access control is provided by a small frame, the token that circulates around the ring when all stations are idle. Only the station possessing the token is allowed to transmit at any given time.

16. Write short notes on FDDI.

- FDDI uses a ring topology of multimode or single mode optical fiber transmission links operating at 100 Mbps to span up to 200 kms and permits up to 500 stations.
- Employs dual counter-rotating rings.
- 16 and 48-bit addresses are allowed.
- In FDDI, token is absorbed by station and released as soon as it completes the frame transmission {multi-token operation}.

17. What are the 2 different classes of traffic used in FDDI?

FDDI is designed to handle two types of traffic:

- Synchronous frames that typically have tighter delay requirements (e.g., voice and video)
- Asynchronous frames have greater delay tolerances (e.g., data traffic)

18. Write short notes on network users.

Network users want the network to provide services that their applications need; e.g., guarantee that each message will be delivered in order, without errors, and within a pre-defined delay

19. Write short notes on Network designers.

Network designers want a cost-effective design; e.g., network resources are efficiently utilized and fairly allocated to users

20. Write short notes on Network Providers.

Network providers want a system that is easy to administer and manage; e.g., faults can be easily found, system can be hot-swapped,

21. What are the requirements of an efficient Network?

- Connectivity
- Efficient Resource Sharing
- Functionality
- Reliability
- Security
- Performance

22. What are the basic building blocks of networks?

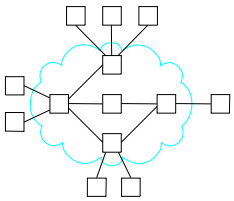
Building Blocks

links: coax cable, optical fiber...

nodes: general-purpose workstations...

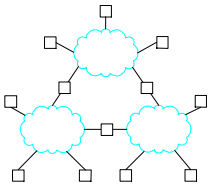
23. What is a switched network?

Two or more nodes connected by a link



24. What is internetwork?

Two or more networks connected by a node



25. Define Network?

A network is two or more nodes connected by a direct link, or two or more networks connected by one or more nodes".

UNIT - II

1. What is a Packet Switch?

A packet switch is a device with several inputs and outputs leading to and from the hosts that the switch interconnects. The core job of a switch is to take packets that arrive on an input and forward them to the right outputs.

2. Write short notes on Switch Congestion.

If the packet arrival rate exceeds the capacity of the output rate of a switch, the switch queues the packet. If the switch is over loaded, the packet may be loosed. If it occurs often, the switch is said to be congested.

3. What do you mean Packet Switching?

The process of forwarding packets from an input of a switch to one or more outputs of the switch is known as packet switching.

4. Define Network Topology.

The Network Topology defines the structure of the network. Ring, Bus, Star these are the examples of network topology.

5. What are the characteristics of Connectionless networks?

- A host can send a packet anywhere at any time
- When a Host sends a packet, it has no way of knowing if the network is capable of delivering it or if the destination host is even up and running.
- Each packet is forwarded independently.
- A Switch or link failure might not have any serious effect on communication.

6. What are the fields available in the VC table in a Switch?

- A virtual circuit identifier
- An incoming interface on which packets for this arrive at the switch
- An outgoing interface in which packets for this VC leave the switch
- A potentially different VCI that will be used for outgoing packets

7. What do you mean by signaling?

Signaling is a mechanism to establishing connection state between a source and destination. Here a host can send messages into the network to cause the state to be established.

8. Write short notes on virtual circuit switching.

Virtual circuit switching is a connection oriented mechanism used for packet forwarding. In this approach it establishes a connection state between the source and destination before sending the packets.

9. What is Packet Contention?

Contention occurs when multiple packets have to be queued at switch because they are competing for the same output link.

10. Write short notes on Source Routing.

Source Routing is a mechanism to forward the packets in a switch, in this all the information about network topology that is required to switch a packet across the network is provided by the source host.

11. Define Bridge.

Bridge is nothing but a switch that is used to forward packets between shared –media LANs such as Ethernet.

12. Define Spanning Tree.

Spanning Tree is a sub graph that covers all the vertices, but contains no cycles.

13. What are the Limitations of Bridges?

- Scale - the ability to extend the network (only a few LANs can be connected)
- Heterogeneity – bridges are fairly limited in the kinds of networks they can interconnect.

14. What is Virtual LAN?

Virtual LAN increase the scalability of extended LAN and allow a single extended LAN to be partitioned into several seemingly separate LANs.

15. What is ATM?

ATM stands for Asynchronous transfer Mode. It is connection oriented, packet switched technology.

16. Write Short notes on segmentation and reassembly?

The process of fragment the high level messages into packets at the source host and transmit the packets over the network and then reassemble the fragments back together at the destination is often called segmentation and reassembly(SAR).

17. Write short notes on CS-PDU?

CS-PDU stands for Convergence sub layer protocol data unit which defines a way of encapsulating variable length PDUs prior to segmenting them into cells.

18. What is routing or forwarding table?

The forwarding table contains the information that switches need to forward datagram in the network. The switch consults with the forwarding table and forwards the frames in the right ports.

19. What is a Cell?

Cell is nothing but packets which are both fixed in length and small in size, used in ATM .

20. What is ATM adaptation Layer?

A protocol which sits in between the ATM and the variable-length packet protocols that might use ATM (such as IP) is Called ATM Adaptation Layer.

21. What is an address?

Address is a byte-string that identifies a node; usually unique

22. What are the different types of addresses?
    - unicast: node-specific
    - broadcast: all nodes on the network
    - multicast: some subset of nodes on the network

23. Say some example for multiplexing techniques?
    - Time Division Multiplexing (TDM) (one user at a time)
    - Frequency Division Multiplexing (FDM) (all users at once)

24. What are the various types of message errors in the network?

    - Message content corruption
    - Messages are dropped
    - Messages are delayed
    - Messages are delivered out-of-order
    - Messages are duplicated.

25. What are the various types failures that can be occurred in a network?

- Bit errors (single and bursty)
- Packet loss
- Link failure

UNIT III

1. Define Internetwork.

Interconnected connection of networks is known as Internetwork.

2. What are the problems of inter connecting various networks?

- Heterogeneity – problem of establishing connectivity between host on different networks
- Scale – (the ability to add nodes to the networks) it lead to the problem of routing and addressing

3. Define Router or Gateways.

Router is a node that interconnects the networks.

4. What is MTU?

MTU stands for Maximum Transmission Unit, Which specifies the largest datagram that it can carry in a frame.

5. How IP address is hierarchical?

IP address is hierarchical, by which means that they are made up of many interconnected networks. IP addresses consist of 2 parts, a network part and a host part. the network part of an IP address identifies the network to which the host is attached.

6. List out the various addressing schemes in IP.

CLASS – A -> Network – 8 bit Host – 24 bit
CLASS – B -> Network – 16 bit Host – 16 bit
CLASS – C -> Network – 24 bit Host – 8 bit

7. Differentiate Bridges, Switches and Routers.

Bridges are Link level nodes they forward frame from one link to another to implement an extended LAN, Switches are network level nodes they forward datagrams from one network to another to implement a packet switched network and routers are internet level nodes they forward datagrams from another to implement an internet.

8. What is hierarchical aggregation?

Hierarchical aggregation is a mechanism to reduce the amount of information that is stored in each node and that is exchanged between nodes. In this letting routers deal only with reaching the right network; the information that a router needs to deliver a datagram to any node on a given network is represented by a single aggregated piece of information.

9. Write short notes on centralized and distributed routers.

In the centralized router, the ip-forwarding algorithm is done in single processing engine that handles the traffic from all ports. In distributed forwarding model, there are several processing engines, perhaps one per port, or more tan one per line card (serve one or more physical ports.

10. What is a network processor?

A network processor is a device, which is used in the design of routers. And it is a programmable device more highly optimized for networking task.

11. What is Link level address?

Link level address is nothing but the Ethernet card address, 48 bit long world wide unique address..

12. What is the job of an ARP?

The ARP enables each host on a network to build up a table of mapping between the IP address and Link level address.

13. What is the responsibility of a DHCP server?

Dynamic Host Configuration Protocol is responsible for providing configuration information to hosts.

14. Write Short notes on ICMP.

ICMP stands for Internet Control Message Protocol. It can be act as companion protocol of IP, that defines a collection of error message that are sent back to the source host whenever a router or host unable to process an ip datagram successfully.

15. Write short notes on VPN.

VPN stands for Virtual Private Network. VPN enables private communication in a public network by establishing a Virtual circuit between the source and destination.

16. What is IP tunnel?

IP tunnel is a virtual point-to-point link between a pair of nodes that are actually separated by arbitrary number of networks. The virtual link is created within the router at the entrance to the tunnel by providing it with the ip address of the router at the entrance to the tunnel by providing it with the IP address of the router at the far end of the tunnel.

17. What is forwarding?

Forwarding consists of taking a packet, looking at its destination address, consulting a table, and sending the packet in a direction determined by the table.

18. What is Routing?

Routing is the process by which forwarding tables are build, which contains the mapping information IP with MAC address.

19. Write short notes on network security.

- Prevent others from copying your data (eavesdropping).
- Verify that data was sent by the appropriate sender (not by an impostor), I.e., digital signatures.
- Ensure data is delivered only once (prevent playback).
- Prevent denial of service attacks.

20. Write short notes on bandwidth.

- Telephony Definition: the range of frequencies that a signal uses on a given medium
- Computer Network Definition: the number of bits per second that can be transmitted on a link

21. What is Throughput?

- Definition: the number of *useful* bits per second that can actually be transmitted over the link in practice
  Transfer size / Transfer time
- Measure of performance Ideal state Throughput= Bandwidth
- I.e., how much of the bandwidth is available for use.

22. What is Latency?

How long it takes a packet to travel from point A to point B through the network.

Latency = Propagation + Transmit + Queuing + Processing

23. What is Propagation delay?

Propagation Delay: speed of wave transmission (light) and distance

24. What is transmission delay?
Transmission Delay: packet size / link bandwidth

25. What is Queuing Delay?
The Packet waiting time in buffers is known as Queing Delay

Unit IV

1.What is NSFNET?

NSFNET stands for the regional networks are connected by a nationwide backbone, which is funded by National Science Foundation (NSF) and was therefore called the NSFNET backbone

2. What do you mean by subletting?

Subnetting provides an elegantly simple way to reduce the total number of network numbers that are assigned. The idea is to take a single IP network number and allocate the IP address with that network number to several physical networks, which are now referred to as subnets.

3. What is the use of CIDR?

CIDR tries to balance the desire to minimize the number of routes that a router needs to know against the need to hand out addresses efficiently.

4. What is an Autonomous system or routing Domain?

An autonomous system is one, which is under the control of a single administrative entity.

5. Write short notes on EGB?

EGB stands for Exterior Gateway Protocol. It is an interdomain protocol that has a number of limitations such as it is concerned on topology.

6. What are the various types of autonomous systems?

Stub AS	– an AS that has only a single connection to other AS
Multihomed AS	– an AS that has connections to more than one other As but that refuses to carry transit traffic
Transit AS	– an As that has connections to more than one other AS and that is designed to carry both transit and local traffic.

7. Define Local traffic and transit traffic.

Local traffic is nothing but a traffic that originates at or terminates on nodes within an AS, an transit traffic as traffic that passes through an AS.

8. How does BGP cancel the previously advertised path?

BGP can cancel the previously advertised path with a form of negative advertisement known as a withdrawn route.

9. What is Routing Area?

An area is asset of routers that are administratively configured to exchange link state information with each other.

10. What is ABR?

A router that is a member of both the backbone area and a non backbone area is an area border router(ABR)

11. Write short notes on Ipv6?

Ipv6 do not have classes, but the address space is still subdivided in various ways based on the leading bits. Rather than specifying different address classes, the leading bits specify different uses of the Ipv6 address.

12. What is the Address notation of Ipv6?

Ipv6 address notation is x:x: x:x: x:x: x:x where each x is a hexadecimal representation of 16-bit piece of the address.

13. Give the ipv6 provider based unicast address.

RegistryID – m bit
ProviderID - n bit
SubscriberID – o bit
SubnetID – p bit
InterfaceID 125-m-n-o-p

14. What do you mean by autoconfiguration?

The 2 steps involved autoconfiguration is as follows

Obtain an interface ID that is unique on the link to which the host is attached.
Obtain the correct address prefix for this subnet.

15. What do you mean by RTT?

Round Trip Time is the time to send a message from A to B and Back to A

16. Write the speed of light in various physical medium.

Speed of Light

- 3.0 x 108 meters/second in a vacuum
- 2.3 x 108 meters/second in a cable
- 2.0 x 108 meters/second in a fiber

17. What is signal is instantaneous?

Suppose that C immediately signals A to stop sending packets after it receives the first packet. Assume that this ‘‘signal’’ is instantaneous.

18. Define protocol.

A protocol defines the format and order of messages exchanged between two or more communicating entities as well as the actions taken on the transmission or receipt of messages.

19. What is the need for Multiplexing and De-multiplexing?

Multiplexing and De-multiplexing uses protocol keys (protocol numbers) in the header to determine correct upper-layer protocol.

20. Draw the internet architecture.

Higher level protocols – HTTP , FTP
End to End protocols - UDP, TCP
Peer to peer protocols - IP
Various networks - Ethernet, FDDI

21. Write the expansion of the following (T)FTP, HTTP, NV, SMTP, FDDI.
    - (T)FTP - (Trivial) File Transfer Protocol
    - HTTP – Hyper-Text Transport Protocol
    - NV - Network Video
    - SMTP – Simple Mail Transfer Protocol
    - FDDI - Fiber Distributed Data Interface

22. Write the expansion of the following NTP, TCP, UDP, ATM and IP.
    - NTP - Network Time Protocol
    - TCP - Transmission Control Protocol
    - UDP - User Datagram Protocol
    - IP - Internet Protocol
    - ATM - Asynchronous Transfer Mode

23. Write short notes on bit errors.
    - 1 in 106 to 107 for copper
    - 1 in 1012 to 1014 for fiber
    - Much worse for wireless
    - Recovery: re-flip bits or discard packet

24. Write short notes on Packet Loss.
    - Uncorrectable bit error
    - Buffer overflow (dropped by switch)
    - Recovery: resend packet (lost vs. late?)

25. Write short notes on Link failure.
    - Software (crash)
    - Hardware (disconnection)
    - Recovery: reroute streams

UNIT V

1. What is an End-to-End Protocol?

The process-to-process communication channel is the role played by the transport level of the network architecture, which, because it supports communication between the end application programs, is sometimes called the end-to-end protocol.

2. List out the properties that a transport can be expected to provide.

Guarantees message delivery
Delivers message in the same order they are sent
Delivers at most one copy of each message
Supports arbitrarily Large message

3. Write short notes on UDP.

UDP stands for User Data gram Protocol. It is transport layer protocol that extends the host-to-host delivery service of the underlying network into a process-to-process communication service.

4. What is called pseudo header?

UDP computes its checksum over the UDP header, the contents of the message body, and something called the pseudo header that consists of three fields from the IP header – protocol number, source ip address, and destination ip address plus the udp length.

4. What is TCP?

TCP is a protocol which grantees the reliable, in-order delivery of a stream of bytes. It is a full duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction

5. What is MSL?

MSL stands for Maximum segment life time. IP throws packets away after their TTL expires; TCP assumes that each packet has maximum life time that is MSL.

6. What are segments?

The packets exchanged between TCP peers are called segments.

7. What are the fields available in the segments?

SrcPort : Source Port
SrcIPlAddr : Sourc IP address
DstPort : Destination Port
DstIPaddr : destion IP address

8. What do you mean by incarnation?

It is possible for a connection between a particular pair of ports to be established, used to send and receive data, and closed, and then at a later time for the same pair of ports to be involved in a second connection. And it is referred to us two different incarnations of the same connection.

9. What is the use of three way handshake algorithm?

This algorithm is used by TCP to establish and terminate a connection; it involves the exchange of three messages between the client and server.

10. Write short notes on active open and passive open messages?

To open a connection server first invoke a active open message. To establish the connection with server, client invokes the passive open message.

11. What is MSS?

MSS stand for Maximum segment size, it is variable maintain by the TCP. It sends the segment as soon as it has collected MSS bytes from the sending process.

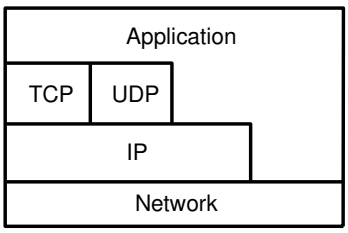
12. What are the various functions of the following layers application, presentation and session?

- Application : Application specific protocols
- Presentation : Format of exchanged data
- Session : Name space for conn. Mgmt (tie multiple transport streams together)

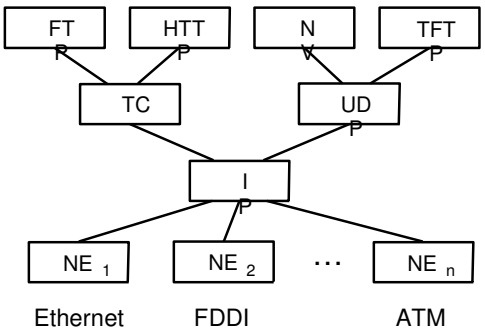
13. What are the various functions of the following layers transport, network, data link and physical?

- Transport: Process-to-process channel (end-to-end)
- Network: Host-to-host packet delivery (routing)
- Data Link: Framing of data bits (single hop issues)
- Physical: Transmission of raw bits

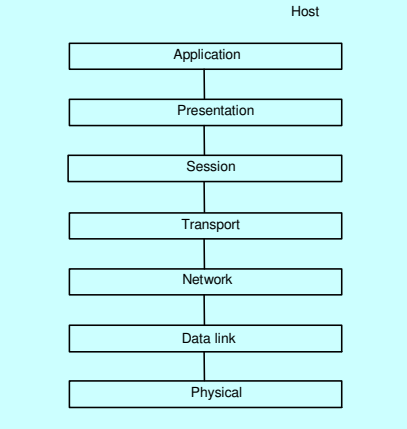
14.Drw the diagram of internet architecture?



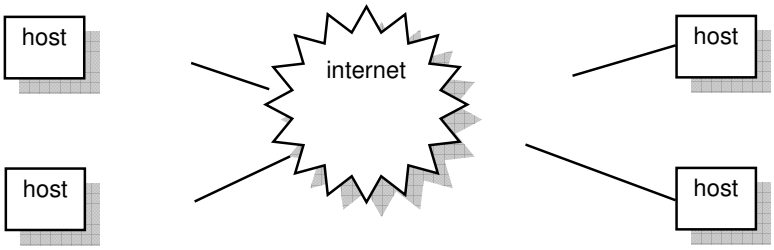
15. Draw the internet protocol graph?



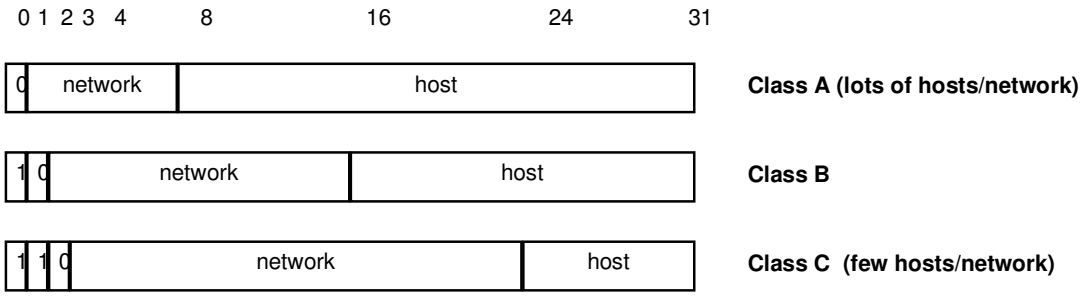
16. Draw the various layers of the OSI model?



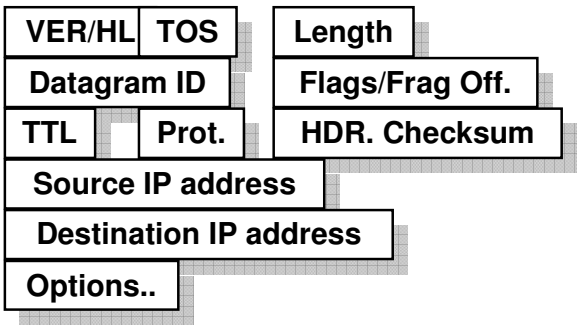
17. Draw the diagram of Inernetwork?



18. Draw the format of various IP classes ?



19. Draw the packet format of IP?



VER	IP version
HL	Header length (in 32-bit words)
TOS	Type of service (unused)
Length	Datagram length (max 64K bytes)
ID	Unique datagram identifier
Flags/Frag	Control flags/fragment offset
TTL	Time to Live
Prot	Higher level protocol (e.g., TCP, UDP)

20. What the steps involved in routing?

(1) Extract final destination host IP address from datagram.
(2) Look up final IP address in routing table.
(3) Returns IP address of next hop.
(4) Use ARP to discover corresponding physical address of next hop.
(5) Forward datagram to next hop.

21. What is the need for fragmentation?

Different networks have a different maximum transfer unit (MTU).
A problem can occur if packet is routed onto network with a smaller MTU.

- e.g. FDDI (4,500B) onto Ethernet (1,500B)

Solution: break packet into smaller fragments.

- each fragment has identifier and sequence number

22. What is TTL?

Goal: drop packets that are stuck in infinite loop in the network.
IP Solution: Decrement TTL field in each hop and drop packet if it reaches 0.

23. What do you mean by full duplex?

Full duplex connections enable concurrent transfers in both directions along a connection.

24. What is buffered data transfer?

Protocol software free to use arbitrary size transfer units is known as buffered data transfer.

25. What do you mean by stream transfer?

In stream transfer, sender transfers stream of bytes; receiver gets identical stream

NOORUL ISLAM COLLEGE OF ENGINEERING

Department of Software Engineering
XCS 353 – Computer Networks
16 Marks Q & A

1. What is a Multiplexing? Explain its types.

Multiplexing

It means that a system resource is shared among multiple users. At an initiative level, multiplexing can be explained by analog to a time-sharing computer system, where a single physical CPU is shared among multiple jobs.

- Synchronous time-division multiplexing. (STDM)
- Frequency division multiplexing. (FDM)

Synchronous time-division multiplexing (STDM)

- The idea of STDM is to divide time in to equal quanta and in a round robin fashion give each flow a chance to send its data over the physical link.
- During time quantam 1, data from the first flow is transmitted during time quantam 2 data from the 2^{nd} flow is transmitted and so on..
- This process continues until all the flows had a turn at which time the first flow gets to go again and the process repeats.

Frequency division multiplexing

- The idea of FDM is to transmit each flow over the physical link at a different frequency, much the same way that the signals for different TV stations are transmitted at a different frequency on a physical cable TV link.
- Both STDM and FDM are limited for reasons.
- If one of the flows (host pair) does't have a data to send.
- The maximum number of flows is fixed as known a head of time.

Statistical Multiplexing

- Another form of multiplexing.
- Similar to STDM
- First data from one flow is transmitted to the physical link, then data from another flow is transmitted and so on.
- Statistical multiplexing has no mechanism to ensure that all the flows eventually get their turn to transmit over the physical link.
- Once a flow begins sending data, we need some way to limit the transmission, so that the other flows can have a turn.
- To account for this need, statistical multiplexing defines an upper bound on the size of the block of that each flow is permitted to transmit at a given time.

2. Explain the network architecture (layering, protocol graph and encapsulation) in detail?

- "A protocol defines the format and order of messages exchanged between two or more communicating entities as well as the actions taken on the transmission or receipt of messages"
- Protocols are the building blocks of network architecture.
- Each layer has its own protocol.
- The idea behind layering is that the services offered by the underlying hardware and then add a sequence of layering each providing a higher (more abstract) level service.
- The services provided at the higher layers are implemented in terms of the services provided by lower layers.
- A network having two layers of abstraction sandwiched between the application program and underlying hardware.

Application Program
Process to Process Channels
Host to Host Channels
Hardware

- Each protocol object has two different interfaces
  - Service interface – Interface to the other object on the same computer that want to use its communication services
  - Peer-to-peer interface – Interface to the object on another machine. It defines the form and meaning of messages exchanged between protocols.

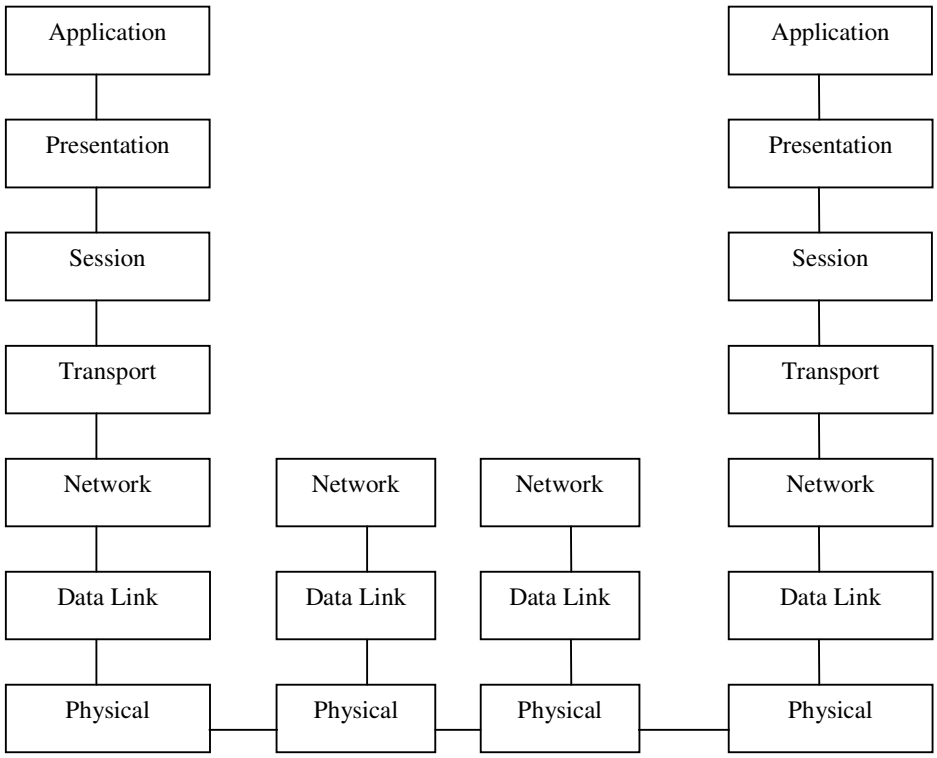
Protocol graph

- Collection of protocols and their dependencies
- Most peer to peer communication is indirect
- Direct only at hardware level

Encapsulation

- It means wrapping up of data and member function in to single unit.
- While sending a message from one to another, the RRP attaches a header with that message.
- A header is a small data structure.
- Headers are usually attached in front of a message. In the case of Peer to Peer control information, the header is send at the end of the message in which case it is called a trailer.
- The format of header is defined by protocol specification.
- The data being transmitted on behalf of the application is called Message body.
- Encapsulation is repeated at each level of the protocol graph.

3. Explain the OSI reference Model in detail?



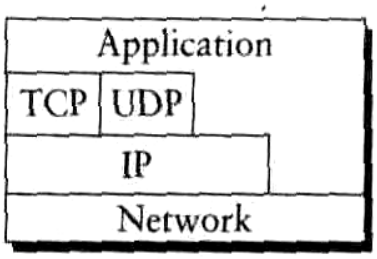
- Open Systems Interconnect (OSI) Architecture
- International Standards Organization (ISO)
- International Telecommunications Union (ITU, formerly CCITT)
- X dot series: X.25, X.400, X.500

Primarily a reference model

- Application : Application specific protocols
- Presentation : Format of exchanged data
- Session : Name space for conn. Mgmt (tie multiple transport streams together)
- Transport : Process-to-process channel (end-to-end)
- Network : Host-to-host packet delivery (routing)
- Data Link : Framing of data bits (single hop issues)
- Physical : Transmission of raw bits

4. Explain Internet Architecture (TCP/IP) in detail ?

- Developed with ARPANET and NSFNET
- Internet Engineering Task Force (IETF)
  - Culture: implement, then standardize
  - OSI culture: standardize, then implement
- Popular with release of Berkeley Software Distribution (BSD) Unix; *i.e.*, free software
- Standard suggestions debated publicly through requests for comments (RFCs)
- No strict layering
- Hourglass shape – IP is the focal point
- Design and implementation go hand-in-hand (must provide an implementation when presenting a new specification).



First Layer (Lowest Layer)

- A wide variety of network protocols are defined.
- These protocols are implemented by combination hardware.

Second layer

- Contains a single protocol called IP
- This Protocol supports the interconnection of multiple networking technologies into a single, logical internetwork.

Third Layer

- Contains two main protocols TCP and UDP are sometimes called end to end protocols
- TCP and UDP provide alternative logic channels to application programs
- TCP provides a reliable byte stream channel.,
- UDP provides an unreliable datagram delivery channel.

Fourth Layer

- Contains a range of application protocols such as FTP, TFTP, Tel net and SMTP.
- These protocols enable the inter operation of popular applications.

5. Explain the various Error detection techniques in detail.

- Bit errors in communication links occur due to noise of various kinds
- Error detection vs error correction
  - Best choise for low error probability?
- Basic idea in error detection: together with n-bit message, send k "redundant" bits that can detect *many* possible errors
    - k/n determines efficiency of error detecting code

One- and Two-dimensional parity
2-dim parity catches all 1-, 2-, and 3-bit errors (and most 4-bit errors)

Checksums

- Add up all words of message, and transmit sum together with message
- Receiver performs same calculation
  - if received sum is different, discard message
- Internet checksum:
  - Split message in 16-bit words
  - Perform ones complement arithmetic in 16-bit words
    - Negative number x: binary complement of positive –x
    - If sum generates carryout, increment result
- 16-bit overhead for arbitrary large message

Cyclic Redundancy Check (CRC)

- Represent (n+1)-bit message x with n-th degree binary polynomial M(x)
- e.g., 10011010: x7+x4+x3+x
- Sender & receiver agree on *divisor* polynomial C(x) of degree k
- e.g., C(x) = x3+x2+1 (k=3)
- Multiply M(x) with xk : T(x)
- T(x) = 10011010000
- Divide T(x) by C(x) in *mod-2 polynomial arithmetic*
- quotient Q(x), remainder R(x)
- Send T(x) – R(x) = C(x) * Q(x) to receiver
- If no errors, T(x)-R(x) should be divisible by C(x)

6. Describe Ethernet (802.3) in detail.

- Ethernet is easily the most successful local area networking technology developed in the middle of 1970's by researchers at the PARC (Xerox Palo Alto Research Center)
- It is a working example of the Carrier Sense Multiple Access with Collusion Detect (CSMA/CD) Local area network technology.
- It is also a multiple access network technology.
- The Carrier sense in CSMA/CD means that all the nodes can distinguish between an idle and busy link.
- Collusion Detect means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered with a frame transmitted by another node.
- It has its roots in an early packet radio network called Aloha.
- It uses the Manchester Encoding scheme.

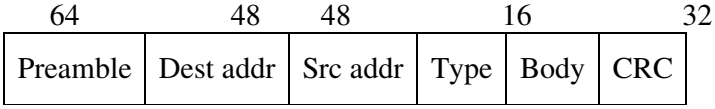
Physical Properties

- An Ethernet segment is implemented on a Coaxial cable of up to 500m.
- Hosts connects to an Ethernet segment by tapping in to it, taps must be atleaast 2.5m apart.
- A transceiver is a small device directly attached in the tap and detects when the line is idle and drives the signal when the host is transmitting.
- The transceiver in turn connected to an Ethernet potential adaptor, which is plugged into the host.
- Multiple segments can be jointed together by repeater. A repeater is a device that forwards digital signals, much like an amplifier that forwards analog signals.

Access Protocol

It is a algorithm that controls access to the shared Ethernet link. This algorithm is commonly called Media Access Control (MAC). It is typically implemented in hardware on the network adaptor.

Frame format



Address

- Every Ethernet host in the world has a unique Ethernet address. Each address belongs to the adaptor not the host, it is usually burned in to ROM.
- Ethernet addresses are typically printed in a form, It can read as a sequence of six numbers separated by colons.

  Eg: 8 : 0 : 2b: c4 : b1 : 2

An Ethernet adaptor receives all frames and accepts

- Frames addressed to its own address
- Frames addressed to the broadcast address
- Frames addressed to a multicast address, if it has been instructed to listen to that address
- All frames, if it has been placed in promiscuous mode.

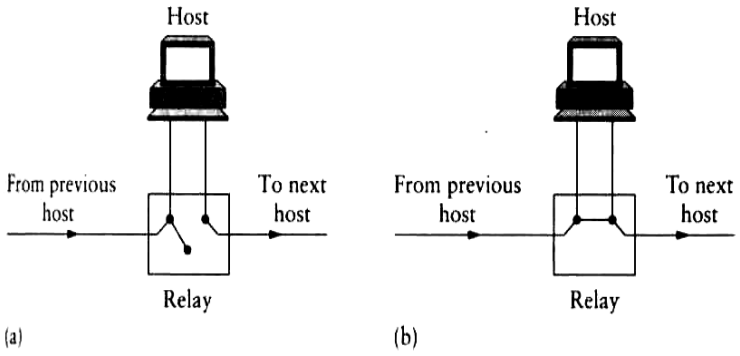
7. Explain the Token Ring and FDDI in detail.

Token Ring

- Token ring are the significant class of shared media network.
- IBM Token ring is nearly identical to IEEE standard
- FDDI (Fiber Distributed Data Interface) is a faster type of token ring.
- Token ring network consists of a set of nodes connected in a ring.
- Data always flows in a particular direction around the ring, with each node receiving frame from its upstream neighbor and then forwards them to its down stream neighbor.

Physical properties

- One of the problems with ring topology is that any node or link failure would render the whole network useless. This problem is addressed by connecting each station in to the ring using an electromagnetical relay.
- If the relay is open, it is included in the ring.
- If the relay is closed then the ring automatically bypasses the station.



Other Physical Details

- The data rate may either 4Mbps or 16 Mbps.
- The encoding bit uses Manchester encoding.
- IBM Token ring may have up to 260 stations per ring.
- 802.5 Token rings sets the limit at 250.
- The physical medium used in IBM is twisted pair.

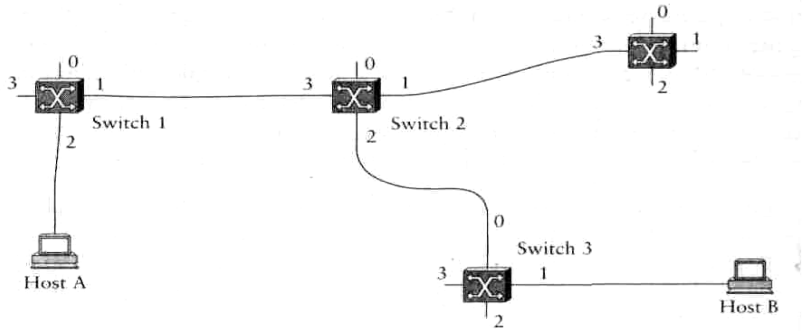
FDDI: Fiber Distributed Data Interface.

- FDDI is a high speed token ring fiber optical cable based technology.
- These technologies can 'self-heal', which means that the hardware can automatically detect and correct hardware problems.
- FDDI consists of two independent rings to connect each computer. Data flows in opposite direction in each ring.
- FDDI can have two types of Network Interface Cards, A and B, that connect to it.
- Class A Network Interface Cards connect to both rings while class B Network Interface Cards connect to only one ring.
- Only class A cards can be used to heal broken rings. Thus the number of class A cards define the fault tolerant characteristics of the network.
- When an error occurs the nearest computer routes frames from the inner ring to the outer ring.

8. Write notes on Virtual Circuit Switching (VCI).

- It is a widely used technique for packet switching which differs significantly from the datagram model.
- It is a connection oriented model.
- The idea is, we first set up a virtual connection from the source host to the destination host before any data is sent.
- When host A wants to send Packet to host. It is known as two-stage process.

  Connection setup
  Data transfer



- In Connection setup phase, it is necessary to establish connection state in each of the switch between the source and destination host.
- The connection state for a single connection consists of an entry in a "VC table".
- VCI (Virtual Circuit Interfere) it uniquely identifies the connection at this switch and that will be carried inside the header of the packets that belong to this connection.
- An incoming interface and out going interface.
- A potential different VCI that will be used for outgoing packet.

Virtual Circuit Table

Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
2	5	1	11

Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
3	11	2	7

Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
0	7	1	4

A Packet switched network that uses the connection oriented model

- Buffers are allocated to each virtual circuit when the circuit is initialized
- The sliding window protocol is run between each pair of nodes along the virtual circuit and this protocol is augmented with flow control to keep the sending node from over running the buffer allocated at the receiving node.
- The circuit is rejected by a given node if not enough buffers are available at that node when the connection request message is processed.

9. Explain the Spanning tree algorithm in detail.

- LANs have physical limitations (e.g., 2500m)
- Connect two or more LANs with a bridge
  - Bridges use "accept and forward" strategy
  - level 2 connection (does not add packet header)

Learning Bridges

- Do not forward when unnecessary
- Maintain forwarding table
- Learn table entries based on source address
- Table is an optimization; need not be complete
- Always forward broadcast frames

Spanning Tree Algorithm

- Problem: loops in cabling can make packets forwarded forever - no mechanism to remove looping frames
  - We can remove loops by maintaining state in the packet, but for layer-2 switching - we are not allowed to change the packet
  - Extra cabling can be good for redundancy if we can remove loops dynamically
- Bridges run a distributed spanning tree algorithm
  - select which bridges actively forward
  - developed by Radia Perlman
  - now IEEE 802.1 specification
- Each bridge has unique id (e.g., B1, B2, B3)
- Select bridge with smallest id as root
  - How to choose root: next slides
- Select bridge on each LAN closest to root as designated bridge (use id to break ties)
  - Each bridge forwards frames over each LAN for which it is the designated bridge
  - Root forwards over all its ports
- Bridges exchange configuration messages
  - id for bridge sending the message
  - id for what the sending bridge believes to be root bridge
  - distance (hops) from sending bridge to root bridge
- Each bridge records current best configuration message for each port
- Initially, each bridge believes it is the root
- When a bridge learns that it is not root, stop generating config messages
  - in steady state, only root generates configuration messages
- When a bridge learns that it is not the designated bridge, stop forwarding config messages
  - in steady state, only designated bridges forward config messages
- Root continues to periodically send config messages
- If any bridge does not receive config message after a period of time, it starts generating config messages claiming to be the root

10. Discuss Cell Switching (ATM)

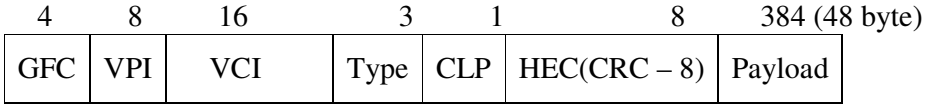
- Cell switching deserves special attention in ATM (Asynchronous Transfer Mode)
- ATM is a connection oriented, packet switched technology that uses small, fixed size packets called cells to carry data.
- In the ATM technology the connection setup phase is called signaling. The main ATM signaling protocol is known as Q.2931
- Q.2931 is the responsible for allocating resources at the switches along the circuit.

Cells

The ATM cell actually comes in two different formulas, depends on the network

UNI (User Network Interface) Format
NNI (Network Network Interface) Format

Cell Format



GFC → Generic flow control
VPI → Virtual path identifier
VCI → Virtual circuit identifier
CLP → Cell loss priority
HEC → Header error check.

Physical layers for ATM

SONET physical layer
TAXI physical layer

ATM in LAN

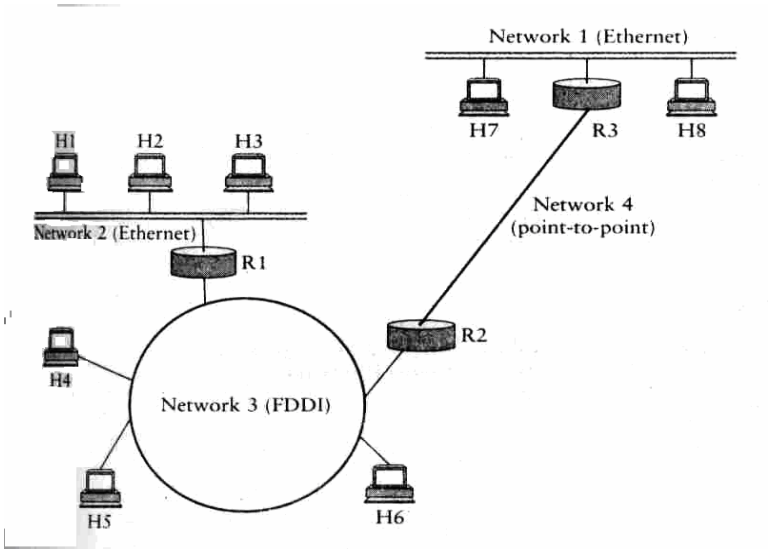
- Instead of using Ethernet in LAN, Now days we are using ATM that support for Voice, Video and data traffic.
- ATM is a switched technology, in Ethernet; it is a shared media technology.
- ATM operates on links with speed of 155 Mbps and above, While in the case of Ethernet it operates on links with speed only 10 Mbps.

Advantage of ATM

- Each host gets its own dedicated link to the switch.
- It gives high performance switch.
- Lack of distance limitation links.
- Because of high performance it is used as a backbone of larger network.
- One significant problem with running ATM in a LAN is that it doesn't look like a traditional LAN. Because most LANs are shared media networks. It is easy to implement broadcast and multicast.

11. Discuss the Datagram forwarding in IP.

- Data gram is a connection less model of data delivery.
- The IP service model is sometimes called "best effort" because although IP makes every effort to deliver datagram's, it makes no guarantees.
- IP addressing scheme has a lot of flexibility, allowing networks of different sizes to be accommodated fairly efficiently.
- IP addressing is written as four decimal integers separated by dots. Each integer represents the decimal value contained in 1 byte of address starting at the most significant. Eg: 171.69.210.245.
- Forwarding is the process of taking a packet from an input and sending it out on the appropriate output.
- Routing is the process of building up the tables that allows the correct output for a packet to be determined.



Main points regarding forwarding of IP datagram are,

- Every IP datagram contains the IP address of the destination host.
- The "network part" of an IP address uniquely identifies a single physical network that is part of the larger Internet.
- All hosts and routers that share the same network part of their address are connected to the same physical network and can communicate with each other by sending frames over that network.
- Every physical network that is a part of the internet has atleast one router.

Network Num	Next Hop
1	R3
2	R1
3	Interface 1
4	Interface 0

12. Address Translation works in Simple Internet Working.

IP datagrams contain IP addresses, but the physical interface hardware on the host (or) router only understands the addressing scheme of that particular network. So we need to translate the IP address to a link level address that makes sense on this network.

Ways to map the IP address in to physical address (link level)

- To encode a host's physical address in the host part of its IP address
- To maintain a table of address pair.
- The table would map IP address in to physical address. Thus table could be centrally managed by a system administrator. The mapping accomplished using the ARP (Address Resolution Protocol)

ARP

- It enables each host on a network to build up a table of mappings between IP addresses. These mapping may change over time.
- The entries are timed out periodically & removed.
- The set of mappings currently stored in host is known as ARP cache or ARP table.
- ARP takes advantage over Ethernet and Token ring.

Packet format

<table>
<tr><td colspan="2">Hardware type = 1</td><td>Protocol Type = 0 x 0800</td></tr>
<tr><td>Hlen = 48</td><td>Plen = 32</td><td>Operation</td></tr>
<tr><td colspan="3">Source Hardware Addr (byte 0 – 3)</td></tr>
<tr><td colspan="2">Source hardware Addr (byte 4 – 5)</td><td>Source protocol Addr (byte 0 – 1)</td></tr>
<tr><td colspan="2">Source Protocol Addr (byte 2 – 3)</td><td>Target Hardware Addr (byte 2 – 5)</td></tr>
<tr><td colspan="3">Target Hardware Addr (byte 2 – 5)</td></tr>
<tr><td colspan="3">Target Protocol Addr (byte 0 – 3)</td></tr>
</table>

Hardware Type → Specifies the ype of physical network (eg: Ethernet)
Protocol Type → Specifies the higher layer protocol (eg: IP)
Hlen → Hardware address length
→ Specifies the length of link layer address
Plen → Protocol address length
→ Specifies the length of higher layer protocol address
Operation field → Specifies whether this is a request or a response.

ATMARP

- It is a different ARP procedure that may be used in an ATM network that doesnot depend on broadcast or LAN emulation. This procedure is known as ATMARP and is part of the classical IP over ATM model.
- A key concept in the classical IP over ATM model is the logical IP subnet (LIS)

13. Discuss Host Configuration in IP (DHCP).

- DHCP means dynamic host configuration protocol.
- It contains many methods for automated configuration.
- It relies on the existence of a DHCP server that is responsible for providing configuration information to hosts
- There is atleast one DHCP server for an administrative domain.
- The DHCP serve can function just as a centralized repository for host configuration
- The configuration information for each host could be stored in the DHCP server and automatically retrieved by each host when it booted or connected to the network.
- A use of DHCP is, it saves the network administrator from ever having to assign address to individual hosts.
- Goal of DHCP is to minimize the amount of manual configuration required for a host to function.
- To Contact a DHCP Server, a newly booted or attached hosts sends a DHCPDISCOVER message to a special IP addresses.

Packet format

<table>
<tr><td>Operation</td><td>Htype</td><td>Hlen</td><td>Hops</td></tr>
<tr><td colspan="4">Xid</td></tr>
<tr><td colspan="2">Secs</td><td colspan="2">flags</td></tr>
<tr><td colspan="4">Ciaddr</td></tr>
<tr><td colspan="4">Yiaddr</td></tr>
<tr><td colspan="4">Siaddr</td></tr>
<tr><td colspan="4">Giaddr</td></tr>
<tr><td colspan="4">Chaddr(16 bytes)</td></tr>
<tr><td colspan="4">Sname (64 bytes)</td></tr>
<tr><td colspan="4">File (128 byte)</td></tr>
<tr><td colspan="4">options</td></tr>
</table>

Error Reporting (ICMP)

- It means Internet Control message protocol
- Defines a collection of error message that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully.
- It defines a handful to control message that a router can send back to a source host.
- ICMP – Redirect → It is a useful control message tell how best route to the source host.

14. Explain the distance vector routing (RIP).

Distance Vector (RIP)

- Each node constructs a one dimensional array (vector) containing distances to all other nodes

  for direct links the cast value is 1

  for others the coast value is 0

- Each node constructs its routing table
- Each node distributes its distance vector to its immediate neighbor nodes.
- Based on the distance vector of its neighbors, all the nodes is called convergence

Types of routing table updation:

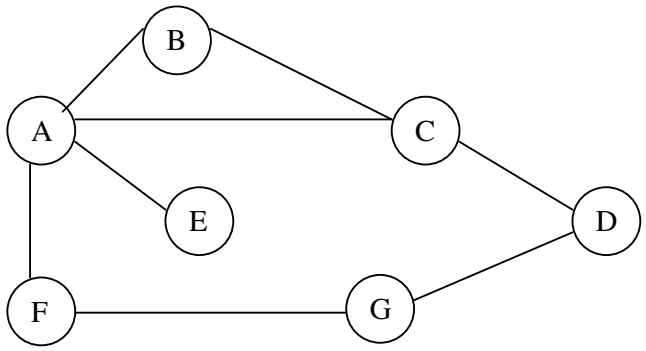
- Periodic updation

  All the nodes automatically sends an update message at regular intervals even if nothing has changed.

- Triggered updation:

  This happens whenever a node an update msg from one of its neighbors that causes it to change its routing table.

Consider the following network



1) Initial distance vector stored at each node

Node	Distance to reach Node						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	1	∞	∞	0	∞	∞	∞
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

ii) Each node constructs its routing table
Routing table for A

Destination	Cast	Next hop
B	1	B
C	1	C
D	∞	-
E	1	E
F	1	F
G	∞	-

iii) Distribute the distance vector to its neighbor so in the above example
A distributes its vector to B, C, E and F

B distributes its vector to A and C

C distributes its vector to A, B and D

D distributes its vector to C and G

E distributes its vector to A

F distributes its A and G

G distributes its D and F

Based on vector received from neighbors change the routing table of all nodes

15. Explain the Stop and Wait protocol in detail?

A stop-and-Wait protocol

Assumptions

- All packets are received
- Packets may be corrupted (i.e., bits may be flipped)
- Checksum to detect bit errors

How to recover from errors? Use ARQ mechanism

- *acknowledgements (ACKs):* receiver explicitly tells sender that packet received correctly
- *negative acknowledgements (NAKs):* receiver explicitly tells sender that packet had errors
- sender retransmits pkt on receipt of NAK

Handling Duplicate Packets

- sender adds *sequence number* to each packet
- sender retransmits current packet if ACK/NAK garbled
- receiver discards (doesn't deliver up) duplicate packet

Sender:

- seq # added to pkt
- two seq. #'s (0,1) will suffice. Why?
- must check if received ACK/NAK corrupted
- twice as many states
  state must "remember" whether "current" pkt has 0 or 1 seq. #

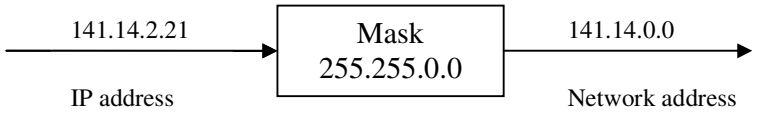
Receiver:

- must check if received packet is duplicate
  - state indicates whether 0 or 1 is expected pkt seq #
- note: receiver can *not* know if its last ACK/NAK received OK at sender

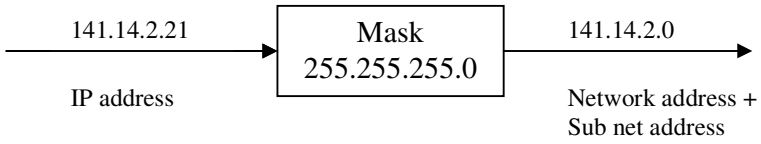
16. Write about Masking in detail.

- It is a process that extracts the address of physical network from an IP address. It can be done whether we have sub netting or not.
- If we have not sub netted the network masking extracts the network address from an IP address.
- If we have sub netted, masking extracts the network address and subnet address from an IP address.

Example
i) Without Sub netting



i) With Sub netting



Types of masking

- Boundary level masking
- Non boundary level masking

Boundary level masking

- The bytes in the IP address that corresponds to 255 in the mask will be repeated the sub network address
- The bytes in the IP address that corresponds to 0 in the mask will change to 0 in the sub network address.

Eg:	IP addr	45	23	21	8
	Mask	255	255	0	0
Subnet addr		45	23	0	0

Non Boundary level masking

- The bytes in the IP address that corresponds to 255 in the mask will be represented in the sub network address
- The bytes in the IP address that corresponds to 0 in the mask will change to 0 in the sub network address.
- For other bytes, use bit wise AND operator

Eg:	IP addr	45	123	21	8
	Mask	255	192	0	0
Subnet addr		45	64	0	0

123 → 0111 1011
192 → 1100 0000

64 → 0100 0000

17. Write about Simple Demultiplexer in detail.

- It is the simplest transport protocol that extends the host to host delivery service of the n/w into a process to process communication service
- So, the protocol needs to add a level of demultiplexing to allow multiple application processes on each host to share the network
- An example for transport protocol is UDP (User Datagram Protocol)
- In UDP, the host's address contain one additional field called process –id (pid) to identify the processes directly which is assigned by the OS process –id unique
- UDP uses port (or) mailbox to indirectly identify the processes. The basic idea is, source process send messages to a port/ mailbox and the destination process will receive the information from that port
- A common approach for the destination process is to accept messages from a well known Port. ie) each node receives its messages from some fixed port that is widely published

  Eg

  i) DNS: Receives messages at well known Port 53
  ii) Mail services receives messages at port 25
  iii) Unix talk program accepts messages at post 517

Implementation of Port

Port is implemented by a message queue is shown below:

When a message arrives the protocol appends the message to the end of the queue. If the queue is full then the message is discarded. When an application wants to receive a message then the message will be removed from the front of the queue. If the Queue is empty then the process blocks until a message becomes available.

Src Port	Dst Port
Length	Check Sum
Data	

Src Port → Identifies the Source Process / Port

Dst Port → Identifies the Destination Process / Port

Length → Length of the UDP header

Check Sum → Used to detect transmission errors

Data → Original data / message have to transfer.

18. Write about Reliable Byte Stream in detail.

- TCP is a transport protocol which offers a reliable, connection oriented byte stream service.
- TCP is a full duplex protocol meaning that each TCP connection supports a pair of byte streams, one following in each direction.
- TCP also includes flow – Ctrl mechanism for each byte streams that allows the receiver to limit how much data the sender can transmit a given time.
- TCP supports demultiplexing mechanism (like UDP) that allows multiple application programs on any given host to simultaneously carry on a conversation with their peers.
- TCP also includes congestion control mechanism which prevents too much amt of data, from being injected into the network thereby causing.
- RTT is the time takes for a bit of information to propagate from one end to other and back again.
- TCP is a byte oriented protocol means that the sender writes bytes into a TCP connection and the receiver reads bytes out of TCP Connection.
- Each segment carries a set of Byte stream and each segment contains TCP header, which is shown below

<table>
<tr><td colspan="3">Src Port</td><td>Dst Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgement</td></tr>
<tr><td>Hdr len</td><td>0</td><td>Flags</td><td>Advertised window</td></tr>
<tr><td colspan="2">Checksum</td><td colspan="2">Urgptr</td></tr>
<tr><td colspan="4">Options (variable)</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

Fig: TCP HEADER FORMAT

Advertised window → Carry enough information about the flow of data.
Flag → It contains SYN, FIN, RESET, PUSH, URG and ACK.
SYN & FN → Indicates connection establishment & termination.
ACK → Means that Acknowledgement field is valid
(ie) receiver will respond.
URG → Urgent data.
URG Ptr → Starting point of urgent data.

19. Discuss about Sliding Window process in detail.

Sliding window algorithm serves several purposes:

(i) It guarantees reliable delivery of data.

(ii) It ensures that data is delivered in order.

(iii) It enforces flow control between sender and Receiver.

(i) & (ii) Reliable and Ordered delivery of data:

TCP on the sending side maintains a send buffer. This buffer is used to store data that has been sent but not yet acknowledged, as well as data that has been written by the application but not transmitted.

The three pointers maintained by the send buffer are:

(i) Last Byte Acked
(ii) Last Byte Sent
(iii) Last Byte Written

Conditions:

Last Byte Acked < Last Byte Sent
Last Byte Sent < Last Byte Written

Receiver Side:

On receiving side, TCP maintains a receive buffer. This buffer holds data that arrives out of order as well as data that is in the correct order.

Conditions:

Last Byte Read < Next Byte Expected.
Next Byte Expected < Last Byte RVCD + 1

Flow control:

Receiver Side:

Last Byte RCVD – Last Byte Read < Max RCV Buffer
Advertised window = Max RCV Buffer – ((Next Byte Expected – 1)- Last Byte Read)
Advertised window --> Represents amt of free Space remaining in its buffer

Sender Side:

Last Byte Sent – Last Byte Acked < Advertised window
Effective window = Advertised window – (Last Byte Sent – Last Byte Acked)
Effective window --> Limits how much data a sender can send?

Triggering Transmissions

TCP has mechanisms to trigger the transmission of a segment.

(i) TCP maintains a variable called MSS (Maximum segment Size)
(ii) Sending process explicitly call the PUSH operation.
(iii) When a timer fires, TCP will trigger the transmission.