I.E.S. College of Engineering

2nd Internal Examination

Date : 22 April 2020

Name : Jovial Joe Jayarson

Roll No. : IES17CS016

Subject : CS306 - Computer Networks

Marks Awarded:

Q.10.) Role of SNMP

- SNMP stands for Simple Network Management Protocol which is an internet standard protocol for collecting and organizing information about managed device on IP networks.
- SNMP is widely used in network management and monitoring.
- It is a standard way of monitoring hardware and software from nearly any manufacturer.
- It releases management data in form of managed systems organized in a management information base.

~ It is also defined as a component of Internet Protocol ~~Security~~ Suite and consists of set of standard for network management.

~ SNMP require only a couple of basic components to work : a management station and an agent.

~ A management station is a software that collects information from ~~your~~ the network.

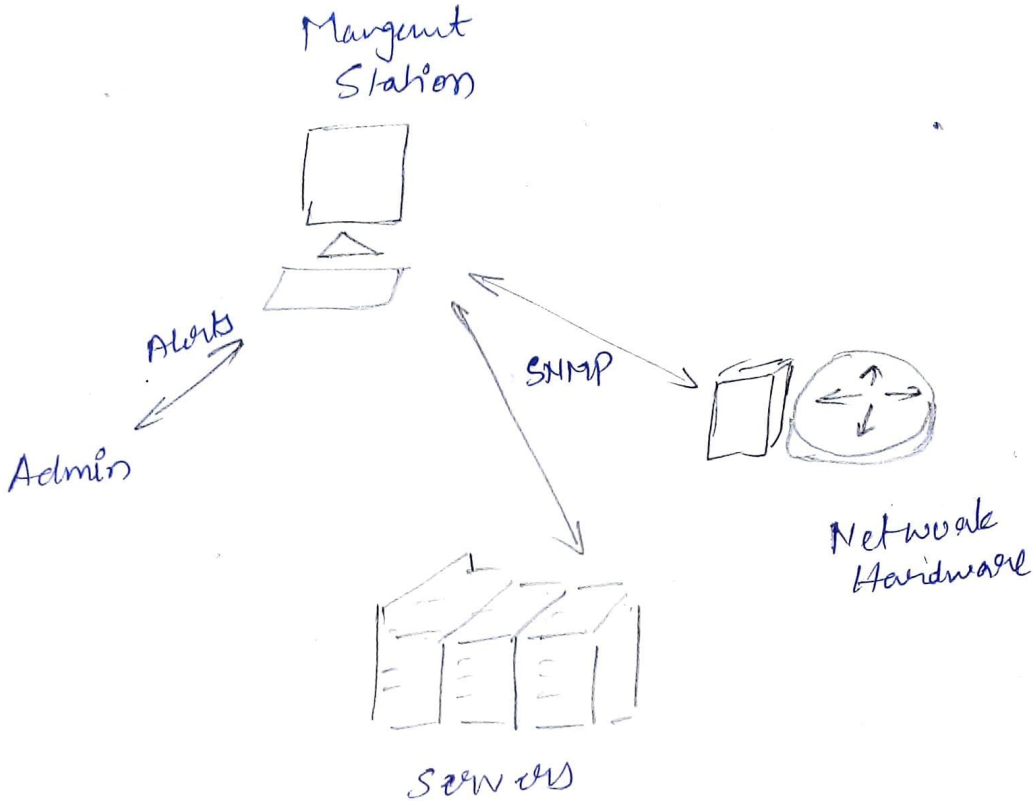
~ Most mangement stations will poll the network for information regularly.

~ They have both simple and complex configuration softwared.

~ Secondaly, the object to be monitored must haven an ajent running.

~ It collects information and sends it the monitoring station when polled.

~ Ajents can also send notification to the managemd stations in case any error has occured (even without being polled).



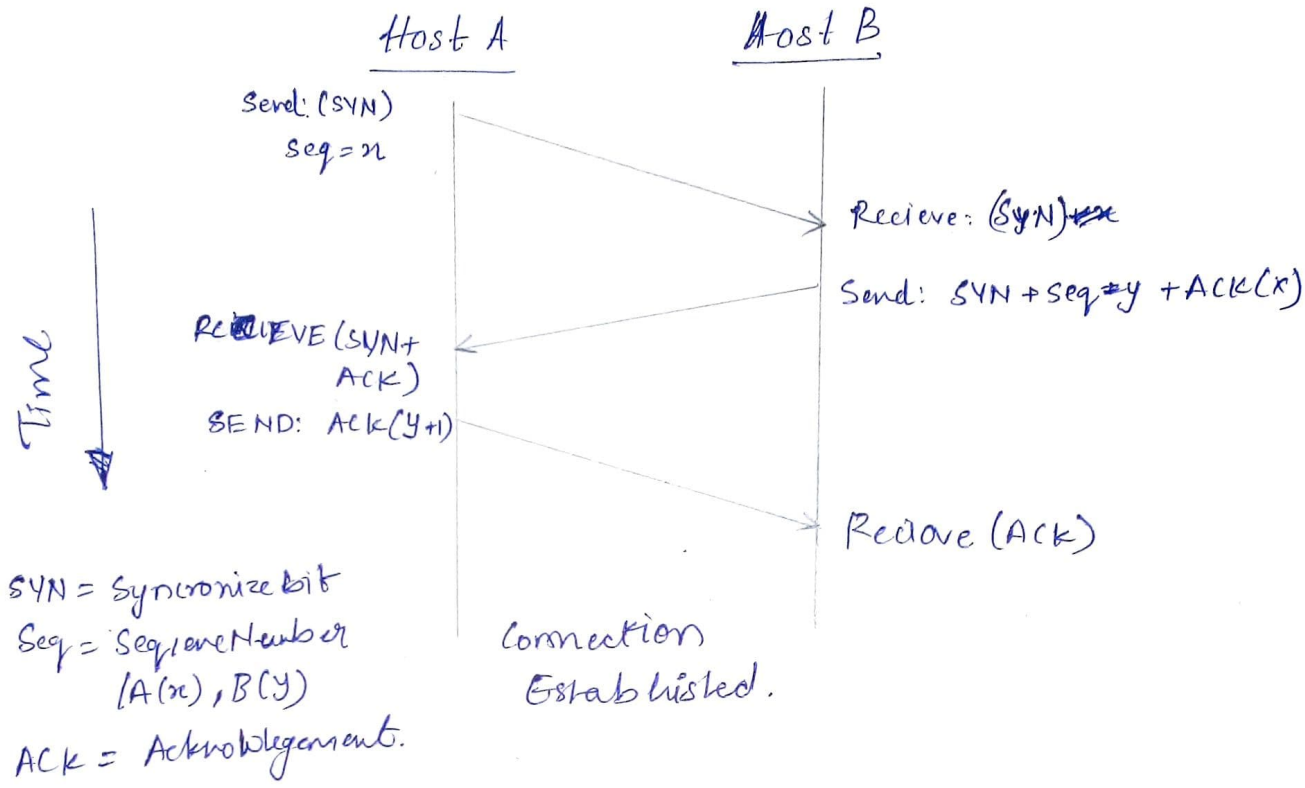
A.9) Diffent Phases of TCP transmission.

- TCP provides connection oriented services which means that there are three phase of the whole communication.

1. Connection Establishment

- Host A initials a connection
- It send as TCP segmut with SYN (control bit) & intial sequence number = x.
- Host B receives it and replies.
- It sends bas a TCP segmut with its own sequme number y and acknoledgment.

~ Next, A recives this and sends as ACK noledgment fining the connection establishment stage with a three-way handshake:



2. Data Transfer

~ After connection establishment Host A & B are free to transmit and receive data through this virtual connection.

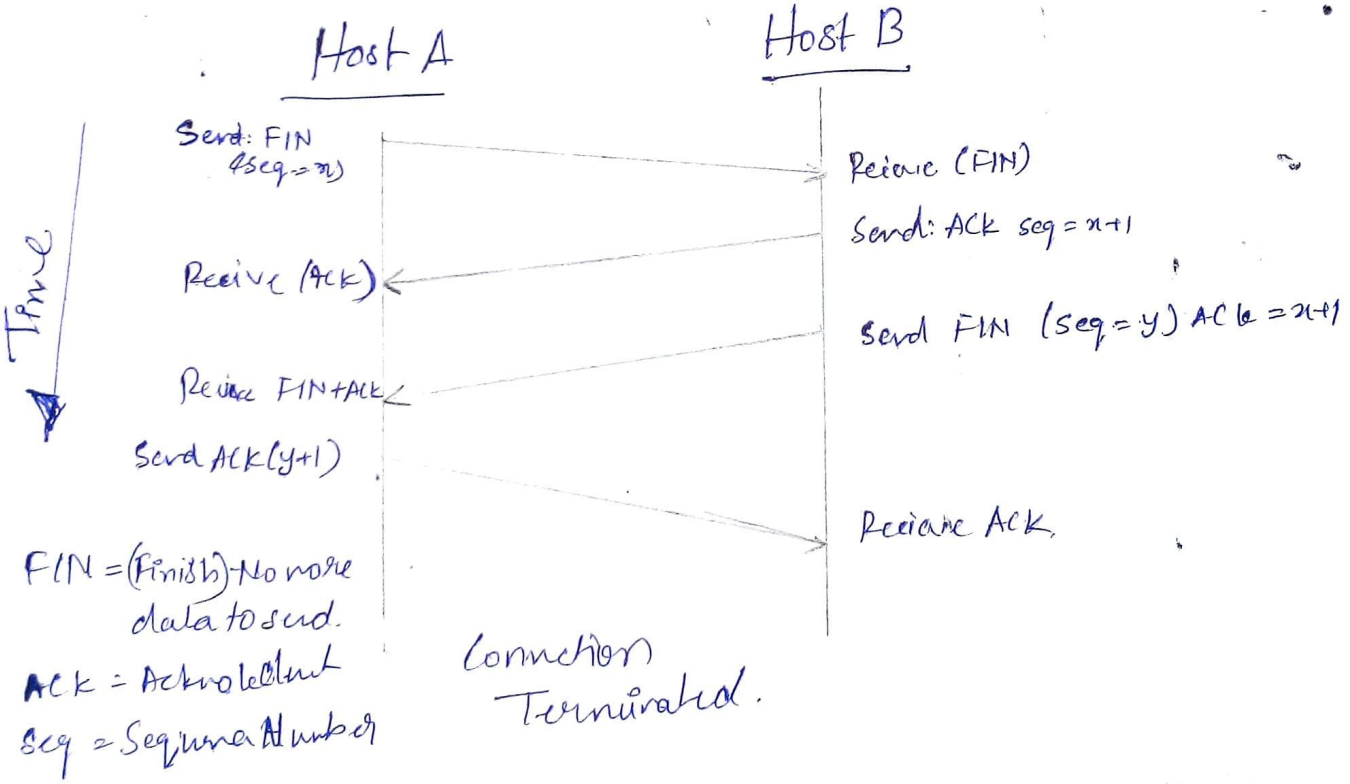
~ If the recive recived correct or error free segment it respond with positive signal

~ TCP will be idle if no data is send or recived.

~ The send is halted if the reciver's buffer size is exceeded.

3. Connection Termination

- This is the final phase of data transfer where the Host A signal a TCP close signal.
- When host B reiud the FIN (bit) from A it sends aiid acknoledgmd and notifies ib own application of the closing conction.
- Hosta again responds with a final acknoledgut indicating the end of virtual connection.



A8) Name - Address Resolution Techniques

- Mapping a domain name to ai IP-address is known as Name address resolution.

~ The domain-name server resolver perform the operation by consulting the name servers.

~ In order to find a particular DNS the requesting host passes the query to the local DNS server.

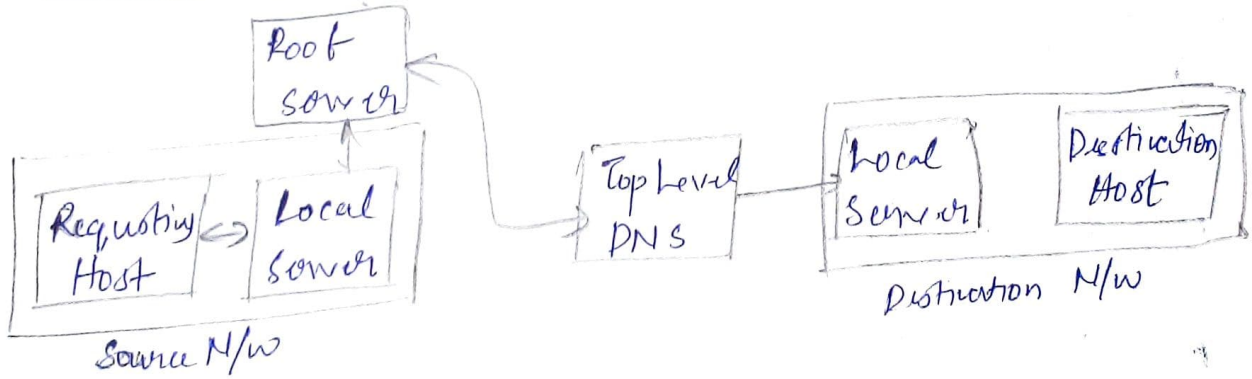
~ It does so with a mapping request.

~ If it has the information the resolver is satisfied otherwise the resolver is refered to other servers to obtain information.

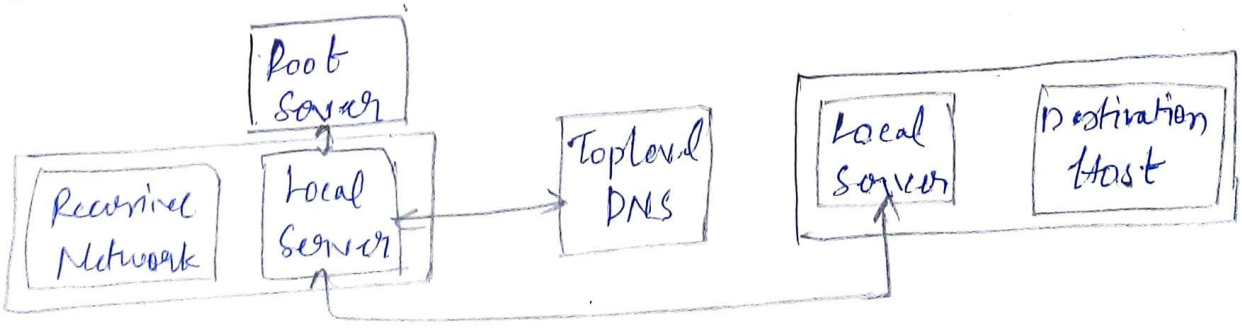
~ This also checks for the correctness of the information.

- The two types of resolver are

(i) Recursive Resolution



(ii) Iterative Resolution



~ Both recursive and iterative servers utilize cache to store the ~~the~~ relive domain-names.

A 7.) Transport Layer

- Transport layer is the layer in the open system interconnection (OSI) model responsible for end-to-end communication over a network.

~ It provides a logical communication channel between application process running on diff hosts.

~ It is also responsible for the managent of error correction too.

~ Following are some of the fuctions performed by the tcp.

1. Addressing / Multiplexing: TCP is multiplexing data received from diff process so that they can be send using the underlying network protocol

2. Connection Managent : TCP provides connection oriented services, therefore it is mandatory for the transport layer protocol is establish and demolish a connection.

3. Data Handling : TCP conceptually is equipped for data transmission and mechanisms to share

data across multiple layers.

4) Flow control : TCP allows the flow of data between two devices to be controlled and managed. It also includs featur to deal with congestion.

5.) Provids reliabilty and QoS: It includ a set of features that alows an applution to send data in a ~~con~~ reliable facion.

TCP vs UDP

TCP	UDP
~ Transmissi Control Protol	~ User Datagram Protocol
~ Connection-oriented services.	~ Connection less services
~ Reliable and guarinteed delivary of data	~ unreliable and guaranteed delivary of data is not provided.
~ Provids good error checking mecanism	~ Does not provided quality error checking mecanism.
~ Overhead of conction-establishment & termination	~ No overhed of whatsover.
~ Retransmisi of lost packes is possible	~ Retransmission lost pakets is not possible.

A6.)

~ Autonomus systems are defineds are a collection of routers that have similar routing table infootion defind as the boundary. line fom routing protocol.

~ The process of transfer of infondtion betwen the neighbowring routes - is the routing upate muanism.

~ Various routing protocols have varius time intorcal.

~ Thus routing upates contain infouidtion of routing protocols suches, anubers of autonom sysems, admistrative distances, matrix vales and intuface details.

~ Border Gateway Protocol (BGP) is an Exterior Gatway Routing protocol designd to exchare rowting and reachable infondon amon autonows systems.

~ It makes routing discios basdon paths, network policies or rule sents configurd by a network admin.

~ This is a path vector protowol involved in routing decisions.

~ Border gate way Protocol or BGP in short enables routers to comicate diffent types of messages but at the same time prevents or avoids routing loops.

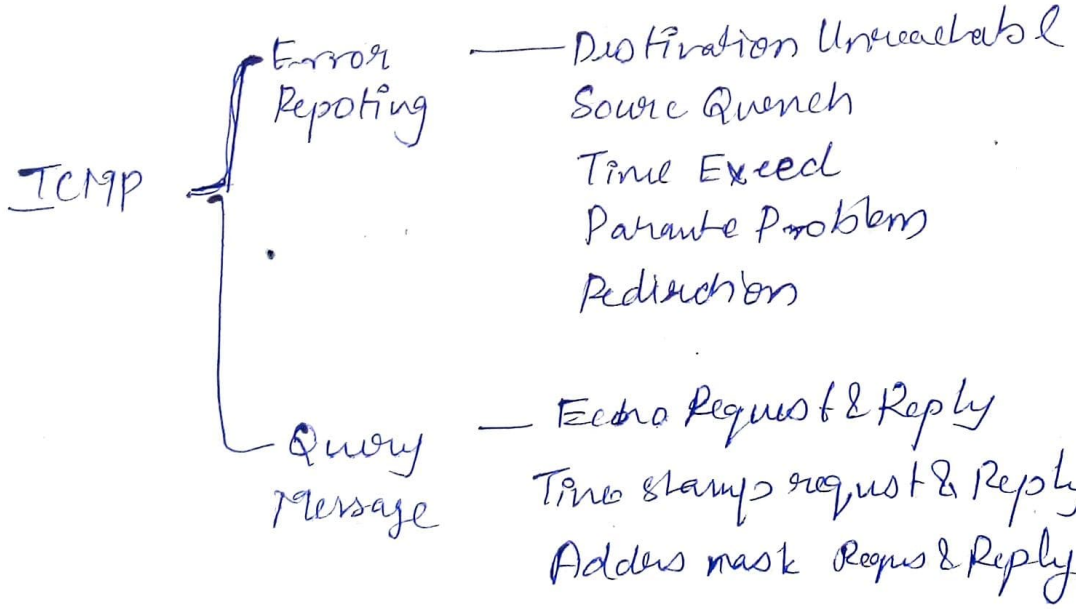
~ BGP does not detect conjection in networks and is weak in load balancing

~ Further since being a path vector protocol and its such deep integration in the network (even to the core) leaves the network vulnerable.

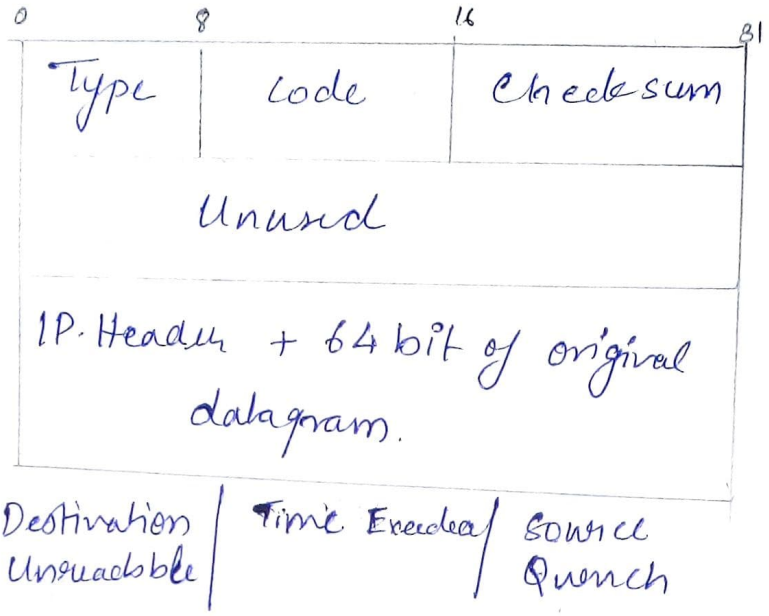
A5.) ICMP Message Formats

~ ICMP (Intercontrol Message Protocol) provides error control.

~ It suppors many fonats and queries.



(1) Message format of Error Reporting Message

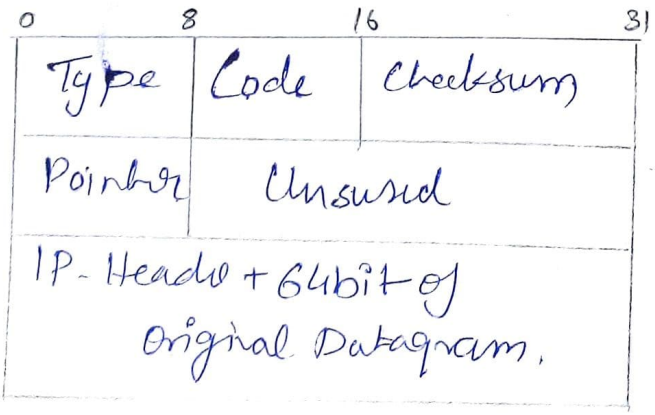


Destination Unreachable | Time Exceed | Source Quench

- Destination Unreachable : The data sent to the destination does not reach the destination for some Reason.

- Source Quench – The sender is fast causing congestion in the network – asks to reduces speed.

- Time Limit Exed – The no. of hops to the destination has crossed its maximum value and the msg is sent back to the sender.

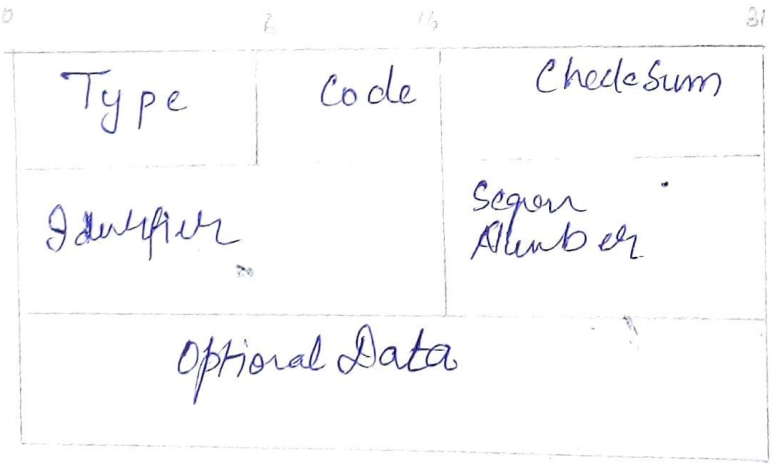


~ Parameter Problem – The calculated checksum mismatch the original checksum the data is corrupt.

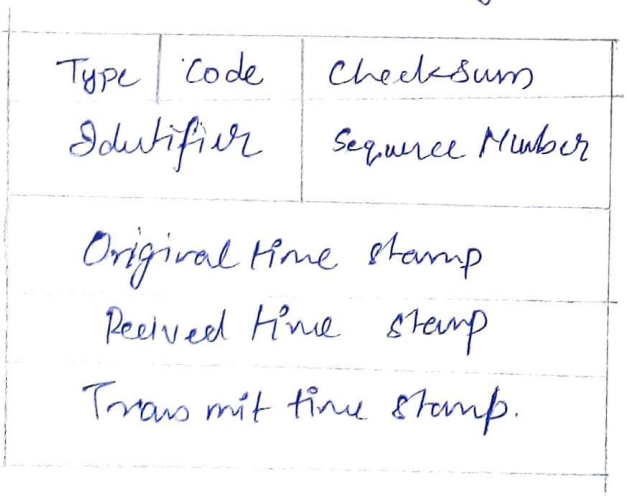
~ Redirection – The packet is sent through a better route to the destination.

(ii) Query Messages

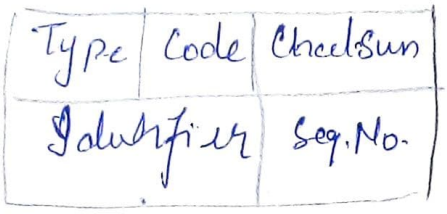
- Echo Request and Reply – To check if devices is online or not we send "echo messages" and if it is online – it does echo reply.



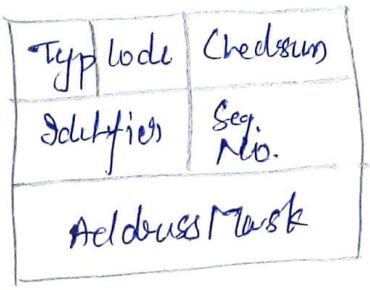
- Time Stamp Request & Reply – Helps in checking the performance of the network by sending & recieving the time stamped packets.



~ Addressmask Request or Reply ~ Used to find out the subnet addres of the destination network where the packets have to be sent.



Request



Reply.

A4.) BootP

~ The BOOTP uses UPP/IP protool.

- It is runs when a machine boots up.

~ The protocols allows diskless machine to discover their IP Address and address of the server host

~ BOOTP does not use the MAC Layer broadcas but uses the user datagram or internet protocol.

eg:- N Computing Suits - are diskless network computs which requires just a monitor keyboard and mouse.

~ When this device boots up it checks for server on its network.

~ But if the server are on a diff'ent networks it podls the router to provide infomations about the server.

~ The router the gives up the conction details.

~ Bout unlikik DHCP bootp requir manal re-configuration with the obtained infonation to ~~a re~~ connect to a remoite server.

A3.) Given:

~ IP Addars (Class C): ~~195.1.1.0~~ 195.1.1.0

~ The requirint is 10 subnets & 12 hosts (atmax)

~ Since we requiar 10 subnets we ~~cannot~~ cannot can take 3 bits — which will ~~only~~ only provide $2^3 = 8$ subnet ~~host~~

~ But if we take 4-bits - then there will be $2^4 = 16$ subnets which exceeds the requirement (of host)

~ The subnetting will beas

195.1.1.0

11000011.0000 0001.0000 0001.0000 0000

1111 1111.1111 1111.1111 1111.1111 0000

255 . 255 . 255 . 240

∴ The required subnet mask will be : 255.255.255.0

⇒ 195.1.1.0 / 28 (28 = 24+4).

∴ The IP-subnet will be like

195.1.1.0 / 28
195.1.1.16 / 28
⋮
195.1.1.256 / 28

↓ (10+6) subnets with (12+4) hosts in each subnet

A.2.) Given:

Maximum rate of channel = M = 10 MBps

Token generation rate = ℓ = 2MBps

Maximum Bucket capacity = C = 16 MB (channel)

we know that

$$\text{Burst Length } S = \frac{C}{M - \ell}$$

⇒ "~~Transient~~ Duration for transmission at full 10MBps is the burst length"

$$\Rightarrow S = \frac{16 \text{ MB}}{(10 - 2) \text{ MBps}} = 2s$$

∴ The maximum duration for which the computer can transmit at full 10MBps is 2s.

A1.) Quality of Service (QoS)

~ Quality of Service (QoS) refers to a network's ability to achieve maximum bandwidth and deal with other network profomance elemts.

~ It also involved controlling and managing network resources by setting priorities for specific types of data on network.

~ It is exclusive applied to network traffic geuratd for video on demand, IPTV, VoIP, streaming media etc.

~ There are few techniques to achieve good QoS.

1.) Over Provision
~ Providing high routing capability with large bandwidth and huge buffer space
~ It will be very costly.

2.) Buffering
~ Packs are buffer at the receiver side
~ It incurs delay and smooths out jitters
eg:- Buffing YouTube Videos

3.) Traffic Shaping

- This is a advanced mechanism to control the amount of data that is sent and received by the network.
- Here shaping affects both the sender's output and receiver's input.
- Whenever a connection is setup the user is agreed upon a certain traffic pattern — known as level agreement.
- Packet loss will occurs if the agreement is broken.
- There are mainly two algorithms to shape trafic

(i) Leaky Bucket Algorithm

- Used to determine whether some sequence of discreet events conforms to defined limits on their average frequency.

(ii) Token Bucket Algorithm

- Used to check that the data transmission conforms to certain defined limits on bandwidth and burstiness.