| Date | Day | Time | Paper Code | Paper Name |
|---|---|---|---|---|
| Dec 20, 2022 | Tuesday | 1:30 - 4:30 PM | TCS 703 | Computer Networks - II |

**NOTE - DM ME FOR NEXT SUBJECT'S ENJOY**
**Phone Number - 9627850233**

# MUST DO

## What is the remainder obtained by dividing $x^6+x^4+1$ by the generator polynomial $x^4+1$ and explain correcting single bit error using single bit parity?

**Explanation Video Link: 1 - HERE**
**Explanation Video Link: 2 - HERE**
A parity bit, also known as a check bit, is a single bit that can be appended to a binary string. It is set to either 1 or 0 to make the total number of 1-bits either even ("even parity") or odd ("odd parity").

The purpose of a parity bit is to provide a simple way to check for errors later. When data is stored or transferred electronically, it's not uncommon for bits to "flip" — change from a 1 to a 0, or vice versa. Parity checks can detect these errors. For example, to check a binary sequence with even parity, the total number of ones can be counted. If the number of ones is not even, an error is likely to have occurred.

## Explain RTCP and RTP packet header fields.

**Explanation Video Link: Part 1 - HERE**
**Explanation Video Link: Part 2 - HERE**

### RTCP Header fields

An RTCP packet is encapsulated in a UDP packet. Usually a UDP packet carries at least two RTP packets, and such a UDP packet is called a "compound RTCP packet.". The header fields present are:

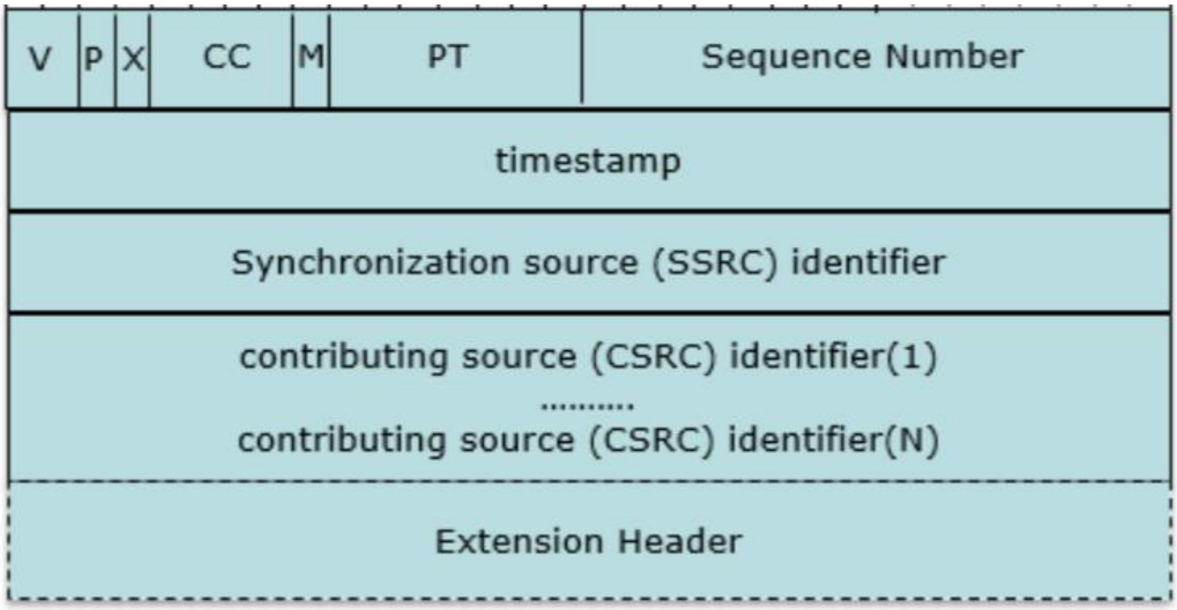
- **V**—2 bits, version number.

-

**P**—1 bits, padding flag.

- **RC**—5 bits, the number of receiving report blocks in the RTCP packet.
- **PT**—8 bits, RTCP packet type flag. This field is 200 for SR-type RTCP packets.
- **Length**—16 bits, length of the RTCP packet.
- **SSRC of Sender**—32 bits, SSRC of the sender.

## RTP Header fields


V
P
X
CC
M
PT
Sequence Number
timestamp
Synchronization source (SSRC) identifier
contributing source (CSRC) identifier(1)
..........
contributing source (CSRC) identifier(N)
Extension Header

- **Version field (V)** – This field specifies the protocol version.
- **Padded bits (P)** – P bit describes the padded bits used for the packet in the multiple of 4 bytes.
- **Extension header (X)** – X indicates the extension header present. Here the first word of extension header provides the length.
- **Contributing sources (CC)** – This CC field indicates the contributing sources from 0 to 15.
- **Marker bit (M)** – M in the header specifies the marker bit which is used in marking the beginning and end of the frame.
- **Payload Type (PT) -** Indicates the type of encoding currently being used.
- **Sequence number** – The sequence number shows the number of RTP packets delivered and it increases by one value each time a packet is sent.
- **Timestamp** – The timestamp field helps in reducing the jitter. It is generated by the stream’s source to recall when the first packet was generated.
- **Synchronization source identifier** – It provides the information about the packet to which stream it is associated.

-

- **Contributing source identifiers** – When the mixers are present in the studio this field is used where the mixer is the synchronizing source and streams going to be mixed are listed under this field.

# Role of SNMP.

Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).
The purpose of SNMP is to provide network devices, such as routers, servers and printers, with a common language for sharing information with a network management system (NMS).
SNMP's client-server architecture has the three following components:

- an SNMP manager;
- an SNMP agent; and

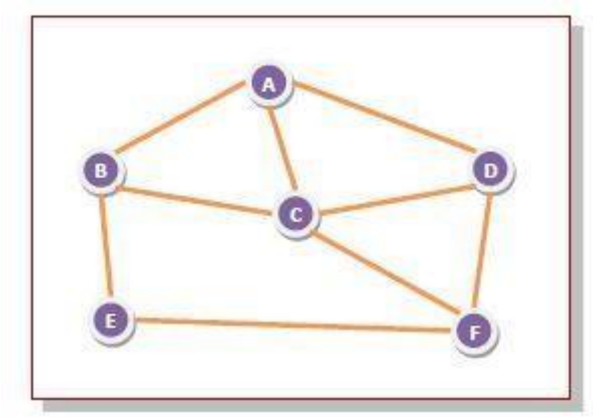
  a management information base (MIB).

The SNMP manager acts as the client, the SNMP agent acts as the server and the MIB acts as the server's database. When the SNMP manager asks the agent a question, the agent uses the MIB to supply the answer.
SNMP is so popular that most network devices come pre-bundled with SNMP agents. To make use of the protocol, however, network administrators must first change the default configuration settings of their network devices so SNMP agents can communicate with the network's management system.
SNMP is part of the original Internet Protocol (IP) suite as defined by the Internet Engineering Task Force (IETF). Multiple versions of the SNMP protocol exist. The most recent version, SNMPv3, includes security mechanisms for authentication, encryption and access control.

# Describe Shortest Path Algorithm and Explain Flooding.

**Explanation Video Link 1 - HERE**
**Explanation Video Link 2 - HERE**
Flooding is a non-adaptive routing technique following this simple method: when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on. For example, let us consider the network in the figure, having six routers that are connected through transmission lines.

-



Using flooding technique:

- An incoming packet to A, will be sent to B, C and D.
- B will send the packet to C and E.
- C will send the packet to B, D and F.
- D will send the packet to C and F.
- E will send the packet to F.
- F will send the packet to C and E.

## Types of Flooding

- **Uncontrolled flooding** − Here, each router unconditionally transmits the incoming data packets to all its neighbours.

**Controlled flooding** − They use some methods to control the transmission of packets to the neighbouring nodes. The two popular algorithms for controlled flooding are Sequence Number Controlled Flooding (SNCF) and Reverse Path Forwarding (RPF). • **Selective flooding** − Here, the routers don't transmit the incoming packets only along those paths which are heading towards approximately in the right direction, instead of every available paths.

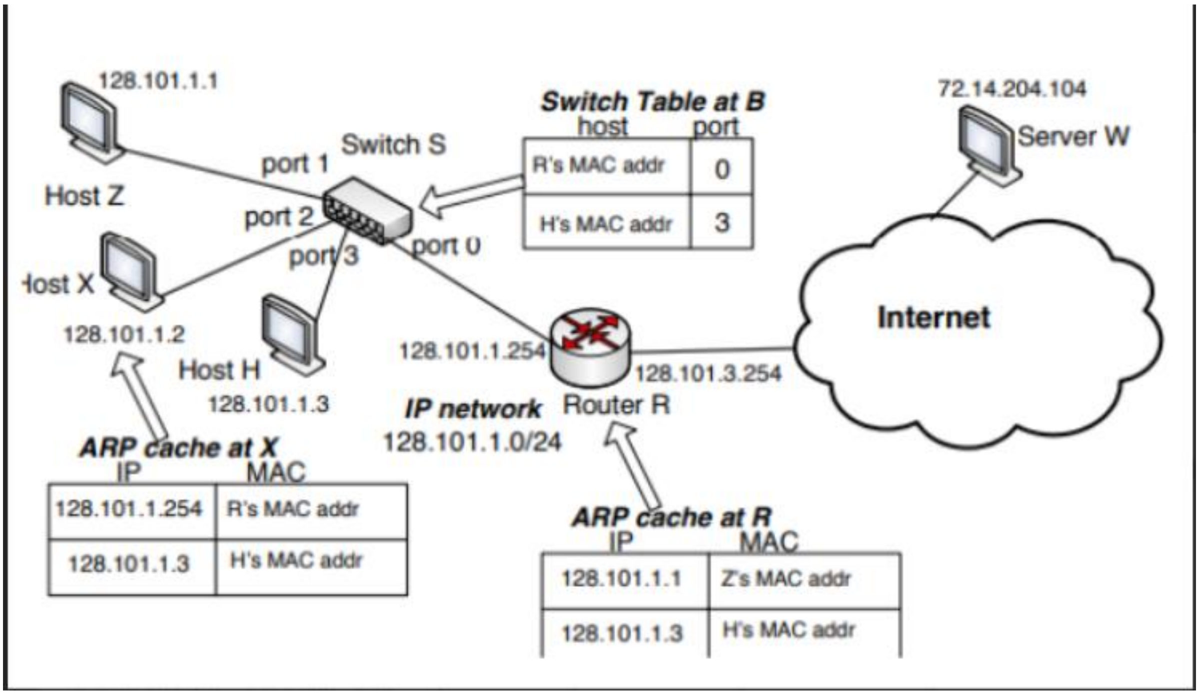
**Advantages** • It is very simple to setup and implement, since a router may know only its neighbours. • It is extremely robust. Even in case of malfunctioning of a large number routers, the packets find a way to reach the destination.

- All nodes which are directly or indirectly connected are visited. So, there are no chances for any node to be left out. This is a main criteria in case of broadcast messages.
- The shortest path is always chosen by flooding.

**Disadvantages**

- Flooding tends to create an infinite number of duplicate data packets, unless some measures are adopted to damp packet generation.
- It is wasteful if a single destination needs the packet, since it delivers the data packet to all nodes irrespective of the destination.
- The network may be clogged with unwanted and duplicate data packets. This may hamper delivery of other data packets.

-

- 

*Switch Table at B*

| host | port |
|---|---|
| R's MAC addr | 0 |
| H's MAC addr | 3 |

*ARP cache at X*

| IP | MAC |
|---|---|
| 128.101.1.254 | R's MAC addr |
| 128.101.1.3 | H's MAC addr |

*ARP cache at R*

| IP | MAC |
|---|---|
| 128.101.1.1 | Z's MAC addr |
| 128.101.1.3 | H's MAC addr |

**Consider the following switched network in the figure below, where we have one Ethernet switch S, connecting three hosts, host Z on port 1, host X on port 2 and host H on port 3, as well as an IP router R (default router for the host) on port 0. These hosts lie on an IP network with the network prefix 128.101.1.0/24. The IP address for the interface of router R that is connected to switch S is 128.101.1.254. The IP addresses for hosts Z,X and H are shown in the figure. Furthermore, the current switch(forwarding) table at switch S and the ARP caches at host X and router R are shown in the figure Suppose host H wants to send an IP datagram to host X, and assume that host H knows the IP address of host X (eg.**

## Via DNS lookup). Briefly explain how host H obtains the MAC address of host X. Describe how switch S handles the ARP request and response messages, and builds its switch table.

## What is TCP and UDP socket programming? Do the practice to write the coding TCP Client and Server application like parsing text and echo server, etc.

## List the types of messages used in SNMP. Explain.

Here are the type of messages used in SNMP:

- **GET Request:** Generated by the SNMP manager and sent to an agent to obtain the value of a variable, identified by its OID, in an MIB.
- **GETBULK Request:** Sent by the SNMP manager to the agent to efficiently obtain a potentially large amount of data, especially large tables.
- **GETNEXT Request:** Sent by the SNMP manager to the agent to retrieve the values of the next OID in the MIB's hierarchy.
- **INFORM Request:** An asynchronous alert similar to a TRAP but requires confirmation of receipt by the SNMP manager.
- **RESPONSE:** Sent by the agent to the SNMP manager, issued in reply to a GET Request, GETNEXT Request, GETBULK Request and a SET Request. Contains the values of the requested variables.
- **SET Request:** Sent by the SNMP manager to the agent to issue configurations or commands.
- **TRAP:** An asynchronous alert sent by the agent to the SNMP manager to indicate a

significant event, such as an error or failure, has occurred.

## Consider 15 Mbps link to Calculate the maximum frame rate a node on Ethernet.

# What does some of the physical network CRC errors means.

# What are Gatekeeper functions in H.323 network.

**Explanation Video Link - HERE**

A gatekeeper is a management tool for H.323 multimedia networks. Its primary functions are to convert phone numbers to IP addresses for VoIP and provide interoperability between different networks. Gatekeepers are available as either hardware devices or software applications, and are offered as proprietary products from a number of vendors, including Cisco and Symantec, or as freeware.

A single gatekeeper controls interactions for each zone, which comprises the terminals, multipoint control units (MCU), and gateways within a particular domain. Although the gatekeeper is an optional component, when it is included, it becomes the central administrative entity.

Depending on the demands of the specific network, the gatekeeper oversees authentication, authorization, telephone directory and private branch exchange (PBX) services, as well as call control and routing. Other functions may include monitoring the network for load balancing and real-time network management applications, intrusion detection and prevention and providing interfaces to legacy systems.

**A gatekeeper provides a variety of functions. Required functions include:**

- **Address translation.** The gatekeeper translates telephone numbers and H.323 IDs to endpoint IP addresses.
- **Admission control.** The gatekeeper an endpoint's admission into the H.323 network.
- **Bandwidth control.** The gatekeeper manages endpoint bandwidth requirements.
- **Zone management.** The gatekeeper manages the zone for all registered endpoints in that zone.

**A gatekeeper may also provide these optional functions:**

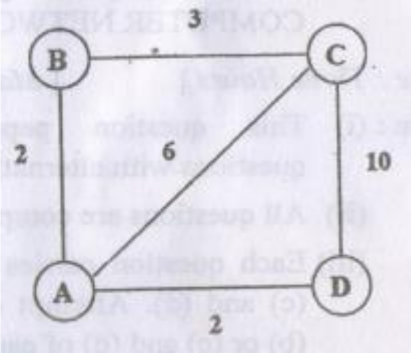
- **Call security.** A gatekeeper might authenticate and authorize calls.
- **Call management.** The gatekeeper keeps information about the state endpoints to indicate when they are busy or to redirect calls.
- **Bandwidth management.** When the required bandwidth is not available for a call, the gatekeeper can reject admission.
- **Call control signaling.** The gatekeeper can reroute a call so that endpoints communicate directly.

## Enumerate Secure socket layer and Token passing protocol. Briefly explain?

**Explanation Video Link: 1 - [HERE](#)**
**Explanation Video Link: 2 - [HERE](#)**

## Justify? How SIP registrar different from that of a home agent in mobile IP?

## Consider the network below with the given link costs. Find the routing table at B after running the DV routing algorithm.

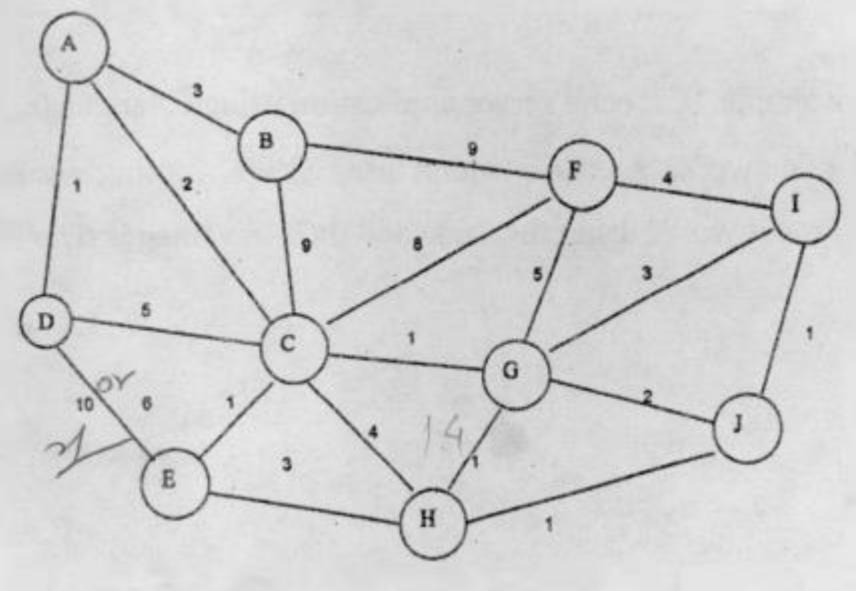


## OR

## Consider the three node topology, the link cost are c (x, y) = 4, c (y, z) = 5, c (z, x) = 2, compute the distance tables after the initialization step and after each iteration of a synchronous version of the distance-vector algorithm.

**Explanation Video Link 1 - HERE**
**Explanation Video Link 2 - HERE**
**Explanation Video Link 3 - HERE**

## Consider the following network. With the indicated link costs, use LS algorithm to compute the shortest path from ‘A’ to all network nodes. Show the result in the tabular format:



**Explanation Video Link 1 - HERE**
**Explanation Video Link 2 - HERE**
**Explanation Video Link 3 - HERE**

## How is RTSP similar to HTTP? Does RTSP have methods like GET & PUT as in HTTP? Can HTTP be used to request a stream? Justify.

RTSP is an application-layer protocol used for commanding streaming media servers via pause and play capabilities. It thereby facilitates real-time control of the streaming media by communicating with the server — without actually transmitting the data itself. Rather, RTSP servers often leverage the Real-Time Transport Protocol (RTP) in conjunction with the RealTime Control Protocol (RTCP) to move the actual streaming data.
While similar in some ways to HTTP, RTSP defines control sequences useful in controlling multimedia playback. While HTTP is stateless, RTSP has state; an identifier is used when needed to track concurrent sessions. Like HTTP, RTSP uses TCP to maintain an end-to-end

connection and, while most RTSP control messages are sent by the client to the server, some commands travel in the other direction (i.e. from server to client).

RTSP uses the following commands, typically sent from the client to the server, when negotiating and controlling media transmissions:

- **Options:** This request determines what other types of requests the media server will accept.
- **Describe:** A describe request identifies the URL and type of data.
- **Announce:** The announce method describes the presentation when sent from the client to the server and updates the description when sent from server to client.
- **Setup:** Setup requests specify how a media stream must be transported before a play request is sent.
- **Play:** A play request starts the media transmission by telling the server to start sending the data.
- **Pause:** Pause requests temporarily halt the stream delivery.
- **Record:** A record request initiates a media recording.
- **Teardown:** This request terminates the session entirely and stops all media streams.
- **Redirect:** Redirect requests inform the client that it must connect to another server by providing a new URL for the client to issue requests to.

HTTP Streaming is a push-style data transfer technique that allows a web server to continuously send data to a client over a single HTTP connection that remains open indefinitely. Technically, this goes against HTTP convention, but HTTP Streaming is an efficient method to transfer all kinds of dynamic or otherwise streamable data between the server and client without reinventing HTTP.

# What are RTP and RTCP ? Discuss their roles in Video conferencing. Discuss RTP packet header fields. How are RTP and RTCP packets (as part of the same session) distinguished?

The **RTP (Real-Time Transport Protocol)** resides in the presentation and session layers of the OSI network model. It is mostly used for real-time applications such as internet radio, video-on-demand, music-on-demand, video conferencing where the VOIP is implemented. It works on the UDP protocol instead of TCP, as a result, it does not ensure the timely delivery of the data.
It transfers the multimedia applications such as more than one stream of audio, text, video, are inserted into RTP library present at the user space along with other application. The library then multiplexes the streams by encoding them into RTP packets, which it packs into sockets. UDP packet is then created at the operating system side of the socket to enclose the RTP packets.
The **RTCP (Real-time Transport Control Protocol)** is companion protocol of the RTP protocol (also known as sister protocol) and defined along with RTP. It is an integral part of

the RTP protocol which offers the required control functionality to the RTP such as feedback, synchronization and user interface.

The RTCP permits senders and receivers to transfer a sequence of reports to one another containing the supplementary information about the data being transferred and the performance of the network. RTCP messages are also encapsulated inside a UDP packet for the transmission and are sent according to protocol number which is greater than the port number of the RTP stream to which they are associated.

### RTP Header

- **Version field** – This field specifies the protocol version.
- **Padded bits** – P bit describes the padded bits used for the packet in the multiple of 4 bytes.
- **Extension header** – X indicates the extension header present. Here the first word of extension header provides the length.
- **Contributing sources** – This CC field indicates the contributing sources from 0 to 15.
- **Marker bit** – M in the header specifies the marker bit which is used in marking the beginning and end of the frame.
- **Sequence number** – The sequence number shows the number of RTP packets delivered and it increases by one value each time a packet is sent.
- **Timestamp** – As we have discussed timestamp above in the article, the timestamp field helps in reducing the jitter. It is generated by the stream's source to recall when the first packet was generated.
- **Synchronization source identifier** – It provides the information about the packet to which stream it is associated.
- **Contributing source identifiers** – When the mixers are present in the studio this field is used where the mixer is the synchronizing source and streams going to be mixed are listed under this field.

## What does Session Initiation Protocol (SIP) do ? Discuss the role of SIP registrars and SIP proxies. How is the role of an SIP registrar different from that of a. home agent in mobile IP? If Alice is making a voice call to Bob@gmail.com and the same is used to make SIP calls explain how does Alice obtain the IP address of the device Bob is currently using?

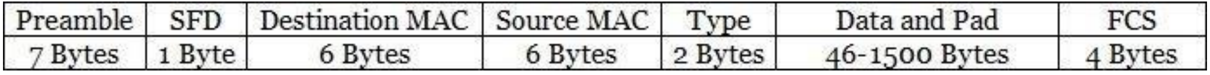
**Explanation Video Link - HERE**

| BASIS FOR COMPARISON | RTP | |
|---|---|---|
| Basic | Used to carry media streams. | Used to monitoring t |
| Ports | Even port number | Odd port number |
| Relation | Specifies the packet structure for real-time data. | Works in conjunction |
| Features provided | Interoperability | Performance controll |
| Packets contain | Payload type, sequence number, timestamp, etc. | Sender and receiver r |
| Identification of source | 32-bit identifier is used | Textual information |

# Explain all the fields present in “Ethernet Frame Structure”.

An Ethernet frame starts with a header, which contains the source and destination MAC addresses, among other data. The middle part of the frame is the actual data. The frame ends with a field called Frame Check Sequence (FCS).

The Ethernet frame structure is defined in the IEEE 802.3 standard. Here is a graphical representation of an Ethernet frame and a description of each field in the frame:



| Preamble | SFD | Destination MAC | Source MAC | Type | Data and Pad | FCS |
|---|---|---|---|---|---|---|
| 7 Bytes | 1 Byte | 6 Bytes | 6 Bytes | 2 Bytes | 46-1500 Bytes | 4 Bytes |

- **Preamble** – informs the receiving system that a frame is starting and enables synchronisation.
- **SFD (Start Frame Delimiter)** – signifies that the Destination MAC Address field begins with the next byte.
- **Destination MAC** – identifies the receiving system.
- **Source MAC** – identifies the sending system.
- **Type** – defines the type of protocol inside the frame, for example IPv4 or IPv6.
- **Data and Pad** – contains the payload data. Padding data is added to meet the minimum length requirement for this field (46 bytes).
- **FCS (Frame Check Sequence)** – contains a 32-bit Cyclic Redundancy Check (CRC) which allows detection of corrupted data.

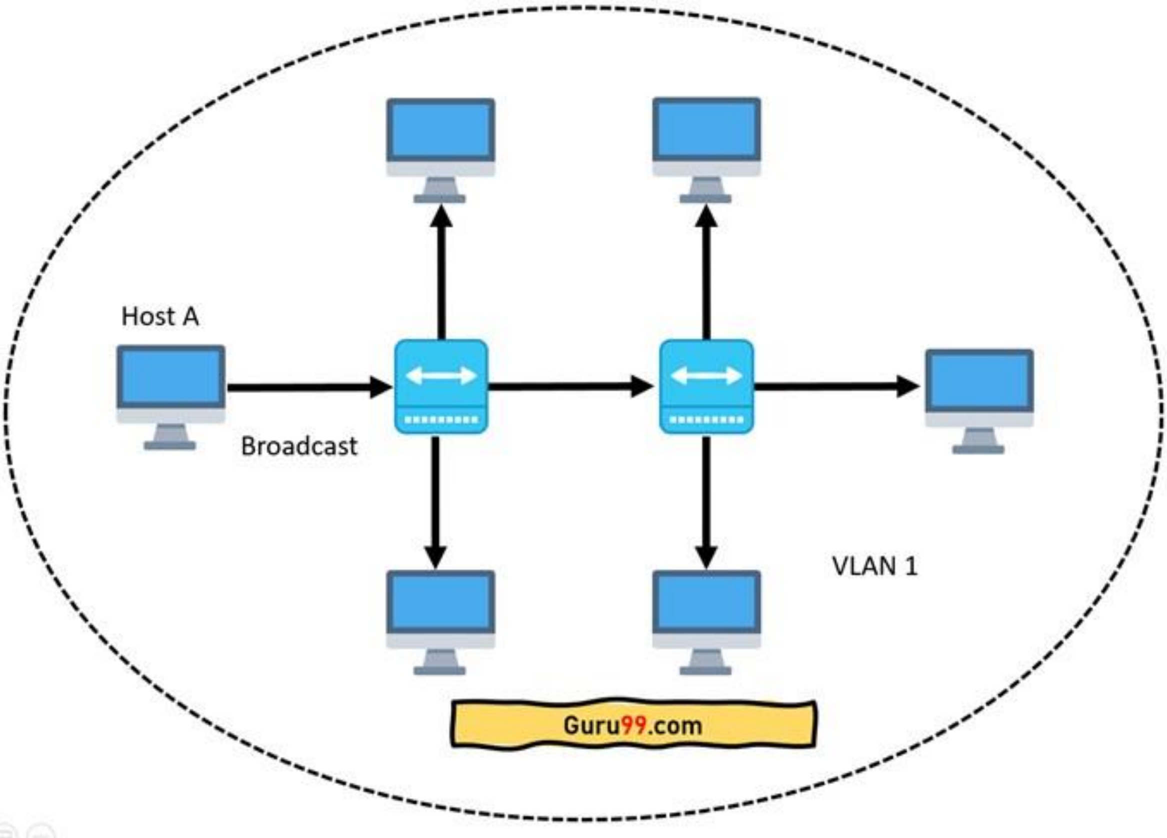
The FCS field is the only field present in the Ethernet trailer. It allows the receiver to discover whether errors occurred in the frame. Note that Ethernet only detects in-transit corruption of data – it does not attempt to recover a lost frame. Other higher level protocols (e.g. TCP) perform error recovery.

# Discuss in detail the concept of VLAN using neat figure.

**Explanation Video Link - HERE**

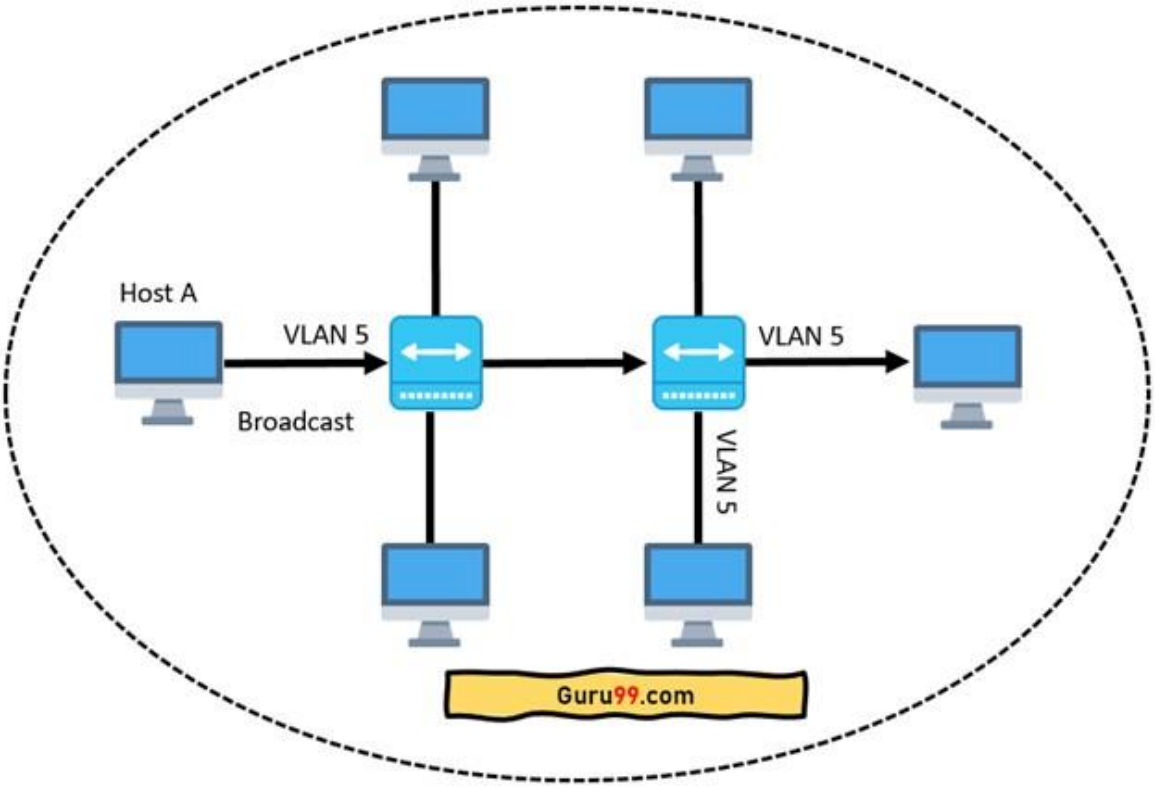
**VLAN** is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

The below topology depicts a network having all hosts inside the same virtual LAN:



Without VLANs, a broadcast sent from a host can easily reach all network devices. Each and every device will process broadcast received frames. It can increase the CPU overhead on each device and reduce the overall network security.

In case if you place interfaces on both switches into separate VLAN, a broadcast from host A can reach only devices available inside the same VLAN. Hosts of VLANs will not even be aware that the communication took place. This is shown in the below picture:



# Explain the RSA algorithm as used in cryptography. Provide steps involved in RSA algorithm, choose p=3 & q=11, & encode the word "hello." Apply the decryption algorithm to the encrypted version to recover the original plain-text message.

# Discuss the different Firewall topologies.

**Explanation Video Link: Part 1 - HERE**
**Explanation Video Link: Part 2 - HERE**

Firewalls are deployed in different network locations, i.e. inside the network or at the perimeter, and they are used to protect different devices, i.e. clients or servers. Depending on where the firewall is deployed and what the firewall protects, the traffic profile seen by the firewall varies. **Types of firewalls**

- **Packet filtering firewall -** Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets; rather they compare each packet received to a set of established criteria, such as the allowed IP addresses, packet type, port number and other aspects of the packet protocol headers. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.

- **Circuit-level gateway** - Using another relatively quick way to identify malicious content, circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered trusted. They don't inspect the packets themselves, however.
- **Application-level gateway** - This kind of device -- technically a proxy and sometimes referred to as a proxy firewall -- functions as the only entry point to and exit point from the network. Application-level gateways filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by other characteristics, such as the HTTP request string. While gateways that filter at the application layer provide considerable data security, they can dramatically affect network performance and can be challenging to manage.

# What do you understand by Adaptive Streaming? Discuss the DASH technique.

Adaptive bitrate streaming is a method for improving streaming over HTTP networks. The term “bitrate” refers to how quickly data travels across a network and is often used to describe an Internet connection speed. A high-speed connection is a high-bitrate connection. Streaming — or the process that makes watching videos online possible — consists of transmitting video files hosted in a remote server to a client. In streaming, videos are segmented into smaller clips so viewers do not need to wait for an entire video to load before they can begin watching it.

First, multiple versions of video files are created and encoded to fit a variety of network conditions. Then, based on factors like bandwidth and device type, the video player selects the highest-quality file that the device can play with the smallest amount of buffering possible. This allows playback to be as smooth as possible for end users around the world, regardless of their device or Internet speed.

Adaptive bitrate streaming offers many benefits that can improve video quality:

- **Widening access:** Without adaptive bitrate streaming, viewers with slower connections or certain devices would never be able to see some videos.
- **Improving the user experience:** Adaptive bitrate streaming decreases buffering, so users experience fewer frustrating loading delays.
- **Enabling mobile viewing with fewer interruptions:** Streaming on mobile devices has increased by 1,000% since 2012, so optimizing for mobile streaming is critical. When a viewer streams mobile video content while moving from place to place, bitrate can vary widely on a single device. For example, connection strength on a home WiFi network may be stronger than a connection on a train or in a shopping mall. By continuously adjusting to changing conditions, adaptive bitrate streaming can minimize disruptions for mobile viewers.

Dynamic Adaptive Streaming over HTTP (DASH), also known as MPEG-DASH, is an adaptive bitrate streaming technique that enables high quality streaming of media content over the Internet delivered from conventional HTTP web servers. Similar to Apple's HTTP Live Streaming (HLS) solution, MPEG-DASH works by breaking the content into a sequence of small segments, which are served over HTTP.

MPEG-DASH is the first adaptive bit-rate HTTP-based streaming solution that is an international standard.[7] MPEG-DASH should not be confused with a transport protocol — the transport protocol that MPEG-DASH uses is TCP. MPEG-DASH uses existing HTTP web server infrastructure that is used for delivery of essentially all World Wide Web content. It allows devices like Internet-connected televisions, TV set-top boxes, desktop computers, smartphones, tablets, etc. to consume multimedia content (video, TV, radio, etc.) delivered via the Internet, coping with variable Internet receiving conditions.

## Given the dataword 1010011010 and the divisor 10111 (using CRC) :

- **Show the generation of the codeword at the sender site.**
- **Show the checking of the codeword at the receiver site (assume no error)**

## Describe CSMA/CD as specific to Ethernet.

**Explanation Video Link - HERE OR**
**Explanation Video Link 1 - HERE**
**Explanation Video Link 2 - HERE**
The **Carrier Sense Multiple Access/ Collision Detection** protocol is used to detect a collision in the media access control (**MAC**) layer. Once the collision was detected, the CSMA CD immediately stopped the transmission by sending the signal so that the sender does not waste all the time to send the data packet. Suppose a collision is detected from each station while broadcasting the packets. In that case, the CSMA CD immediately sends a jam signal to stop transmission and waits for a random time context before transmitting another data packet. If the channel is found free, it immediately sends the data and returns it. **Advantages of CSMA CD:**

1. It is used for collision detection on a shared channel within a very short time.
2. CSMA CD is better than CSMA for collision detection.
3. CSMA CD is used to avoid any form of waste transmission.

4. When necessary, it is used to use or share the same amount of bandwidth at each station.
5. It has lower CSMA CD overhead as compared to the CSMA CA.

**Disadvantage of CSMA CD**

1. It is not suitable for long-distance networks because as the distance increases, CSMA CD' efficiency decreases.
2. It can detect collision only up to 2500 meters, and beyond this range, it cannot detect collisions.
3. When multiple devices are added to a CSMA CD, collision detection performance is reduced.

# Discuss, the five different areas of Network Management as defined by International Organization for Standardization (ISO). Discuss the principal components of a network management architecture. What is the role of SNMP in network management?

the ISO defines five main types of network management solutions as the following:

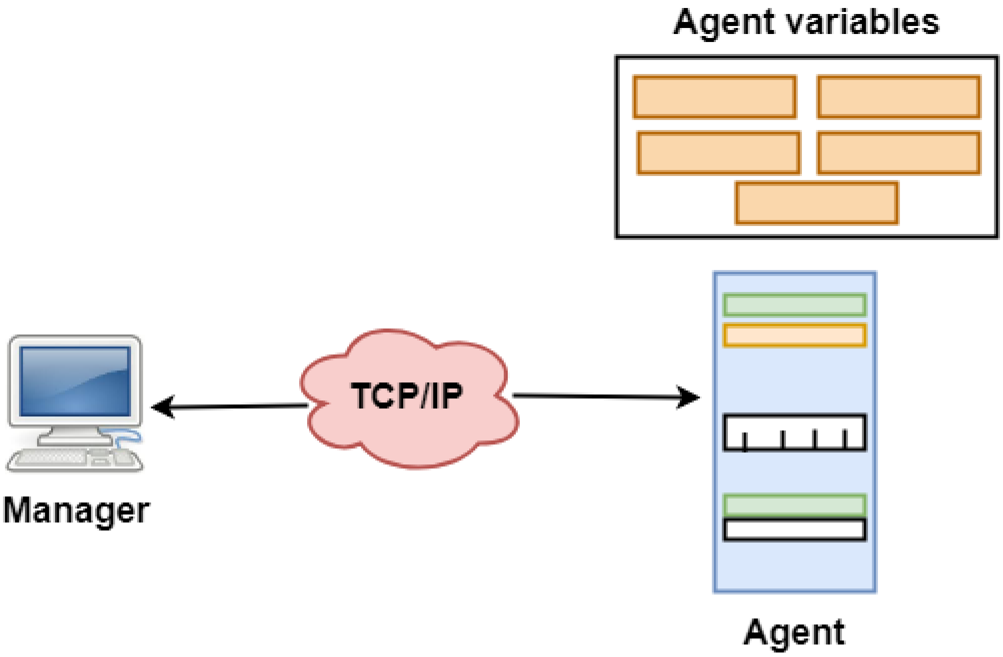
- **Performance Management**: Measure and monitor the different network components that impact the overall performance of your network.
- **Fault Management**: Detect, isolate, and correct any non-normal network conditions.
- **Configuration Management**: Monitor network configuration consistency, change control, and generate documentation to create redundancies and backup systems.
- **Accounting Management**: Regulate network resources and allocate costs by tracking actions on a user-by-user basis.
- **Security Management**: Prevent security and data breaches by analyzing security policies, security-related events, and access to network resources.

**Principal of a network management architecture**

- **Switches** – Switches connect devices, allowing them to communicate over the network. On-premise and cloud-based switches are the two main options. An onpremise switch requires a company/IT department to configure, maintain, and monitor the LAN, giving companies greater control over their network operations. For larger companies, this is completely feasible, but smaller companies may be better off using a cloud-based switch, where a cloud provider manages it, pushes updates, and provides a user interface.
- **Routers** – Routers connect networks and devices on the networks to the Internet. This means instead of each device having a direct connection, multiple devices, via the router, share one Internet connection. A router also determines the best route for data transmission by analyzing other data traveling over the network. The router has the power to prioritize certain computers. More complex routers allow consumers and companies to use a built-in firewall or VPN.

- **Wireless Access Points (WAPs)** – WAPs allow devices to connect to the Internet without a cable, making it easier to add multiple devices or move about within a building. Routers provide the initial bandwidth, but WAPs expand the covered area. Additionally, WAPs show data about connected devices, which can be used for security assessments.

SNMP stands for **Simple Network Management Protocol**. SNMP is a framework used for managing devices on the internet. It provides a set of operations for monitoring and managing the internet.



- SNMP has two components Manager and agent.
- The manager is a host that controls and monitors a set of agents such as routers.
- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

# Suppose Alice wants to send a message to Bob. Bob has a public-private key pair (KB+, KB-) and Alice has Bob's certificate. But Alice does not have a public, private key

**pair. Alice and Bob (and the entire world) share the saine hash function Ho(.).**

- **In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message ? If so, show how with a block diagram for Alice and Bob.**
- **Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.**

The answer is as follows:

- In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.
  - No, it is not possible
  - Without setting up a public-private-key pair, or a pre-shared secret, there is no way for Bob to verify that Alice was or had created the message.
- Is it possible to design a scheme that provides confidentiality for sending the message from (4 points) ○ Yes, it is possible. ○ The most straightforward way to provide confidentiality is for Alice to encrypt the message with symmetric key technology (such as DES or AES) and for

  Bob to decrypt the message on receipt (p706) ○ Alice encrypts her message with Bob's public key, and she sends the encrypted message to Bob's e-mail address. When Bob receives the message, he simply decrypts it with his private key.

**What is the difference between message confidentiality and message integrity? Consider Host A sending a message to Host B. Can you achieve Confidentiality without Message Integrity ? Can you achieve Integrity without Confidentiality ? Explain each of the case with proper figure and the cryptographic algorithms that can be used.**

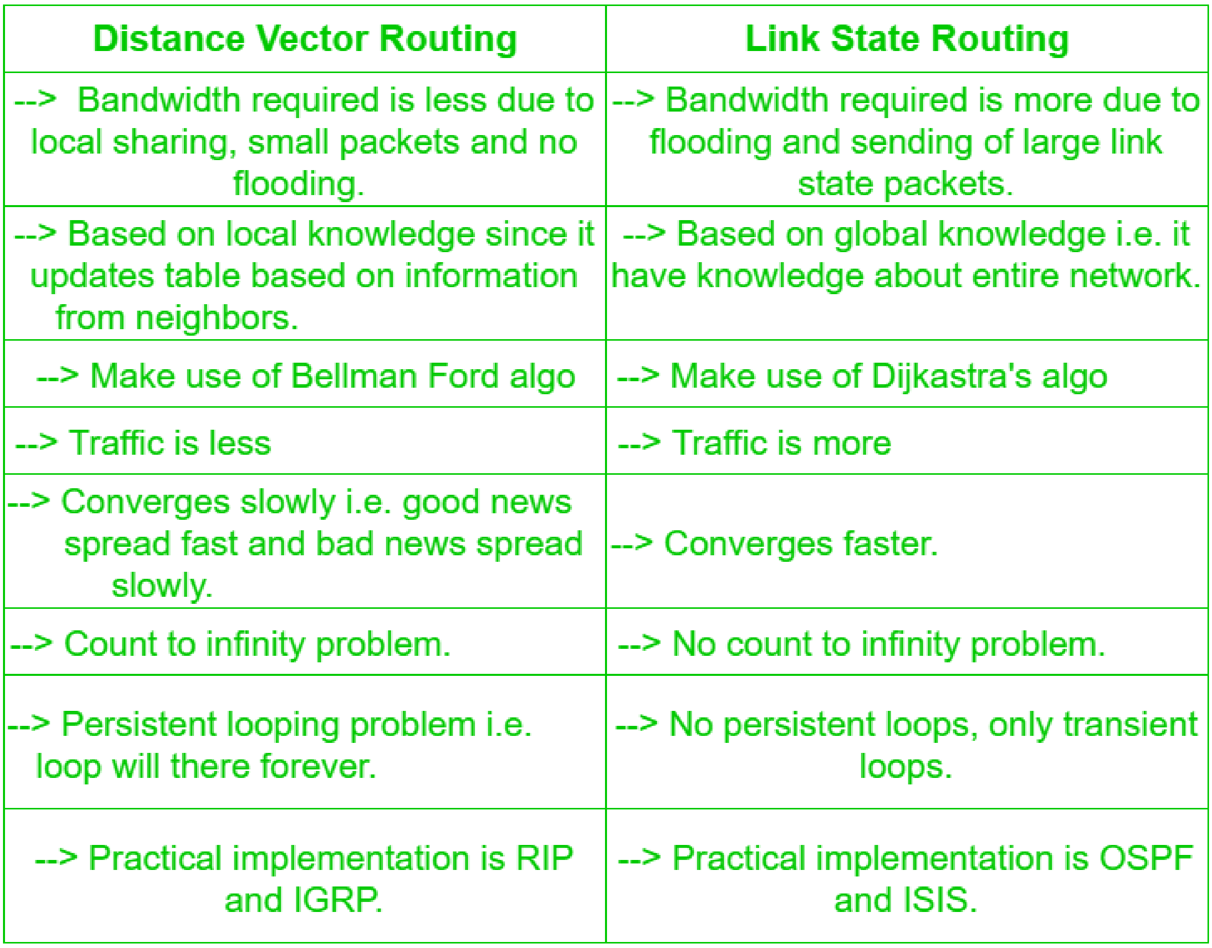
**Confidentiality**. Confidentiality means that the contents of the message are kept secret from unintended listeners. An unintended listener is typically going to be someone that is trying to eavesdrop on your messages, although it’s possible for the unintended listener to come from logging or other normal network monitoring. Confidentiality protects you from spying.

**Integrity**. Message integrity means that you have confidence that the message you received is the same as the one that the sender sent.

It’s possible to have confidentiality without integrity. Someone can hand you an encrypted message, and you can start changing bits in the message without knowing what those bits mean. Thus, the message could still remain confidential [as it is encrypted], but it has lost it’s integrity as the message has been tampered with.

Similarly, it’s possible to have integrity without confidentiality. You can transmit a message whose contents are in cleartext, but provide a tamper-resistant envelope for the message. Thus, the confidentiality of the message is non-existent [it is cleartext], but it cannot be tampered with [or traces of tampering shall be evident].

## Comparison of LS and DV.



| Distance Vector Routing | Link State Routing |
|---|---|
| --> Bandwidth required is less due to local sharing, small packets and no flooding. | --> Bandwidth required is more due to flooding and sending of large link state packets. |
| --> Based on local knowledge since it updates table based on information from neighbors. | --> Based on global knowledge i.e. it have knowledge about entire network. |
| --> Make use of Bellman Ford algo | --> Make use of Dijkastra's algo |
| --> Traffic is less | --> Traffic is more |
| --> Converges slowly i.e. good news spread fast and bad news spread slowly. | --> Converges faster. |
| --> Count to infinity problem. | --> No count to infinity problem. |
| --> Persistent looping problem i.e. loop will there forever. | --> No persistent loops, only transient loops. |
| --> Practical implementation is RIP and IGRP. | --> Practical implementation is OSPF and ISIS. |

# SHOULD DO

What is Socket and what does it consist of? Explain raise condition.

Design a simple TCP echo server application using C language.

Design a networks scenario which uses OSPF routing protocol and explain how it works using the same and their advantages over RIP.

Discuss the classification of routing algorithms . For each of the category provide the concept and names of typical algorithms.

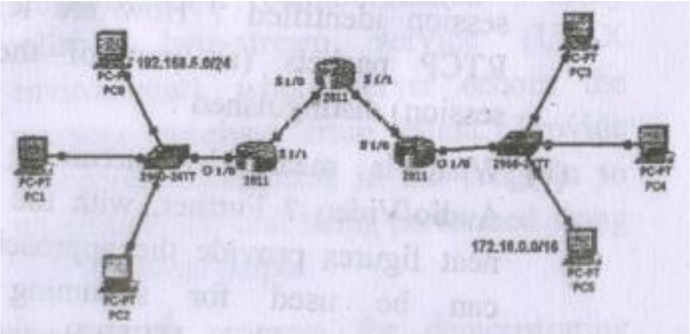
Why do you think the networks are arranged in hierarchical order ? Provide a typical figure showing the hierarchical organization of network and provide the details of protocols used in brief.

A large number of consecutive IP addresses are available starting at 198.16.0 .0. Suppose that four organizations, A, B, C and D, request 4000, 2000, 4000 and 8000 addresses, respectively and in that order . For each of these , give the first IP address assigned, the last IP address assigned and the mask in the w.x.y.zls notation.

Define and differentiate the following terms: Subnet, IP prefix and BGP route. Further explain, how does BGP use the NEXT-HOP and AS-PATH attribute?

Discuss in brief the services offered by Link Layer. Why is an ARP query sent within a broadcast frame ? Why is an ARP response sent within a frame with a specific destination MAC address?

Consider a network diagram given below:



- Identify all active devices based on the icons provided.
- Assign IP addresses to each of the active devices· (Refer given IP addresses and assume where these are not applicable).
- PCO from LANl intends to send data to PCS ofLAN2. Provide the steps how is the data sent and which of the addresses (Network layer Ethernet Layer) are used at each of the steps.

What is meant by streaming stored Audio/Video ? Further, with the help of neat figures provide the approaches that can be used for streaming stored audio/video using HTTP/Browser and Non- HTTP protocol.

What is the difference between end-to-end delay and packet jitter? What are the causes of packet jitter? Further, with the help of a neat figure explain, how can client overcome jitter?

Explain the concept of Client/Server Communication with the help of neat figure. Further, list out names of the functions required to be used by Server and Clients Programs for reliable communication (UNIX environment) and explain their task in brief.

Develop a program for demonstrating Client/Server communication using reliable bytestream service (UNIX environment), where server echoes. the message received from client. Provide appropriate comments in the program to understand the task being performed along with a typical output.

Develop a program for demonstrating Client/Server. communication using best effort datagram service (UNIX environment), where server echoes the message received from client. Provide appropriate comments in the program to understand the task being performed along with a typical output.

What does it mean to say that a nonce is a once-in-a-lifetime value ? In whose lifetime?

A sender has two data items to send 0 x 4668 and 0 x BB97. What is the value of the Internet checksum and how will receiver ensures that the received data items are error free.

Explain pure ALOHA and comment on its performance.

Switches are self-learning. Explain taking an example.
Describe how authentication can be achieved between two endpoints (say Alice and Bob) using public-key cryptography.

Calculate the maximum frame rate of a node on. an Ethernet LAN. Also calculate he maximum throughput of the link layer service provided by Ethernet. Assume 10 Mbps in both cases.

Consider building a CSMA/CD network running at 1 Gbps over a 1 km cable with no repeaters. The signal speed in the cable is 200000 km/sec. What is the minimum frame size?

A frame is m bits long and there is a bit error probability p. Suppose we can use an error correcting code that has an.overhead of 3 bits and can detect any errors and correct errors of up to 1 bit. What is the probability of a successful transmission ?

Explain the following with an example in relation to 'Providing Multiple Classes of Service in Multimedia Networking'. "It is desirable to provide a degree of isolation among traffic classes and among flows, so that one class or flow is not adversely affected by another that misbehaves".

Discuss Content Distribution Networks.

Consider the two ways in which communication occurs between a managing entity and a managed device request response mode and trapping. What are the pros and cons of these two approaches. in terms of (i) overhead, (ii) notification time when exceptional events occur, and (iii) robustness with respect to lost messages between the managing entity and the device.

What is the role of SMI in Network Management? Define the following terms : managing entity, managed entity, management agent, Mm, network management protocol.

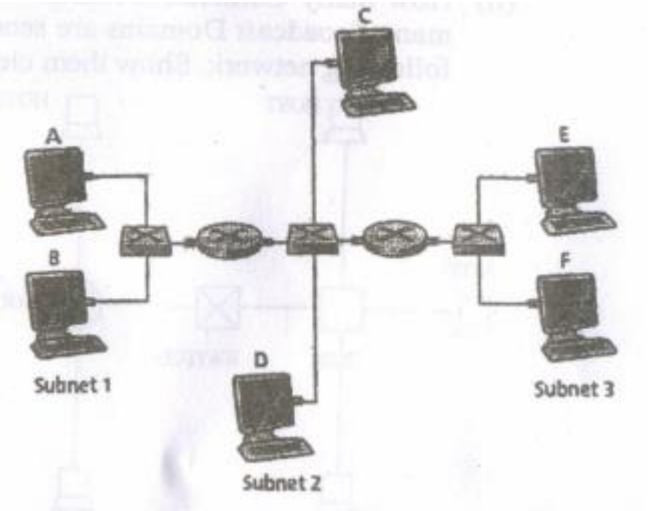
Compare mathematically Digital Certificates and Message Authentication Code.

Ten thousand airline reservation stations are competing for the use of a single slotted ALOHA channel. The average station makes 18 requests/hour. A slot is 125 usec. What is the approximate total channel load?

Briefly describe 10 Base 5 and 100 Base T.

Describe the SSL Algorithm.

Consider the following figure. First provide any suitable MAC and IP addresses for the interfaces at different Hosts and routers. Now suppose Host A sends a datagram to Host F. Give the source and destination MAC addresses when the associated frame is transmitted from : (i) A to left router, (ii) left to right router, (iii) right router to F. Now suppose leftmost router is replaced by a switch. A, B, C, D and the right router are all star connected to the switch. Now give the source and destination MAC addresses for the same frame when transmitted from (i) A to left router, (ii) left to right router, (iii) right router to F.



Alice wants to send a message m to Bob and wants to make sure that its authenticity, integrity, and confidentiality are assured. Alice sends $\{\{m\}K^{+}_{B}\}\ K^{-}_{A}$ to Bob. Does this accomplish Alice's security goals. Why or why not?

What is Public Key Certification?

Describe ARP.

Discuss, how one can achieve endpoint authentication , using nonce and public key cryptography.