1. Write note on optical Networking. Explain optical fiber & also give advantage and disadvantage of optical Networking.

- Optical networking is based on optical technology. Which uses lasers and fiber optics media for propagate of optical signal? It’s technique to transmit information to one end to other of an optical fiber using light as a signal.
- The important parameter for determine the performance of communication system are the volume of traffic, speed and clarity. Communication medium plays important roll to decide the quality of communication.
- In traditional medium is wire conductor cable is used in telephone system. But the wire conductor cable has limited bandwidth. Now information the handling capability directly proportional to the bandwidth of the communication medium.
- Now increase demand of telephony need to greater bandwidth. So that new medium optic cable is gaining popularity. This transmission medium exhibits great advantage over the conventional medium such as co-axial cable, microwave lines.
- The use of the optical fiber has increase he network capability and decrease cost of network infrastructure. The speed and quality of optical signal carry new development of the optical communication.
- The optical cable is the light pipe which is used to carry a light beam from one place to another. The frequency of light extreme high. So its transfer wide bandwidth of information also high data rate can be gain.

- Optic fiber is the transparent material, which can be transmitting light. It’s made from silica, glass or plastic. Fiber optical cable has inner core of glass which is surrounded by cladding, a layer of the glass that reflects the light back into core.
Types of fiber:

**Plastic core and cladding:**
- Plastic fiber is more flexible and more rugged than glass. It’s easy to install on network. It’s less expensive, it’s weight also low.
- But plastic cable has high attenuation, they don’t propagate as efficiency as glass.
- Plastic cable is limited temporary use. Normally for single complex or a building.

**Glass core with plastic cladding:**
- This fiber with a glass core it has less attenuation. It’s also less affected by radiation so it’s used in military application.

**Glass core and glass cladding:**
- It’s have best propagation characteristics. This kind of cable is least rugged, and they are more susceptible to increase in attenuation when exposed to radiation.

**Advantage and Disadvantage of optical networking:**

**Advantages:**
- Wide bandwidth: the light wave carries high range of frequency. thus information carrying capability is much higher.
- Low losses: It’s less attenuation over long distance.
- Immune to cross talk: It’s non-conductor of electricity so don’t produce magnetic field so It is immune to cross talk between cable cause magnetic induction.
- Interference immune: It’s also immune to conductive and radioactive interferences cause by electrical noise.
- Light weight: it’s made from glass or plastic so it is cheaper and also lighter.
- Small size: Diameter of fiber is much small compare other cables, so require less storage space.
- More strength: It is stronger and rugged to support weight.
- Security: It is more secure than other cables, they do not radiate signals.
- Long distance transmission: It’s less attenuation so transmission at longer distance.
- Environment immune: It is more immune to external environment. They can operate on high temperature variation.
- Safe and easy to install: Cables are sager and easy to install because there is no current or voltage with them. Size makes installation easy.
- Long term: Cost of cable is less than any other system.

**Disadvantage:**
- High initial cost: the installation cost is very high compare other system
- Maintenance and repairing cost: Maintenance and repair of fiber optic system difficult and expensive too.

2. **Explain SONET/SDH standards, SONET layered architecture ,and SONET structure.**
   - SONET/SDH is a standard multiplication protocol transmits information over optical fiber using lasers. SONET uses synchronous transmission medium that all digital transitions in the signals occur at precisely same rate.
   - Different specifications and frame design of SONET:
     - Digital signal level zero(DS0): single digital data channel of 64 kbps
     - Digital signal level one(DS1): Singling scheme to 24 DS) channels
     - Digital signal level two(DS2): Equivalent to 4 DS1 circuit
     - Digital signal level three(DS3): Equivalent to 2 DS1 circuit

   **SONET Layered Architecture:**

   ![SONET Layered Architecture Diagram](image)

   **SONET Architecture**

   - SONET has four layered architecture model:

     **Physical Layer:**
     - It is also call as photonic layer as it provide photonic interface. It specifies the type of fiber used and characteristic of medium.
Section Layer:
- It supports physical integrity of network. It carries SONET frames between adjacent network equipment. If performs synchronization, channel multiplexing etc.

Line Layer:
- It manages synchronous transport signal level n (STS-n) frames.

Path Layer:
- It carries information end to end across SONET network. It is responsible for data transport within network.

SONET Structure:
- SONET transmission uses there basic devices these are:
  - Synchronous transport signal (STE) multiplexer
  - Regenerator
  - Add/drop multiplexer
  - STS multiplexer/ Demux
- It multiplies signals into STS and de multiplexes STS into different signals
- Regenerator:
  - Regenerator receives optical signal and regenerate it. It replaces some overhead information with new information.
- Add/drop multiplexer:
  - Add/drop multiplexer can add or remove signals to and from a path. The signal can be redirected without de multiplexing the entire signal.

3. Explain DWDM & Give advantage and disadvantage of DWDM.
• DWDM is the data transmission technology having very large capacity and efficiency. Multiple data channels of optical signals are assigned different wavelengths and are multiplexed onto one fiber.
• DWDM system is consists of transmitters, multiplexers, optical amplifier and de-multiplexer. DWDM use single mode fiber to carry multiple light waves of different frequencies.
• DWDM system uses Erbium-Doped fiber Amplifiers for its long haul application, and to overcome the effects of dispersion and attenuation channel spacing of 100 GB is used.

Advantages:
• The most advantage is capability to provide unlimited transmission capacity from both technical and economical perceptions.
• Network capacity can enhanced according to user demand by increase number of channels on the fiber.
• Provide capacity to support 160 wavelengths, more traffic can transport.
• Works with ATM, for this provides interface over a common physical layer.
• Provide fast, simple and dynamic network connection, provide higher bandwidth service.
• Provide cost saving optical amplifiers.

Disadvantages:
• Several fiber do not support DWDM
• DWDM do not support ring architecture, that’s why point to point protection used, which waste bandwidth.
• DWDM system difficult to troubleshoot, manage and provision.

4. Explain SONET Hardware, SONET network configuration and give Advantage and Disadvantage of SONET/SDH.

<table>
<thead>
<tr>
<th></th>
<th>E1</th>
<th>STS-1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>E2</td>
<td></td>
<td>STS-N</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>VT 1.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STS-M</td>
<td>V13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STS-N</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SONET terminal multiplexer**

**SONET Hardware:**
• SONET hardware includes STEs, LTEs and PTEs. Other SONET equipments are SONET terminal adapter (SONET multiplexer), SONET add/drop multiplexer (SADM), SONET digital top carrier system (DLCs).

Prepared by: M.D. Trivedi
- SONET terminal multiplexer multiplex different electric signals in STS-n or STM-n signal

**SONET Network Configuration:**
- SONET can offer a variety of topologies, these topologies use the network elements.
- Topologies are:
✓ Point to point topology:
✓ Point to multipoint topology
✓ Ring architecture

**Advantages:**
- Enables the combination of low speed transmission channels into regular high-speed backbone network
- Provide the capacity to transmit all type of traffic. That is voice, data and video.
- Offers the vendor interoperability through the standard optical format specification.
- Provides proficient and restoration than electric system.
- Provides potential to make optical links between carries.

**Disadvantages:**
- SONET/SDH devices are complex and more expensive than optical Ethernet and other technologies.
- SONET/SDH offers limited node network management functions and Storage area network support.
- SONET/SDH protocol overhead covers most of the part of STS frame.
1. Explain ATM Cell format.

- An ATM cell header can be one of two formats:
  - User network interface (UNI)
  - Network network interface (NNI)

- The UNI header is used for communication between ATM card end points and ATM switches in private ATM networks.
- The UNI header is used for communication between ATM switches.
- Figure shows the basic ATM cell format. Unlike the UNI, the NNI header does not include the Generic Flow Control (GFC) field.

![ATM Cell Format Diagram]

**a. User-network interface**

- Functions of field are given below.

**Generic flow control (GFC):**

- GFC provides local functions; such as identifying multiple stations that share a single ATM interface. This field is typically not used and is set to its default value.

**Virtual path identifier (VPI):**

- In conjunction with the VCI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination. It is 8-bit at the UNI and 12-bit for NNI.
Virtual channel identifier (VCI):
• VCI is used for routing to and from the end user. It is used in conjunction with VPL.

Pay load type (PT):
• It indicates type of information field. PT indicates in the first bit whether the cell contains user data or control data. If the cell contains user data, the second bit indicates congestion. Following is the list of table for pay load type field coding.

Congestion loss priority (CLP):
• CLP indicates whether the cell should be discarded if it encounters extreme congestion as it moves through the network. If the CLP = 1 the cell should be discarded in preference to cells with the CLP bit equal to zero.

Header error control (HEC):
• It calculates checksum only on the header itself.

2. Explain QOS (Quality of Service)
• ATM supports QOS guarantees composed of traffic contract, traffic shaping and traffic policing.
• A traffic contact specifies an envelope that describes the intended flow. This envelope specifies values for peak bandwidth, average sustained bandwidth, and burst size, among others.
• When an ATM end system connects to an ATM networks, it enters a contract with the network, based on QOS parameters.
• Traffic shaping is the use of queues to constrain data bursts, limit peak data rate and smooth jitters so that traffic will fit within the promised envelope. ATM device are responsible for adhering to the contract by means of traffic shaping.
• ATM switches can use traffic policing to enforce the contract. The switch can measure the actual traffic flow and compare it against the agreed-upon traffic envelope.
• If the switch finds that traffic is outside of the agreed-upon the parameters, it can set the cell-loss priority (CLP) bit of the offending cells. Setting the CLP bit makes the cell discard eligible, which means that any switch handling the cell is allowed to drop the cell during periods of congestion.
• When ATM device wants to establish a connection with another ATM device, it sends a signal request packet to its directly connected ATM switch. This request contains the ATM address of the desired ATM endpoint, as well as any QOS parameters required for the connection.
• ATM signaling protocols vary by the type of the ATM link, which can be either UNI signals or NNI signals.

3. Explain ATM Traffic management.
• The following function have been define:
Resource management having virtual paths:
• To allocate network resource in such way as to separate traffic flows according to service characteristics.
• The network provides aggregate capacity and performance characteristic on the virtual path and these are shared by the virtual connections.
• There are three cases to consider
  ✓ Users to user application
  ✓ User to network application
  ✓ Network to Network application

Connection Admission Control (CAC):
• When user request a new VPC the user must specify the service require in both directions for that connection.
• The request consists of the following:
  ✓ Service category
  ✓ Connection traffic descriptor consisting of
    a. Source traffic descriptor
    b. CDVT
    c. Requested conformance definitions
  ✓ Requested and acceptable value of each QOS parameters.

Usage parameter control:
• The main purpose is to protect network resource from an overload on one connection that would adversely affect.
• The QOS on other connections by detecting violations of assigned parameters and taking appropriate actions.

Selective cell discard:
• The objective is to discard lower priority cell to protect the performance for higher priority cells.
Traffic shaping:
- Traffic shaping is used to smooth out a traffic flow and reduce cell clumping. This can result in a fairer allocation of resources and reduced average delay time.
- A simple approach to traffic shaping is to use a form of the leaky bucket algorithm known as token bucket.

Explicit forward congestion indication:
- Any ATM network node is experiencing congestion may set and explicit forward congestion indication in the cell header and cells on connections passing through the node.

4. Write note on ATM and explain B-ISDN Reference Model.
- ATM is a cell relay technique. ATM works on statically multiplexing that uses features of both packet switching and circuit switching.
- The cells are considered as packets and relay an switching. Example ATM uses packet switching technology. ATM networks are connection oriented example it requires connection setup before cell transmission. Therefore it also follows circuit switching technology.
- The following important features encourage the widespread use of ATM for telecommunications.
  ✓ High speed data rate
  ✓ Low error rate between switching centers
  ✓ Digitized video speech
  ✓ Comparatively low operating cost
- The faces of ATM are listed below:
  1. ATM as an economical and integrated service
  2. ATM as an architecture and technology
  3. ATM as an interface and a protocol
  4. ATM as a Wan transport service
ATM/B-ISDN Reference Model

- ATM (B-ISDN) id defines by means of layered architecture. It is called as ATM reference model. Figure shows ATM reference model.
- Vertical planes represent the different functions occurring at each layer and are addition to ISO-OSI model. All layers has a separate management and layered management
- Plane management incorporates the management functions for whole system whereas layered management incorporated management functions of specific layer.

4. Explain ATM Adaption Layer.

- AAL provide the flexibility of single communications process to carry multiple types of traffic such as data, voice, video and multimedia.
- ATM adaption layer divides the information into smaller segments that are capable of being inserted into cells for transport between two end nodes.
- ATM adaption layer is divided into two major parts. Upper part of the ATM adaption layer is called the convergence sub layer, provides interface to application. Lower part of AAL is call as the segmentation and Reassembly (SAR) sub layer. It can add headers and trailers to the data units.
- AAL functions four type:

AAL-1(Constant Bit Rate Services)

- It is connection oriented service ,suitable for handling circuit emulation application.AAL-1 require time synchronization between source to destination.AAL-1 depends on a medium SONET, that support clock.
- AAL-1 uses a convergence sub layer and SAR sub layer. Convergence sub layer detects lost and miss inserted cells at a constant rate.
- AAL-1 convergence sub layer does not have any protocol headers of its own.AAL-1 SAR sub layer does have a protocol.
- Format of its cell given.

<table>
<thead>
<tr>
<th>ATM header(5 octets)</th>
<th>Sequence number (SN)</th>
<th>Sequence number protection(SNP)</th>
<th>Payload (47 octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSI</td>
<td>SC 3</td>
<td>CRC 3</td>
<td>parity 1-0</td>
</tr>
</tbody>
</table>

- Sequence number(SN): 4 bit
- Sequence number protection: 4 bit
• The SN is further divide into a 3 bit sequence count (SC) field and 1 bit convergence sub layer indication (CSI) field.

**AAL-2(Variable Bit Rate)**

1 byte | 2 byte

| SN | IT | 45 byte payload | LI | CRC |

• It’s used for compressed audio and video, here in figure we can see the format which consists of 48 bytes. AAL-2 layers is divided into the common part sub layer (CPS) and the service specific convergence sub layer.

• In above cell contains 1-byte header and a 2-byte trailer. 45 byte is used for data per cell. the SN field is used for numbering cell in order to detect missing cell.

• The information type (IT) is used to indicate that the cell is the start, middle or end of the message. The length indicator (LI) field tells how big the payload is. The CRC field is a checksum over the entire cell, by that error can be detected.

• AAL-2 functions:
  - Segmentation and reassembly of cells
  - Handling of cell delay variation
  - Handling of loss and miss inserted cells
  - Source clock recovery
  - Monitoring errors and take corrective action

**AAL-3/4(Connection Oriented)**

• AAL-3/4 support both connection oriented and connection less data. It operates in stream and message mode. Message mode message boundaries are preserved. In stream mode message boundaries are not preserved.

• Both the modes allow for assured or non-assured operation. In assured the end to end protocol is implemented in the SSCS to allow for the error free delivery of the message. In non assured operation, messages may be delivered in error.

<table>
<thead>
<tr>
<th>1</th>
<th>1</th>
<th>2</th>
<th>1-65535</th>
<th>0-3</th>
<th>1</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPI</td>
<td>B TAG</td>
<td>BA size</td>
<td>payload</td>
<td>Padding</td>
<td>Al</td>
<td>E tag</td>
<td>Length</td>
</tr>
</tbody>
</table>

CS Header | AAL-3/4 convergence sub layer | CS Header
AAL-5 (Coding):

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Payload</th>
<th>UU</th>
<th>Length</th>
<th>CRC</th>
</tr>
</thead>
</table>

AAL5 convergence sub layer

- AAL-5 is the primary AAL for data and supports both connection oriented and connectionless data. It is used to transfer most non SMDS data, such as classical IP over ATM and LAN emulation. AAL-5 also known as the simple efficient adaption layer (SEAL).
- AAL-5 doesn’t have a convergence sub layer header, only have 8-byte trailer.
- AAL-5 is more efficient than AAL-3/4. AAL-5 does not add any overhead. It doesn’t include sequence number.
1. Explain various layer of x.25 packet switching network

OSI Reference Model

<table>
<thead>
<tr>
<th>Application Layer</th>
<th>X.25 Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation Layer</td>
<td>Packet level</td>
</tr>
<tr>
<td>Session Layer</td>
<td>Link level</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Physical Level</td>
</tr>
<tr>
<td>Network Layer</td>
<td></td>
</tr>
<tr>
<td>Data Link Layer</td>
<td></td>
</tr>
<tr>
<td>Physical Layer</td>
<td></td>
</tr>
</tbody>
</table>

- There are three levels. These levels correspond to Level 1, 2, and 3 of OSI model

**Physical Layer:**
- The physical level activates maintain and deactivate the physical circuit between DTE (Data terminal equipment) and DCE (Data circuit terminal equipment). The physical level has following functions.
- Activate and deactivate physical circuits using electric signals.
- Maintain line characteristic of selected interface.
- Indicate faulty incoming frames, such as frames with the wrong length.
- Allow configuration of auto call for system with dial up x.25 connections.

**Link Level (Frame Level):**
- The packet layer produces x.25 packets to establish calls and transfer data. all these packets are then passed to the frame layer for transmission to the local DCE
- The frame layer uses a link-access procedure to ensure that data and control information are accurately exchanged over the physical circuit between the DTE and DCE.
- It provides recovery procedure and is based on a subnet of the protocol called LAP-B which is synchronous and full-duplex.
- Here each frame has a header containing address; control information and trailer contain a frame-check sequence.
- Frames are three types:
  1. Information frames
  2. Supervisory frames
  3. Unnumbered frames
Packet Level:
- The packet layer protocol specifies how x.25 controls the call and data transfers between systems. Each system connected to the network has an address to identify it and the address when a connection from local to remote system made.
- The data transfer capacity of the X.25 line may be shared between a sessions, max number of subscription is based on the network subscription and capacity of DTE hardware and software.
- Virtual circuit is the data circuit between the local and remote system and circuit may have its route switched within the network.

Logical Channels:
- Logical channels are the communication paths between a DTE and its data circuit-terminating equipment.
- For 15 simultaneous connections across the network, supplier must have 13 logical channels.
- The network provider assign the specific logical channels numbers and each network

2. Explain Packet Switching.
- Packet switching is often used in computer networks where individuals have to use channels intermittently. Channel application requires high bandwidth.
- In packet switching, message are broken into the short blocks interact with other messages. Thus users queue for the channels and share it with one another efficiently. Data is sent in individual packet, each packet is forwarded to the switch to switch and reach to destination.
- Each outgoing node has a small amount of buffer space to temporary hold packets. If the outgoing line is busy the packet is stay in queue until the line becomes available.
- Packet switching methods uses two routing approaches:
  ✓ Datagram packet switching
  ✓ Virtual circuit packet Switching

![Packet Switching Diagram]

Datagram packet Switching

Prepared by: M. D. Trivedi 180704 – Advance Computer Network
Packet switching:

- In packet switching each packet is routed independently through the network. Header is attached to the each packet. It provides all of the information required to route the packet to its destination. While routing the packet destination address in the header are examined to determine the next address of destination.
- Datagram approach is also called connectionless.
- Disadvantage of datagram approach is a lot of overhead because of independent routing. Another is packet may not arrive in the order at destination in which they were sent.

Virtual Circuit Packet Switching:

- In virtual circuit packet switching a fixed path between a source and a destination is established prior to transfer of packets.
- Connection-oriented network is also known as virtual circuit. Virtual circuit is similar to the telephone system. A route which consists of a logical connection is first establish is not a dedicated path between stations. The path is generally shared by many other virtual connections.
- There are three main phases:
  - Establishment phase
  - Data transfer phase
  - Connection release phase

Establishment phase:

- During this phase logical connection is establish, not only connection but user also decide quality of service with the connection.

Data transfer phase:

- During this error control and flow control service performs. Error control ensures correct sequence of packet and flow control ensures receive rate and transmit rate.

Connection release:

- When station is close down the virtual circuit, one station can terminate the connection with a clear request packet.
3. Write a short note on X.25 equipment.

- Equipment used in X.25 PSN is categorized as data terminal equipment, data circuit terminating equipment. Packet switching exchange and packet assembler/disassemble. The description of the equipment is as follows:
- **Data Terminating Equipment (DTEs):** equipment serving as the data source and data sink, that is, end systems, such as PCs or work stations.
- **Data Circuit-Terminating Equipment (DCEs):** device that offers the functions required to create a connection and signal conversation. (Required for communications between the DTE and communication channel).
- **Packet Switching Exchange (PSE):** Switches that create most of the carrier’s network and transmit data from the one DTE to the other DTE through the X.25 PSN.
- **Packet Assembler/Disassembler (PAD):** refers to equipment usually used in X.25 PSNs. PADs are used between DTE and DCE devices and following function executed.
- **Buffering:** Storing data until a device is ready to process the data.
- **Packet assembly:** adding header with the corresponding data to from a packet
- **Packet disassembly:** removing data and header apart in a packet.
- The PAD buffers and assembles data sent to/ from the DTE and it also passes the assembled data towards the DCE. Moreover the PAD disassembles the received packets before passing them to the DTE.

4. Explain working of SMD

- Switched Multimegabit Data Service (SMDS) is a wide area networking service designed for LAN interconnection through the public telephone network. SMDS is a connectionless service.
- SMDS is designed for moderate bandwidth connections, between 1 to 34 Mbps.
• SMDS network is composed of the following components:
  • A series of SMDS switches inside the service providers network
  • A series of Channel Service Unit/ Data Service Unit connecting the subscriber to the providers network at each location.
  • A router, gateway or terminal connected to each CSU/DSU.
  • Figure shows the SMDS network.
  • SMDS Interface protocol which connects the CSU/DSU to the public network, there by defining the subscriber network interface(SNI)
  • Data exchange Interface(DXI), which connects the customers equipment to the CSU/DSU
  • Within the public network, the inter-Switching System Interface (ISSI) connects the individual SMDS switches. ISSI includes other functions relevant to the provider, including routing and maintenance functions.
  • Inter-Carrier Interface (ICI) is used to make connections between different SMDS service providers, such as between a local SMDS provider and a long distance provider.

Characteristic s of SMDS:
• Uses ATM-like 53 cells, but a different address format.
• Provides datagram-based transmission services. So it is a connectionless service.
• Data unit is large enough to encapsulate frames of Ethernet, token ring and FDDI
• An unreliable packet service like ATM and frame relay. Like ATM and frame relay, SMDS does not perform error checking
• Speed ranging 56kpps to 44.37 Mbps
• Not yet a widely accepted standard.
• Its future is uncertain.
1. Explain classful IP addressing scheme.

<table>
<thead>
<tr>
<th>Class</th>
<th>Net ID</th>
<th>Host ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>0</td>
<td>Net ID</td>
</tr>
<tr>
<td>Class B</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Class C</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Class D</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Class E</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Five classes of IP address

- The IP address structure is divided into five address classes: Class A, Class B, Class C, Class D and Class E which are identified by the most significant bits of the address.
- In figure we can see the five classes of IP address.
- Class A address was designed for large organization with a large number of attached hosts or routers.
- Class B address were designed for midsize organization with tens of thousands of attached hosts or routers.
- Class D address is used to multicast services that allow a host to send information to a group of hosts simultaneously.
- Class E addresses are reserved for future use.
- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having fixed size.
- In a Class Anetwork, the first byte is assigned to the network address, and the remaining three bytes used for the node addresses. The class A format is Network.Node.Node.Node.
• For Example: 14.28.101.120 in this IP address 14 is the network address and 28.101.120 is the node address.

• In Class B network, the first two bytes are assigned to the network address and the remaining two bytes are used for node address.

• For Class B format is: Network.Network.Node.Node

• For example 150.51.30.40 in this IP address network address is 150.51 and node address is 30.40.

• In Class C network, the first three bytes are assigned to network address and only one byte is used for node address. The format is Network.Network.Network.Node

• For example: 200.20.42.120 in this 200.20.42 is the network address and 120 is the node address.

2. With Example Explain Subnetting.

Multiple Network

• If the organization is large or if its computers are geographically dispersed, it makes good sense to divide network into smaller ones, connected together by routers.

• The benefits for doing things this way include.
• Reduced network traffic
• Optimized network performance
• Simplified network management
• Facilities spanning large geographical distance

• If network information center assign only one network address to the organization which having multiple network, that organization has a problem. A single network address can be used to refer to multiple physical networks.

• An organization can request individual network address for each one of its physical networks. If there were granted, there wouldn’t be enough to go around for everyone.

• Another problem if each router on the internet needed to know about each existing physical network, routing tables would be impossibly huge. This is the physical overhead on the router. To solve this type of problem, the subnet addressing method is used.

• To allow single network address to span multiple physical networks is called subnet addressing or subnet routing or subnetting. Subnetting is a required part of IP addressing.

• Example: consider the site has a single class B IP network address assigned to it, but the organization has two or more physical networks. Only local routers know that there are multiple physical networks and how to route traffic among them.

• Organization is using the single class B network address for two networks. For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning each machine a subnet mask.

• The network admin creates a 32 bit subnet mask comprised of ones and zeros. The ones in the subnet mask represent the positions that refers to the network or subnet addresses.

• The zeros represent the position that refers to the host part of the address. Class B address format is Net.Net.Node.Node. The third byte, normally assigned as part of the host address is now used to represent the subnet address.

• These bit positions are represented with ones in the subnet mask. The fourth byte is the only part in example that represent the unique host address.

• 1= positions representing network or subnet address, 0=positions representing the host address.

• The subnet mask can also be denoted using the decimal equivalents of the binary patterns.

• For Class A default subnet mask is 255.0.0.0, Class B 255.255.0.0, Class C 255.255.255.0

• A process that extracts the address of the physical network from the IP address is called masking. If we done subnetting, then masking extracts the subnetwork address from an IP address.
• To find the subnetwork address two methods are used. There are boundary level masking and non-boundary level masking.

• In boundary level masking, two masking numbers are consider(0 to 255)

• In non-boundary level masking other value of masking is used apart from 0 to 255.

3. Show and explain various field of IP(Internet Protocol) Datagram.

<table>
<thead>
<tr>
<th></th>
<th>VER (4 bits)</th>
<th>HEL (4 bits)</th>
<th>Service type</th>
<th>Total length (16 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Datagram identification (16 bits)</td>
<td>Flags (3 bits)</td>
<td>Fragment offset (13 bits)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time to live (8 bits)</td>
<td>Protocol (8 bits)</td>
<td>Header checksum (16 bits)</td>
<td></td>
</tr>
<tr>
<td>Source IP address</td>
<td>32 bits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination IP address</td>
<td>32 bits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IP Datagram

• The term 'datagram' or 'packet' is used to describe a chunk of IP data. Each IP datagram contains a specific set of fields in a specific order so that the reader knows how to decode and read the stream of data received.

VERSION (4 bits)

• The version field is set to the value '4' in decimal or '0100' in binary. The value indicates the version of IP (4 or 6, there is no version 5).

HEL (4 bits)

• The Internet Header Length (HEL) describes how big the header is in 32-bit words. For instance, the minimum value is 5, as that is the minimum size of an IP header that contains all the correct fields is 160 bits, or 20 bytes.

• This allows the receiver to know exactly where the payload data begins.

TOS (8 bits)

• Type of service allows the intermediate receiving stations (the routers) to have some notion of the quality of service desired. This allows the network to make adaptations for delay, throughput, or reliability.
TOTAL LENGTH (16 bits)

- This informs the receiver of the datagram where the end of the data in this datagram is. This is the length of the entire datagram in octets, including the header.
- This is why an IP datagram can be up to 65,535 bytes long, as that is the maximum value of this 16-bit field.

IDENTIFICATION (16 bits)

- Sometimes, a device in the middle of the network path cannot handle the datagram at the size it was originally transmitted, and must break it into fragments.
- If an intermediate system needs to break up the datagram, it uses this field to aid in identifying the fragments.

FLAGS (3 bits)

- The flags field contains single-bit flags that indicate whether the datagram is a fragment, whether it is permitted to be fragmented, and whether the datagram is the last fragment, or there are more fragments. The first bit in this field is always zero.

FRAGMENT OFFSET (13 bits)

- When a datagram is fragmented, it is necessary to reassemble the fragments in the correct order.
- The fragment offset numbers the fragments in such a way that they can be reassembled correctly.

TIME TO LIVE (8 bits)

- This field determines how long a datagram will exist. At each hop along a network path, the datagram is opened and it's time to live field is decremented by one (or more than one in some cases).
- When the time to live field reaches zero, the datagram is said to have 'expired' and is discarded. This prevents congestion on the network that is created when a datagram cannot be forwarded to its destination.
- Most applications set the time to live field to 30 or 32 by default.

PROTOCOL (8 bits)

- This indicates what type of protocol is encapsulated within the IP datagram.

HEADER CHECKSUM (16 bits)

- The checksum allows IP to detect datagrams with corrupted headers and discard them. Since the time to live field changes at each hop, the checksum must be re-calculated at each hop. In some cases, this is replaced with a cyclic redundancy check algorithm.
**SOURCE ADDRESS (32 bits)**

- This is the IP address of the sender of the IP datagram.

**DESTINATION ADDRESS (32 bits)**

- This is the IP address of the intended receiver(s) of the datagram. If the host portion of this address is set to all 1's, the datagram is an 'all hosts' broadcast.

**OPTIONS & PADDING (variable)**

- Various options can be included in the header by a particular vendor's implementation of IP. If options are included, the header must be padded with zeroes to fill in any unused octets so that the header is a multiple of 32 bits, and matches the count of bytes in the Internet Header Length (HEL) field.

4. **Discuss the protocols associated with layers of TCP/IP protocol suite.**

![TCP/IP model diagram]

**TCP/IP protocol suite**

- Communications between computers on a network is done through protocol suits. The most widely used and most widely available protocol suite is TCP/IP protocol suite.

- A protocol suit consists of a layered architecture where each layer depicts some functionality which can be carried out by a protocol.

- Each layer usually has more than one protocol options to carry out the responsibility that the layer adheres to. TCP/IP is normally considered to be a 4 layer system.

- The 4 layers are as follows:
  - Application layer
  - Transport layer
  - Network layer
  - Internet layer

TCP/IP protocol suite
✓ Data link layer

Application layer:

• This is the top layer of TCP/IP protocol suite. This layer includes applications or processes that use transport layer protocols to deliver the data to destination computers.

• At each layer there are certain protocol options to carry out the task designated to that particular layer. So, application layer also has various protocols that applications use to communicate with the second layer, the transport layer.

• Some of the popular application layer protocols are:
  ✗ HTTP (Hypertext transfer protocol)
  ✗ FTP (File transfer protocol)
  ✗ SMTP (Simple mail transfer protocol)
  ✗ SNMP (Simple network management protocol) etc

Transport Layer:

• This layer provides backbone to data flow between two hosts. This layer receives data from the application layer above it. There are many protocols that work at this layer but the two most commonly used protocols at transport layer are TCP and UDP.

• TCP is used where a reliable connection is required while UDP is used in case of unreliable connections.

• TCP divides the data (coming from the application layer) into proper sized chunks and then passes these chunks onto the network.

• It acknowledges received packets, waits for the acknowledgments of the packets it sent and sets timeout to resend the packets if acknowledgements are not received in time.

• The term ‘reliable connection’ is used where it is not desired to loose any information that is being transferred over the network through this connection.

• So, the protocol used for this type of connection must provide the mechanism to achieve this desired characteristic. For example, while downloading a file, it is not desired to loose any information (bytes) as it may lead to corruption of downloaded content.

• UDP provides a comparatively simpler but unreliable service by sending packets from one host to another. UDP does not take any extra measures to ensure that the data sent is received by the target host or not.

• The term ‘unreliable connection’ are used where loss of some information does not hamper the task being fulfilled through this connection.

• For example while streaming a video, loss of few bytes of information due to some reason is acceptable as this does not harm the user experience much.
**Network Layer:**

- This layer is also known as Internet layer. The main purpose of this layer is to organize or handle the movement of data on network.
- By movement of data, we generally mean routing of data over the network. The main protocol used at this layer is IP.
- While ICMP (used by popular ‘ping’ command) and IGMP are also used at this layer.

**Data Link Layer:**

- This layer is also known as network interface layer. This layer normally consists of device drivers in the OS and the network interface card attached to the system.
- Both the device drivers and the network interface card take care of the communication details with the media being used to transfer the data over the network.
- In most of the cases, this media is in the form of cables. Some of the famous protocols that are used at this layer include ARP (Address resolution protocol), PPP (Point to point protocol) etc.

For More in Chapter-4 Refer: *Tanenbaum and Forouzan Book*
1. Introduce Intra domain and inter domain routing. Give difference between them.

- The Internet is so large that no routing protocol can single handedly update the routing table of all routers. Therefore the internet is partitioned into autonomous system with each autonomous system being a group of network and router under the authorization of a single administration. It has been mentioned earlier that routing within and autonomous system is referred to as intra-domain routing.

- While routing between autonomous system is referred to as inter-domain routing. There are multiple IGP in intra-domain routing. Whereas there is only a single EGP in inter-domain routing.

- Two most popular intra-domain routing methods are as follows:
  - Distance Vector
  - Link state
  - However, path vector is the most popular inter-domain routing methods. Here the routing protocols and their classification:

![Routing Protocols Diagram]

Routing Protocols and their classification

- **Routing Information Protocol (RIP):** Denotes an IGP that implements the distance vector routing.
- **Open Shortest Path First (OSPF):** Denotes another IGP that implements the link-state routing.
- **BGP:** Denotes an EGP that implements the path vector routing.
Difference between Inter & Intra domain routing:

Inter-Domain Routing
- Routing between autonomous system
- Assume that the internet consists of a collection of interconnected autonomous system
- Protocols for inter-domain routing are also called Exterior Gateway protocols
- Routing protocols are BGP

Intra-Domain Routing
- Routing within an autonomous system
- Ignores the Internet outside the autonomous system
- Protocols for intra-domain routing are also called Interior Gateway protocol
- Popular protocols are RIP and OSPF

2. What is difference between static and dynamic routing?
- Static routing manually sets up the optimal paths between the source and the destination computers. On the other hand, the dynamic routing uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.

- The routers that use the static routing algorithm do not have any controlling mechanism if any faults in the routing paths. These routers do not sense the faulty computers encountered while finding the path between two computers or routers in a network.

- The dynamic routing algorithms are used in the dynamic routers and these routers can sense a faulty router in the network. Also, the dynamic router eliminates the faulty router and finds out another possible optimal path from the source to the destination.

- If any router is down or faulty due to certain reasons, this fault is circulated in the entire network. Due to this quality of the dynamic routers, they are also called adaptive routers.

- The static routing is suitable for very small networks and they cannot be used in large networks. As against this, dynamic routing is used for larger networks. The manual routing has no specific routing algorithm.

- The dynamic routers are based on various routing algorithms like OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol) and RIP (Routing Information Protocol).

- The static routing is the simplest way of routing the data packets from a source to a destination in a network. The dynamic routing uses complex algorithms for routing the data packets.

- The static routing has the advantage that it requires minimal memory. Dynamic router, however, have quite a few memory overheads, depending on the routing algorithms used.
• The network administrator finds out the optimal path and makes the changes in the routing table in the case of static routing.

• In the dynamic routing algorithm, the algorithm and the protocol is responsible for routing the packets and making the changes accordingly in the routing table.

3. Give brief description of RIP with message format.

• RIP is the implementation of the distance vector routing in which a router finds the route with minimum distance between any two nodes known as the least cost route. RIP treats all networks as equal and the cost to travel the distance between two consecutive nodes is the same, that is a single hop count.

• An autonomous system consists of routers and networks. Where in RIP used by the router. The routers are called active machines and networks are called passive machines.

• Each router has a routing table consists of 3 columns.

• **First column:** Shows the address of the destination network
• **Second column:** Shows the cost or hop count
• **Third column:** Shows the address of the next router that receives the packet from the source

• All routers and networks receive broadcast message at a regular interval, and update their routing tables as per the distance vector routing algorithm.

• The least cost route between any two nodes is the route with the minimum distance.

• There are some rules that all routers follows in RIP. For example when a router receives a routing table from any other node. It compares the received table with the existing table and updates only when the received table has a lower cost. It retains the existing table when both the costs are same.

• The following problem should be addressed by RIP for efficient routing:
  1. No detection of routing loops
  2. Instability due to high value of Infinity
  3. Slow convergence or count to Infinity problem
RIP Version 1:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>16</td>
<td>31</td>
</tr>
<tr>
<td>command</td>
<td>Version</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>Family</td>
<td>Must be zero</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address of network 1</td>
<td>Must be zero</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Must be zero</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address of network 2</td>
<td>Must be zero</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Must be zero</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distance to Network1</td>
<td>Must be zero</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distance to Network2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**RIP 1 Version**

- RIP1 message format consists of a fixed header followed by a list of IP addresses of network and distance in hop counts to these networks.
- A router sends message format either for sending routing information or for requesting routing information.
- After the 32-bit header. The message contains a sequence of pairs where each pair consists of a network IP address and an integer distance to network.

**Different fields of message:**

- **Command**: specify type of message which for request, response and acknowledgement.
- **Version**: Denotes version of RIP protocol. Either RIP version 1 and RIP version 2.
- **Reserved**: Indicate this field is not in use by RIP.
- **Family**: Define the type of protocol.
- **Network Address**: Address of the destination network.
- **Distance**: Shows the total number of hop counts required to reach destination.
RIP Version 2:

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>Version</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>Family</td>
<td>Routing tag</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address of network 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet mask</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next Hop address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distance to Network1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Family</td>
<td>Must be zero</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address of network 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet mask</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next Hop address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distance to Network2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**RIP 2 Version**

- The restriction on address interpretation was removed in RIP version 2.
- RIP2 was extended to include subnet mask along with the existing addresses. RIP2 also includes the next hop address to avoid routing loops count to infinity problem.
- The following fields are updated in RIP1 message format:
  - **Route tag:** Carries information regarding autonomous system number.
  - **Subnet mask:** Denotes a subnet mask for subnet addressing as RIP2 support class addressing.
  - **Next hop address:** specifies the address of the next hop.

4. **Explain Multicast Routing Protocols.**

- Multicast means one to group mapping as compared to broadcasting. In multicasting a router may contact a group of other routers at a time. Example- Video conferencing session.
- Broadcasting is a special case of multicasting when the group becomes the large enough to comprise all mapping.
- Distance vector multicast routing protocol (DVMRP) and Multicast open shortest path first (MOSPF)
Distance Vector Multicast Routing Protocol:

- One of the Multicast routing protocol is DVMRP is used for global Internet. This protocol allows routers to pass routing information among them.
- DVMRP is based on RIP protocol, but it is updated for multicast routing. And used source based tree approach.
- Receiver router need to send copy of the packet to the attached network. DVMRP is extended for Internet Group Management Protocol (IGMP) used for communication among multicast routers.
- It specifies additional IGMP message types that allow the routers to declare membership in a multicast group.
- The extensions also provide message that carry the routing information.

Multicast Open Shortest Path First Protocol:

- MOSPF is an extension of the OSPF and uses multicast link-state routing for source based tree. Each router has a routing table that represents as many shortest path tree as there are groups.
- MOSPF is demand-driven, means that the shortest path tree will created when needed. when router receive a packet with a multicast destination address pairs, it calculates the shortest path tree for that group.
- The result is saved for future use by the same group. MOSPF sends less data traffic but sends more routing protocols than the data-driven protocol.
- MOSPF defines inter-area multicast routing in a different way. OSPF designate one or more routers in an area to be and ABR(area border router). Which then propagates the routing information to other areas.
- Then MOSPF further designates one or more of the area’s ABRs to be a Multicast Area Border Router(MABR), which propagates group member information to other areas.
- MABR transmit membership information from their area to the backbone area but don’t transmit information from the backbone down.
- An MABR transmit multicast information to another area without acting as active receiver for traffic.
- When an outside areas sends multicast traffic, the traffic for all the groups in the area is sent to the designated receiver, which is referred as a multicast wildcard receiver.
MBOne:

- MBone is multicast internet backbone. Interconnected set of routers and subnets that provide IP multicast delivery in internet.

- MBOne routers run a protocol to decide where to forward IP multicast packets. Routers treat MBOne topology as a single flat routing domain.

- There is a problem of additional processing resources and memory. If nothing is done by MBOne will collapse.

- Solution lies in using hierarchical distance vector multicast routing for the MBOne. Use the two-level hierarchy in which the MBOne is divided into regions and the regions contain subnets.
5. **Give a brief description of OSPF.**

- OSPF is a link state routing protocol. OSPF is based on the distributed map concept all nodes have a copy of the network map which is regularly updated. Each node contains the routing directory database.

- The database contains information about the routers interface that are operable, as well as status information about adjacent routers.

- The OSPF computes the shortest path to the other routers. OSPF protocol is now widely used as the interior router protocol in TCP/IP networks.

- OSPF computes the route through the internet that incurs the least cost based on a user-configurable metric of cost.

- The user can configure the cost to express a function of delay, data rate or other factors. OSPF is able to equalize loads over multiple equal cost paths.
• OSPF is classified as an internal gateway protocol (IGP) because it support routing within the autonomous system only. The exchange of routing information between autonomous system is the responsibility of another protocol and external gateway protocol (EGP).

❖ **Following are the features of the OSPF:**

• Support multiple circuit load balancing it can store multiple routes to a destination.

• OSPF can converge very quickly to network topology change.

• OSPF support multiple metrics.

• OSPF support for variable length sub netting by including the subnet mask in the routing message.

• OSPF allows an AS to be partitioned into several groups called areas, that are interconnected by a central backbone area show in figure.

• OSPF uses four type of routers.

• An internal router is a router with all it’s link connected to the networks within the same area.

• An area border router is a router that has its links connected to more than one area.

• A backbone router is a router that has its links connected to the backbone.

• An Autonomous system boundary router (ASBR) is a router that has its links connected to another autonomous system.

• As shown in figure router R1, R2 and R7 are internal routers. Routers R3, R6, R8 are area border routers. Routers R3, R4, R5, R6, R8 are backbone routers.

❖ **OSPF header analysis is given below:**

• **Version:** This field specifies the protocol version

• **Type:** This field indicate message.

• **Packet length:** This field specifies the length of OSPF packet. Include the OSPF header.

• **Router ID:** It indicate sending router. This field is set to the IP address of one of its interfaces.

• **Area ID:** This field identifies the area this packet belongs to transmitted.

• **Checksum:** The checksum field is used to detect errors in the packet.

• **Authentication Type:** it identifies the authentication type that is used

• **Authentication:** This field includes a value from the authentication type.
Advantages:

- Low traffic overload.
- Fast convergence.
- Larger network metrics
- Area based topology
- Authentication
- Support for complex address structures

Disadvantages:

- Memory overhead
- Processor overhead
- Complex Configuration

6. Give a brief description of BGP.

- The purpose of the gateway protocol is to enable two different autonomous system to exchange routing information so that IP traffic can flow access the autonomous system border.

- The BGP is an inter domain routing protocol that is used to exchange network ratability information among BGP routers.

- Each BGP routers establishes a TCP connection with one or more BGP routers. Two routers are considered to be neighbours if they are attached to the same sub network.

- Neighbour acquisition

- Neighbour reachability

- Network reachability

- Neighbour acquisition procedures used for exchanging the routing information between two routers in different autonomous system. To perform neighbor acquisition, one router sends an open message to another.

- Once neighbor relationship is established the neighbor reachability procedure is used to maintain the relationship. Both sides needs to be assured that the other side still exists and is still engaged in the neighbor relationship.

- For this purpose both routers sends keep alive messages to each other. Both sides router maintains a database of the sub networks that it can reach and the preferred route for reaching that sub network.
• If the database changes, router issues an update message that is broadcast to all other routers implementing BGP.

• By the broadcasting of these up data message, all the BGP routers can build up and maintain routing information. BGP connections inside an autonomous system are called internal BGP(iBGP) and BGP connections between different autonomous system are called external BGP.

❖ BGP Messages:

0 8 16 24 31

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Marker</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td>Type</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• **Marker:** Marker field is used for authentication. The sender may insert value in this field that would be used as part of an authentication mechanism to enable the recipient to verify the identity the sender.

• **Length:** this field indicates the total length of the message in octets, including the BGP header.

• **Type:** Type field indicates type of message. There are four type of message type:
  - Open
  - Update
  - Notification
  - KEEPALIVE

• The KEEPALIVE message is just the BGP header with the type field. the KEEPALIVE message are exchanged often as to not cause the hold timer to expire.

• A recommended time between successive KEEPALIVE message is one-third of the hold time interval. This value ensures that KEEPALIVE messages arrive at the receiving router almost before the hold timer expires even if the transmission delay of a TCP is variable.

• When a BGP router detects an error the router sends a NOTIFICATION message the close the TCP Connection. After the connection is established, BGP peers exchange routing information by using the UPDATE messages.

• The UPDATE message may contain three pieces of information. Unfeasible routes, path attributes and network layer rechability information.
• An UPDATE message can withdraw multiple unfeasible routes from service. A BGP router uses Network layer Reachability information, the total path attributes length and the path attributes to advertise a route.

❖ **Advantage:**

• BGP is a very robust and scalable routing protocol.
• CIDR is used by BGP to reduce the size of the Internet routing tables
• BGP easily solves the count-to-infinity problem.

❖ **Disadvantage:**

• BGP is complex
• BGP routes to destination network, rather than to specific hosts.

![Diagram](image)
1. Describe the multiprotocol label switching’s (MPLS’s) working and operation? Compare MPLS with ATM network.

- MPLS is emerged as solution to problem identified with carrying IP over Asynchronous Transfer Mode-ATM networks.
- The ATM control is not directly compatible with IP; also the advantaged QoS mechanisms that ATM offered were not widely used except in carrier networks.
- Therefore, solutions were presented to use the efficient switching capability of ATM switches but to remove ATM control functionality and replace it with an alternatives control mechanism that is known as MPLS.

- MPLS is much more efficient mechanism to manage ATM switches also it is a general methodology for controlling circuit switched networks.
- It is called as “multiprotocol” because it can use multiple link layer protocol to carry labeled traffic of a number of higher network layer protocols.
- MPLS is not a particular protocol but a set of protocols that enable MPLS networking.
- Main component are:
  1. Label Switched Routers-LSR
  2. Edge Label Switched Routers-ELSR
- Every node in MPLS is an IP router on a control plane and there might be more than one protocol running on each node to exchange IP routing information between its peers within a network.
The routers in MPLS network contain an IP routing table which is used to exchange the label binding information. That information is used by the adjacent MPLS peers for exchanging labels for individual subnets, which is found in the routing table.

A specified LDP is used in label binding exchange for unicast destination based IP routing.

In MPLS transmission takes place on the basis of labels attached to packets that direct it all the way towards the destination and that is done only when labels are exchanged with adjacent peers in order to form a Label Forwarding Table.

A **Label Forwarding Table** is therefore acts as a database in forwarding packets within the MPLS network.

**LERs devices** are edge operators at the accessing network and MPLS networks and can support multiple ports connecting to dissimilar networks such as frame relay, ATM and Ethernet.

At each incoming packet a label is inserted (pushed) at the **edge router** (Ingress). With the help of signaling protocol label switch paths are established which help in forwarding the traffic onto MPLS network.
Label switch path is established using label signaling protocol. Label Switch Routers are the core routers in the MPLS domain and usually called core network routers.

As a packet enters in to MPLS network a label or labels are attached and as those packets leaves the MPLS networks those label are removed by the edge routers.

A Forwarding Equivalence Class (FEC) is a type of class that represents a group of packets that share the same characteristics and have the same requirements for transport.

Packets having the same FEC are forwarded in the same manner on the same path and given the same treatment.

In regular IP forwarding a router consider two packets to be in the same FEC, but in MPLS FEC is assigned to a packet only once by the label edge router as it enters the MPLS network.

Compare MPLS with ATM network

ATM and Multiprotocol Label Switching (MPLS) are data transport protocols, meaning that both reside above the physical data layers in the OSI model and aid in moving data from one point to another.

The primary difference between ATM and MPLS is that while ATM was designed to exist in a circuit-switched environment, MPLS has its place within modern packet-switched networks such as Ethernet or IP.

This difference is most apparent in how the two types of network topologies are deployed. ATM is primarily designed as a point-to-point connection, requiring an ATM adapter on each end of a physical or virtual circuit.

MPLS, on the other hand, operates similar to an Ethernet switch in an any-to-any topology, allowing each of the network endpoints to be connected to the MPLS network and mesh with a particular customer’s virtual mesh.

For ATM to replicate this level of meshing, multiple ATM connections would have to be installed at each of an organization’s locations.

The multi-protocol nature of MPLS also enables the technology to label and pass other protocols, including ATM, across an MPLS network.

Two ATM endpoints, for example, could be connected across an MPLS network, with the network itself quickly guiding traffic to each other transparently.

ATM, MPLS separate networks in their own right different service models, addressing, routing from Internet.

Viewed by Internet as logical link connecting IP routers just like dialup link is really part of separate network (telephone network)

2. Write a short note on SNMP (standard network management protocol).

Basic concepts of SNMP

SNMP protocols are specified in RFC 1157. It is a tool for multivendor, interoperable network management. It includes a protocol, a data base structure specification, and set of data objects.

It was adopted as the standard of TCP/IP based internets. RMON is a supplement to SNMP.
• SNMPv2 has functional enhancements to SNMP and codifies use of SNMP over OSI based networks.
• SNMPv3 defines a security capability for ANMP and architecture of future enhancements.

Operations Supported by SNMP
Generals operations:

• Get: Station retrieves a scalar object value from managed station.
• Set: Station updates a scalar object value from managed station.
• Trap: Station sends an unsolicited scalar object value to management station.

SNMP Formats
• The information is exchanged between management station and an agent as SNMP message. Every message has a version number, community name to be used for the exchange and any one of protocol data units. Various formats are:
  1. SNMP message
  2. Get request PDU
  3. Get response PDU
  4. Trap PDU
  5. Variable bindings

Strength of SNMP
• It is simple to implement.
• Agents are widely implemented.
• Agent level overhead is minimal.
• It is robust and extensible.
• Polling approach is good for LAN based managed object.
• It offers the best direct manager agent interface.
• SNMP meet a critical need.

Weakness of SNMP
• It is too simple and does not scale well.
• There is no object oriented data view.
• It has no standard control definition.
• It has many implementation specific (private MIB) extensions.
• It has high communication overhead due to polling.
3. **Write short note on Spanning tree protocol (STP).**

- STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network.
- For an Ethernet network to function properly, only one active path must exist at Layer 2 between two stations.

![Spanning Tree Protocol Diagram]

- **STP operation** is transparent to end stations, which do not detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.
- The Catalyst series switches use STP (IEEE 802.1D bridge protocol) on all Ethernet virtual LANS (VLANs). When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network.
- In STP, an algorithm calculates the best loop-free path throughout a Catalyst-switched network. The switches send and receive spanning-tree packets at regular intervals (2 seconds).
- The switches do not forward the packets, but use the packets to identify a loop-free path. The default configuration has STP enabled for all VLANs.
- Multiple active paths between stations cause loops in the network. If a loop exists in the network, you might receive duplicate messages.
- When loops occur, some switches see stations on both sides of the switch. This condition confuses the forwarding algorithm and allows duplicate frames to be forwarded.
- To provide path redundancy, STP defines a tree that spans all switches in an extended network.
- STP forces certain redundant data paths into a standby (blocked) state. If one network segment in the STP becomes unreachable, or if STP costs change, the spanning-tree algorithm
reconfigures the spanning-tree topology and reestablishes the link by activating the standby path.

- Defined as IEEE 802.1d
- It first elects a root bridge (only 1 per network); root bridge ports are called designated ports which operate as forwarding-state ports. Forwarding-state ports can send and receive traffic. Other switches in your network are non-root bridges.
- The non-root bridge’s port with the fastest link to the root bridge is called the root port, and it sends and receives traffic.
- Ports that have the lowest cost to the root bridge are called designated ports. The other ports on the bridge are considered non-designated and will not send or receive traffic, (blocking mode).
- Switches or bridges running STP, exchange information with what are called Bridge Protocol Data Units (BPDU). BPDUs send configuration information using multicast frames, BPDUs are also used to send the bridge ID of each device to other devices.
- The bridge ID is used to determine the root bridge in the network and to determine the root port. The Bridge ID is 8 bytes long, includes priority and MAC address. The default priority of devices using IEEE STP is 32,768.
- To determine the root bridge the priority and the MAC addresses are combined, if priority is the same, the MAC address is used to determine the who has the lowest ID, which determines who will be the root bridge.
- Path Cost is used to determine which ports will be used to communicate with the root bridge (designated ports). STP cost is the total accumulated path cost based on the bandwidth of the links. The slower the link the higher the cost.

**Spanning Tree Protocol Port States**

- **Blocking** - doesn’t forward any frames, but still listens to BPDUs. Ports default to blocking when the switch powers on. Used to prevent network loops. If a blocked port is to become the designated port, it will first enter listening state to ensure that it won't create a loop once it goes into forwarding state.
- **Listening** - listens to BPDUs to ensure no loops occur on the network before passing data frames.
- **Learning** - learns MAC addresses and builds filter table, doesn't forward frames.
- **Forwarding** - sends and receives all data on the bridge ports. A forwarding port has been determined to have the lowest cost to the root bridge.
4. Explain real time transport protocol (RTP).

- RTP is used for transporting PCM, GSM, and MP3 for sound and video formats in real-time formats.
- Real-time Transport Protocol (RTP) is the protocol designed to handle real-time traffic on the Internet.
- RTP does not have a delivery mechanism (multicasting, port numbers, and so on); it must be used with UDP. RTP stands between UDP and the application program. The main contributions of RTP are time-stamping, sequencing, and mixing facilities.
RTP basics

RTP Packet Format

- Figure shows the format of the RTP packet header. The format is very simple and general enough to cover all real-time applications.
- An application that needs more information adds it to the beginning of its payload. A description of each field follows.
- **Ver.**: This 2-bit field defines the version number. The current version is 2.
- **P.**: This 1-bit field, if set to 1, indicates the presence of padding at the end of the packet. In this case, the value of the last byte in the padding defines the length of the padding. Padding is the norm if a packet is encrypted. There is no padding if the value of the P field is 0.
- **X.**: This 1-bit field, if set to 1, indicates an extra extension header between the basic header and the data. There is no extra extension header if the value of this field is 0.
- **Contributor count**: This 4-bit field indicates the number of contributors. Note that we can have a maximum of 15 contributors because a 4-bit field only allows a number between 0 and 15.
- **M.**: This 1-bit field is a marker used by the application to indicate, for example, the end of its data.
- **Payload type**: This 7-bit field indicates the type of the payload. Several payload types have been defined so far.
- **Sequence number**: This field is 16-bits in length. It is used to number the RTP packets. The sequence number of the first packet is chosen randomly; it is incremented by 1 for each subsequent packet. The sequence number is used by the receiver to detect lost or out-of-order packets.
• **Payload number and audio/video encoding techniques:**

<table>
<thead>
<tr>
<th>Type</th>
<th>Application</th>
<th>Type</th>
<th>Application</th>
<th>Type</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>PCMμ Audio</td>
<td>7</td>
<td>LPC audio</td>
<td>15</td>
<td>G728 audio</td>
</tr>
<tr>
<td>1</td>
<td>1016</td>
<td>8</td>
<td>PCMA audio</td>
<td>26</td>
<td>Motion JPEG</td>
</tr>
<tr>
<td>2</td>
<td>G721 audio</td>
<td>9</td>
<td>G722 audio</td>
<td>31</td>
<td>H.261</td>
</tr>
<tr>
<td>3</td>
<td>GSM audio</td>
<td>10–11</td>
<td>L16 audio</td>
<td>32</td>
<td>MPEG1 video</td>
</tr>
<tr>
<td>5–6</td>
<td>DV14 audio</td>
<td>14</td>
<td>MPEG audio</td>
<td>33</td>
<td>MPEG2 video</td>
</tr>
</tbody>
</table>

• **Timestamp:** This is a 32-bit field that indicates the time relationship between packets. The timestamp for the first packet is a random number. For each succeeding packet, the value is the sum of the preceding timestamp plus the time the first byte is produced (sampled). For example, audio applications normally generate chunks of 160 bytes; the clock tick for this application is 160. The timestamp for this application increases 160 for each RTP packet.

• **Synchronization source identifier:** If there is only one source, this 32-bit field defines the source. However, if there are several sources, the mixer is the synchronization source and the other sources are contributors.

• The value of the source identifier is a random number chosen by the source. The protocol provides a strategy in case of conflict (two sources start with the same sequence number).

• **Contributor identifier:** Each of these 32-bit identifiers (a maximum of 15) defines a source. When there is more than one source in a session, the mixer is the synchronization source and the remaining sources are the contributors.

5. **Explain functionality of ARP and RARP protocol.**

**ARP Basics**

• The Address Resolution Protocol (ARP) was designed to provide a mapping from the logical 32-bit TCP/IP addresses to the physical 48-bit MAC addresses.

• Network interface cards (NICs) each have a hardware address or MAC address associated with them. Applications understand TCP/IP addressing, but network hardware devices, such as NICs.

• For example, when two Ethernet cards are communicating, they have no knowledge of the IP address being used.

• Instead, they use the MAC addresses assigned to each card to address data frames.

• Address resolution is the process of finding the address of a host within a network.

• In this case, the address is resolved by using a protocol to request information via a form of broadcast to locate a remote host.
How ARP Works

- When a data packet destined for a computer on a particular local area network arrives at a host or gateway, the ARP protocol is tasked to find a MAC address that matches the IP address for the destination computer.

- The ARP protocol then looks inside its cache table for the appropriate address.
- If the address is found, the destination address is then added in the data packet and forwarded.
- If no entry exists for the IP address, ARP broadcasts a request packet to all the machines on the local area network to determine which machine maintains that IP address.
- If found, the host with that IP address will send an ARP reply with its own MAC address.
• If the destination is on a remote subnet, the address of the router or gateway used to reach that subnet is placed in the packet and forwarded on.
• If the ARP cache does not contain an IP address for the router or gateway, it will use the same methods to resolve the address. The ARP cache is then updated for future reference and the original data packets are then forwarded to the correct host.
• As protocols go, ARP provides a very basic function. Only four types of messages can be sent out by the ARP protocol on any machine:
  o ARP request
  o ARP reply
  o RARP request
  o RARP reply

RARP Basics
• **Reverse Address Resolution Protocol (RARP)** is a network protocol used to resolve a data link layer address to the corresponding network layer address. For example, RARP is used to resolve an Ethernet MAC address to an IP address.
• A little-known protocol exists to facilitate the reverse function of ARP.
• RARP belongs to the OSI data link layer (layer 2).

How RARP works
• A RARP server containing these mappings can respond with the IP address for the requesting host.
• In most cases, a machine knows its own IP address; therefore RARP is primarily used for situations such as diskless workstations, or machines without hard disks.
• Dumb terminals and PCs are good examples of diskless workstations.
When a diskless system is booted up, it broadcasts a RARP request packet with its MAC address. This packet is received by all the hosts in the network.

When the RARP server receives this packet, it looks up this MAC address in the configuration file and determines the corresponding IP address.

It then sends this IP address in the RARP reply packet. The diskless system receives this packet and gets its IP address.

A RARP request packet is usually generated during the booting sequence of a host. A host must determine its IP address during the booting sequence. The IP address is needed to communicate with other hosts in the network.

When a RARP server receives a RARP request packet it performs the following steps:
  - The MAC address in the request packet is looked up in the configuration file and mapped to the corresponding IP address.
  - If the mapping is not found, the packet is discarded.
  - If the mapping is found, a RARP reply packet is generated with the MAC and IP address. This packet is sent to the host, which originated the RARP request.

When a host receives a RARP reply packet, it gets its IP address from the packet and completes the booting process. This IP address is used for communicating with other hosts, till it is rebooted.

The length of a RARP request or a RARP reply packet is 28 bytes.

6. Explain function of VP and VPC switches in ATM.

Understanding the Concept of Transmission Path, Virtual Path and Virtual Circuit

- ATM is a connection-oriented technology in which connection between two nodes is accomplished through TP, VP and VC.
- A TP is the physical channel. Such as co-axis cable and fiber-optic channel through which data is transmitted in the form of stream of bits.

![Figure: Pictorial Representation of VP & VC](image)

- A TP contains various VPs that connect two nodes or switch in an ATM network. These VPs in turn contain several VCs to carry the ATM cells. Figure 3 shows a pictorial representation of TP, VP and VC.
• To understand the concept of TP, VP and VC more clearly. Let’s take a simple analogy. Let us between an ATM network and the highway roads.
• Assume that the two nodes between which the data is to be transferred as two cities.
• A number of highways might be connecting these two cities together and we say that, so assume this set of highways as TP and.
• Out of this set each highway is as VP and which means set of all VPs is a TP. Further, the lanes of on the highway can be considered as VC; therefore which means the set of all VCs is a VP.

Understanding ATM Virtual Connection and Identifiers
• A VC as discussed in the preceding section is analogous to a lane in a highway, which carries a single line of vehicles through it.
• These VC forms a Virtual Channel Connection (VCC) that links two users or devices. Similarly, a VP is analogous to a highway that has many lanes through it. Consequently, a set of all VCCs form a Virtual Path Connection (VPC).
• ATM is a VC network, and to transfer data from one node to another, it is necessary to identify the virtual connection through which the cells would be sent.
• Therefore, ATM uses a pair of identifiers, namely a Virtual Circuit Identifier (VCI) and Virtual Path Identifier (VPI) to identify the virtual connections.
• A VCI defines a particular VC through which stream of cells of single message will flow. A VPI defines a particular VP where in all VCs bundled into this VP will have the same VPI.
• These VPI and VCI are integer identifiers and their length for different interfaces differs which will be discussed in subsequent sections.

7. Explain time division multiplexing in ATM.

![Time-division multiplexing (TDM).](image)

Figure: Time-division multiplexing (TDM).

• Time-division multiplexing (TDM) is a digital technology.
• TDM involves sequencing groups of a few bits or bytes from each individual input stream, one after the other, and in such a way that they can be associated with the appropriate receiver.
• If done sufficiently and quickly, the receiving devices will not detect that some of the circuit time was used to serve another logical communication path.
• For example, an application requiring four terminals at an airport to reach a central computer. Each terminal communicated at 2400 bps, so rather than acquire four individual circuits to carry such a low-speed transmission; the airline has installed a pair of multiplexers.

• A pair of 9600 bps modems and one dedicated analog communications circuit from the airport ticket desk back to the airline data center are also installed. Synchronous time division multiplexing (Sync TDM):

There are two types of Time-division multiplexing:

1. Synchronous Time division multiplexing (Sync TDM)

2. Statistical time-division multiplexing (Stat TDM)
   There are three types of (Sync TDM): T1, SONET/SDH and ISDN

Synchronous digital hierarchy (SDH):

• Be service-oriented – SDH must route traffic from End Exchange to End Exchange without worrying about exchanges in between, where the bandwidth can be reserved at a fixed level for a fixed period of time.

• Allow frames of any size to be removed or inserted into an SDH frame of any size.

• Easily manageable with the capability of transferring management data across links.

• Provide high levels of recovery from faults.

• Provide high data rates by multiplexing any size frame, limited only by technology.

• Give reduced bit rate errors.

• SDH has become the primary transmission protocol in most PSTN networks. It was developed to allow streams 1.544 Mbit/s and above to be multiplexed, in order to create larger SDH frames known as Synchronous Transport Modules (STM). The STM-1 frame consists of smaller streams that are multiplexed to create a 155.52 Mbit/s frame. SDH can also multiplex packet based frames e.g. Ethernet, PPP and ATM.

Statistical time-division multiplexing (Stat TDM):

• STDM is an advanced version of TDM in which both the address of the terminal and the data itself are transmitted together for better routing.

• Using STDM allows bandwidth to be split over 1 line. Many college and corporate campuses use this type of TDM to logically distribute bandwidth.

• If there is one 10MBit line coming into the building, STDM can be used to provide 178 terminals with a dedicated 56k connection (178 * 56k = 9.96Mb). A more common use however is to only grant the bandwidth when that much is needed. STDM does not reserve a time slot for each terminal, rather it assigns a slot when the terminal is requiring data to be sent or received.
This is also called asynchronous time-division multiplexing (ATDM), in an alternative nomenclature in which "STDM" or "synchronous time division multiplexing" designates the older method that uses fixed time slots.

8. Compare IPv4 and IPv6 with their header format.

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Header size is 32 bits.</td>
<td>1. Header size is 128 bit.</td>
</tr>
<tr>
<td>2. It cannot support auto configuration.</td>
<td>2. Supports auto configuration</td>
</tr>
<tr>
<td>3. Cannot support real time application.</td>
<td>3. Supports real time application</td>
</tr>
<tr>
<td>4. No security at network layer</td>
<td>4. Provides security at network layer</td>
</tr>
<tr>
<td>5. Throughput and delay is more.</td>
<td>5. Throughput and delay is less</td>
</tr>
</tbody>
</table>

IPv4 vs. IPv6 Header format:

9. Write and explain ATAMP packet format.

10. Write a short note on Storage Area Network.

- A Storage Area Network (SAN) is defined as a set of interconnected devices (for example, disks and tapes) and servers that are connected to a common communication and data transfer infrastructure such as fiber channel.
- A SAN is a network designed to transfer data from servers to targets, and it is alternative to directly attached target architecture, or to a DAS architecture, where the storage is connected to the serves on general purpose networks.
• Multiple technology can be used when building a SAN; traditionally the dominant technology is fiber channel, but IP based solutions are also quite popular for specific applications.
• The concept of SAN is also independent from the devices that are attached to it. Can be disks, tapes, RAID, file servers, or other.
• The purpose of the SAN is to allow multiple servers access to a pool of storage in which any server can potentially access any storage unit.

Storage area network requirement
• Serial transmission for high speed and long distance
• Low transmission errors
• Low delay of transmitted data. Needs to make it feel like using a local disk
• The disk subsystem has around 1 ms – 10 ms latency itself
• The communication protocol should not use CPU.

SAN environment provides the following benefits
• Centralization of storage into a single pool. This allows storage resources and server resources to grow independently, and allows storage to be dynamically assigned from the pool as and when it required.
• Common infrastructure for attaching storage allows a single common management model for configuration and deployment.
• Storage devices are inherently shared by multiple systems. Ensuring data integrity guarantees and enforcing security policies for access rights to a given device is a core part of the infrastructure.
• Data can be transferred directly from device to device without server intervention.
• Because multiple servers have direct access to storage devices, SAN technology is particularly interesting as a way to build clusters where shared access to a data set is required.

• Write short note on Inter Gateway Routing Protocol (IGRP)

• Interior Gateway Routing Protocol (IGRP) is a Cisco-proprietary distance-vector routing protocol. This means that to use IGRP in your network. All your routers must be Cisco routers.
• Cisco created this routing protocol to overcome the problem associated with RIP.
• The main difference between RIP and IGRP configuration is that when IGRP is configured the autonomous system number is to be supplied. All routers must use the same number in order to share routing table information.
• IGRP has a maximum hop count of 255 with a default of 100. This is helpful in larger networks and solves the problem of 15 hops being the maximum possible in a RIP network.
Comparison of IGRP and RIP

<table>
<thead>
<tr>
<th></th>
<th>IGRP</th>
<th>RIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Uses an autonomous system number for</td>
<td>2. Does not use autonomous system numbers.</td>
</tr>
<tr>
<td></td>
<td>activation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>seconds.</td>
<td>seconds.</td>
</tr>
<tr>
<td>4.</td>
<td>Has an administrative distance of 100.</td>
<td>4. Has an administrative distance of 120.</td>
</tr>
<tr>
<td>5.</td>
<td>Uses bandwidth and delay of the lines as</td>
<td>5. Use only hop count to determine the best</td>
</tr>
<tr>
<td></td>
<td>metric (lowest composite metric), with a</td>
<td>path to remote networks, with 15 hops</td>
</tr>
<tr>
<td></td>
<td>maximum hop count of 255.</td>
<td>being the maximum.</td>
</tr>
</tbody>
</table>

11. **Give & Explain traffic characteristics.**

1. **Delay**

Delay is the time required for a signal to traverse the network. End-to-end delay is the sum of delay at different network devices across the network. Many factors contribute to end-to-end delay.

- **PSTN Delay:** Due to long distance delay
- **IP network Delay:** Because of buffering, queuing, switching, routing delay.
- **Packet capture delay:** It is time required to receive entire packet before processing and forwarding through router determined by packet length and transmission speed.
- **Switching/routing delay:** It is the time that router takes to switch the packet. It depends on architecture of route engine and size of routing table.
- **Queuing delay:** Queuing delay exists due to statistical multiplexing. It is a function of traffic load on packet switch and packet length.
- **VOIP device delay:** it is due to signal processing (codec) at both ends. The more complex the processing longer this delay component.

`Jitter`

- Jitter is defined as variation in the delay of received packets. Jitter is caused by network congestion, timing drift, improper queuing, configuration errors, electromagnetic interference, and cross-talk.
- Jitter is the deviation in or displacement of some aspect of pulses in high-frequency digital signal. The deviation can be in terms of amplitude, phase timing, or the width of the signal pulse. A delay buffer is used to eliminate the effect of jitter.
- Large jitter causes packets to be received out of range i.e. packets are discarded. This missing packet creates problem.
- In frame relay three parameters need to be addressed to find the jitter.
  a. Traffic Shaping
  b. Fragmentation

Prepared by: M. D. Trivedi
2. Jitter Control

- Jitter is variation in delay for packets belonging to the same flow.
- For applications such as audio and video streaming, it does not matter much if the packets take 20 msec or 30 msec to be delivered, as long as the transmit time is constant.
- Real time audio and video cannot tolerate high jitter. For example, a real time video broadcast is useless if there is a 2 ms delay for the first and second packets and 60 ms delay for the third and fourth.
- On the other hand, it does not matter if packets carrying information in a file have different delays.
- The transport layer at the destination waits until all arrive before delivery to the application layer.

![Diagram showing high and low jitter](image)

*Figure shows the high and low jitter.*

- When a packet arrives at a router, the router checks to see how much the packet is behind or ahead of the schedule. This information is stored in the packet and update on each hop.
- If the packet is ahead of the schedule, it is held just long enough to get it back on schedule. If it is a behind schedule, the router tries to get it out the door quickly.
- In this way, packets that are ahead of schedule get slowed down and packet that are behind schedule get speeded up, in both cases reducing the amount of jitter.
- The application such as video on demand, jitter can be eliminated by buffering at the receiver and then forwarding data for display from the buffer instead of from the network in real time.

3. Throughput

1. Throughput:
   - The amount of data transferred from one place to another or processed in a specified amount of time. Data transfer rates for networks are measured in terms of throughput. Typically, throughputs are measured in Kbps, Mbps or Gbps.
2. **Offered traffic:**
   - The offered traffic is the average number of packets per slot time which are presented to the network for transmission by users. It is denoted by $G$. The throughput is expressed in terms of offered load or traffic $G$. Practically $G$ can have any value between 0 to infinity.

3. **Channel capacity**
   - The maximum achievable throughput for a particular type of access scheme is called the capacity of the channel.
   - To find the throughput of channel. Let us assume that the probability ($p_k$) that $k$ packets generated during a given slot-time follows a Poisson’s distribution with a mean $G$ per packet time is given by
     \[ p_k = \frac{G^k e^{-G}}{k!} \]
   - The throughput $S$ is then just the offered load $G$ times the probability of a transmission being successful.
     \[ S = G \cdot p_0 \]

Where $p_0 = \text{probability that a packet does not suffer a collision}$

- The probability of no other traffic being initiated during the entire vulnerable period is thus given by
  \[ p_0 = e^{-2G} \]

From equation
\[ S = G \cdot e^{-2G} \]

4. **Bandwidth**
   - Bandwidth is the difference between the top and bottom limiting frequencies of a continuous frequency band.
   - Bandwidth indicates the information carrying capacity of a particular channel. Digital transmission capacity is expressed in bps or Mbps.
   - Fiber optics bandwidth is often expressed as capacity to transmit information within a specific time period for a specific length. (i.e. 12 Mbps/km).
   - Wide bandwidth can support large amount of data transfer but there are physical and technical limitations for the channel or media.

1. **Nyquist Bit Rate**
   - Nyquist bit rate defines the theoretical maximum bit rate for a noiseless channel or ideal channel.
• The formula for maximum bit rate in bits per second (bps) is:

\[
\text{Max. bit rate} = 2 \times BW \times \log_2 L
\]

Where, \(BW\) = Bandwidth at channel
\(L\) = No. of signal levels used to represent data

2. Shannon Capacity

• An ideal noiseless channel never exists. The maximum data rate for any noisy channel is:

\[
C = BW \times \log_2 \left(1 + \frac{S}{N}\right)
\]

Where, \(C\) = Channel capacity in bits per second
\(BW\) = Bandwidth of channel
\(\frac{S}{N}\) = Signal - to - Noise ratio

• The channel capacity is also called as Shannon capacity. The channel capacity does not depend upon the signal levels used to represent the data.

5. Reliability and Survivability

Survivability

• Network Survivability is the ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques.

Reliability

• Network reliability is:
  o Availability of end to end functionality for customers.
  o Ability to experience failures or systematic attacks without impacting operations.

• Network reliability include following aspects – Survivability, dependability, robustness, fault tolerance, maintainability, scalability.

• Network reliability is the ability of the network to provide the required function end to end for a specified period of time.

6. Quality of Service

Requirements

• A stream of packets from a source to destination is called a flow.

• Application with their quality of service requirements is given below.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Application</th>
<th>Reliability</th>
<th>Delay</th>
<th>Jitter</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>E-mail</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>File transfer</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>Web access</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>Remote login</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
</tbody>
</table>
12. Explain business requirement, technical requirements and challenges in traffic engineering.

**Business challenge & Requirement**
Challenges faced by corporate management are:
1. Requirements for increasing the business.
2. Maintain the financial control.
3. Complete the current competitive environment.
4. Integrate the business operations with suppliers, partners and customers.

Business requirements are:
2. Financial control
3. Competitiveness
4. Business coverage
5. Adaptability
6. Security
7. Customer support

**Technical challenge & Requirement**
The technical challenges for establishing network are;
1. Interconnection
2. Compatibility of network
3. Reliability of network
4. Availability of network

Technical requirements are:
1. Scalability
2. Portability
3. Accessibility
4. Performance
5. Security
6. Reliability & availability
7. Architecture
8. Storage
13. **Explain network management architecture.**

Three important components of network management architecture are:

1. Managing entity
2. Managed devices
3. Network management protocol

![Diagram of network management architecture](image)

Figure shows principal components of network management architecture.

- Managing entity is an application. It controls the collection, processing, analysis of networks management information.
- A managed device is network equipment. It can be a host, router, bridge, hub, printer or modem. A managed device may have several managed objects or pieces of hardware.
- The objects have information associated with them. This information is collected into **Management Information Base (MIB).**
- Also in each managed device a **network management agent** is residing. It is a process running in the managed device that communications with the managing entity, taking local actions at the managed device. Under the command and control of the managing entity.
- **Network management protocol** runs between managing entity and managed devices and indirectly takes actions at these devices through its agents. It is a tool by which network administrator can manage the network.

14. **Write and explain ATMARP packet format. (Same as ARP)**

- ATMARP provides a means of resolving Internet Protocol (IP) addresses to ATM addresses.

15. **List and explain five commands to configure router. (Practical file)**