NETWORKING ANALYST
(Interview Questions)
Compiled by: Rajashekar Tuppada
Document Reference Code: i3Q-SDTC-NAS-0101

1. PURPOSE

- The Purpose of this document is to provide the basic understanding of the Computer Networks fundamentals to face the Interview for the Network Analyst Role in any Information Technology Organization
- This document helps you with the Frequently Asked Questions(FAQ) during the Interview for the Network Analyst Role
- The Document Provides Pictorial Representation of the various Topics for the formidable Understanding and takes a head for your Success
- This article is useful for those who are attending the interview on Networking. As networking is a complex topic, one needs to be careful while answering the questions in an interview. If you go through the interview questions on the networking of this article, you can easily get through the interview

Disclaimer: These are just the guidelines but not the only Questions

2. PART 1: NETWORKING QUESTIONS

2.1. What is a Network

Network is defined as a set of devices connected to each other using a physical transmission medium.

For Example,
A computer network is a group of computers connected with each other to communicate and share information and resources like hardware, data, and software. In a network, nodes are used to connect two or more networks.

2.2. What is a Node

Two or more computers are connected directly by an optical fiber or any other cable. A node is a point where a connection is established. It is a network component that is used to send, receive and forward the electronic information.

A device connected to a network is also termed as Node. Let's consider that in a network there are 2 computers, 2 printers, and a server are connected, then we can say that there are five nodes on the network.

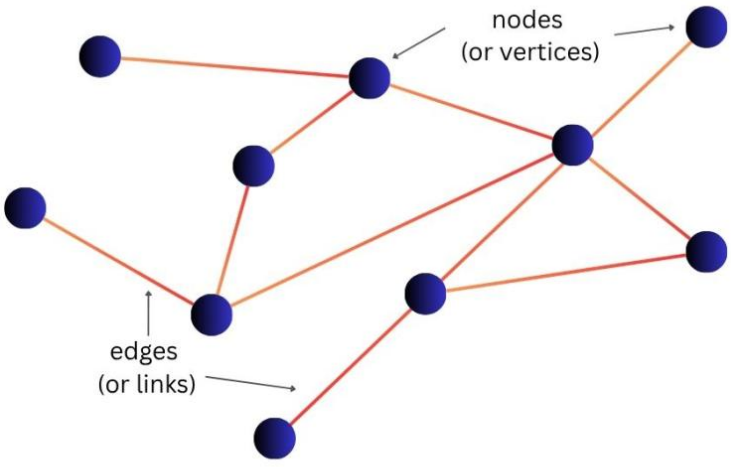

Fig. 2.2(1)

2.3. What is Network Topology

Network topology is a physical layout of the computer network and it defines how the computers, devices, cables, etc are connected to each other.

© i3Qube Software 2023 Confidential

2.4. What are Routers

The router is a network device that connects two or more network segments. It is used to transfer information from the source to the destination.

Routers send the information in terms of data packets and when these data packets are forwarded from one router to another router then the router reads the network address in the packets and identifies the destination network.

2.5. What is the OSI Reference Model

Open System Interconnection(OSI), the name itself suggests that it is a reference model that defines how applications can communicate with each other over a networking system.

It also helps to understand the relationship between networks and defines the process of communication in a network.

2.6. What are the Layers in OSI Reference Model, Describe Each Layer Briefly

There are Seven layers in OSI Reference Models:

1. Physical Layer (Layer 1):
   It converts data bits into electrical impulses or radio signals.
   Example: Ethernet

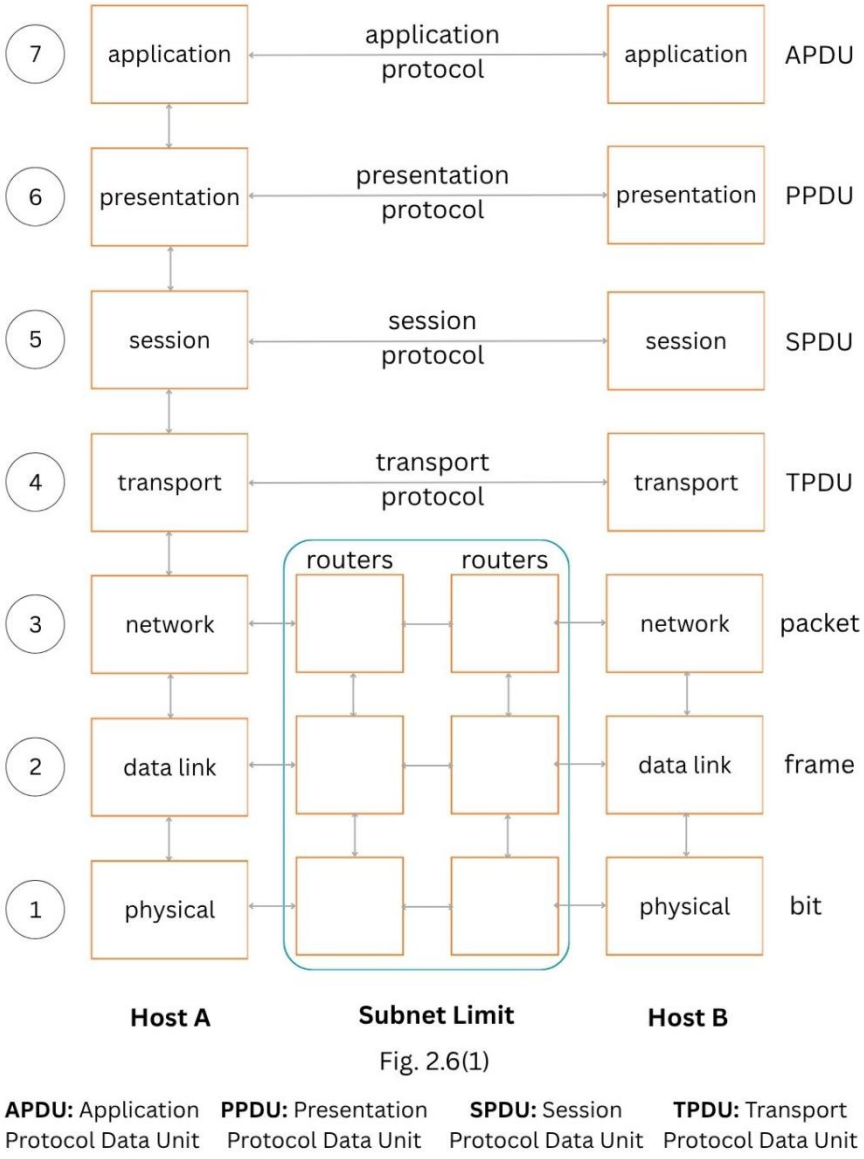

Fig. 2.6(1)

APDU: Application Protocol Data Unit **PPDU:** Presentation Protocol Data Unit **SPDU:** Session Protocol Data Unit **TPDU:** Transport Protocol Data Unit

© i3Qube Software 2023 Confidential

2. Data Link Layer (Layer 2):
   At the Data Link layer, data packets are encoded and decoded into bits and it provides a node to node data transfer. This layer also detects the errors that occurred at Layer 1.
3. Network Layer (Layer 3):
   This layer transfers variable length data sequence from one node to another node in the same network. This variable-length data sequence is also known as "Datagrams".
4. Transport Layer (Layer 4):
   It transfers data between nodes and also provides acknowledgment of successful data transmission. It keeps track of transmission and sends the segments again if the transmission fails.
5. Session Layer (Layer 5):
   This layer manages and controls the connections between computers. It establishes, coordinates, exchange and terminates the connections between local and remote applications.
6. Presentation Layer (Layer 6):
   It is also called as "Syntax Layer". Layer 6 transforms the data into the form in which the application layer accepts.
7. Application Layer (Layer 7):
   This is the last layer of the OSI Reference Model and is the one that is close to the end-user. Both end-user and application layer interacts with the software application. This layer provides services for email, file transfer, etc.

2.7. What is the difference between Hub, Switch and Router

Hub	Switch	Router
Hub is least expensive, least intelligent and least complicated of the three. It broadcast all data to every port which may cause serious security and reliability concern	Switches work similarly like Hubs but in a more efficient manner. It creates connections dynamically and provides information only to the requesting port	The router is smartest and most complicated out of these three. It comes in all shapes and sizes. Routers are similar like little computers dedicated for routing network traffic
In a Network, Hub is a common connection point for devices connected to the network. Hub contains multiple ports and is used to connect segments of LAN	Switch is a device in a network which forwards packets in a network	Routers are located at gateway and forwards data packets

2.8. Explain TCP/IP Model

The most widely used and available protocol is TCP/IP i.e. Transmission Control Protocol and Internet Protocol. TCP/IP specifies how data should be packaged, transmitted and routed in their end to end data communication.

Terms:

- Telnet:
  Telnet is a network protocol and command-line tool used to connect to remote computers and network devices over a local area network or the internet.
- FTP:
  FTP (File Transfer Protocol) is a standard network protocol used to transfer files between a client and a server over a TCP/IP network.

© i3Qube Software 2023 Confidential

- SMTP:

  SMTP (Simple Mail Transfer Protocol) is an application-layer communication standard used to send and relay electronic mail messages across a network.
- DNS:

  DNS stands for the Domain Name System, which acts as the phone book of the internet by translating human-readable website names into machine-readable IP addresses.
- RIP:

  Routing Information Protocol (RIP) is an old distance-vector routing protocol that uses hop count to find the best path for data across a small network.
- SNMP:

  Simple Network Management Protocol (SNMP) is an application-layer standard used to monitor, configure, and manage connected network devices like routers, switches, and servers.
- UDP:

  User Datagram Protocol (UDP) is a fast, connectionless transport layer protocol that sends data packets (datagrams) without a prior handshake or delivery guarantee.
- IGMP:

  The Internet Group Management Protocol (IGMP) is a network layer protocol used on IPv4 networks to manage multicast group memberships between hosts and routers.
- ICMP:

  The Internet Control Message Protocol (ICMP) is a network-layer protocol used by routers and devices to send error messages and operational information.
- IPSEC:

  IPsec (Internet Protocol Security) is a secure network protocol suite that authenticates and encrypts data packets to provide safe, encrypted communication over public networks like the internet.
- Ethernet:

  Ethernet is a wired technology used to connect devices in a local area network (LAN) for fast, secure, and reliable data transfer.
- Token Ring:

  A Token Ring network is a local area network (LAN) technology where devices are connected in a logical ring and use a token-passing method to control data transmission.
- Frame Relay:

  Frame relay is a fast, cost-effective wide area network (, WAN) protocol that connects multiple local area networks (, LANs) using shared packet-switching infrastructure.
- ATM:

  Asynchronous Transfer Mode (ATM) network is a high-speed telecommunications standard that uses connection-oriented cell switching to integrate data, voice, and video traffic.

There are four layers as shown below:

- Application Layer:

  This is the top layer in the TCP/IP model. It includes processes that use the Transport Layer Protocol to transmit the data to their destination. There are different Application Layer Protocols such as HTTP, FTP, SMTP, SNMP protocols, etc.

© i3Qube Software 2023 Confidential

- Transport Layer:

  It receives the data from the Application Layer which is above the Transport Layer. It acts as a backbone between the host's system connected with each other and it mainly concerns about the transmission of data. TCP and UDP are mainly used as Transport Layer protocols.

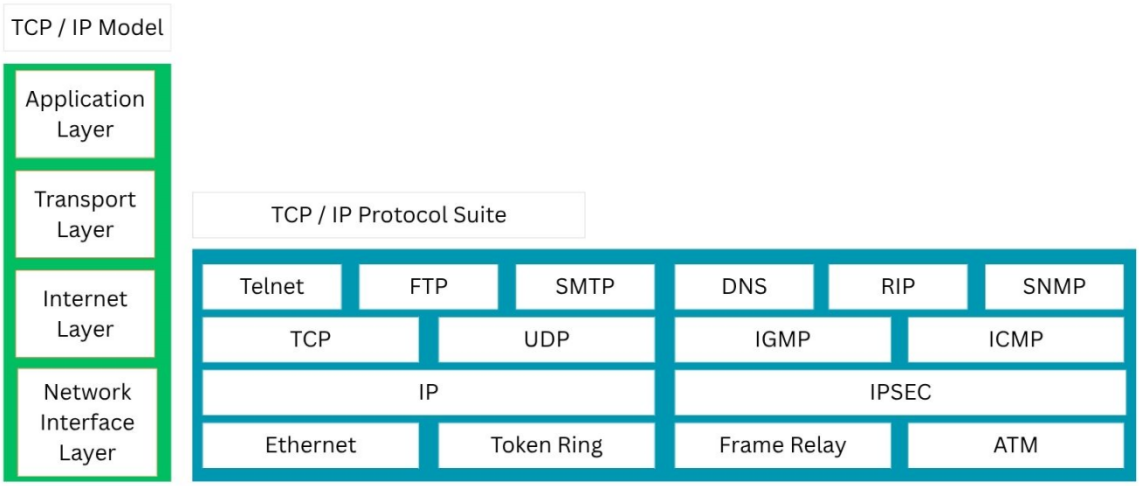

Fig. 2.8(1)

- Network or Internet Layer:

  This layer sends the packets across the network. Packets mainly contain source & destination IP addresses and actual data to be transmitted.

- Network Interface Layer:

  It is the lowest layer of the TCP/IP model. It transfers the packets between different hosts. It includes encapsulation of IP packets into frames, mapping IP addresses to physical hardware devices, etc.

2.9. What is HTTP and What Port does it Use

HTTP is HyperText Transfer Protocol and is responsible for web content. Many web pages are using HTTP to transmit the web content and allow the display and navigation of HyperText. It is a primary protocol and port used here is TCP port 80.

2.10. What is HTTPs and What Port does it Use

HTTPs is a Secure HTTP. HTTPs is used for secure communication over a computer network. HTTPs provides authentication of websites that prevents unwanted attacks. In bi-directional communication, the HTTPs protocol encrypts the communication so that the tampering of the data gets avoided. With the help of an SSL certificate, it verifies if the requested server connection is a valid connection or not. HTTPs use TCP with port 443.

2.11. What are TCP and UDP

Common factors in TCP and UDP are:

- TCP and UDP are the most widely used protocols that are built on the top of the IP protocol.
- Both protocols TCP and UDP are used to send bits of data over the Internet, which is also known as 'packets'.
- When packets are transferred using either TCP or UDP, it is sent to an IP address. These packets are traversed through routers to the destination.

The difference between TCP and UDP are:

TCP	UDP
TCP stands for Transmission Control Protocol	UDP is stands for User Datagram Protocol or Universal Datagram Protocol

© i3Qube Software 2023 Confidential

Once the connection is setup, data can be sent bi-directional i.e. TCP is a connection oriented protocol	UDP is connectionless, simple protocol. Using UDP, messages are sent as packets
The speed of TCP is slower than UDP	UDP is faster compared to TCP
TCP is used for the application where time is not critical part of data transmission	UDP is suitable for the applications which require fast transmission of data and time is crucial in this case.
TCP transmission occurs in a sequential manner	UDP transmission also occurs in a sequential manner but it does not maintain the same sequence when it reaches the destination
It is heavy weight connection	It is lightweight transport layer
TCP tracks the data sent to ensure no data loss during data transmission	UDP does not ensure whether receiver receives packets are not. If packets are misses then they are just lost

2.12. What is Firewall

Firewall is a network security system that is used to protect computer networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.

The firewall consists of a hardware device, software program or a combined configuration of both. All the messages that route through the firewall are examined by specific security criteria and the messages which meet the criteria are successfully traversed through the network or else those messages are blocked

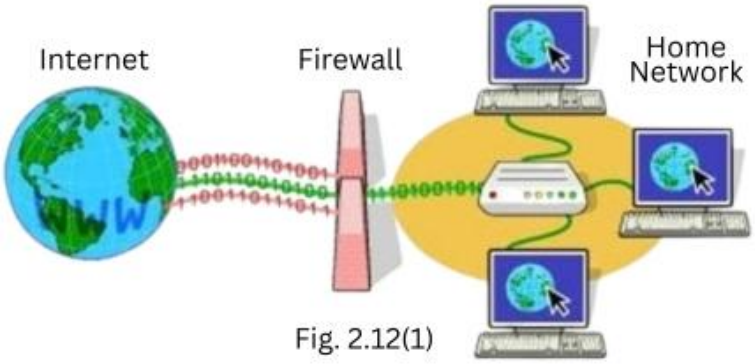

Fig. 2.12(1)

Firewalls can be installed just like any other computer software and later can be customized as per the need and have some control over the access and security features."

Windows Firewall" is an inbuilt Microsoft Windows application that comes along with the operating system. This "Windows Firewall" also helps to prevent viruses, worms, etc.

2.13. What is DNS

Domain Name Server (DNS), in a non-professional language and we can call it an Internet's phone book. All the public IP addresses and their hostnames are stored in the DNS and later it translates into a corresponding IP address.

For a human being, it is easy to remember and recognize the domain name, however, the computer is a machine that does not understand the human language and they only understand the language of IP addresses for data transfer.

There is a "Central Registry" where all the domain names are stored and it gets updated on a periodic basis. All Internet service providers and different host companies usually interact with this central registry to get the updated DNS details.

For Example,

© i3Qube Software 2023 Confidential

When you type a website www.softwaretestinghelp.com, then your Internet service provider looks for the DNS associated with this domain name and translates this website command into a machine language – IP address – 151.144.210.59 (note that, this is the imaginary IP address and not the actual IP for the given website) so that you will get redirected to the appropriate destination.

This process is explained in the below diagram:



Fig. 2.13(1)

2.14. What is the difference between Domain and a Workgroup

In a computer network, different computers are organized in different methods and these methods are – Domains and Workgroups. Usually, computers which run on the home network belong to a Workgroup.

However, computers that are running on an office network or any workplace network belong to the Domain.

Their differences are as follows:

Workgroup	Domain
All computers are peers and no computer has control over another computer	Network admin uses one or more computer as a server and provide all accesses, security permission to all other computers in a network
In a Workgroup, each computer maintains their own database	The domain is a form of a computer network in which computers, printers, and user accounts are registered in a central database.
Each computer has their own authentication rule for every user account	It has centralized authentication servers which set the rule of authentication
Each computer has set of user account. If user has account on that computer then only user able to access the computer	If user has an account in a domain then user can login to any computer in a domain
Workgroup does not bind to any security permission or does not require any password	Domain user has to provide security credentials whenever they are accessing the domain network
Computer settings need to change manually for each computer in a Workgroup	In a domain, changes made in one computer automatically made same changes to all other computers in a network
All computers must be on same local area network	In a domain, computers can be on a different local network
In a Workgroup, there can be only 20 computers connected	In a domain, thousands of computers can be connected

© i3Qube Software 2023 Confidential

2.15. What is the Proxy Server and How do they Protect the Computer Network

For data transmission, IP addresses are required and even DNS uses IP addresses to route to the correct website. It means without the knowledge of correct and actual IP addresses it is not possible to identify the physical location of the network.

Proxy servers prevent external users who are unauthorized to access such IP addresses of the internal network. It makes the computer network virtually invisible to external users.



Fig. 2.15(1)

Proxy Server also maintains the list of blacklisted websites so that the internal user is automatically prevented from getting easily infected by viruses, worms, etc.

2.16. What are IP Classes and How can you Identify the IP Class of given IP Address

An IP address has 4 sets (octets) of numbers each with a value up to 255.

For Example,

the range of the home or commercial connection started primarily between 190 x or 10 x. IP classes are differentiated based on the number of hosts it supports on a single network. If IP classes support more networks then very few IP addresses are available for each network.

There are three types of IP classes and are based on the first octet of IP addresses which are classified as Class A, B or C. If the first octet begins with 0 bit then it is of type Class A.

Class A type has a range up to 127.x.x.x (except 127.0.0.1). If it starts with bits 10 then it belongs to Class B. Class B having a range from 128.x to 191.x. IP class belongs to Class C if the octet starts with bits 110. Class C has a range from 192.x to 223.x.

2.17. What is meant by 127.0.0.1 and localhost

IP address 127.0.0.1, is reserved for loopback or localhost connections. These networks are usually reserved for the biggest customers or some of the original members of the Internet. To identify any connection issue, the initial step is to ping the server and check if it is responding.

If there is no response from the server then there are various causes like the network is down or the cable needs to be replaced or the network card is not in good condition. 127.0.0.1 is a loopback connection on the Network Interface Card (NIC) and if you are able to ping this server successfully, then it means that the hardware is in a good shape and condition.

127.0.0.1 and localhost are the same things in most of the computer network functioning.

© i3Qube Software 2023 Confidential

2.18. What is NIC

NIC stands for Network Interface Card. It is also known as Network Adapter or Ethernet Card. It is in the form of an add-in card and is installed on a computer so that the computer can be connected to a network.

Each NIC has a MAC address which helps in identifying the computer on a network.

2.19. What is Data Encapsulation

In a computer network, to enable data transmission from one computer to another, the network devices send messages iin the form of packets. These packets are then added with the IP header by the OSI reference model layer.

The Data Link Layer encapsulates each packet in a frame that contains the hardware address of the source and the destination computer. If a destination computer is on the remote network then the frames are routed through a gateway or router to the destination computer.

2.20. What is the difference between Internet, Intranet and Extranet

The terminologies Internet, Intranet, and Extranet are used to define how the applications in the network can be accessed. They use similar TCP/IP technology but differ in terms of access levels for each user inside the network and outside the network.

- Internet:
  Applications are accessed by anyone from any location using the web.
- Intranet:
  It allows limited access to users in the same organization.
- Extranet:
  External users are allowed or provided with access to use the network application of the organization.

2.21. What is a VPN

VPN is the Virtual Private Network and is built on the Internet as a private wide area network. Internet-based VPNs are less expensive and can be connected from anywhere in the world.

VPNs are used to connect offices remotely and are less expensive when compared to WAN connections. VPNs are used for secure transactions and confidential data can be transferred between multiple offices. VPN keeps company information secure against any potential intrusion.

Three types of VPN's are:

- Access VPN:
  Access VPN's provide connectivity to mobile users and telecommuters. It is an alternative option for dial-up connections or ISDN connections. It provides low-cost solutions and a wide range of connectivity.
- Intranet VPN:
  They are useful for connecting remote offices using shared infrastructure with the same policy as a private network.
- Extranet VPN:
- Using shared infrastructure over an intranet, suppliers, customers, and partners are connected using dedicated connections.

© i3Qube Software 2023 Confidential

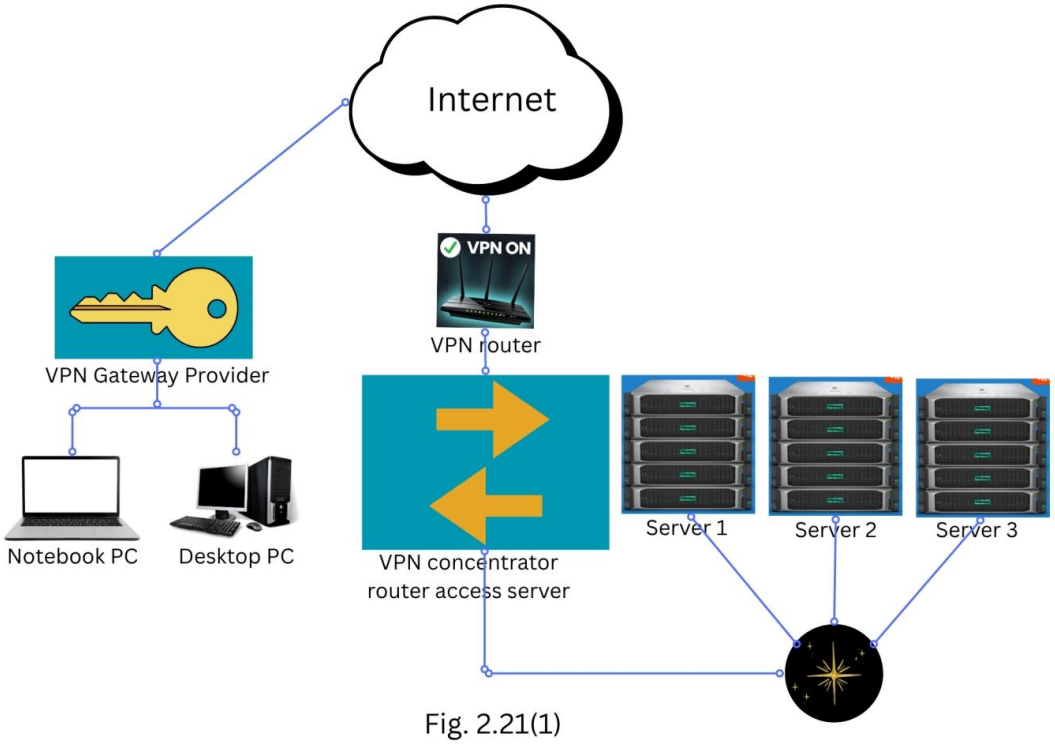

Fig. 2.21(1)

2.22. What are ipconfig and ifconfig

ipconfig stands for Internet Protocol Configuration and this command is used on Microsoft Windows to view and configure the network interface.

The command Ipconfig is useful for displaying all TCP/IP network summary information currently available on a network. It also helps to modify the DHCP protocol and DNS setting.

ifconfig (Interface Configuration) is a command that is used on Linux, Mac, and UNIX operating systems. It is used to configure, control the TCP/IP network interface parameters from CLI i.e. Command Line Interface. It allows you to see the IP addresses of these network interfaces.

2.23. Explain DHCP briefly

DHCP stands for Dynamic Host Configuration Protocol and it automatically assigns IP addresses to the network devices. It completely removes the process of manual allocation of IP addresses and reduces the errors caused due to this.

This entire process is centralized so that the TCP/IP configuration can also be completed from a central location. DHCP has a "pool of IP addresses" from which it allocates the IP address to the network devices. DHCP cannot recognize if any device is configured manually and assigned with the same IP address from the DHCP pool.

In this situation, it throws the "IP address conflict" error.

DHCP environment requires DHCP servers to set-up the TCP/IP configuration. These servers then assign, release and renew the IP addresses as there might be a chance that network devices can leave the network and some of them can join back to the network.

© i3Qube Software 2023 Confidential



Fig. 2.23(1)

2.24. What is SNMP

SNMP stands for Simple Network Management Protocol. It is a network protocol used for collecting organizing and exchanging information between network devices. SNMP is widely used in network management for configuring network devices like switches, hubs, routers, printers, servers.

SNMP components:

- SNMP Manager
- Managed device
- SNMP Agent
- Management Information Base (MIB)

The below diagram shows how these components are connected with each other in the SNMP architecture:

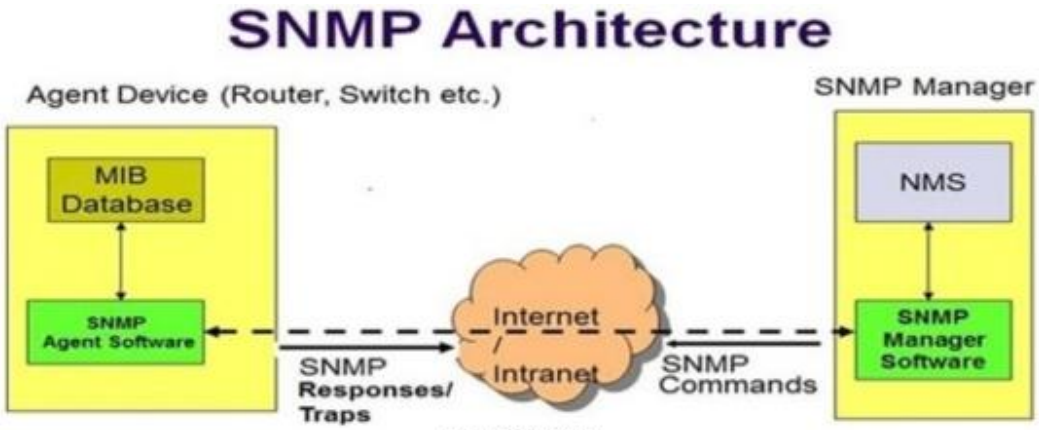

Fig. 2.24(1)

SNMP is a part of the TCP/IP suite. There are 3 main versions of SNMP which include SNMPv1, SNMPv2, and SNMPv3.

2.25. What are different types of Networks. Explain Briefly

There are 4 major types of networks.

- Personal Area Network (PAN):
  It is the smallest and basic network type that is often used at home. It is a connection between the computer and another device such as phone, printer, modem tablets, etc
- Local Area Network (LAN):
  LAN is used in small offices and Internet cafes to connect a small group of computers to each other. Usually, they are used to transfer a file or for playing the game in a network.

© i3Qube Software 2023 Confidential

- Metropolitan Area Network (MAN):
  It is a powerful network type than LAN. The area covered by MAN is a small town, city, etc. A huge server is used to cover such a large span of area for connection.
- Wide Area Network (WAN):
  It is more complex than LAN and covers a large span of the area typically a large physical distance. The Internet is the largest WAN which is spread across the world. WAN is not owned by any single organization but it has distributed ownership.

Additional types of the networks:

- Storage Area Network (SAN)
- System Area Network (SAN)
- Enterprise Private Network (EPN)
- Passive Optical Local Area Network (POLAN)

3. PART 2: Networking Questions

3.1. Differentiating Communication and Transmission

Through Transmission

the data gets transferred from source to destination (only one way). It is treated as the physical movement of data.

Communication

means the process of sending and receiving data between two media (data is transferred between source and destination in both ways)

3.2. Explain Various types of Networks based on their sizes

The size of the network is defined as the geographic area and the number of computers covered in it.

Based on the size of the network, they are classified as below:

- Local Area Network (LAN):
  A network with a minimum of two computers to a maximum of thousands of computers within an office or a building is termed as LAN. Generally, it works for a single site where people can share resources like printers, data storage, etc.
- Metropolitan Area Network (MAN):
  It is larger than LAN and used to connect various LANs across small regions, a city, campus of colleges or universities, etc which in turn forms a bigger network.
- Wide Area Network (WAN):
  Multiple LANs and MAN's connected together form a WAN. It covers a wider area like a whole country or world.

3.3. Define Various types of Internet Connections

There are three types of Internet connections:

- Broadband Connection:
  This type of connection gives continuous high-speed Internet. In this type, if we log off from the Internet for any reason then there is no need to log in again. For Example, Modems of cables, Fibres, wireless connection, satellite connection, etc.
- Wi-Fi:
  It is a wireless Internet connection between the devices. It uses radio waves to connect to the devices or gadgets.

© i3Qube Software 2023 Confidential

- WiMAX:
  It is the most advanced type of Internet connection which is more featured than Wi-Fi. It is nothing but a high-speed and advanced type of broadband connection.

3.4. Terminologies in Networking Concepts

- Network:
  A set of computers or devices connected together with a communication path to share data.
- Networking:
  The design and construction of a network are termed as networking.
- Link:
  The physical medium or the communication path through which the devices are connected in a network is called a Link.
- Node:
  The devices or the computers connected to the links are named as nodes.
- Router/Gateway:
  A device/computer/node that is connected to different networks is termed as a Gateway or Router. The basic difference between these two is that Gateway is used to control the traffic of two contradictory networks whereas the router controls the traffic of similar networks.
- The router
  Router is a switch that processes the signal/traffic using routing protocols.
- Protocol:
  A set of instructions or rules or guidelines that are used in establishing communications between computers of a network is called Protocol.
- Unicasting:
  When a piece of information or a packet is sent from a particular source to a specified destination then it is called Unicasting.
- Anycasting:
  Sending the datagrams from a source to the nearest device among the group of servers that provide the same service as the source is termed as Anycasting.
- Multicasting:
  Sending one copy of data from a single sender to multiple clients or receivers (selected clients) of the networks which are in need of such data.
- Broadcasting:
  Sending a packet to each device of the network is termed as broadcasting.

3.5. Explain the Characteristics of Networking

The main characteristics of networking are mentioned below:

- Topology:
  This deals with how the computers or nodes are arranged in the network. The computers are arranged physically or logically.
- Protocols:
  Deals with the process of how computers communicate with one another.
- Medium:
  This is nothing but the medium used by computers for communication.

© i3Qube Software 2023 Confidential

3.6. How many types of modes are used while transferring Data through Networks

Data transferring modes in computer networks are of three types. They are:

- Simplex:
  Data transferring which takes place only in one direction is called Simplex. In Simplex mode, the data gets transferred either from sender to receiver or from receiver to sender.
  For Example,
  Radio signal, the print signal given from computer to printer, etc.
- Half Duplex:
  Data transferring can happen in both directions but not at the same time. Alternatively, the data is sent and received.
  For Example,
  Browsing through the internet, a user sends the request to the server and later the server processes the request and sends back the web page.
- Full Duplex:
  Data transferring happens in both directions that too simultaneously.
  For Example,
  Two-lane roads where traffic flows in both directions, communication through telephone, etc.

3.7. Name the different types of Network Topologies and brief their advantages

- Network Topology
  is nothing but the physical or logical way in which the devices (like nodes, links, and computers) of a network are arranged. Physical Topology means the actual place where the elements of a network are located.
- Logical Topology
  deals with the flow of data over the networks. A link is used to connect more than two devices of a network. And more than two links located nearby form a topology.

Network topologies are classified as below:

1. Bus Topology:
   In Bus Topology, all the devices of the network are connected to a common cable (also called as the backbone). As the devices are connected to a single cable, it is also termed as Linear Bus Topology.

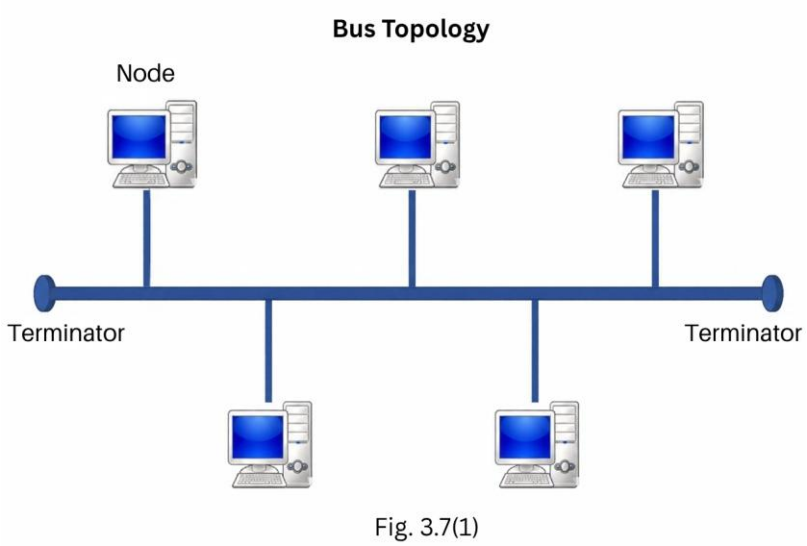

Fig. 3.7(1)

© i3Qube Software 2023 Confidential

- Advantage:
  Easy to install.
- Disadvantage:
  If the backbone cable breaks then the whole network will be down.

2. Star Topology:
   In Star Topology, there is a central controller or hub to which every node or device is connected through a cable. In this topology, the devices are not linked to each other. If a device needs to communicate with the other, then it has to send the signal or data to the central hub. And then the hub sends the same data to the destination device.

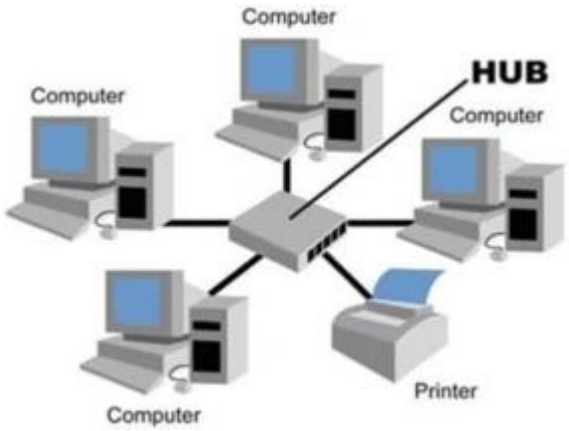

Fig. 3.7(2)

- Advantage:
  If a link breaks then only that particular link is affected. The whole network remains undisturbed.
- Main Disadvantage:
  All the devices of the network are dependent on a single point (hub), If the central hub fails, then the whole network gets down.

3. Ring Topology:
   In Ring Topology, each device of the network is connected to two other devices on either side which in turn forms a loop. Data or Signal in ring topology flow only in a single direction from one device to another and reaches the destination node.

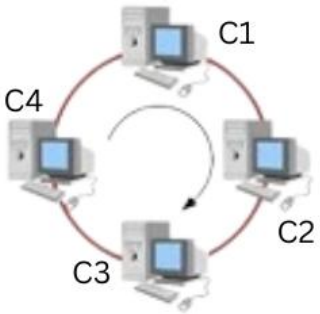

Fig. 3.7(3)

C1, C2, C3 & C4 - Computers

- Advantage:
  Easy to install & Easy to add or delete devices to the network.

© i3Qube Software 2023 Confidential

- Main Disadvantage:
  Data flows only in one direction. and a break at a node in the network can affect the whole network.

4. Mesh Topology:
   In a Mesh Topology, each device of the Network is connected to all other devices of the Network. Mesh Topology uses Routing and Flooding techniques for data transmission.

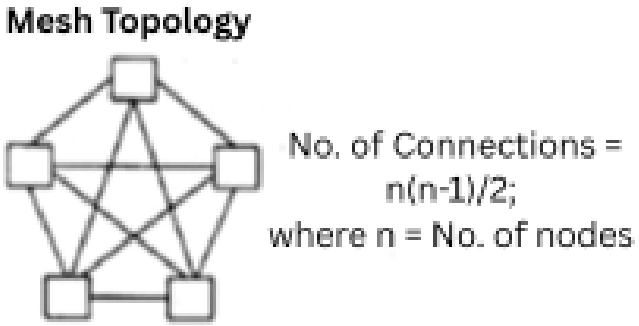

Fig. 3.7(4)

- Advantage:
  If one link breaks then it does not affect the whole network.
- Main Disadvantage:
  Huge cabling is required and it is expensive.

3.8. What is the full form of IDEA

'IDEA' stands for International Data Encryption Algorithm.

3.9. Define Piggybanking

In data transmission, if the sender sends any data frame to the receiver then the receiver should send the acknowledgment to the sender. The receiver will temporarily delay (waits for the network layer to send the next data packet) the acknowledgment and hooks it to the next outgoing data frame, this process is called Piggybacking.

3.10. In How many ways the data is represented and What are they

Data transmitted through the networks' comes in different ways like text, audio, video, images, numbers, etc.

- Audio:
  It is nothing but the continuous sound which is different from text and numbers.
- Video:
  Continuous visual images or a combination of images.
- Images:
  Every image is divided into pixels. And the pixels are represented using bits. Pixels may vary in size based on image resolution.
- Numbers:
  These are converted into binary numbers and are represented using bits.
- Text:
  Text is also represented as bits.

3.11. What is the full form of ASCII

ASCII stands for American Standard Code for Information Interchange.

© i3Qube Software 2023 Confidential

3.12. How Switch is different from HUB

Fig. below depicts the differences:

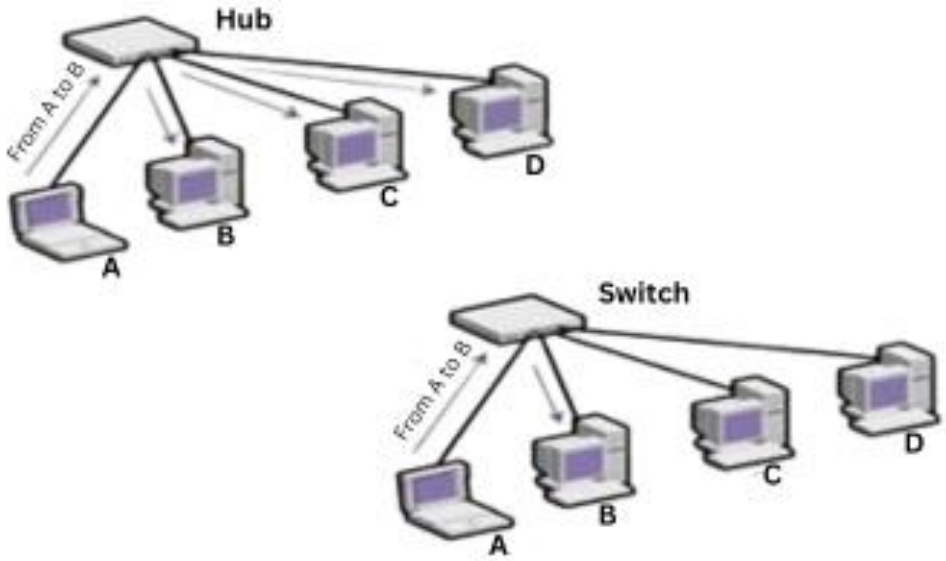

Fig. 3.12(1)

3.13. Define Round Trip Time

The time taken for a signal to reach the destination and travel back to the sender with the acknowledgment is termed as Round Trip Time (RTT). It is also called Round Trip Delay (RTD).

3.14. Define Brouter

Brouter or Bridge Router

is a device that acts as both a bridge and a router. As a bridge, it forwards data between the networks. And as a router, it routes the data to specified systems within a network.

3.15. Define Static IP & Dynamic IP

When a device or computer is assigned a specified IP address then it is named as Static IP. It is assigned by the Internet Service Provider as a permanent address.

Dynamic IP is the temporary IP address assigned by the network to a computing device. Dynamic IP is automatically assigned by the server to the network device.

3.16. How VPN is used in the Corporate World

VPN stands for Virtual Private Network. With the help of a VPN, remote users can securely connect to the organization's network. Corporate companies, educational institutions, government offices, etc use this VPN.

3.17. What is the difference between Firewall & Antivirus

Firewall and Antivirus are two different security applications used in networking. A firewall acts as a gatekeeper which prevents unauthorized users to access the private networks as intranets. A firewall examines each message and blocks the same which are unsecured.

Antivirus is a software program that protects a computer from any malicious software (virus, spyware, adware, etc.}

Note:

A Firewall cannot protect the system from viruses, spyware, adware, etc.

© i3Qube Software 2023 Confidential

3.18. Explain Beaconing

If a network self-repair its problem then it is termed as Beaconing. Mainly, it is used in the token ring and FDDI (Fiber Distributed Data Interface) networks. If a device in the network is facing any problem, then it notifies the other devices that they are not receiving any signal. Likewise, the problem gets repaired within the network.

3.19. Why the standard of an OSI model is termed as 802.xx

The OSI model was started in the month of February in 1980. So it is standardized as 802.XX. This '80' stands for the year 1980 and '2' represents the month of February.

3.20. Expand DHCP and describe how it works

DHCP

stands for Dynamic Host Configuration Protocol.

DHCP is used to assign IP addresses automatically to the devices over the network. When a new device is added to the network, it broadcasts a message stating that it is new to the network. Then the message is transmitted to all the devices of the network.

Only the DHCP server will react to the message and assigns a new IP address to the newly added device of the network with the help of DHCP, IP management became very easy.

3.21. How can a network be certified as an effective network What are the factors affecting them

A network can be certified as an effective network based on below-mentioned factors:

- Performance:
  A network's performance is based on its transmitted time and response time. The factors affecting the performance of a network are hardware, software, transmission medium types and the number of users using the network.
- Reliability:
  Reliability is nothing but measuring the probability of failures occurred in a network and the time taken by it to recover from it. The factors affecting the same are the frequency of failure and recovery time from failure.
- Security:
  Protecting the data from viruses and unauthorized users. The factors affecting the security are viruses and users who do not have permission to access the network.

3.22. Explain DNS

DNS stands for Domain Naming Server. DNS acts as a translator between domain names and IP addresses. As humans remember names, the computer understands only numbers. Generally, we assign names to websites and computers like gmail, hotmail, etc. When we type such names the DNS translates it into numbers and executes our requests.

Translating the names into numbers or IP address is named as a Forward lookup. Translating the IP address to names is named as a Reverse lookup.

3.23. Define IEEE in the Networking World

IEEE stands for the Institute of Electrical and Electronic Engineer. This is used to design or develop standards that are used for networking.

3.24. What is the use of Encryption and Decryption

Encryption

is the process of converting the transmission data into another form that is not read by any other device other than the intended receiver.

© i3Qube Software 2023 Confidential

Decryption

is the process of converting back the encrypted data to its normal form. An algorithm called cipher is used in this conversion process.

3.25. Brief Ethernet

Ethernet is a technology that is used to connect computers all over the network to transmit the data between each other.

For Example,

if we connect a computer and laptop to a printer, then we can call it as an Ethernet network. Ethernet acts as the carrier for the Internet within short distance networks like a network in a building.

The main difference between the Internet and Ethernet is security. Ethernet is safer than the Internet as Ethernet is a closed-loop and has only limited access.

3.26. Explain Data Encapsulation

Encapsulation means adding one thing on top of the other thing. When a message or a packet is passed through the communication network (OSI layers), every layer adds its header information to the actual packet. This process is termed as Data Encapsulation.

Note:

Decapsulation is exactly the opposite of encapsulation. The process of removing the headers added by the OSI layers from the actual packet is termed as Decapsulation.

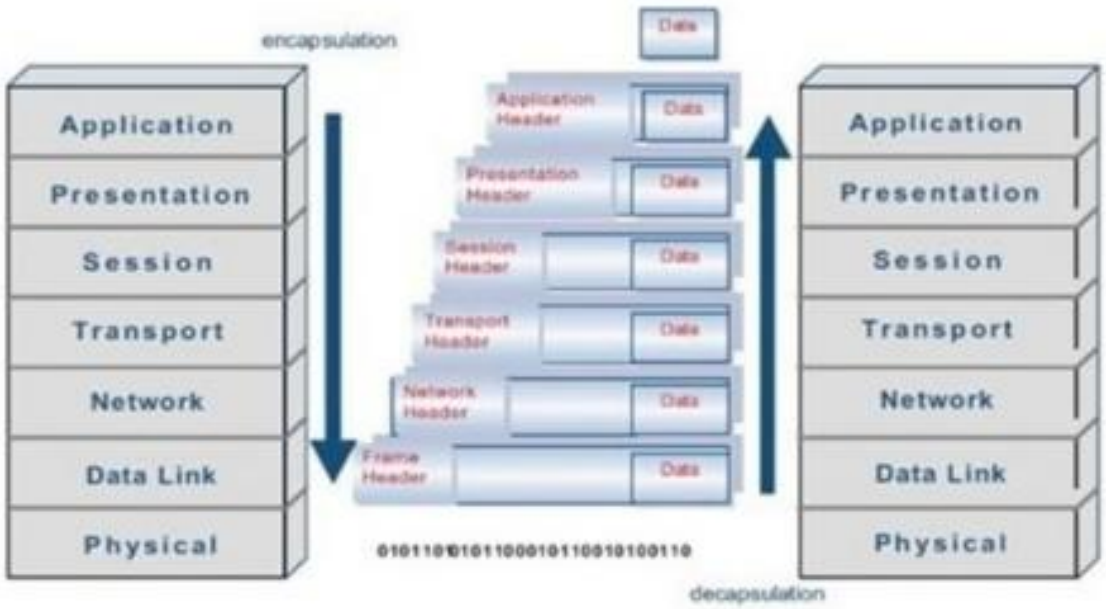

Fig. 3.12(1)

3.27. How are Networks classified based on their Connections

Networks are classified into two categories based on their connection types. They are:

- Peer-to-peer networks (P2P):
  When two or more computers are connected together to share resources without the use of a central server is termed as a peer-to-peer network. Computers in this type of network act as both server and client. It is generally used in small companies as they are not expensive.
- Server-based networks:
  In this type of network, a central server is located to store the data, applications, etc of the clients. The server computer provides the security and network administration to the network.

© i3Qube Software 2023 Confidential

3.28. Define Pipelining

In Networking, when a task is in progress another task gets started before the previous task is finished. This is termed as Pipelining.

3.29. What is an Encoder

Encoder is a circuit that uses an algorithm to convert any data or compress audio data or video data for transmission purposes. An encoder converts the analog signal into the digital signal.

3.30. What is a Decoder

Decoder is a circuit that converts the encoded data to its actual format. It converts the digital signal into an analog signal.

3.31. How can you recover the data from a system which is infected with a Virus

In another system (not infected with a virus) install an OS and antivirus with the latest updates. Then connect the HDD of the infected system as a secondary drive. Now scan the secondary HDD and clean it. Then copy the data into the system.

3.32. Describe the key elements of the protocol

Below are the 3 key elements of the protocol:

- Syntax:
  It is the format of the data. That means in which order the data is displayed.
- Semantics:
  Describes the meaning of the bits in each section.
- Timing:
  At what time the data is to be sent and how fast it is to be sent.

3.33. Explain the difference between baseband and broadband transmission

- Baseband Transmission:
  A single signal consumes the whole bandwidth of the cable.
- Broadband Transmission:
  Multiple signals of multiple frequencies are sent simultaneously.

3.34. Expand SLIP

SLIP stands for Serial Line Interface Protocol. SLIP is a protocol used for transmitting IP datagrams over a serial line.

3.35. What are the types of MAC Addresses

There are two types of MAC addresses: Static and Dynamic.

Depending on their type, MAC addresses are either stored in the Static Address table or in the Dynamic Address table, along with VLAN and port information.

Static addresses are configured by the user, and therefore, they do not expire.

3.36. What is RPI

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

4. PART 3: Recap (Test Your Understanding)

Revise/Recap and Answer the Following Questions

1. Name Two Devices needed to form Network
2. What is the port used for HTTP
3. What is the Bit Rate of a Serial Interface of a Network Device
4. What is the Backbone Network

© i3Qube Software 2023 Confidential

5. What is a point-to-point link
6. What is the Maximum length allowed for a UTP Cable
7. What is NOS
8. What is SLIP
9. What is the main Job of ARP
10. What is the importance of Encryption in Networking
11. What do you mean by Tunnel Mode
12. What is IPv6
13. What is a Link
14. What is a Node
15. What are the Layers of the OSI Reference Model
16. What is LAN
17. What are Routers
18. What is Anonymous FTP
19. What is FTP
20. What are Proxy Servers and How do they Protect Computer Networks
21. What is the use of a default gateway
22. What are the important elements of a Protocol
23. Briefly Describe NAT
24. What is DOS
25. What is a hybrid Network
26. What Protocol can be applied when you want to transfer files between different platforms, such as UNIX Systems and Windows Servers
27. What is the application of Hamming Code
28. What are the types of MAC Addresses
29. What is RIP
30. Explain the term Pipelining
31. What is the Meaning of Tunnel Mode
32. What is Default Gateway
33. What are the important elements of Protocol
34. What is a Datagram
35. What is Checksum

Good Luck and All the Best !!!

CONFIDENTIAL

© i3Qube Software 2023 Confidential