Network+ (N10-005) Cram Notes

3.7 Compare and contrast different LAN technologies.

3.8 Identify components of wiring distribution.

4. Network Management

4.1 Explain the purpose and features of various network appliances.

4.2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues.

4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

4.4 Given a scenario, use the appropriate network monitoring resource to analyze traffic.

4.5 Describe the purpose of configuration management documentation.

4.6 Explain different methods and rationales for network performance optimization.

5. Network Security

5.1 Given a scenario, implement appropriate wireless security measures.

5.2 Explain the methods of network access security.

5.3 Explain methods of user authentication.

5.4 Explain common threats, vulnerabilities, and mitigation techniques.

5.5 Given a scenario, install and configure a basic firewall.

5.6 Categorize different types of network security appliances and methods.

1. Networking Concepts

1.1 Compare the layers of the OSI and TCP/IP models

OSI model

Application Layer

1. Application layer is responsible for identifying and establishing the availability of desired communication partner and verifying sufficient resources exist for communication.

2. Some of the important application layer protocols are: WWW, SMTP, FTP, etc.

Presentation Layer

1. This layer is responsible for presenting the data in standard formats.

2. This layer is responsible for data compression, decompression, encryption, and decryption.

3. Some Presentation Layer standards are: JPEG, MPEG, MIDI, PICT, Quick Time, TIFF.

Session Layer

1. Session Layer is responsible for co-coordinating communication between systems/nodes.

2. The Session Layer: The following are some of the session layer protocols and interfaces: a) Network File System (NFS), SQL, RPC (Remote Procedure Call), X-Windows, ASP, DNA SCP.

Transport Layer

1. The Transport Layer is responsible for multiplexing upper-layer applications, session establishment, and tearing-down of virtual circuits.

2. This layer is responsible for flow control, to maintain data integrity.

Network Layer

1. There can be several paths to send a packet from a given source to a destination. The primary responsibility of Network layer is to send packets from the source network to the destination network using a per-determined routing methods.

2. Routers work at Network layer.

Data Link Layer

1. Data Link Layer is layer 2 of OSI reference model. This layer is divided into two sub-layers

A. Logical Link Control (LLC) sub-layer: It handles error control, flow control, framing, and MAC sub-layer addressing.

B. Media Access Control (MAC) sub-layer: It is the lower of the two sub-layers of the Data Link layer. MAC sub-layer handles access to shared media, such a Token passing or

Ethernet.

Physical Layer

1. The actual flow of signals take place through Physical layer. At Physical layer, the interface between the DTE and DCE is determined.

The following are some of the standard interfaces are defined at Physical layer: EIA/TIA-232, EIA/TIA 449,V.24,V.35,X.21,G.703,HSSI (High Speed Serial Interface).

TCP/IP Model

Application Layer

1. Provides user interface for communication.
2. Defines TCP/IP application protocols and how host program interface with Transport layer .
3. When sending transmit data to Transport Layer.
4. When receiving transmits data to Transport Layer.
5. Protocols included are DNS, HTTP, Telnet, FTP, RDP etc.

Transport Layer

1. It allows host-host communication. It provides reliable, connection-oriented transport b/w two sockets on two computers using Internet Protocol to communicate.
2. Defines level of service and status of connection used when transporting data.
3. When sending transmits data to Internet Layer.
4. When receiving transmits data to Application Layer.
5. Protocols include TCP, UDP

Internet Layer

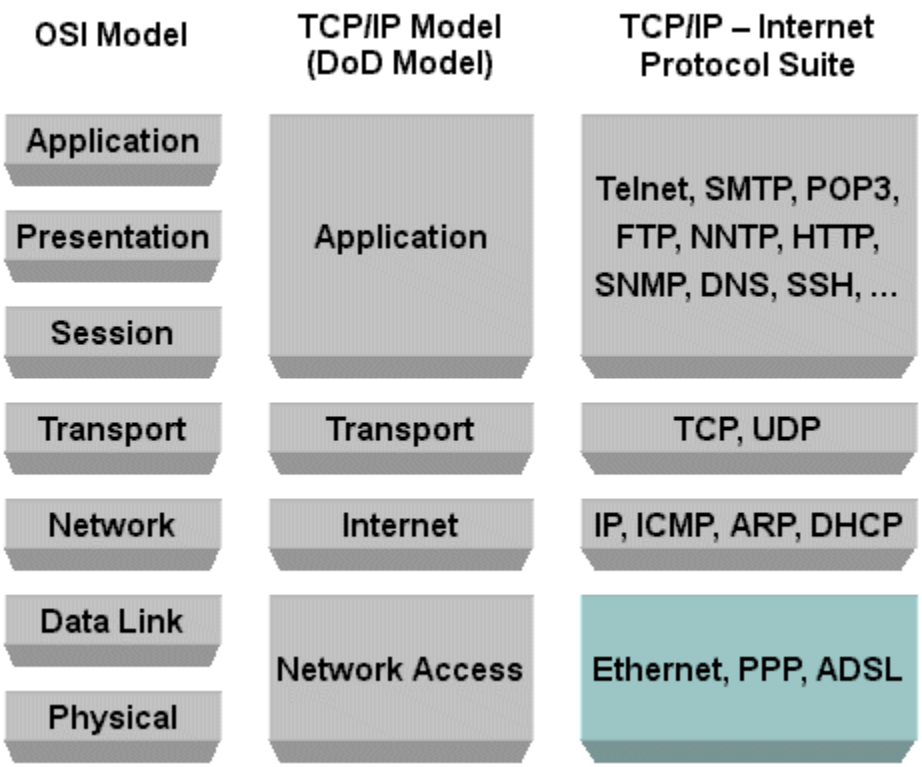
1. It packs data in to data packets called IP datagrams(contains sources and destination IP address).
2. Also does logical addressing and routing of data on network.
3. When sending it transmit data to Network Access Layer.
4. When receiving transmit data to Transport Layer,
5. Protocols included are IP,ICMP, ARP, RARP and IGMP

Network Access Layer

1. Defines how data is sent physically through the network.

2. Provides access to physical network that is allow your computer to access wire, wireless or optical network.
3. When sending it transmit data to physical network.
4. When receiving transmit data to Internet layer.
5. Protocols included are Ethernet, Token Ring, FDDI.

The following diagram provides a mapping of OSI to DoD (TCP/IP) Model:



In the Application layer lies many of network aware programs and services such as:

1. HTTP (80) - HyperText Transport Protocol which is used for transferring webpages.
2. SNMP (161/162) - Simple Network Management Protocol which is used for managing network devices.
3. FTP (20/21) - File Transfer Protocol which is used for transferring files across the network.
4. TFTP (69) - Trivial File Transfer Protocol which is a low overhead fast transfer FTP protocol.
5. SMTP (25) - Simple Mail Tranfer Protocol which is used for transferring email across the Internet.
6. Telnet (23) - An application for remotely logging into a server across the network.
7. NNTP (119) - Network News Transfer Protocol which is used for transferring news.

The numbers, shown in brackets next to the protocols, are called the Well Known Port Numbers,

1.2 Classify how applications, devices, and protocols relate to the OSI model layers.

- MAC Address : Data link layer
- IP address : Network Layer
- EUI-64 (Extended Unique Identifier): Data Link Layer
- Frames : Data Link Layer
- Packets: Network Layer
- Layer-2 Switch: Data Link Layer
- Router: Network Layer
- Multilayer Switch: Data Link Layer and Network Layer
- Hub: Physical Layer
- Encryption devices: Presentation Layer
- Cable: Physical Layer
- NIC: Data Link Layer and Physical Layer
- Bridge: Data Link Layer

1.3 Explain the purpose and properties of IP addressing

IP addresses are written using decimal numbers separated by decimal points. This is called dotted decimal notation of expressing IP addresses. 2 types of IP addressing is used. 1. IP v4 addressing and 2. IP v6 addressing convention.

The different classes of IP addresses is as below:

IP v4 Addressing:

Class	Format	Leading Bit Pattern	Network Address Range	Max Networks	Max nodes/hosts
A	N.H.H.H	0	01/01/26	127	16777214
B	N.N.H.H	10	128-191	16384	65534

C	N.N.N.H	110	192-223	2097152	254

- Network address of all zeros means "This network or segment".
- Network address of all 1s means " all networks", same as hexadecimal of all Fs.
- Network number 127 is reserved for loop-back tests.
- Host (Node) address of all zeros mean "This Host (Node)".
- Host (Node) address of all 1s mean "all Hosts (Nodes) " on the specified network.

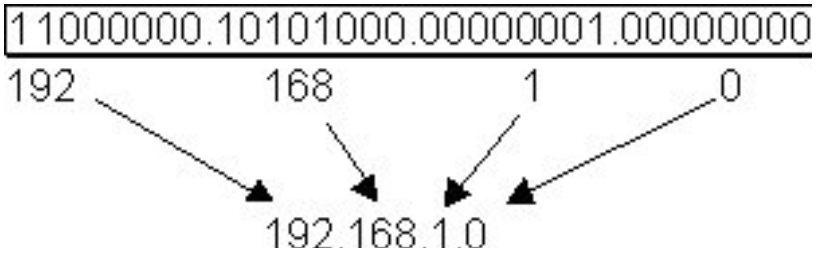
CIDR (Classless Inter-Domain Routing)

Classless Inter Domain Routing (CIDR) is a method for assigning IP addresses without using the standard IP address classes like Class A, Class B or Class C. In CIDR notation, an IP address is represented as A.B.C.D /n, where "/n" is called the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network.

Ex: 216.3.128.12, with subnet mask of 255.255.255.128 may be written as 216.3.128.12/25 using CIDR Notation.

Ipv4 addressing

1. An IP address (32 bit number, 4 bytes) consists of four octets seperated by dots. The octet is a binary number of eight digits, which equals the decimal numbers from 0 to 255.



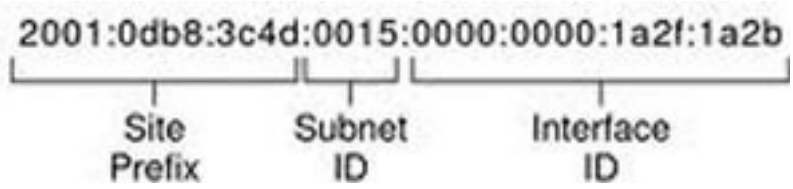
2. The internet protocol defines the special network address 127.0.0.1 as a local loopback address.

2. IP v6 addressing

1. IPv6 address is 128 bits in length represented in hexadecimal
2. IPv6 Loopback address is 0:0:0:0:0:0:0:1, also expressed as ::1.
3. IPv6 reserves two special addresses. They are 0:0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1.
4. Three transition strategies for migration from ipv6 to ipv4 are dual stacking, 6-to-4 tunneling and NAT-PT

IPv6 address consists of 8 groups of four hexadecimal digits separated by colons and which mainly consists of 3 segments called Global Prefix which is of 48 bits, subnet part with 16 bits and Interface ID called as Host part with 64 bits. The first 3 octets constitute Global Prefix, the fourth octet constitute subnet

part and the last four form the Interface ID.



Rules :
a) One set of 0's in the address can be replaced by :: but this can be done only once
b) One or any number of consecutive groups of 0 value can be replaced with two colons (::)

MAC address

It is a unique value associated with a network adapter. These are also known as hardware addresses or physical addresses. It contains 12-digit hexadecimal numbers (48 bits in length)
By convention, MAC addresses are usually written in one of the following two formats:

Format 1.....MM:MM:MM:SS:SS:SS
Format 2.....MM-MM-MM-SS-SS-SS
The first half of a MAC address contains the ID number of the adapter manufacturer. The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer. In the example, 00:A0:C9:14:C8:29
The prefix 00A0C9 indicates the manufacturer is Intel Corporation.
The number 14C829 is the serial number assigned by the manufacturer.

Subnetting

It is nothing but creating networks within a network. Subnetting allows an organization with a single IP address (Class A /ClassB /ClassC) to have multiple subnetworks, thus allowing several physical networks within the organization.

Default subnet mask for Class A network: 255.0.0.0
Default subnet mask for Class B network: 255.255.0.0
Default subnet mask for Class C network: 255.255.255.0

The directed broadcast should reach all Hosts on the intended network (or subnet, if sub netted). For example, the directed broadcast address for an IP network 196.233.24.15 with default subnet mask is 196.233.24.255. This is arrived by putting all 1s for the host portion of the IP address.

Unicast	Packets are sent from single source to specific destination. There is only one sender and one receiver. It uses IP delivery methods such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), which are session-based protocols Examples FTP, Telnet

Broadcast	Packets are sent from one source to all other clients. There is only one sender and all connected clients are receivers. It is largely confined to local area network (LAN) technologies, mostly Ethernet and token ring
Multicast	Packets are sent from one or more sources to set of receivers. There can be one or more senders and one or more receivers. It is useful if a group of clients require a common set of data at the same time, or when the clients are able to receive and store (cache) common data until needed

APIP (Automatic Private IP Addressing)

APIPA (Short for Automatic Private IP Addressing), is a feature that allows DHCP clients to automatically self-configure an IP address and subnet mask when a DHCP server isn't available. When a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself.. The IP address range is 169.254.0.1 through 169.254.255.254. The client also configures itself with a default class B subnet mask of 255.255.0.0.

1.4 Explain the purpose and properties of routing and switching.

Routing is the process of directing the messages generated at source host towards the destination host over a computer network. The path may consist of several nodes that forward the messages (packets) towards the destination. Due to complexity of the protocols, and user requirements, several routing protocols have come in to existence. Most popular among these protocols are 1. RIP v1 and v2, OSPF, EIGRP, and BGP. Routing protocols should not be confused with routed protocols such as TCP and UDP. Routed protocols typically carry user data, whereas routing protocols provide the route information for user data packets. For most part, routing protocols are transparent to the end user. Routing protocols may be classified as below:

Distance Vector

Distance vector routing determines the direction and distance to any link in the internetwork. Smaller the metric, better the path. Distance vector routing is useful for smaller networks. Ex: RIP and IGRP.

Link State

Also known as SPF algorithms, SPF generates the exact topology of the entire network for route computation by listening to the first hand information. Bandwidth and delay are the most widely used metrics. Ex: OSPF and NLSP.

Balanced Hybrid

Balanced Hybrid combines some aspects of Link State and Distance Vector routing protocols. It uses distance vectors with more accurate metrics to determine the best paths to destination networks. Ex: EIGRP

Routing protocols may also be classified as IGP and EGP routing protocols.

IGP(Interiror Gateway Protocols)

- Handles routing in one domain (Automonus system) that is they send routing information between routers on the same internal network.
- These fall in two categories : Distance Vector Protocol and Link State Protocol
- RIP, OSPF are examples of IGP.
-

EGP(Exterior Gateway Protocols)

- Handles routing outside Autonomous network it takes you from your network through ISP on to another network.
- BGP is an examples of EGP protocol.

Static And Dynamic Routing

Static Routing	1. location of the remote resource is specified at design time 2. administrator constructs the routing table in every router by putting in the entries for every network that could be a destination. 3. Static routes to network destinations are unchangeable.
Dynamic routing	1. location of the remote resource is decided at run time. 2. Routing protocol operating on the router is responsible for the creation, maintenance and updating of the dynamic routing table. 3. enables routers to select paths according to real-time logical network layout changes.

Routing metrics

It is unit calculated by a routing algorithm for selecting or rejecting a routing path for transferring data/traffic.

- Hop count: It is the number of nodes between starting node and destination node.
- MTU(Maximum Transmission Unit): It is size of largest protocol data unit that can be transmitted. It is measured in bytes and is associated with a communications interface
- Latency: It refers to several kinds of delays that come in network transmission
- Costs
- Bandwidth

EIGRP (Enhanced Interior Gateway Protocol, a Cisco proprietary protocol)

Important terms used in EIGRP

- Successor: A route (or routes) selected as the primary route(s) used to transport packets to reach destination. Note that successor entries are kept in the routing table of the router.

- Feasible successor: A route (or routes) selected as backup route(s) used to transport packets to reach destination. Note that feasible successor entries are kept in the topology table of a router.
- DUAL (Diffusing Update Algorithm): Enhanced IGRP uses DUAL algorithm to calculate the best route to a destination

Routing metrics used by EIGRP

- Bandwidth: This is represents the maximum throughput of a link.
- MTU (Maximum Transmission Unit): This is the maximum message length that is acceptable to all links on the path. The larger MTU means faster transmission of packets.
- Reliability: This is a measurement of reliability of a network link. It is assigned by the administrator or can be calculated by using protocol statistics.
- Delay: This is affected by the band width and queuing delay.
- Load: Load is based among many things, CPU usage, packets processed per sec

For IGRP routing, you need to provide AS (Autonomous System) number in the command. Routers need AS number to exchange routing information. Routers belonging to same AS exchange routing information.

OSPF(Open Shortest Path First) Routing Protocol:

OSPF is a link state technology that uses Dijkstra algorithm to compute routing information.

An OSPF area is a collection of networks and routers that have the same area identification.OSPF process identifier is locally significant.
OSPF Area Types

- Backbone Area (Area 0) - The backbone area is the central area to which all other areas in OSPF connect.
- Standard Area : Default OSPF area type -Standard areas are defined as areas that can accept intra-area, inter-area and external routes. Intra-area routes refer to updates that are passed within the area. Inter-area routes refer to updates that are passed between areas. External routes refer to updates passed from another routing protocol into the OSPF domain by the Autonomous System Border Router (ASBR).
- Stub Area : These areas do not accept routes belonging to external autonomous systems (AS); however, these areas have inter-area and intra-area routes. In order to reach the outside networks, the routers in the stub area use a default route which is injected into the area by the Area Border Router (ABR). A stub area is typically configured in situations where the branch office need not know about all the routes to every other office, instead it could use a default route to the central office and get to other places from there. Hence the memory requirements of the leaf node routers is reduced, and so is the size of the OSPF database.
- Totally Stubby Area : These areas do not allow routes other than intra-area and the default routes to be propagated within the area. The ABR injects a default route into the area and all the routers belonging to this area use the default route to send any traffic outside the area.

- Not So Stubby Area (NSSA) : This type of area allows the flexibility of importing a few external routes into the area while still trying to retain the stub characteristic.

OSPF router ID determined based on the following criteria:

- Use the address configured by the ospf router-id command, if not configured, then
- Use the highest numbered IP address of a loopback interface, if not configured, then
- Use the highest IP address of any physical interface,
- If no interface exists, set the router-ID to 0.0.0.0

Ref.: http://packetlife.net/blog/2008/jun/24/ospf-area-types/

OSPF Priority:

The ip ospf priority command is used to set manually which router becomes the DR. The range is 0- 255 and the default is 1. 0 means it will never be DR or BDR.

One important criteria in Multi-access NBMA (Non Broadcast Multi Access) networks is the selection of Designated Router (DR) and Backup Designated Router (BDR).

DR and BDR are elected for every multi-access net work, using Hello packets as "ballots."
• The router's priority field can be set to either ensure that it becomes the DR or prevent it from being the DR.
• The highest Router ID breaks any ties. The router with the highest Router ID is elected the DR.

Spaning Tree Protocol

Spanning Tree Protocol (STP) 802.1d is used to prevent loops within a switch network. STP uses Spanning Tree Algorithm (STA) to prevent loops ensuring stable network topology (also called convergence, where all the switches in the network converge to a known network topology). The following are the important features of STP:

- STP is a layer 2 protocol that runs on switches and bridges. The purpose of STP is to remove switching loops.

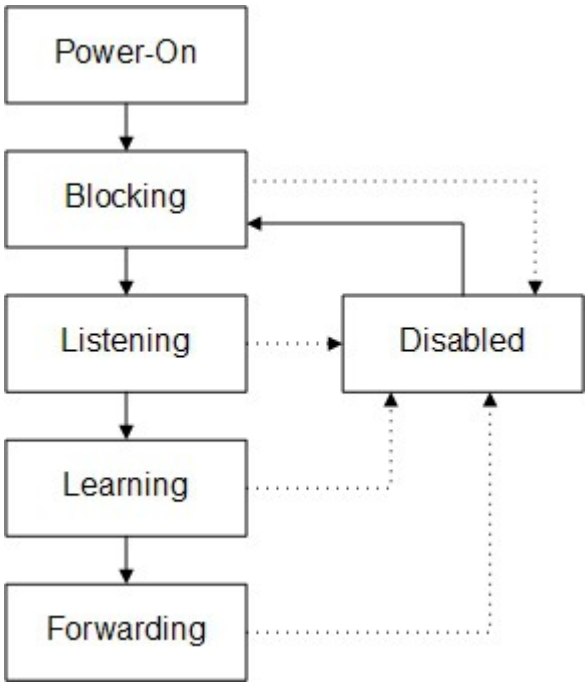
- All switches participating in STP exchange info with other switches in the network through messages known as BPDUs.

- STP port states are Blocked, Listen, Learn, Forward, Disabled

STP Port States:

As mentioned, the purpose of STP is to prevent switching loops throughout a LAN. It is done by

controlling the redundant links that connect into the same network segment. Each network segment is only allowed to have a single designated port that is used to forward traffic onto it. All other access points into the same segment are enabled, but in a blocking state that disallows traffic flow. If a failure should occur on the forwarding port, one of the blocking ports will be transitioned into forwarding state to continue to allow access to the network segment. This transition process includes a number of different states, including each of the states shown in the figure below:



- Blocking - A port that would cause a switching loop if it were active. No user data is sent or received over a blocking port, but it may go into forwarding mode if the other port in use fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state. Prevents the use of looped paths.
- Listening - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.
- Learning - While the port does not yet forward frames it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC Address table, but does not forward frames.
- Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

Different port designations are given below:

- Root : A bridge can have only one root port. The root port is the port that leads to the root bridge. All bridges except the root bridge will have a root port. the root port is in the STP forwarding state.

- Designated : One designated port is elected per link (segment). The designated port is the port closest to the root bridge. Each designated port is in the STP forwarding state

- Alternate : Alternate ports lead to the root bridge, but are not root ports. The alternate ports maintain the STP blocking state.

- Backup: This is a special case when two or more ports of the same bridge (switch) are connected together, directly or through shared media. In this case, one port is designated, and the remaining ports block. The role for this port is backup.

VLAN – Virtual Local Area Networks:

VLAN derives it's name from the fact that there is only one physical network, but two or more logical networks. A VLAN may be created by any of these methods:

1. VLAN by port association - Membership in a VLAN can be defined based on the ports that belong to the VLAN. For example, in a bridge with four ports, ports 1, 2, and 4 belong to VLAN 1 and port 3 belongs to VLAN 2. The main disadvantage of this method is that it does not allow for user mobility. If a user moves to a different location away from the assigned bridge, the network manager must reconfigure the VLAN.
2. VLAN by MAC address association: Here, membership in a VLAN is based on the MAC address of the workstation. The switch tracks the MAC addresses which belong to each VLAN (see Figure4). Since MAC addresses form a part of the workstation's network interface card, when a workstation is moved, no reconfiguration is needed to allow the workstation to remain in the same VLAN. This is unlike Layer 1 VLAN's where membership tables must be reconfigured. The main problem with this method is that VLAN membership must be assigned initially. In networks with thousands of users, this is no easy task. Also, in environments where notebook PC's are used, the MAC address is associated with the docking station and not with the notebook PC. Consequently, when a notebook PC is moved to a different docking station, its VLAN membership must be reconfigured.
3. VLANs by Protocol Type - VLAN membership for Layer 2 VLAN's can also be based on the protocol type field found in the Layer 2 header. For example, VLANs that carry only IP traffic and those that carry only IPX traffic. However this type of VLANs are not popular.
4. VLANs by IP subnet address - Membership is based on the Layer 3 header. The network IP subnet address can be used to classify VLAN membership. Although VLAN membership is based on Layer 3 information, this has nothing to do with network routing and should not be confused with router functions. In this method, IP addresses are used only as a mapping to determine membership in VLAN's. No other processing of IP addresses is done. In Layer 3 VLAN's, users can move their workstations without reconfiguring their network addresses. The only problem is that it generally takes longer to forward packets using Layer 3 information than using MAC addresses. This is the most widely used VLAN type.

The 802.1Q draft standard defines Layer 1 and Layer 2 VLAN's only.

The following are the important terms associated with VLANs:

- VLAN 1 is the management VLAN.

- Static VLAN : VLAN is statically assigned to the physical port and never changes.
- Dynamic VLAN : VMPS automatically assigns VLAN based on MAC
- Access Link : An access link can carry only one VLAN (used between host and switch port)
- Trunk Link : A trunk link can carry multiple VLANs. Used to connect to other switches, routers, or servers
- Two types of Trunk framing: ISL (Cisco only) and 802.1.q

1.5 Identify common TCP and UDP default ports.

Protocol	IP protocol	Port Used
FTP (File Transfer Protocol)	TCP	21
SFTP (Secure FTP)	SCTP,TCP	22
FTPS (FTP Secure)	FTP	443
TFTP (Trivial FTP)	UDP	69
Telnet	TCP	23
HTTP (Hyper Text Transfer Protocol)	TCP	80
HTTPS (HTTP Secure)	TCP	443
SCP (Secure Copy)	SCTP, TCP	22
SSH (Secure SHell)	SCTP, TCP	22
SMTP (Simple Mail Transfer Protocol)	TCP	25
DNS (Domain Name Service))	UDP	53
SNMP (Simple Network Management Protocol)	TCP, UDP	161
SNMP Trap (Simple Network Management Protocol Trap)	TCP, UDP	162
ISAKMP (VPN) – Internet Security Association and Key Management Protocol (virtual private network)	UDP	500
TACACS (Terminal Access Controller Access-Control System)	TCP,UDP	49
POP3 (Post Office Protocol version 3)	TCP	110
NNTP (Network News Transfer Protocol)	TCP	119
IMAP4 (Internet message access protocol version 4)	TCP	143

Kerberos	UDP	88
Syslog	TCP,UDP	514
L2TP (Layer 2 Tunneling Protocol)	UDP	1701
PPTP (Point-to-Point Tunneling Protocol)	TCP	1723
RDP (Remote Desktop Protocol)	TCP, UDP	3389

1.6 Explain the function of common networking protocols.

- TCP/IP is the protocol, which is used by all internet applications such as WWW, FTP, Telnet etc. IPX/SPX is proprietary protocol stack of Novell NetWare.
- UDP (User Datagram Protocol): UDP is a thin protocol. UDP is a connectionless protocol. It doesn't contact the destination before sending the packet and doesn't care whether the packet is reached at the destination.
- Telnet is used for terminal emulation that runs programs remotely. Telnet uses TCP/IP protocol. Telnet requires a username and password to access. It is client-server protocol
- FTP (File Transfer Protocol) is a connection oriented protocol. It uses TCP/IP for file transfer. It is client-server protocol
- TFTP (Trivial File Transfer Protocol) that uses UDP (Connectionless protocol).
- SNMP is part of TCP/IP protocol suite. It allows you to monitor and manage a network from a centralized place by using SNMP Manager software. The systems or devices that provide the responses are called agents (or MIBs). An SNMP agent is any computer running SNMP agent software. MIB stands for Management Information Base. It is part of SNMP agent database. A MIB records and stores information abut the host it is running on. An SNMP manager can request and collect information from an agent's MIB. Routers are typical MIB agents. SNMP agent generates "trap" messages that are then sent to an SNMP management console, which is a trap destination.
- HTTP is the protocol used for accessing the World Wide Web services. HTTP operates over TCP/IP. 15. TCP: TCP is a full-duplex, connection-oriented protocol. It incorporates error checking as well.

1.7 Summarize DNS concepts and its components

The most common type of DNS record is a Host record (also called an A record). In the Internet, a Host record is used to associate a domain name (FQDN – Fully Qualified Domain Name) with an IP address. An MX record stores the IP address of your SMTP server, so e-mail clients can determine where a message should be sent. They perform a DNS query against a domain's MX record to get the IP address of the organization's SMTP server.

An Alias record's job is to associate an alternate name with a computer for which there is already a Host record. For example, suppose that the host record for relevant looked like this:

Relevant Host (A) 200.100.100.199

Alias record is like a redirect. For example, you have a site mydomain.com. However, someone enters www.mysite.com, You want him or her to be directed to the web.mysite.com. Since there is no server on the network named "www," set up an Alias record that associates www with mysite.com. The Alias record looks something like this:

www Alias (CNAME) mysite.com

MAC address record is not associated with DNS server records

1.8 Given a scenario, implement the following network troubleshooting methodology

Given below is the sequence of steps recommended to be following is solving a network problem:

1. Information gathering - Identify symptoms and problems
2. Identify the affected areas of the network
3. Determine if anything has changed
4. Establish the most probable cause
5. Determine if escalation is necessary
6. Create an action plan and solution identifying potential effects
7. Implement and test the solution
8. Identify the results and affects of the solution
9. Document the solution and the entire process

Indirect enquires are usually not a recommended practice.

1.9 Identify virtual network components

- Virtual Switch is a software program that allows one virtual machine to communicate with another.It can intelligently direct communication on the network by inspecting packets before passing them on.

- Virtual Server is a server which is shared by multiple website owners. Each owner can use use and administrate

- With virtual desktops, a user's data is stored in a data center rather than on an office computer's hard drive. By providing authentication credentials, a secure connection can be established between the centralized repository of user data and that user's device , thus allowing the user to remotely access her document.

- PBX A Private Branch Exchange (PBX) is a privately owned telephone switch traditionally used in corporate telephony systems. Although a PBX is not typically considered a VoIP device, it can connect into a VoIP network through a gateway.

- In Naas (Network as a Service), the service provider offers services like e-mail and DNS for use by the clients. In SaaS (Software as Service), typically access is provided to a software application.

2. Network Installation and Configuration

2.1 Given a scenario, install and configure routers and switches.

The most common configuration problems araise out of switching loops, bad cables, wrong switch/router port configuration, LAN segmentation, wrong IP subnetting, etc. In addition to the physical connections, it is important to confgure your network properly. Protocols such as NAT, PAT, VLAN, PoE , QoS are widely used in configuring a network. Hence. it is imporant to know the types of problems that mignt occur due to misconfigurations.
and QoS will give you options within your net work

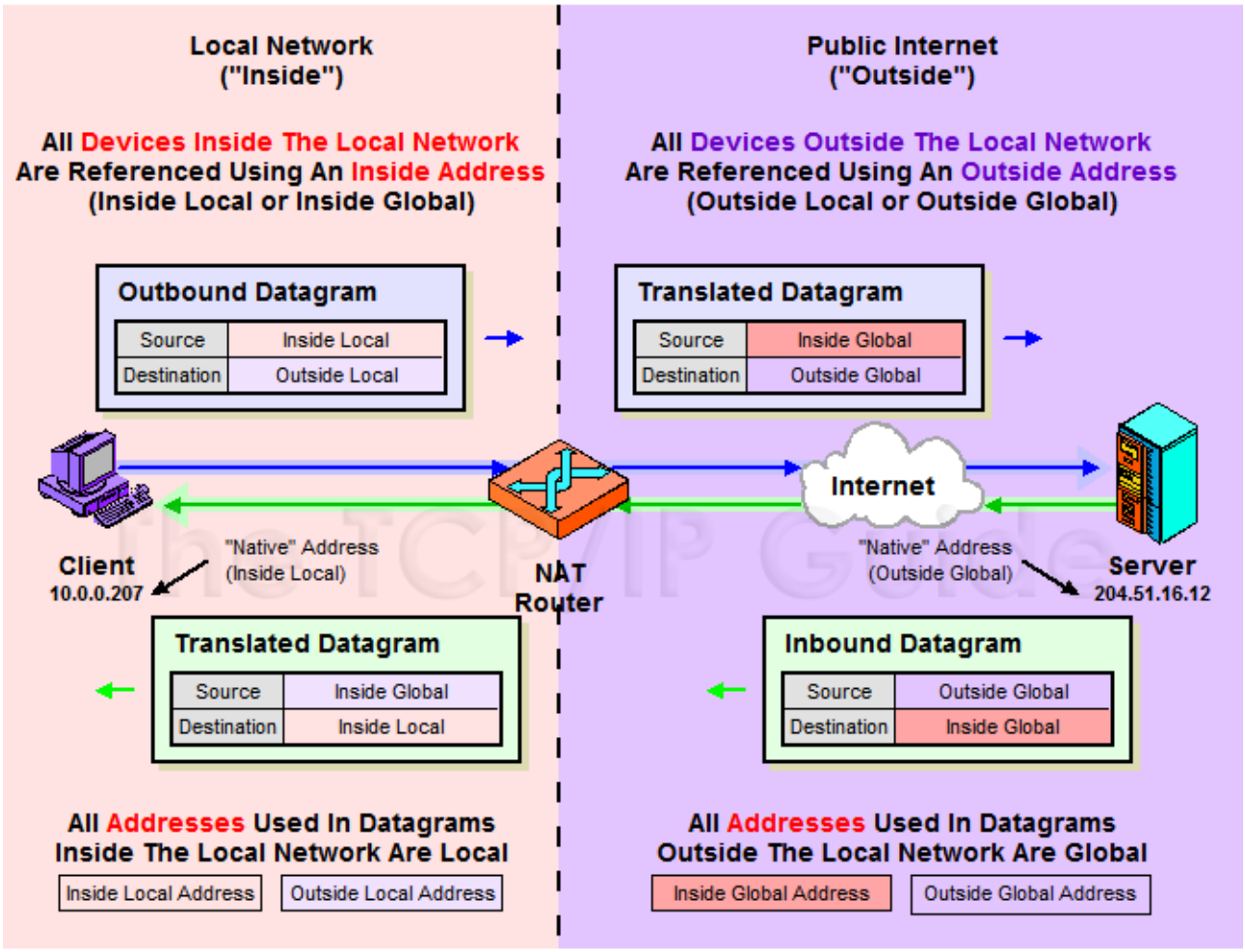
Some of these protocols have been explained in the following sections:

NAT – Network Address Translation.

NAT is very widely used in computer networking. The NAT router has the job of translating the inside network IP addresses to the outside global IP address network (the Internet) enabling inside devices to talk to outside devices and vice-versa, but inside devices can only use addressing consistent with the local network addressing scheme. Similarly, outside devices cannot use local addressing. Thus, both inside and outside devices can be referred to with local or global address versions.

- Address Classification – Initially, it would be a little confusing to understand the terminology like Inside, Outside, Local, and Global. The figure attempts to clear the concepts associated with NAT terminology.
    - Inside Global : An inside address seen from the outside. This is a global, publicly-routable IP address used to represent an inside device to the outside world. In a NAT configuration, inside global addresses are those “real” IP addresses assigned to an organization for use by the NAT router.
    - Inside Local - An address of a device on the local network, expressed using its normal local device representation. So for example, if we had a client on a network using the 10.0.0.0 private address block, and assigned it address 10.0.0.207, this would be its inside local address.
    - Outside Global : An address of an external (public Internet) device as it is referred to on the global Internet. This is basically a regular, publicly-registered address of a device on the Internet. In the example above, 204.51.16.12 is an outside global address of a public server.
    - Outside Local : An address of an external device as it is referred to by devices on the local network.
    - NAT Pool : A pool of IP addresses to be used as inside global or outside local addresses in translations.

  The figure provides a conceptual understanding of the Inside and Outside networks and addressing.



There are different ways that a NAT be configured on a network. These are:

- Static Nat: Maps an unregistered IP address to registered IP (globally unique) addresses on one-to-one basis.
- Dynamic NAT:Maps an unregistered IP address to a registered (globally unique) IP address from a group of registered (globally unique) IP addresses.
- Overloading: A special case of dynamic NAT that maps multiple unregistered IP addresses to a single registered (globally unique) IP address by using different port numbers. Dynamic NAT with overloading is also known also as **PAT (Port Address Translation)**.

• Overlapping: This occurs when your internal IP addresses belong to global IP address range that belong to another network

- Configuring NAT

When configuring NAT, NAT should be enabled on at least one inside and one outside interface.

Typical configuration commands on Cisco router are given below.

1. The command for enabling NAT on inside interface is:

R1(config-if)#ip nat inside

2. The command for enabling NAT on the outside interface is:

R1(config-if)#ip nat outside

Remember to enter into appropriate configuration modes before entering the commands. Usually, the inside NAT will be configured on an Ethernet interface, whereas the outside NAT is configured on a serial interface.

VLAN and VTP Configuration and Troubleshooting:

When you are configuring VLANs and trunks on a switched network, the following types of configuration errors are most likely to be encountered:

1. Native VLAN mismatches
2. Trunk mode mismatches
3. VLANs and IP Subnets config issues
4. Allowed VLANs on trunks – Configuring a trunk route for allowed VLANs.

Things to remember in configuring VTP:

1. VTP is a Layer 2 messaging protocol. It carries configuration information throughout a single domain

2. VTP Modes are

Server : Create, modify, or delete VLANs (This is the deafult vtp mode on a switch)
Client : Can't create, change, or delete VLANs
Transparent : Used when a switch is not required to participate in VTP, but only pass the information to other switches

3. VTP domain is common to all switches participating in VTP

4. Pruning is a technique where in VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic

5. Configuration revision number is a 32-bit number that indicates the level of revision for a VTP packet. Each time the VTP device undergoes a VLAN change, the config revision is incremented by one.

Typical VTP Configuration commands on a Cisco switch are given below:

SW1#vlan database

SW1(vlan)#vtp mode (Server/Client/Transparent)
SW1(vlan)#vtp domain <name>
SW1(vlan)#vtp password <password>
SW1(vlan)#vtp pruning

2.2 Given a scenario, install and configure a wireless network.

When installing and configuring a wireless network, you need to remember the following:

Driver Compatibility - It is important to make sure that you have installed the correct device driver for your wireless network adapter.

Low Signal Strength - There are a number of factors that can cause the signal of your access point to deteriorate and the performance of your network to fall under par. Practically any appliance that operates on the same frequency level (2.4 GHz) as 802.11b or 802.11g can cause interference with your wireless network. Be sure to keep cordless phones, microwaves and other electrical equipment at least 1m away from the access point. Try changing channels on the access point and test it out on one of the clients.

Access Point Location - You may also want to try changing the position of your access point antenna to improve performance.

Installing a repeater for a performance boost:

If you're looking for a boost you can always choose to install a repeater. The job of a repeater is to receive the signal, regenerate it and rebroadcast it therefore extending the range of your wireless network. This would sit somewhere between your Access Point and your wireless client.

Changing the Antenna:

Changing the antenna of your access point can increase signal range and overall performance. Typical access points come with a 2dB or 4dB gain antenna but there are one's available with higher gain. Antenna gain is measured in dBi (decibels-isotropic) which basically means how powerful the antenna is and how far it can provide a signal. .

There are three main categories of antennas:

- Omni-directional - Omni-directional antennas radiate RF in a fashion similar to the way a table or floor lamp radiates light. They are designed to provide general coverage in all directions.
- Semi-directional - Semi-directional antennas radiate RF in a fashion similar to the way a wall sconce is designed to radiate light away from the wall or the way a street lamp is designed to shine light down on a street or a parking lot, providing a directional light across a large area. Yagi antenna is an example of this type of antennas.
- Highly-directional - Highly-directional antennas radiate RF in a fashion similar to the way a spotlight is designed to focus light on a flag or a sign. Each type of antenna is designed with a different objective in mind. Phased array antenna is an example of this type of antenna.

Choose which ever antenna type is most suitable.

Other configuration issues that one may need to know are DNS, DHCP, MAC filtering, and encryption settings.

2.3 Explain the purpose and properties of DHCP.

Static Addressing

You can request a static IP address it is one IP address for only one customer and is constant. These are more reliable for VOIP, for hosting gaming websites and to use VPN. Another advantage is that because you IP is static that is it will not be assigned to any other you need not worry of your IP getting blacklisted because of some only else sending SPAM.

Dynamic addressing

When DHCP client boots, it sends out a DHCP discover message. All DHCP servers answer with an offer message that includes an address which is available to the client. client machine typically repeats the discover message several times to make sure it hears from all the servers, then eventually chooses one server The currently active DHCP server is configured by hand to handle and reserve IP addresses and the IP configuration information that goes with them. Addresses are made available in an order that permits a client to have the best chance of getting back the same address it was using most recently. IP configuration information gets automatically configured for your client machine by the DHCP server.

DHCP reservation

If you set a DHCP Reservation the computer you set will get the same IP each time but it will be given out by the DHCP server. DHCP reservation is a permanent IP address assignment. It is a specific IP address within a DHCP scope that is permanently reserved for leased use to a specific DHCP client.

DHCP scope

DHCP scope is the consecutive range of possible IP addresses that the DHCP server can lease to clients on a subnet. These are the primary way for the DHCP server to manage distribution and assignment of IP addresses. These define a single physical subnet on network to which DHCP services are offered.

DHCP lease

DHCP clients get a lease for IP address from server. DHCP server must renew the lease before it expires for the client or client should obtain a new lease. DHCP server database provides an extension of one day after expiration that is database will retain lease information in database for one after expiration this grace period is provided to handle time zone difference , internal clock differences.

2.4 Given a scenario, troubleshoot common wireless problems.

- Interference :Wireless networks use radio signals to transmit signals and are subjected to interference from many factors. Any electrical device around wireless access point that produce radio waves can cause interference.

- Signal strength: User always want to connect to the network with highest signal strength. If a user is getting low signal strength either user or WAP can be moved to improve signal strength. Also changing the antenna type can improve signal strength.

- Configuration: User should not be required to do many configuration changes. Broadcasting SSID will allow user to detect the network and make connection. Any security protocol information and password required by end user should also be communicated in order to make connection.

- Encryption type: To ensure maximum security for wireless networks highest encryption protocols must be used that are supported by both WAP and clients. Both WAP and clients must be configured with same encryption type.

2.5 Given a scenario, troubleshoot common router and switch problems.

- Bad Cables/ improper cables: For a network to work efficiently proper cable should be used. Use of improper cable can cause connection issues and low performance.

- Port configuration: Port configurations should be done according to design of network , topology being used and main use of the port. Some port configuration include opening and shutting the port, setting duplex, encryption type, protocols etc..

- VLAN assignment: It can be used to create virtual networks. This assignment should be done properly to include clients in specific subnet. If assignment is not done correctly it can lead to in efficiency, connectivity issues and some time security issues too.

- Mismatched MTU/MTU black hole: Maximum Transmission Unit is Maximum Transmission Unit it is largest size packet that will be expected by a network. It interfaces used to connect devices are not with same MTU then packet drop can occur and client will not be able to receive data properly.

- Power failure: power failure can can stop routers and switches to stop working and can effect working of the network so UPS should be used to provide continuous power.

- Bad/missing routes: If some information in routing tables is incorrect or is missing it can effect routers ability to make proper decision. If a routing protocol is properly configured it will automatically provide all routing information.

- Duplicate IP address: Because of some misconfiguration duplicate address can be placed in the network. This issue can be detected by operating system can will be reported easily.

2.6 Given a set of requirements, plan and implement a basic SOHO network.

- Cable length: Some basic requirements are twisted-pair cable should not be more than 100 meters from a

switch. Also to prevent fire spreading from Ethernet cables installed between ceiling and floor and prevent spreading of spread toxic gases Special plenum type cables should be used

- Device types/requirements: Some devices required for SOHO networks are desktops, laptops, routers, switches, printers, faxes machines.
- Environment limitations: Routers and switches should be saved from flooding or high humidity and optimum operating temperature should be maintained. In wireless networks absorption or refection of radio waves should be accounted.
- Equipment limitations: SOHO net works are generally a scaled-down version of the same type of device you would use for an enterprise network, should use SOHO equipment for SOHO environment, but you should generally not use it for a larger enterprise environment
- Compatibility requirements: A compatible media, client or service, and protocol must be used.

3. Network Media and Topologies

3.1 Categorize standard media types and associated properties.

- Multimode fiber: It carry multiple rays of light concurrently and different reflection angle. These can carry short distances as strength weakens over distance.
- Single mode fiber: It can carry single direct ray of light. It can travell longer distance as distortion is less as compared to multimode fiber.
- UTP stands for Un-shielded Twisted Pair cabling. A cable made up of 8 individual wires. 4 pairs twisted together. f wires in a cable are not twisted or shielded, that cable can act as an antenna, which might receive or transmit EMI. To help prevent this type of behavior, the wires (which are individually insulated) can be twisted together in pairs.
- STP for Shielded Twisted Pair cabling. environments in which greater resistance to EMI and attenuation is required. provides the extra shielding by using an insulating material that is wrapped around the wires within the cable. This extra protection increases the distances that data signals can travel over STP but also increases the cost of the cabling.
- CAT3: This standard was used in 90's for homes and offices. It can transmit data up to 10Mbps with a possible bandwidth of 16MHz
- CAT5: It uses either the 10BASE-T or 100BASE-T standard for data transmission Using two cable pairs to signal over copper wire. It provides a minimum of 100MHz of bandwidth.
- CAT5e: It uses four pairs of copper wire. In addition, the wire pairs are twisted more tightly and are

sheathed in heavy-duty shielding to eliminate crosstalk. It is used for 1000BASE-T networks, which carry data at a rate of 1 Gbps.

- CAT6: It can transmit data up to 10Gbps, has a minimum of 250MHz of bandwidth and specifies cable lengths up to 100 meters with 10/100/1000Mbps transfer, along with 10Gbps over shorter distances. It is made up of four twisted pairs of copper wire, an longitudinal separator separates each of the four pairs of wires from each other

- CAT 6a: It can operate at a frequency of up to 750 MHz and is even less susceptible to interference and crosstalk CAT6a is the preferred cable for 10GBASE-T Ethernet

- Straight-through: The Cable is wired the same on both sides following the 568a or 568b wiring schematic.

- Plenum cable: It is fire retardant and minimize toxic fumes released if a networking cable catches fire.

3.2 Categorize standard connector types based on network media.

- ST(Straight tip): Also called as bayonet connector used with MMF. It connects to terminating device by pushing the connector and housing to lock it.

- SC (Subscriber connector): Also called standard connector , or square connector . Can be connected by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device.

- LC(Lucent connector) : connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pressing the tab on the connector and pulling it out of the terminating device.

3.3 Compare and contrast different wireless standards.

	802.11a	802.11b	802.11g	802.11n
Distance	35m indoors/ 120 m outdoors	32m indoors/140m outdoors	32m indoors/140m outdoors	70m indoors/250 m outdoors
Speed	54 Mbps	11 Mbps	48Mbps	130-150Mbps
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz and 5GHz

Multiple Input Multiple Output

It uses multiplexing to increase the range and speed of wireless networking. It enables the transmission of multiple data streams traveling on different antennas in the same channel at the same time. A receiver reconstructs the streams, which have multiple antennas as well.

3.4 Categorize WAN technology types and properties.

- The transmission speed of a T1 circuit (Used mainly in North America) is 1.544Mbps
- The transmission speed of an E1 circuit (Used mainly in Europe) is 2.048Mbps.
- The transmission speed of a T3 circuit (Used mainly in North America) is 44.736 mbps

- OC stands for Optical Carrier and is used to specify the speed of fiber optic networks conforming to the SONET standard.
  Below are the speeds for some common OC levels.
  OC level Speed
  OC-1 = 51.85 Mbps
  OC-3 = 155.52 Mbps
  OC-12 = 622.08 Mbps
  OC-24 = 1.244 Gbps
  OC-48 = 2.488 Gbps
  OC-192 = 9.952 Gbps

- DSL: DSL uses existing copper telephone lines. DSL technologies typically provide speeds up to 1.544 Mbps.

- Cable modem: Cable modem uses the same line as cable TV. Possible bandwidth for Internet access reaches up to 27 Mbps.

- ISDN: ISDN comes in two flavors- BRI and PRI. The most commonly used is BRI, Basic Rate Interface. BRI is composed of two 64-Kbps B (bearer) channels and one 16 Kbps D (delta) channel. ISDN supports both voice and video.
  ISDN specifies two standard access methods:

  1. BRI (Basic Rate Interface): Consists of two B channels (64Kbps) and one D channel (16Kbps).
  The B channels can be used for digitized speech transmission or for relatively high-speed data transport.
  The D channel carries signaling information (call setup) to control calls on B channels at the UNI (User-Network Interface)

  2. PRI (Primary Rate Interface): Consists of 23 B channels and one D channel with a bandwidth of 1.544Mbps. PRI uses a DSU/CSU for a T1 connection. B stands for Bearer Channel.

- WiMAX is a short name for Worldwide Interoperability of Microwave Access. WiMAX is described in IEEE 802.16 Wireless Metropolitan Area Network (MAN) standard. It is expected that WiMAX compliant systems will provide fixed wireless alternative to conventional DSL and Cable Internet. Typically, a WiMAX system consists of two parts:

  1. A **WiMAX Base Station:**Base station consists of indoor electronics and a WiMAX tower. Typically, a base station can cover up to 10 km radius (Theoretically, a base station can cover up to 50 kilo meter radius

or 30 miles, however practical considerations limit it to about 10 km or 6 miles). Any wireless node within the coverage area would be able to access the Internet.

2. A **WiMAX Receiver**- The receiver and antenna could be a stand-alone box or a PCMCIA card that sits in your laptop or computer. Access to WiMAX base station is similar to accessing a Wireless Access Point in a WiFi network, but the coverage is more.

- LTE, or long-term evolution, is a type of mobile broadband that rivals WiMAX. Both services are IP-based and use a technology called orthogonal frequency-division multiplexing (OFDM) access. They also use a type of wireless technology that lets people get high-speed Internet across coverage areas that span miles. The standard is maintained as a project of the 3rd Generation Partnership Project (3GPP), operating under a name trademarked by one of the associations within the partnership, the European Telecommunications Standards Institute (ETSI).
- The goal of LTE is to increase the capacity and speed of wireless data networks utilizing cutting-edge hardware and DSP techniques that have recently been developed. Its wireless interface is incompatible with 2G and 3G networks, and so it must be operated on separate wireless spectrum.
- Features of LTE include an all-IP flat network architecture, end-to-end QoS including provisions for low-latency communications, peak download rates nearing 300 mbps and upload rates of 75 mbps, capacity exceeding 200 active users per cell, the ability to manage fast-moving mobiles, and support for multi-cast and broadcast streams.

3.5 Describe different network topologies.

A topology is physical and logical network layout. Physical layout include actual layout of cables and other network devices where as Logical layout include the way in which the network appears to the devices that use it.

Mesh : In this topology each computer is connected to every other. This topology is rarely used.

Advantages:

- It provide multiple paths between two devices so if one path fails other can be used.

- Network can be expanded without distruption to current uses

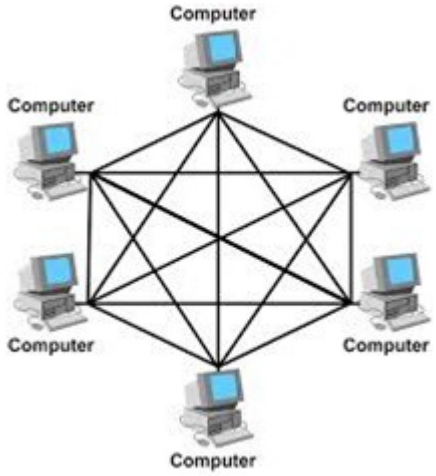
Disadvantages

- It has high level of redundancy

- wiring is very complicated

- Cabling cost is very high

- Finding fault in cabling is very tricky



Ring : In this topology each network computer and device are connected to each other forming a large circle (or similar shape). Each packet is sent around the ring until it reaches its final destination. Typically FDDI, SONET or Token Ring technology are used to implement a ring network.

Advantages:

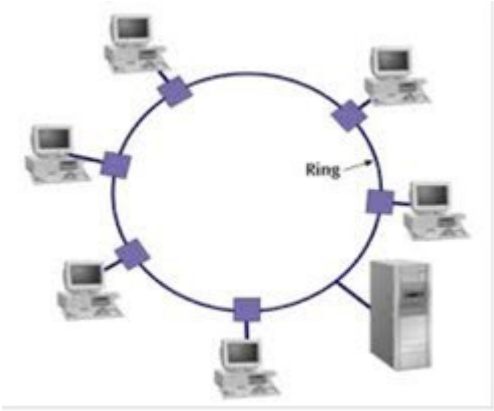
- Any fault in cable can be found easily.

- These networks are comparatively easy to install.

Disadvantages:

- Expansion will cause disruption in current network

- Single fault in cable will disrupt entire network.



BUS : Bus networks use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the

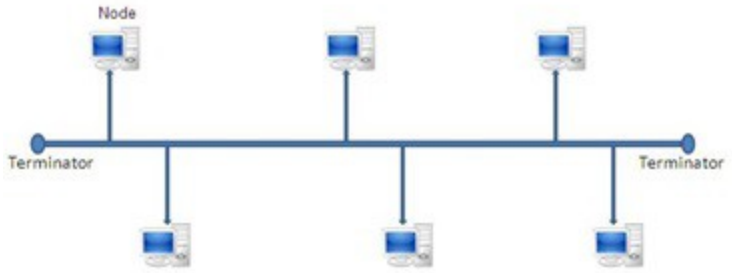
wire that all other devices see, but only the intended recipient actually accepts and processes the message.

Advantages:

- Easy to implement
- Less cable is used
- No specialized network equipment is needed.

Disadvantages

- Single fault in cable will disrupt entire network.
- Expansion will cause disruption in current network
- Troubleshooting is difficult.



Star: In Star topology, all the components of network are connected to the central device called “hub” which may be a hub, a router or a switch. All the data on the star topology passes through the central device before reaching the intended destination. Hub acts as a junction to connect different nodes present in Star Network, and at the same time it manages and controls whole of the network. Depending on which central device is used, “hub” can act as repeater or signal booster. Central device can also communicate with other hubs of different network. Unshielded Twisted Pair (UTP) Ethernet cable is used to connect workstations to central node.

Advantages:

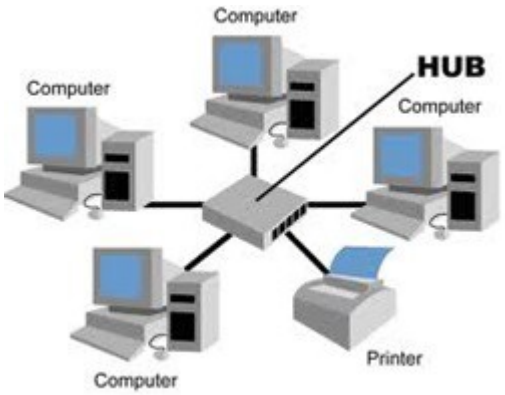
- Gives better performance compared to BUS
- New devices can be added easily.
- Centralized management makes monitoring the network is easier.
- Single node failure will not affect entire network.

Disadvantages

- If central device (Hub) fails whole network goes down.

- Use of central device increase overall cost.

- Performance of network depends on capacity of central device.



Hybrid: It is an integration of two or more different topologies to form a resultant topology. This combination of topologies is done according to the requirement of the organization.

For example an office can use a star topology in each of its department and ring topology to connect these departments.

Advantages:

- Fault detection is easier.

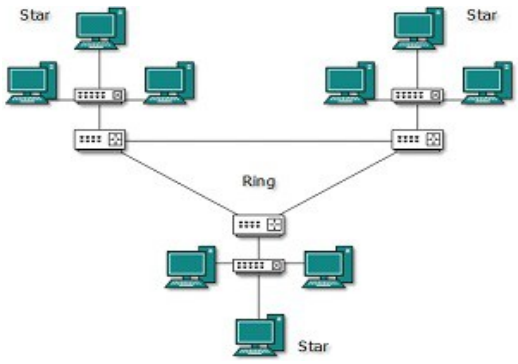
- Size of the network can be increased easily without distruption to current network.

- It is very flexible as network can be designed according to requirements and available resources.

Disadvantages

- Overall cost of network is high as it requires lot of cables, many network devices like HUB to connect various networks.

- Design becomes more and more complex as number of networks increase



3.6 Given a scenario, troubleshoot common physical connectivity problems.

- DB loss :Difference between signal at source and signal at destination is calculated using DB loss algorithm. Getting DB loss as 0 is impossible as there will be some DB loss in network. This number should be tried to keep minimum.

- TXRX reversed: A TX that is Transmitter should be connected to RX that is Receiver. If crossover cables are used to connect similar devices then TX to TX and RX to RX connection can cause problems.

- Cable placement: Right cable should be used in right location. If incorrect cable is used like a cable is used that is outside wiring standards can cause problems like interference, and attenuation. Ethernet cables should not be placed in close proximity with high voltage cables .

- EMI/Interference: If cables run too close to devices which created electromagnetic waves like monitors it can corrupt the signals. So cables should be placed away from these devices also proper shielding should be used.

- Distance: Network design should consider distance between devices. If devices are connected using cables that are at a distance more limitation of Ethernet cables then can cause in errors in transmission.

- Crosstalk: It occurs when two cables running close to each other and are carrying signals interfere with each other and creates undesired effect. This is usually experienced in analog phone calls. It can be minimized by using higher category of cabling.

3.7 Compare and contrast different LAN technologies.

- Ethernet: It is IEEE 802.3 standard. Speed is uoto 10 Mbps and distance is 100m.

- 1000Base-T: Uses UTP cabling and supports up to 100 m. It has 4 pairs of cat 5e or higher cable.

- 1000Base-SX: Uses MMF cabling and supports up to 550 m. It uses SC fiber connectors.

- 1000Base-LX: It uses both MMF and SMF cabling. It can support up to 550 m in multi mode and up to 2000 m in single mode. Further, it uses LC and SC connectors.

- 1000Base-CX: It uses balanced shielded copper, and can support up to a distance of 25 meters. It uses a special connector, the HSSDC.

- 10Gbase-T: 10GbaseT uses UTP cabling and connect to networks using Fast Ethernet. The standard supports a maximum distance of 100 m.

- 10GBASE-SR (802.3ae) - Supports up to 300 m, cable type used: Multi Mode Fiber (MMF)
- 10Gbase-LR (802.3ae) – supports 10 km, cable type used: Single mode fiber (SMF)
- 10GbaseER(802.3ae) – Supports up to 40 km, cable type used: Single mode fiber (SMF)
- 10Gbase-SW(802.3ae)- Supports up to 300 m, cable type used Multi Mode Fiber (MMF)
- 10Gbase-LW(802.3ae)- supports 10 km, cable type used: Single mode fiber (SMF), typically used with SONET
- 10Gbase-EW(802.3ae)- supports 40 km, cable type used: Single mode fiber (SMF)

3.8 Identify components of wiring distribution.

- IDF (Intermediate Distribution Frame) : It is connected to MDF using a backbone cable when multiple wiring closets are used.
- MDF (Main Distribution Frame): It is a wiring point which is a reference point for telephone lines. It holds switches, routers, servers etc..
- Demarc: It is a point in telephone network after which maintanance will be done by telephone company.
- Demarc extension: This extens demarcation point to a more functional location.
- Smart jack: It is also known as NID(Network Interface Device) and is a hardware at dearction point. It contains connection and electronic testing equipments fro loo[back testing and other troubleshooting.

4. Network Management

4.1 Explain the purpose and features of various network appliances.

- Load Balancer :A load balancer is used to distribute workload across multiple computers or a computer cluster. It could be done by a dedicated hardware or software.
- Proxy server: proxy servers cache website information for the clients, reducing the amount of requests that need to be forwarded to the actual corresponding web server on the Internet. These save time, use bandwidth efficiently also help to secure the client connections.
- Content Filter: filtering is used categorize the websites on the internet. You can allow/block specific

website access to the web users of the organization. This can be done by referring to central database or by classifying the websites in real time. filtering can also be made applicable only during certain times of a day or days of a week, if required.

- VPN concentrators allow for secure encrypted remote access

4.2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues.

- Shielded cables usually comprise of one or two insulated wires that are surrounded by an aluminum Mylar foil or a woven braided shield. The foiled shield of the cable ensures better signal transmission by eliminating irregular power frequency and external radio interference. Mostly, power cables which carry high-voltage of electricity are shielded for greater protection and better electric transmission. Shielded cables exhibit better interference rejection characteristics compared to unshielded cables.

- The IEEE 1394 interface is a serial bus interface standard for high-speed communications frequently used by personal computers, as well as in digital audio, and digital video, The interface is also known by the brand names of FireWire (Apple), i.LINK (Sony), and Lynx (Texas Instruments).

- A punch down tool, also called a punch down tool is used widely by network technicians. It is used for inserting wire into insulation-displacement connectors on punch down blocks or patch panels.

- A crimping tool is a tool designed to crimp or connect a connector to the end of a cable. For example, network cables and phone cables are created using a crimping tool to connect the RJ-45 and RJ-11 connectors to the end of the cable.

- RG-6 may be used for both analog and digital television transmission.

- A toner probe is a simple cable continuity tester. It consists of two pieces of equipment. One is the tone generator and the other is the probe. One end of the cable is hooked to the tone generator, and the other end is observed for tone using a matching probe. It is also called “fox and hound” wire tracer.

- A protocol analyzer is used to monitor and troubleshoot problems such as suspicious activity on the network, verification of network load and type of traffic, artificially injecting load on to a network for the purpose of load testing, and other hard to detect problems with the network.

- Certifier, or a certification tester is used to examine whether the network complies with ISO or TIA standards as applicable. Some certifiers will also have the capability to test the email, DNS, and DHCP servers for proper response times.

- TDR, Time Domain Reflectometer is a tool that finds faults in metallic cabbles like twisted wire pairs and coaxial cables. A similar device, OTDR (short for Optical Time-Domain Replectometer)

is used for testing fiber optic cables.

4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

- PING Used to ping the remote system (or the local host) to see that the TCP/IP connection is through.
- NBTSTAT This utility displays current NetBIOS over TCP/IP connections, and display NetBIOS name cache.
- NETSTAT Displays protocol statistics and current TCP/IP connections since the server was last booted. The command netstat provides active connections on the host with detail like local address, foreign address, etc.
- TRACERT Used to determine which route a packet takes to reach its destination from source.
- IPCONFIG Used to display Windows IP configuration information. The command ipconfig can be used to display the current TCP/IP configuration of a Windows 2000 computer. Note that on a Win9x, we use winipconfig command to view the current TCP/IP configuration.
- NSLOOKUP This utility enables users to interact with a DNS server and display resource records.
- ROUTE Used to display and edit static routing tables.
- ARP: It is used to view the logical and physical address mapping. (Short for Address Resolution Protocol) cache entries are added to an arp cache table either as static entries (manually entered) or as dynamic (system learned) entries. The cache entries help in minimizing the network load, since it is not necessary to resolve an IP address to hardware address every time a packet is received. "Fixed arp cache entry" and "Temporary arp cache entry" are fictitious anwers.
- RARP (Reverse Address Resolution Protocol): RARP is used to obtain IP address from a known MAC address.
- BootP (Bootstrap Protocol): When a diskless workstation is powered on, it broadcasts a BootP request on the network. A BootP server responds with its IP address, Default gateway, etc.
- Protocol Analyzer And Packet Analyzer (Sniffer): These are loaded on a computer and are controlled by the user in a GUI environment; they capture packets enabling the user to analyze them and view their contents. Example Network Monitor

4.4 Given a scenario, use the appropriate network monitoring resource to analyze traffic.

- Application log: The application log contains events logged by applications or programs. For example, a

database program might record a file error in the application log. The developer decides which events to record.

- System log: The system log contains events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined.

- Security log: The security log can record security events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.

- Antivirus log: Antivirus log analyzer can process log files from various antivirus packages and generate dynamic statistics from them, analyzing and reporting events.

- Protocol Analyzer And Packet Analyzer (Sniffer): These are loaded on a computer and are controlled by the user in a GUI environment; they capture packets enabling the user to analyze them and view their contents. Example Network Monitor

- Network Sniffer: These are third party equipments which perform network tests like load, connectivity, throughput. These include both hardware and software are provide results to improve network.

- SNMP (Simple Network Management Protocol): It enables monitoring of remote systems. There are three main parts of SNMP a manager, an agent, and a database of management information. The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device(s) being managed. The manager and agent use a Management Information Base (MIB) and a set of commands to exchange information.

4.5 Describe the purpose of configuration management documentation.

- Wire schemes: A networks requires lot of wiring depending on its complexity. Mostly wiring in hidden in walls and ceiling therefore documentation of wiring should be kept up to date. It should include where wires are placed and what wires are used. This documentation will help in troubleshooting.

- Network Maps: Network maps of both physical and logical topologies should be documneted. Physical topology documentation will include location of network devices, ports used etc. and logial topology documentation will contain VLAN networks.

- Well-functioning networks are characterized by documented
  1. policies
     - Privacy policy: This policy is used to secure user identities and other information related to user. If an internet based application provided by an organization require users to register with them using name and email id then this information provided by the user should be secure and not shared with

any third party without user knowledge. Privacy policy should state what information is stored and will be accessed by whom, it should also state if information will be shared with third party.

- Acceptable use: This policy restricts how a computer network and other devices and systems will be used. It states what users can do and what not with technology infrastructure of an organization. It is signed by the employees before they begin working on any systems. This protects the organization from employees misusing the systems or network. The policy may put limits on personal use of resources, and resource access time.
- Security policy: A company's security policy outlines the security measures to be taken. Implementing the security policy is the first thing that needs to be done.

2. procedures: These describe how tasks are performed. Like admin is supposed to take backups, how often backups are to be taken, where to store them etc.

3. configurations: Both software and hardware configuration should be documented.

4. Regulations: All the restrictions with its legal consequences are documented.

- Cable management: Proper documentation of networks cable infrastructure should be maintained. This will help in troubleshooting. It may include diagram of network's conduit system, location of punch down blocks etc.

- Asset Management: It is procedure to track network components and managing thir lifecycle. It includes following steps:
  - prepare
  - plan
  - design
  - implement
  - Operate
  - Optimize

- Baseline: It is used to measure network performance by setting a base line for comparision.

4.6 Explain different methods and rationales for network performance optimization.

- QoS stands for quality of service. In SOHO environment, QoS is normally set at router level. If you want to enforce QoS policies in your network, make sure you use a router, which is equipped with QoS software.

- Load balancing is the process of distributing a server or network load over a multiple servers or networks. An example of load balancing is a clustered solution where each server in a clustered pool shares the load as per the design parameters.

- High availability is incorporated in the system design so that the uptime of a system is maintained as per the designed standards under all circustances. High availability is usually design specific where as the fault tolorence is device or network specific.

- Caching improves network performance by locally caching content, thereby limiting surges in traffic.

- A VoIP telephony solution hosted by a service provider, which interconnects with a company's existing telephone system is known as Virtual PBX. A hosted PBX is one that is hosted by the telephone company on behalf of its customer. The important elements and the functions of a VOIP network are given below:

  a. IP phone: An IP phone is a telephone with an integrated Ethernet connection. Although users speak into a traditional analog handset (or headset) on the IP phone, the IP phone digitizes the spoken voice, packetizes it, and sends it out over a data network (via the IP phone's Ethernet port).

  b. Call agent A call agent is a repository for a VoIP network's dial plan. For example, when a user dials a number from an IP phone, the call agent analyzes the dialled digits and determines how to route the call toward the destination.

  c. Gateway A gateway in a VoIP network acts as a translator between two different telephony signaling environments. In the figure, both gateways interconnect a VoIP network with the PSTN. Also, the gateway on the right interconnects a traditional PBX with a VoIP network. PBX A Private Branch Exchange (PBX) is a privately owned telephone switch traditionally used in corporate telephony systems. Although a PBX is not typically considered a VoIP device, it can connect into a VoIP network through a gateway.

  d. Analog phone An analog phone is a traditional telephone, like you might have in your home. Even though an analog phone is not typically considered a VoIP device, it can connect into a VoIP network via a VoIP or, as shown in the figure, via a PBX, which is connected to a VoIP network.

  e. SIP Session Initiation Protocol (SIP) is a VoIP signaling protocol used to set up, maintain, and tear down VoIP phone calls. Notice in the figure that SIP is spoken between the IP phone and the call agent to establish a call. The call agent then uses SIP to signal a local gateway to route the call, and that gateway uses SIP (across an IP WAN) to signal the remote gateway (on the right) about the incoming call.

  f. RTP Real-time Transport Protocol (RTP) is a Layer 4 protocol that carries voice (and interactive video). Notice in the figure that the bi-directional RTP stream does not flow through the call agent.

5. Network Security

5.1 Given a scenario, implement appropriate wireless security measures.

WEP (Wired Equivalent Privacy)

A deprecated wireless network security standard, less secure than WPA. Key size is 64 bit. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not very secure. WEP is used at the two lowest

layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

WPA (Wi-Fi Protected Access)

A wireless encryption standard created by the Wi-Fi Alliance to secure wireless computer networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). Key size is 128 bits. WPA provides stronger encryption than WEP through use of either of two standard technologies: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). WPA also includes built-in authentication support that WEP does not offer. WPA provides comparable security to VPN tunneling with WEP, with the benefit of easier administration and use.

WPA2 (Wi-Fi Protected Access Version 2)

It is wireless encryption protocol and is based on the IEEE 802.11i technology standard for data encryption. Key size is 256 bits. It is more secure than WPA and WEP. WPA2 also improves the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires. Specifically, WPA2 does not allow use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes (limitations) in the original WPA implementation. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

MAC Filtering

Every Wi-Fi device is assigned a MAC (Media Access Control) address, a unique 12-digit hexadecimal identifier issued by the IEEE, the standards body that developed the Wi-Fi protocol. The MAC address is "hard-coded" in to the device and sent automatically to a Wi-Fi access point when the device tries to connect to the network.

Using the access point configuration software, you can create a safe list of allowed client devices or a black list of banned devices. If MAC filtering is activated, regardless of what encryption security is in place, the AP only allows devices on the safe list to connect, or blocks all devices on the black list – irrespective of encryption used.

Encryption protocols like WPA2 (Wi-Fi Protected Access 2), reduced the necessity for using MAC filtering. Hackers may break in to MAC filtering device by sniffing addresses of connected devices and then spoofing or masquerading as one of them.

To enable MAC address filtering and to allow the devices with matching MAC addresses, perform these steps (these steps are generic in nature, and likely to change from one device type to another):

- Step 1: Access the router's web-based setup page.
- Step 2: When the router's web-based setup page appears, click Wireless, look for MAC address filtering tab.
- Step 3: Enter the MAC addresses of the devices that are allowed to use the wireless network in the table provided.
- Step 3: Click on Save Settings

5.2 Explain the methods of network access security.

- VPN stands for Virtual Private Network. A VPN provides a mechanism to access corporate networks safely using Internet. VPN uses encryption to ensure only authorized user can access the corporate resources. A secure tunnel is created through the public network through which the packets are transported between the remote computer and the corporate network. Vit is used for accessing a corporate network securely from remote locations using public Internet. There are two widely known protocols that can be implemented for enabling VPN communications:

  1. PPTP: PPTP stands for Point to Point Tunneling Protocol. It is a PPTP is pioneered by Microsoft and others is a widely used protocol.

  2. L2TP: L2TP stands for Layer Two (2) Tunneling Protocol. L2TP merges the best features of PPTP and L2F (from Cisco Systems).

  PPTP and L2TP protocols together with PPP protocol enable ISPs to operate Virtual Private Networks (VPNs).

- PGP is used primarily for securing email communications.

- IPSEC stands for IP SECurity. The protocol is developed by IETF and supports secure exchange of packets at IP layer. When using IPSEC, the sending and receiving devices share a public key. IPSEC is the most widely used protocol in Virtual Private Networks (VPNs).

- ISAKMP (Short for Internet Security Association and Key Management Protocol) defines payloads for exchanging key generation and authentication data.

- SSH (Secure Shell): It is a protocol that can create a secure channel between two computers or network devices, enabling one computer or device to remotely control the other. It is commonly used on Linux and Unix systems, and nowadays also has widespread use on Windows clients. It uses public key cryptography to authenticate remote computers. One computer (the one to be controlled) runs the SSH daemon, while the other computer runs the SSH client and makes secure connections to the first computer (which is known as a server), as long as a certificate can be obtained and validated.

5.3 Explain methods of user authentication.

- EAP (Extensible Authentication Protocol) :It is a framework for transporting authentication protocols. EAP defines the format of the messages. It uses four types of packets : request, response, success and failure. Request packets are issued by authenticator and ask for response packet from supplicant. If authentication is successful, a success packet is sent to the supplicant is not a failure packet is sent.

- Public Key Infrastructure (PKI): It is a framework for all of the entities involved in digital certificates—including hardware, software, people, policies, and procedures to create, store, distribute, and revoke digital certificates. PKI is essentially digital certificate management.

- Kerberos: Kerberos is basically an authentication protocol that uses secret-key cryptography for secure authentication. In Kerberos, all authentication takes place between clients and servers. The name Kerberos comes from Greek mythology; it is the three-headed dog that guarded the entrance to Hades. It was developed by the Massachusetts Institute of Technology, USA Kerberos require that the time sources are approximately in synchronization (with in 5 minutes) with each other. However, with recent revisions of Kerberos software, this rule has become flexible. Some of the features of Kerberos authentication system:

    - Uses client-server based architecture.
    - Kerberos server, referred to as KDC (Key Distribution Ceter) implements the Authentication Service (AS) and the Ticket Granting Service (TGS).
    - The term "application server" generally refers to Kerberized programs that clients communicate with using Kerberos tickets for authentication purpose. For example, the Kerberos telnet daemon (telnetd) is an example of an application server.

- When the user wants to talk to a Kerberized service, he uses the TGT to talk to the Ticket Granting Service (TGS, also runs on the KDC). The TGS verifies the user's identity using the TGT and issues a ticket for the desired service. The TGT ensures that a user doesn't have to enter in their password every time they wish to connect to a Kerberized service. The TGT usually expires after eight hours. If the Ticket Granting Ticket is compromised, an attacker can only masquerade as a user until the ticket expires. The following are the important properties of Kerberos:

    - It uses symmetric encryption
    - Tickets are time stamped
    - Passwords are not sent over the network

- Remote Authentication Dial-In User Service (RADIUS): It provides centralized administration of dial-up, VPN, and wireless authentication and can be used with EAP and 802.1X.

- Terminal Access Controller Access-Control System (TACACS): It is remote authentication protocol used more often in UNIX networks. In UNIX, the TACACS service is known as the TACACS daemon. The newer and more commonly used implementation of TACACS is called TACACS+. It is not backward compatible with TACACS. TACACS+, and its predecessor XTACACS, were developed by Cisco. TACACS+ uses inbound port 49. TACACS and XTACACS are not commonly seen anymore. The two common protocols used today are RADIUS and TACACS+.

- CHAP: It is an authentication type that uses three-way handshake. The passwords are transmitted in encrypted form ensuring security. Compare this with PAP, which transmits passwords in clear text. It uses a three step process for authentication (excluding making the connection itself). If making the connection is also involved, it would be a 4 step process.

- Multifactor authentication: Here two or more number of authentication methods are used for granting access to a resource. Usually, it combines a password with that of a biometric authentication.

5.4 Explain common threats, vulnerabilities, and mitigation techniques.

- The evil twin is another access point or base station that uses the same SSID as an existing access point. It attempts to fool users into connecting to the wrong AP, compromising their wireless session.
- Wardriving is the act of using a vehicle and laptop to find open unsecured wireless networks
- Rogue access points can be described as unauthorized wireless access points/routers that allow access to secure networks
- war chalking: On finding an open WLAN user writes a symbol on the structure nearby for others to know the credentials of the network.
- WEP cracking: Many utilites are available on internet to find preshared key (PSK) by using mathematical algorithms. These collect packets transmitted by secure access point and use algorithm on them to get information.
- Distributed Denial of Service (DdoS): It is an attack where multiple compromised systems (which are usually infected with a Trojan) are used to send requests to a single system causing target machine to become unstable or serve its legitimate users. A hacker begins a DDoS attack by exploiting a vulnerability in one computer system and making it the DdoS "master", also called as “zombie”. It is from the zombie that the intruder identifies and communicates with other systems that can be compromised. The intruder loads hacking tools on the compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. This causes Distributed Denial of Service (DDoS) attack on the target computer.
- Denial-of-service (DoS): These attacks, are explicit attempts to block legitimate users system access by reducing system availability. Any physical or host-based intrusions are generally addressed through hardened security policies and authentication mechanisms. Although software patching defends against some attacks, it fails to safeguard against DoS flooding attacks, which exploit the unregulated forwarding of Internet packets. Hackers use zombies to launch DoS or DDoS attacks. The hacker infects several other computers through the zombie computer. Then the hacker sends commands to the zombie, which in turn sends the commands to slave computers. The zombie, along with slave computers start pushing enormous amount of useless data to target computer, making it unable to serve it legitimate purpose.
- Smurf attack : It is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system
- Man-In-The-Middle: These attacks intercept all data between a client and a server. It is a type of active interception. If successful, all communications now go through the MITM attacking computer. The attacking computer can at this point modify the data, insert code, and send it to the receiving computer. This type of eavesdropping is only successful when the attacker can properly impersonate each endpoint.

- Virus: A computer virus attaches itself to a program or file so it can spread from one computer to another.Almost all viruses are attached to an executable file, and it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going.

- Worm: Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. The danger with a worm is its capability to replicate itself. Unlike Virus, which sends out a single infection at a time, a Worm could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

- Buffer overflow occurs when the input is more than that allocated for that purpose. The system doesn't know what to do with the additional input, and it may result in freezing of the system, or sometimes to take control of the system by a hacker. By validating the inputs, it is possible to reduce this vulnerability to a great extent.

- Packet sniffing is a form of wire-tap applied to computer networks instead of phone networks. It came into vogue with Ethernet, which is known as a "shared medium" network. This means that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus see everyone traffic.

5.5 Given a scenario, install and configure a basic firewall.

- Port Security: It deals more with switches and the restriction of MAC addresses that are allowed to access particular physical ports.

- Dynamic Packet Filters: Also referred to as Stateful Inspection, DPF, unlike static packet filters, monitors each session and makes sure they are valid. Note that a static packet filtering uses only the header information in a packet traversing the FireWall, whereas a Dynamic Packet Filter inspects all the interfaces based on a state table. CheckPoint's ® FireWall-1 uses stateful inspection.

- Implicit deny: It requires that all access is denied by default and access permissions are granted to specific resources only when required. An implicit deny clause is implied at the end of each ACL, and it means that if the provision in question has not been explicitly granted, then it is denied.

- Access control lists (ACLs) :ACL resides on a router, firewalls or computers and decides who can access the network and who cannot. That means it enable or deny traffic. It specify which user or group of users are allowed what level of access on which resource. It makes use of IP addresses and port numbers.

- NAT (Network Address Translation) :It is primarily used to hide internal network from external network, such as the Internet. A NAT basically translates the internal IP addresses to external IP addresses and vice-versa. This functionality assures that external users do not see the internal IP addresses, and hence the hosts.

- DMZ (DeMilitalized Zone) :It is a place separate from the LAN where servers reside that can be reached by users on the Internet. If a company intends to host its own servers to be accessed from public Internet, a DMZ is most preferred solution. The network segment within the DMZ is secured by two firewalls, one interfacing with the public Internet, and the other interfacing the internal corporate network. Thus, a DMZ provides additional layer of security to internal corporate network. The type of servers that are hosted on DMZ may include web servers, email servers, file servers, DNS servers, etc.

5.6 Categorize different types of network security appliances and methods

- IDS stands for Intrusion Detection System. There are primarily two types of IDSs. These are Network based IDS (NIDS), and Host based IDS (HIDS).
    - If the IDS monitors network wide communication, it is called Network based IDS.
    - If the IDS monitors security on a per host basis, it is called Host based IDS. A host based IDS should be place on a host computer such as a server.
    - Network based IDS is typically placed on a network device such as a router.

- Honeypots: Honeypots are designed such that they appear to be real targets to hackers. That is a hacker can not distinguish between a real system and a decoy. This enables lawful action to be taken against the hacker, and securing the systems at the same time.

- Honeynet :It is one or more computers, servers, or an area of a network; these are used when a single honeypot is not sufficient. Either way, the individual computer, or group of servers, will usually not house any important company information.

- Vulnerability testing is part of testing corporate assets for any particular vulnerability. These may include:
    - Blind testing: Here the hacker doesn't have a prior knowledge of the network. It is performed from outside of a network.
    - Knowledgeable testing: Here the hacker has a prior knowledge of the network.
    - Internet service testing: It is a test for vulnerability of Internet services such as web service.
    - Dial-up service testing: Here the hacker tries to gain access through an organization's remote access servers.
    - Infrastructure testing: Here the infrastructure, including protocols and services are tested for any vulnerabilities.
    - Application testing: The applications that are running on an organization's servers are tested here.
- Examples of Vulnerability scanner are NESSUS, NMAP