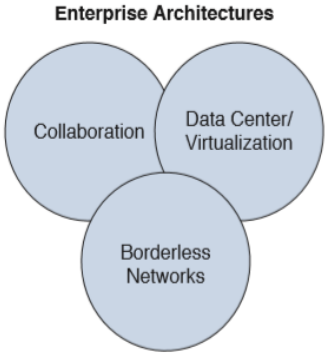
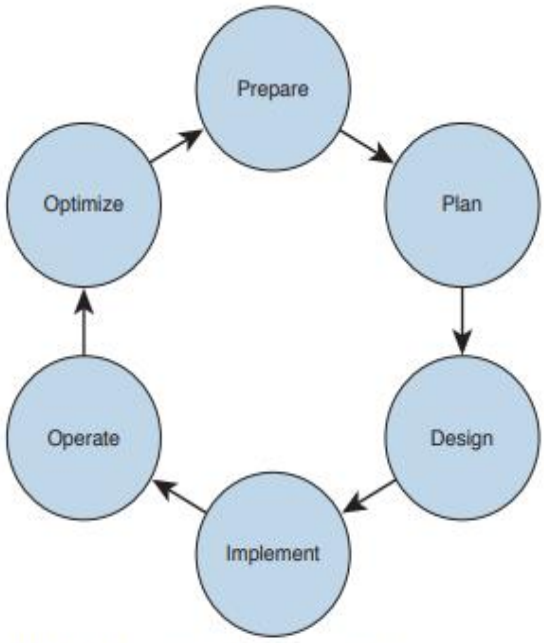
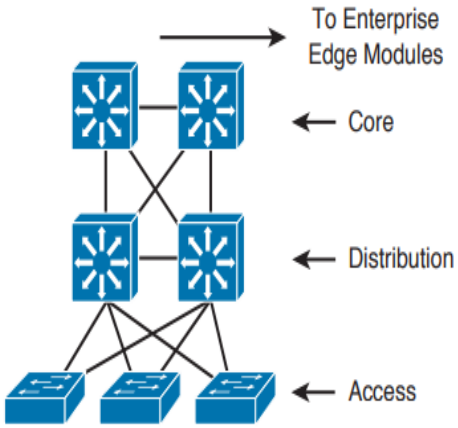
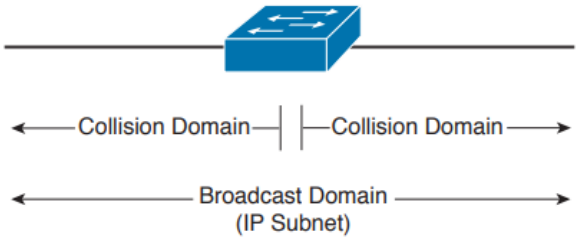
1	Attempt any three of the following.
a	Explain in details Architectures for the enterprise.
Ans:	Cisco has created an interwoven framework to create three architectures for each group that provides for optimization at an individual level and the integration with other areas: ■ Borderless networks architecture ■ Collaboration architecture ■ Data center and virtualization architecture  **Figure 1-1** *Cisco enterprise architectures* **Borderless Networks Architecture:** ■ Policy and Control: Policies are applied to all users and devices across the architecture. ■ Network Services: These services include resiliency and control. Cisco EnergyWise and MediaNet provide capabilities to borderless networks. ■ User Services: These services include mobility, performance, and security. ■ Connection Management: This block delivers secure access anytime and anywhere, regardless of how the network is accessed. **Collaboration and Video Architecture:** ■ Communication and Collaboration Applications: This layer contains conferencing, customer care, enterprise social software, IP communications, messaging, mobile applications, and TelePresence. ■ Collaboration Services: This layer contains services that support the collaboration applications: presence, location, session management, contact management, client frameworks, tagging, and policy and security management. ■ Infrastructure: This layer is responsible for allowing collaboration anytime, from anywhere, on any device. It includes virtual machines, the network, and storage. **Data Center and Virtualization Architecture:** ■ Unified Management: Features automation, orchestration, and lifecycle management to simplify deployment and operation of physical/bare metal, virtual, and cloud infrastructures. ■ Unified Fabric: This component delivers high-performance data and storage networking to simplify deployment, help ensure quality of experience, and reduce operating costs. Cisco integrated network services provide high-speed connectivity and high-availability, increase application performance, and reduce security risk in multitenant environments.

	■ Unified Computing: This component provides a highly scalable, system-level computing solution that integrates computing, access networking, and storage networking. Embedded management capabilities simplify operations across physical, virtual, and cloud infrastructures.
b	Discuss the PPDIOO phases in details.
Ans:	 **Figure 1-5** *Cisco PPDIOO network lifecycle* Explaination
c	Explain different layers of hierarchical Network design.
Ans:	**Hierarchical Network Design:** ■ The core layer provides fast transport between distribution switches within the enterprise campus. ■ The distribution layer provides policy-based connectivity. ■ The access layer provides workgroup and user access to the network.

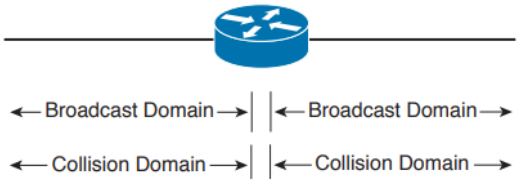
	 **Core Layer:** The core layer is the network's high-speed switching backbone that is crucial to corporate communications. It is also referred as the backbone. **Distribution Layer:** The network's distribution layer is the isolation point between the network's access and core layers. **Access Layer:** The access layer provides user access to local segments on the network. The access layer is characterized by switched LAN segments in a campus environment.
d	What are the different redundancy techniques? Discuss in details.
Ans:	1.Workstation-to-Router Redundancy and LAN High Availability Protocols • Use of HSRP • VRRP • GLBP • VSS 2. Server redundancy • Uses dual-attached NICs, • FEC • GEC port bundles 3. Route redundancy • Provides load balancing and high availability 4. Link redundancy • Uses multiple WAN links that provide primary and secondary failover for higher availability • On LAN • use EtherChannel
e	Explain HSRP, VRRP and GLBP.
Ans:	**HSRP:** The Cisco HSRP provides a way for IP workstations that support only one default router to keep communicating on the internetwork even if their default router becomes unavailable. HSRP works by creating a virtual router that has its own IP and MAC addresses. The workstations use this virtual IP address as their default router.

	HSRP also works for proxy ARP. When an active HSRP router receives an ARP request for a node that is not on the local LAN, the router replies with the phantom router's MAC address instead of its own. If the router that originally sent. **VRRP:** VRRP is a router redundancy protocol defined in RFC 3768. RFC 5768 defined VRRPv3 for both IPv4 and IPv6 networks. VRRP is based on Cisco's HSRP, but is not compatible. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP addresses associated with a virtual router is called the master, and it forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first-hop router by end hosts. The virtual router backup assumes the forwarding responsibility for the virtual router should the master fail. **GLBP:** GLBP protects data traffic from a failed router or circuit, such as HSRP, while allowing packet load sharing between a group of redundant routers. Methods for load balancing with HSRP and VRRP work with small networks, but GLBP allows for first-hop load balancing on larger networks.
f	Explain in details different Network Audit Tools.
Ans:	When performing a network audit, you have three primary sources of information: ■ Existing documentation ■ Existing network management software tools ■ New network auditing tools After gathering the existing documentation, you must obtain access to the existing management software. The client may already have CiscoWorks tools, from which you can obtain hardware models and components and software versions. You can also obtain the existing router and switch configurations. The network audit should provide the following information: ■ Network device list ■ Hardware specifications ■ Software versions ■ Configuration of network devices ■ Auditing tools' output information ■ Interface speeds ■ Link, CPU, and memory utilization ■ WAN technology types and carrier information
2.	Attempt any three of the following:
a	Compare and Contrast between Switches, Routers and Layer 3 switches.
Ans:	**Switches** Switches use specialized integrated circuits to reduce the latency common to regular bridges. Switches are the evolution of bridges. Some switches can run in cut-through mode, where the switch does not wait for the entire frame to enter its buffer; instead, it begins to forward the frame as soon as it finishes reading the destination MAC address.



Routers

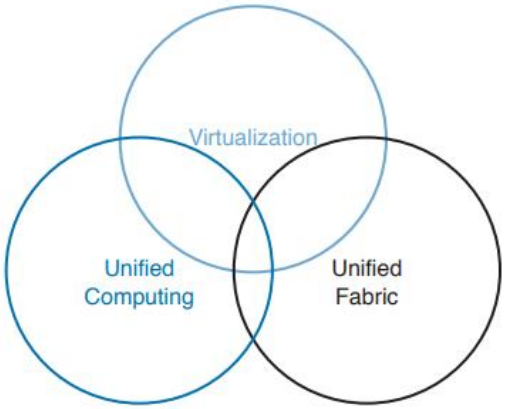
Routers make forwarding decisions based on network layer addresses. When an Ethernet frame enters the router, the Layer 2 header is removed; the router forwards based on the Layer 3 IP address and adds a new Layer 2 address at the egress interface. In addition to controlling collision domains, routers bound data link layer broadcast domains. Each interface of a router is a separate broadcast domain. Routers do not forward data link layer broadcasts. IP defines network layer broadcast domains with a subnet and mask. Routers are aware of the network protocol, which means they can forward packets based on IP layer information.



Layer 3 Switches

LAN switches that can run routing protocols are Layer 3 switches. These switches can run routing protocols and communicate with neighboring routers. They are also referred to as multilayer switches. Layer 3 switches have LAN technology interfaces that perform network layer packet forwarding. The use of switching technologies at the network layer greatly accelerates packet forwarding between connected LANs, including VLANs. You can use the router capacity you save to implement other features, such as security filtering and intrusion detection.

b	What are data center foundation components?
Ans:	**Data Center Foundation Components:**



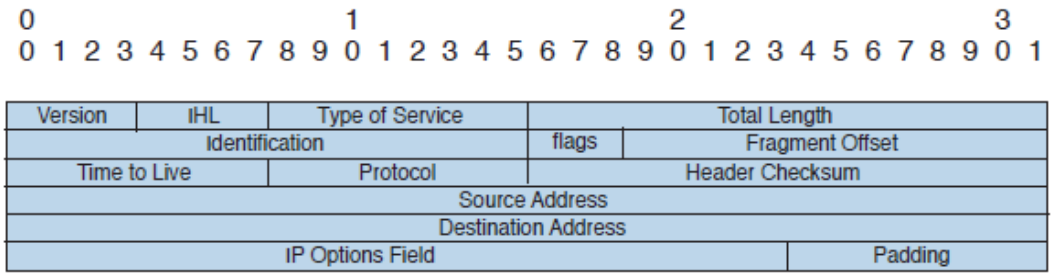
■ Virtualization

	■ Unified fabric ■ Unified computing
c	What are different types of Virtualizations?
Ans:	Enterprise networks consist of two main types of virtualization technology groupings • Network virtualization • Device virtualization ■ **Network virtualization** encompasses logical isolated network segments that share the same physical infrastructure. Each segment operates independently and is logically separate from the other segments. Each network segment appears with its own privacy, security, independent set of policies, QoS levels, and independent routing paths. ■ VLAN: Virtual local area network ■ VSAN: Virtual storage area network ■ VRF: Virtual routing and forwarding ■ VPN: Virtual private network ■ vPC: Virtual Port Channel ■ **Device virtualization** allows for a single physical device to act like multiple copies of itself. Device virtualization enables many logical devices to run independently of each other on the same physical piece of hardware. The software creates virtual hardware that can function just like the physical network device. Another form of device virtualization entails using multiple physical devices to act as one logical unit. ■ Server virtualization: Virtual machines (VM) ■ Virtual Switching System (VSS) ■ Cisco Adaptive Security Appliance (ASA) firewall context ■ Virtual device contexts (VDCs)
d	Explain Spanning Tree Protocol.
Ans:	Spanning Tree Protocol (STP) is defined by IEEE 802.1D. It prevents loops from being formed when switches or bridges are interconnected via multiple paths. STP switch ports enter the following states: ■ **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 links in use fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in the blocking state. It 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, in 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.
e	What is campus LAN Design? What are the Best Practices for the same?

Ans:	LANs can be classified as large-building LANs, campus LANs, or small and remote LANs. The large-building LAN typically contains a major data center with high-speed access and floor communications closets; the large-building LAN is usually the headquarters in larger companies. Campus LANs provide connectivity between buildings on a campus. Redundancy is usually a requirement in large-building and campus LAN deployments. Campus design factors include the following categories: ■ Network application characteristics: Different application types ■ Infrastructure device characteristics: Layer 2 and Layer 3 switching, hierarchy ■ Environmental characteristics: Geography, wiring, distance, space, power, number of nodes **Best Practices:** Access layer: • Limit VLANs to a single closet when possible to provide the most deterministic and highly available topology. • Use RPVST+ if STP is required. It provides the best convergence. • Set trunks to ON and ON with no-negotiate. • Manually prune unused VLANs to avoid broadcast propagation. Distribution layer: • Use Layer 3 links between the distribution and core switches to allow for fast convergence and load balancing. • Build Layer 3 triangles, not squares. • Use the distribution switches to connect Layer 2 VLANs that span multiple access layer switches. Core layer: • Reduce the switch peering by using redundant triangle connections between switches. • Use routing that provides a topology with no spanning-tree loops. • Use two equal-cost paths to every destination network.
f	Discuss different strategies for load Balancing in the Data Center.
Ans:	**Application Load Balancing** Application load balancing is when the application actually performs the load balancing between the tiers of the application stack. For example, with a standard three-tier application that uses Web, Application, and Database tiers, multiple web servers can redirect traffic to the different application servers without the need for network-based load balancing. The web servers themselves would control the load-balancing algorithms that can be used. **Network Load Balancing** ■ Dedicated L4-7 load balancers ■ DNS based ■ Anycast based
3	**Attempt any three of the following.**
a	Write a short note on different WLAN Standards.
Ans:	1. WLAN applications include inside-building access, LAN extension, outside building-tobuilding communications, public access, and small office/home office (SOHO) communications.The first standard for WLANs was IEEE 802.11, approved by the IEEE

	in 1997. The current specification is IEEE 802.11-1999, with many amendments thereafter. 2. In 1999, the 802.11b amendment was introduced, providing an 11Mbps data rate. It provides speeds of 11, 5.5, 2, and 1 Mbps and uses 11 channels of the Industrial, Scientific, and Medical (ISM) frequencies. IEEE 802.11b uses DSSS and is backward compatible with 802.11 systems that use DSSS. 3. The IEEE approved a second standard in 1999. IEEE 802.11a provides a maximum 54Mbps data rate but is incompatible with 802.11b. It provides speeds of 54, 48, 36, 24, 18, 12, 9, and 6 Mbps. IEEE 802.11a uses 13 channels of the Unlicensed National Information Infrastructure (UNII) frequencies and is incompatible with 802.11b and 802.11g. IEEE 802.11a is also known as WiFi5. 4. In 2003, the IEEE 802.11g standard was approved, providing a 54Mbps data rate using the ISM frequencies. The advantage of 802.11g over 802.11a is that it is backward compatible with 802.11b. 5. The second wave for 802.11ac includes the following features: ■ Support for multiuser multiple-input, multiple-output (MU-MIMO) ■ Support for speeds up to 2.34 Gbps ■ 160MHz channel width ■ 256 QAM modulation ■ Four spatial streams ■ PHY rate of 2.34 to 3.47 Gbps
b	Write in details WLAN Controller Components.
Ans:	The CCDA candidate must understand the three major components of WLCs: ■ WLANs ■ Interfaces ■ Ports WLANs are identified by unique SSID network names. The LAN is a logical entity. Each WLAN is assigned to an interface in the WLC. Each WLAN is configured with radio policies, quality of service (QoS), and other WLAN parameters. A WLC interface is a logical connection that maps to a VLAN on the wired network. Each interface is configured with a unique IP address, default gateways, physical ports, VLAN tag, and DHCP server. The port is a physical connection to the neighboring switch or router. By default, each port is an IEEE 802.1Q trunk port. There may be multiple ports on a WLC into a single port channel interface. These ports can be aggregated using link aggregation (LAG). Some WLCs have a service port that is used for out-of-band management.
c	Write a Short notes on 1) Frame Relay 2) Metro Ethernet
Ans:	**1) Frame Relay** Frame Relay is a packet-switched connection-oriented Layer 2 WAN protocol. Frame Relay is an industry standard networking protocol that uses virtual circuits between connected devices. The data link layer in Frame Relay establishes connections using a DTE device such as a router and a DCE device such as a frame switch. Frame Relay circuits between sites can be either permanent virtual circuits (PVCs) or Switched virtual circuits (SVCs). PVCs are used more predominantly because of the connections' permanent nature. SVCs, on the other hand, are temporary connections created for each data transfer session.

	A point-to-point PVC between two routers or endpoints uses a data-link connection identifier (DLCI) to identify the local end of the PVC. The DLCI is a locally significant numeric value that can be reused throughout the Frame Relay WAN if necessary. **2) Metro Ethernet** Metro Ethernet uses well-known "Ethernet" to deliver low-cost and high-speed MAN/ WAN connectivity for organizations. Many service providers now offer Metro Ethernet solutions to deliver a wide range of converged network services such as data, voice, and video on the same wire. Metro Ethernet provides enterprise LAN type functionality out in the MAN and WAN, increasing the throughput available for applications. Metro Ethernet bandwidths can range from 100 Mbps to 10 Gbps, and even higher in some cases, allowing for support for higher performance and increased QoS requirements. In contrast to the rigid nature of traditional TDM provisioning, metro Ethernet services are much easier to deploy and scale due to the flexible bandwidth increments. Metro Ethernet technology is appealing to many customers because they are already comfortable using Ethernet throughout their LAN environments.
d	Discuss WAN and Edge design Methodologies.
Ans:	The Plan, Build, and Manage methodology should be used when designing enterprise edge networks. Some keys to PBM are the processes of identifying business and technology strategies, assessing the existing network, and creating a design that is scalable, flexible, and resilient: ■ Identifying the network requirements includes reviewing the types of applications, the traffic volume, and the traffic patterns in the network. ■ Assessing the existing network reviews the technologies used and the locations of hosts, servers, network equipment, and other end nodes. ■ Designing the topology is based on the availability of technology as well as the projected traffic patterns, technology performance, constraints, and reliability. When designing the WAN topology, remember that the design should describe the functions that the enterprise modules should perform. The expected service levels provided by each WAN technology should be explained. WAN connections can be characterized by the cost of renting the transmission media from the service provider to connect two or more sites together. New network designs should be flexible and adaptable to future technologies and should not limit the customer's options going forward. Voice over IP and video are examples of technologies that network designs should be able to support if the customer decides to move to a converged network. The customer should not have to undergo major hardware upgrades to implement these types of technologies. In addition, the ongoing support and management of the network is another important factor, along with the design's cost effectiveness.
e	What are the different methodologies for Optimizing Bandwidth Using QoS? Explain.
Ans:	1. Queuing, Traffic Shaping, and Policing 2. Classification

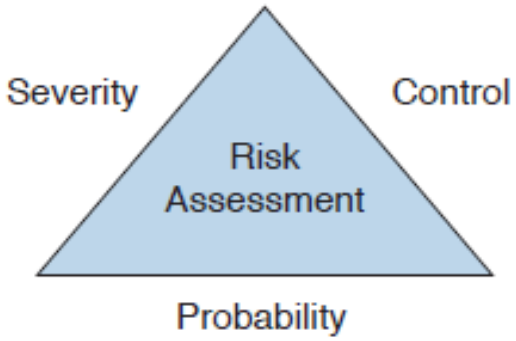
	3. Congestion Management 4. Priority Queuing 5. Custom Queuing 6. Weighted Fair Queuing 7. Class-Based Weighted Fair Queuing 8. Low-Latency Queuing 9. Traffic Shaping and Policing 10. Link Efficiency 11. Window Size
f	Explain various DMZ Connectivity implementation techniques?
Ans:	DMZ types include the following: ■ **Internet DMZ:** These types of DMZs provide Internet-facing services such as web, email, DNS, and e-commerce services for corporate users and/or customers. ■ **Remote access VPN DMZ:** DMZ for network access by corporate users via SSL or IPsec VPN sessions. ■ **Site-to-site VPN DMZ:** DMZ for remote site or branch office connectivity via IPsec VPN tunnels as an alternative to private network WAN service. ■ **Cloud services DMZ:** DMZ to connect to public cloud services such as Amazon Web Services (AWS) or Microsoft Azure via encrypted tunnels. ■ **Unified communications DMZ:** DMZ to host UC services such as voice and video over the Internet. ■ **Security services DMZ:** Security-based DMZ for services such as web application firewalls (WAPs), intrusion prevention services (IPSs), email, and URL filtering services.
4	Attempt any three of the following:
a	Explain IPV4 header structure.
Ans:	 **Version:** This field is 4 bits in length. It indicates the IP header's format, based on the version number. Version 4 is the current version; therefore, this field is set to 0100 (4 in binary) for IPv4 packets. This field is set to 0110 (6 in binary) in IPv6 networks. **IHL (Internet Header Length):** This field is 4 bits in length. It indicates the length of the header in 32-bit words (4 bytes) so that the beginning of the data can be found in the IP header. The minimum value for a valid header (five 32-bit words) is 5 (0101). **ToS (Type of Service):** This field is 8 bits in length. Quality of service (QoS) parameters such as IP precedence or DSCP are found in this field. **Total Length:** This field is 16 bits in length. It represents the length of the datagram or packet in bytes, including the header and data. **Identification:** This field is 16 bits in length. It identifies fragments for reassembly.

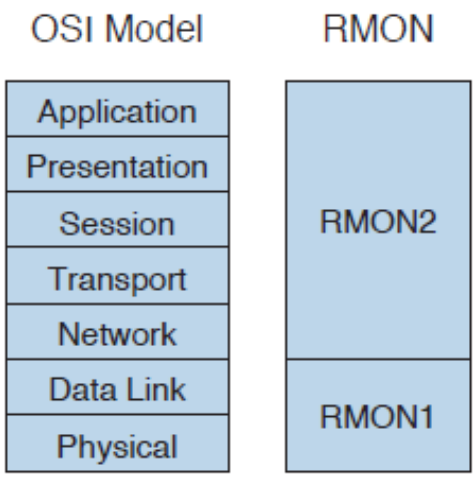
	Flags: This field is 3 bits in length. It indicates whether the packet can be fragmented and whether more fragments follow. **Fragment Offset:** This field is 13 bits in length. It indicates (in bytes) where in the packet this fragment belongs. The first fragment has an offset of 0.
b	Write short notes on 1) BOOTP 2) DHCP
Ans:	1) **BOOTP** The basic BOOTP was first defined in RFC 951. It has been updated by RFC 1497 and RFC 1542. It is a protocol that allows a booting host to configure itself by dynamically obtaining its IP address, IP gateway, and other information from a remote server. You can use a single server to centrally manage numerous network hosts without having to configure each host independently. BOOTP is an application layer protocol that uses UDP/IP for transport. The BOOTP server port is UDP port 67. The client port is UDP port 68. Clients send BOOTP requests to the BOOTP server, and the server responds to UDP port 68 to send messages to the client. The destination IP of the BOOTP requests uses the all-hosts address (255.255.255.255), which the router does not forward. If the BOOTP server is one or more router hops from the subnet, you must configure the local default gateway router to forward the BOOTP requests. **2) DHCP** DHCP provides a way to dynamically configure hosts on the network. Based on BOOTP, it is defined in RFC 2131 and adds the capability to reuse network addresses and additional configuration options. DHCP improves on BOOTP by using a "lease" for IP addresses and providing the client with all the IP configuration parameters needed to operate in the network. DHCP has three address allocation mechanisms: ■ **Manual:** In manual allocation, DHCP is used to dispatch a preallocated IP address to a specific MAC address. ■ **Automatic:** For automatic allocation, IP addresses are permanently assigned to a host.The IP address does not expire. ■ **Dynamic:** For dynamic allocation, IP addresses are assigned for a limited time or until the host explicitly releases the address. This dynamic allocation mechanism can reuse the IP address after the lease expires.
c	Explain IPV6 Unicast Address, Anycast Address and Multicast Address.
Ans:	**IPv6 Unicast Address** The IPv6 unicast (one-to-one) address is the logical identifier of a single-host interface. With a unicast address, a single source sends to a single destination. It is similar to IPv4 unicast addresses. Unicast addresses are divided into: ■ Global unicast address ■ Link-local address ■ Unique local address Global Unicast Addresses IPv6 global addresses connect to the public network. These unicast addresses are globally unique and routable. This address format is initially defined in RFC 2374. RFC 3587 provides updates to the format. Link-Local Addresses

	IPv6 link-local addresses are significant only to nodes on a single link. Routers do not forward packets with a link-local source or destination address beyond the local link. Linklocal addresses are identified by leading FE8 hexadecimal numbers. Link-local addresses are configured automatically or manually. Unique Local IPv6 Address RFC 4193 defines the unique local address. Unique local addresses designed for use in local networks and are not routable in the Internet. It substitutes the deprecated site-local addresses. As shown in Figure 9-4, the format of the unique local address is an FP of 1111 110 (FC00::/7) followed by global ID, followed by the subnet ID and then the 64-bit interface identifier (ID). **IPv6 Anycast Addresses** The IPv6 *anycast* (one-to-nearest) address identifies a set of devices. An anycast address is allocated from a set of unicast addresses. These destination devices should share common characteristics and are explicitly configured for anycast. You can use the anycast address to identify a set of routers or servers within an area. When a packet is sent to the anycast address, it is delivered to the nearest device as determined by the routing protocol. An example of the use of anycast addresses is to assign an anycast address to a set of servers—one in North America and the other in Europe. Users in North America would be routed to the North American server, and those in Europe to the European server. **IPv6 Multicast Addresses** The IPv6 *multicast* (one-to-many) address identifies a set of hosts. The packet is delivered to all the hosts identified by that address. This type is similar to IPv4 multicast (Class D) addresses. IPv6 multicast addresses also supersede the broadcast function of IPv4 broadcasts.You use an "all-nodes" multicast address instead. One additional function of IPv6 multicast is to provide the IPv4 broadcast equivalent with the all-nodes multicast group.
d	Discuss IPV6 Address-Assignment Strategies
Ans:	Assignment of IPv6 addresses to a host can be statically or dynamically configured. Static IPv6 address assignment just involves manual configuration on the host's configuration files .Dynamic IPv6 address assignment can be done via stateless or stateful methods. The stateless method may result in a link-local or globally unique address. The three methods to assign IPv6 addresses are: ■ Manual configuration ■ Stateless address autoconfiguration (SLAAC) ■ Stateful configuration with DHCPv6 Manual Configuration As with IPv4, devices such as routers, switches, servers, and firewalls should be configured with their IPv6 addresses manually. SLAAC of Link-Local Address The dynamic configuration of link-local IPv6 addresses is a stateless autoconfiguration method, without DHCP. Hosts obtain their link-local addresses automatically as an

	interface is initialized. First, the host performs a duplicate address-detection process. The host joins the all-nodes multicast group to receive neighbor advertisements from other nodes. SLAAC of Globally Unique IPv6 Address RFC 4862 describes IPv6 stateless address autoconfiguration. With autoconfiguration of globally unique IP addresses, IPv6 hosts can use SLAAC, without DHCP, to acquire their own IP address information.
e	What are the techniques for IPV4-to-IPV6 Transition Mechanisms?
Ans:	This section describes transition mechanisms and deployment models to migrate from IPv4 to IPv6. During a transition time, both protocols can coexist in the network. The three major transition mechanisms are: ■ **Dual-stack**: IPv4 and IPv6 coexist in hosts and networks. ■ **Tunneling**: IPv6 packets are encapsulated into IPv4 packets. ■ **Translation**: IPv6 packets are translated to IPv4 packets.
f	What are routing Protocol Metrics and Loop Prevention techniques?
Ans:	Routing protocols use a metric to determine best routes to a destination. Some routing protocols use a combination of metrics to build a composite metric for best path selection. This section describes metrics and also covers routing loop-prevention techniques. You must understand each metric for the CCDA exam. Some routing metric parameters are: ■ Hop count ■ Bandwidth ■ Cost ■ Load ■ Delay ■ Reliability ■ Maximum transmission unit (MTU)
5	**Attempt any three of the following:**
a.	What are different Network security threats?

Ans:	Security threats can be classified into the following categories: ■ **Reconnaissance:** The goal of reconnaissance is to gather as much information as possible about the target host/network. Generally, this type of information gathering is done before an attack is carried out. ■ **Unauthorized access:** Refers to the act of attacking or exploiting the target system or host. Operating systems, services, and physical access to the target host have known system vulnerabilities that the attacker can take advantage of and use to increase his or her privileges. ■ **Service disruption:** Attacks aimed at disrupting normal infrastructure services. ■ **Denial of service (DoS) attacks:** DoS attacks aim to overwhelm resources such as memory, CPU, and bandwidth that impact the target system and deny legitimate user's access. ■ **Adware :** Automatic ads used to generate revenue for the hackers that are seeking monetary gains. ■ **Malware:** Hostile software used to gain access, gather information, or disrupt normal operations. ■ **Spyware:** Software that is used to obtain covert information secretly. ■ **Disclosure and modification of data :** As data is in transit, an attacker can use packetsniffing tools to read data on the wire while it is in flight. ■ **Network abuse:** The network can be abused from peer-to-peer file sharing, out-of-policy network browsing, and access to forbidden content on the network. ■ **Data leaks:** The loss of data from servers or users' workstations while in transit or at rest.To prevent loss of data, data loss prevention (DLP) software can help to control what data users can transfer. ■ **Identity theft and fraud :** Would-be attackers use phishing techniques such as email spam to gather personal information such as usernames, passwords, and credit card accounts by posing as a person who can be trusted.
b	Explain Security Risks.
Ans:	To protect network resources, processes, and procedures, technology needs to address several security risks. Important network characteristics that can be at risk from security threats include system availability, data integrity, and data confidentiality: ■ **System availability** should ensure uninterrupted access to critical network and computing resources to prevent service disruption and loss of productivity. ■ **Data integrity** should ensure that only authorized users can change critical information and guarantee the authenticity of data. ■ **Data confidentiality** should ensure that only legitimate users can view sensitive information to prevent theft, legal liabilities, and damage to the organization.
c	Write short note on Risk assessment.

Ans:	Within network security, proper risk management is a technique used to lower risks to within acceptable levels. A well thought-out plan for network security design implements the components that are part of the security policy. The security policies that an organization employs use risk assessments and cost-benefit analysis to reduce security risks.  Risk assessments should explain the following: ■ What assets to secure ■ The monetary value of the assets ■ The actual loss that would result from an attack ■ The severity and the probability that an attack against the assets will occur ■ How to use security policy to control or minimize the risks
d	Write short notes on 1) RMON 2) NetFlow
Ans:	**1) RMON** RMON is a standard monitoring specification that enables network monitoring devices and console systems to exchange network monitoring data. RMON provides more information than SNMP, but more sophisticated data collection devices (network probes) are needed. RMON looks at MAC-layer data and provides aggregate information on the statistics and LAN traffic. Enterprise networks deploy network probes on several network segments; these probes report back to the RMON console. RMON allows network statistics to be collected even if a failure occurs between the probe and the RMON console. RMON2



2) NetFlow

Cisco NetFlow allows the tracking of IP flows as they are passed through routers and multilayer switches. An IP flow is a set of IP packets within a specific timeslot that share a number of properties, such as the same source address, destination address, type of service, and protocol number. NetFlow information is forwarded to a network data analyzer, network planning tools, RMON applications, or accounting and billing applications. NetFlow allows for network planning, traffic engineering, usage-based network billing, accounting, Denial of Service monitoring capabilities, and application monitoring.

■ **NetFlow accounting:** Collects IP data flows entering router or switch interfaces and prepares data for export. It enables the accumulation of data on flows with unique characteristics, such as IP addresses, application, and class of service (CoS).

■ **Flow collector engines:** Captures exported data from multiple routers and filters and aggregates the data according to customer policies, and then stores this summarized or aggregated data. Examples of collectors are Cisco NetFlow Collector, SolarWinds, and CA NetQoS.

■ **Network data analyzers:** Displays a graphical user interface (GUI) and analyzes NetFlow data collected from flow collector files. This allows users to complete near-real-time visualization or trending analysis of recorded and aggregated flow data. Users can specify the router and aggregation scheme and the desired time interval.

e.	What are the techniques for Detecting and Mitigation Threats?
Ans:	solutions include the following: ■ **Endpoint protection:** Viruses and worms can create havoc by propagating infections from host to host throughout the network. Antivirus services can help hosts detect and remove infections based on known virus pattern markings. ■ **Application security and content security defense:** Several new application layer network products have been released that help address new classes of threats, such as spam, phishing, spyware, packet abuse, and unauthorized point-to-point file sharing. Content security products such as Cisco WSA Appliances provide comprehensive antivirus, antispyware, file-blocking, antispam, URL blocking, and content-filtering services.

	Infection containment: The Cisco ASA, ASA Services Module, and IOS firewalls protect the network by creating security zones that partition the network into separate segments. The firewall services provide perimeter network security but do not eliminate the need for continuous network monitoring. ■ **Inline IPS:** Cisco has innovated in the area of IPS by being the first to incorporate IPS into the IOS on routing and switching platforms. In addition, IPS solutions have inline filtering features that can remove unwanted traffic with programmable features that classify traffic patterns.
f	Compare and contrast IPS and IDS.
Ans:	Intrusion prevention and intrusion detection systems are network security devices that proactively identify and block security threats. Today's security threats are far too complex to be secured by a single security device. Although security techniques such as access control, firewall services, and device hardening help secure the network from attacks, they cannot provide adequate protections from fast moving malware or zero-day attacks. Intrusion prevention systems are classified into two categories: ■ **Intrusion detection systems (IDSs)** are passive devices that monitor traffic and generate alerts or logs when suspicious traffic is detected from attacks such as reconnaissance or DoS attacks. Since IDS devices are only analyzing traffic flows, there is no impact at all to network performance. ■ **Intrusion prevention systems (IPSs)** are active devices that not only can detect but also block malicious traffic from coming into the network. For the IPS to actually block traffic, it has to be deployed in inline mode, where traffic is forced through the IPS. That way, the IPS can detect and prevent suspicious traffic in real time from accessing the internal network. IPS/IDS technologies are commonly deployed as sensors, and they are available in many options. IPS sensors can be deployed on dedicated hardware appliances or using IPS software on routers, switches, or firewall modules. Both IPS and IDS technologies need to be able to detect malicious traffic, which has unique characteristics identified through the use of signatures.