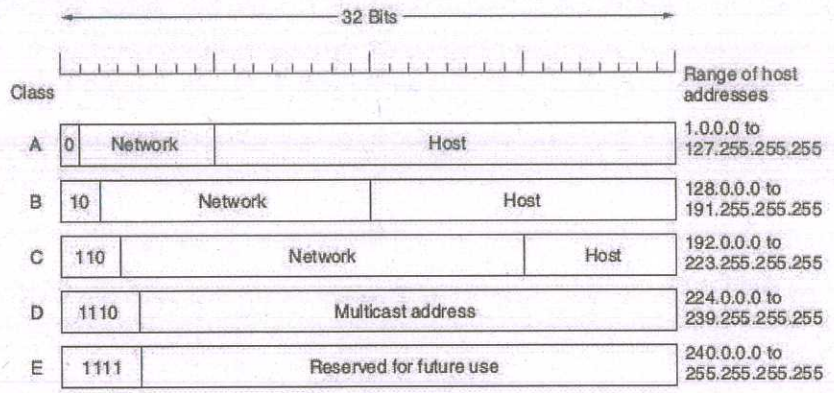
Scoring Indicators

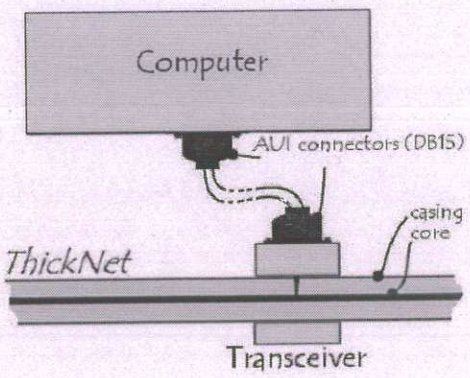
Code: 6135 (15), Network Infrastructure Management **Version: A**

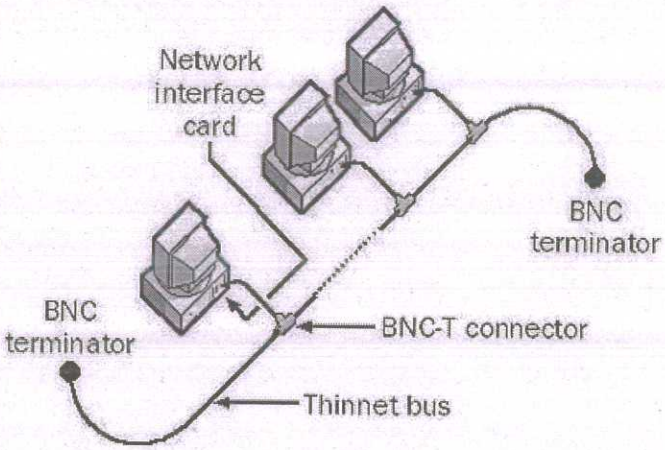
Qn. No.	Scoring Indicators	Split Up score	Sub Total	Total Score
	Part A			
I (1)	Physical layer device that amplifies the transmission signal between two cable segments.	2	2	10
I (2)	A special address block 169.254.x.x is used as link local addresses which is obtained to a system when IP functionality fails (eg: DHCP failure). Microsoft termed this addressing as Automatic Private IP Addressing (APIPA).	2	2	
I (3)	1. Read Only Memory (ROM) 2. Flash memory 3. Non-volatile random access memory (NVRAM) 4. Dynamic random access memory (DRAM)	0.5x4	2	
I (4)	Different parts of a network may use different dynamic routing protocols. Redistribution helps to announce each other's routing information.	2	2	
I (5)	An AS is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS and using an exterior gateway protocol to route packets to other autonomous systems.	2	2	
	Part B			
II (1)	Layer 3 device. Works at Network layer, data link layer and physical layer. Connects two or more different networks. Reads the IP address in the packet and with the help of routing tables, forwards the packet to the destination. May have different types of physical layer connections such as copper cables, fiber optic, or wireless transmission, and can support different network layer standards.	6	6	42

	Working of routers rely on routable protocols and routing protocols. Routable protocols: To identify the systems and binding. Eg:TCP/IP. Routing Protocol: To communicate with other routers and to know the routes. Eg: DV, LS.			
II (2)	 Explanation of each with the number of networks and hosts.	3 3	6	
II (3)	Dynamic Host Configuration Protocol (DHCP) is used to dynamically (automatically) assign TCP/IP configuration parameters to network devices (IP address, Subnet Mask, Default Gateway, DNS server etc). The Dynamic Host Configuration Protocol (DHCP) client TCP/IP software is not configured with a static IP address and it is configured to obtain an IP address dynamically from a Dynamic Host Configuration Protocol (DHCP) Server. When a DHCP client device boots up, it not capable send and receive network traffic, because TCP/IP is not configured. But it can participate in broadcast traffic. DHCP Clients and DHCP Servers uses limited broadcast messages (address 255.255.255.255) to communicate with each other. The scope of a broadcast message is only within the local broadcast domain and cannot cross the gateway router. There are four types of messages in a DHCP address assignment. Those are collectively called DORA. 1. DISCOVER: When a DHCP client boots up, it will have the IP address 0.0.0.0 and it will broadcast a DISCOVER message.	3 3	6	

	2. OFFER: When received the DISCOVER message the server broadcast an OFFER message containing an IP address. 3. REQUEST: If the OFFERed IP address can be used, the client broadcast a REQUEST message requesting to use the OFFERed address. 4. ACK: The server broadcasts an ACK message to indicate that the offered IP can be used by the client.			
II (4)	<copy> command is used to copy configuration files on and off the router's NVRAM, DRAM, and flash file systems. The <copy> command is used with the syntax <copy> <from> <to>. The common use of <copy> command is to store/load running/startup configurations. Use: *Router#copy running-config startup-config* The <copy /erase> command is introduced in IOS version 12.x, and when used in conjunction with the [null] file system will erase a memory partition. For example, to erase NVRAM, *Router#copy /erase null: nvram:startup-config* command is used. The following can be used as the from/to locations. flash: Copy from/to flash: file system ftp: Copy from/to ftp: file system running-config Copy from/to current system configuration startup-config Copy from/to startup configuration tftp: Copy from/to tftp: file system	4 2	6	
II (5)	Router's clock can be set either <u>manually</u> each time the router reboots, or by using the <u>Network Time Protocol (NTP)</u>. Most routers when boot up the clock will be set to March 1, 1993. <u>Manual method</u>: The IOS uses Universal Time Coordinated (UTC). Hence offset must be provided to make it for different locale. To set the time zone, use the global configuration command <clock timezone> *Syntax: clock timezone zone hours-offset [minutes-offset]* *Eg: Router(config)#clock timezone I 5 30* (I for India, 5:30 hrs ahead of UTC)	3	6	

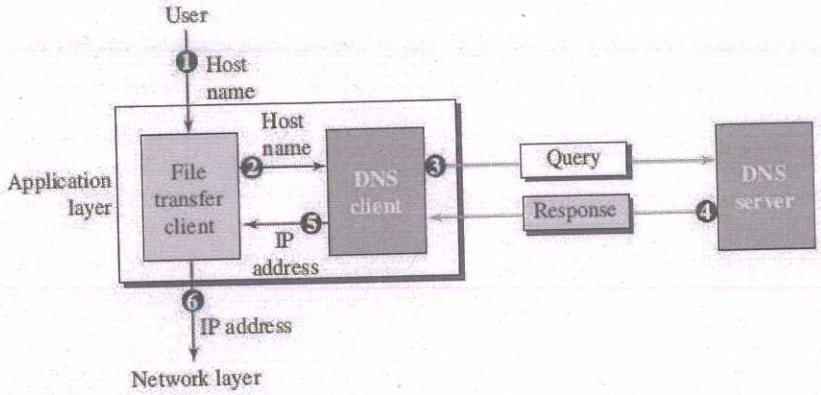
	To set the router's system clock, use the privileged EXEC command <clock set>. The convention is *hour:min:second day month year* *Eg: Router#clock set 14:00:15 29 Jan 2019* NTP: Automatic time update can be done using NTP (Network Time Protocol). IOS provides the facility for the router to act as an NTP client, an NTP server, or an NTP peer. As an NTP client, the router contacts the defined NTP server, then verifies and synchronizes its system clock. The commands are; *router(config)#ntp server 128.4.1.1* *router(config)#interface FastEthernet1/0* *router(config-if)#ntp broadcast client* *Router#show ntp status* is used to check whether NTP is working correctly or not.	3		
II (6)	1. Physical infrastructure, interconnection cabling and patch panel design, installation and management, end-station patching and network hardware installation. Cable testing and length validation also fall into this category. 2. Device configuration, bridge, router, switch, and repeater configuration. Backup, archiving, and documenting device configurations. Creating and updating network topology maps, showing device relationships, installation location, and other basic configuration information (IP address, device type, manufacture, and so on). Proper network documentation is essential when diagnosing network problems and performing performance testing. 3. Link and services monitoring, network performance baselining, and periodic performance revaluation. Proactive and reactive hardware, link and network service failure detection. Network security monitoring.	2 2 2	6	
II (7)	1) Better reliability: OSPF routers construct their own routing table describing network reachability from their perspective form within	6x1 mark	6	

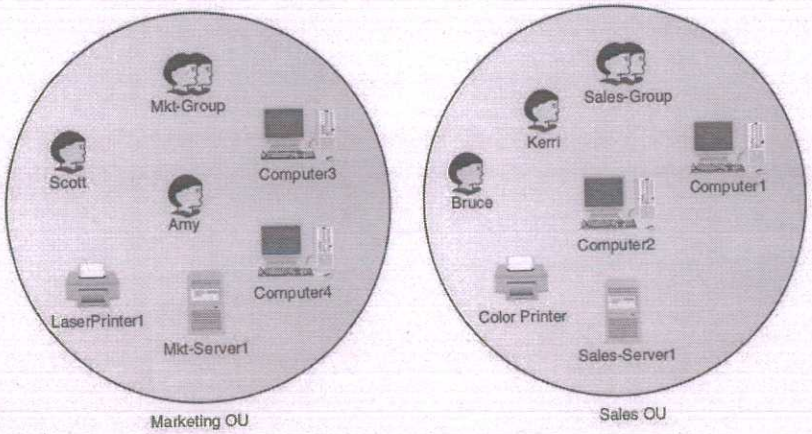
	the network. All network routes are stored in the topological or link state database, where they can be retrieved quickly in the event that a routing change must be made. 2) Fast convergence: After the network has converged and all the routers have constructed their own routing tables and network maps, updates are sent out only when changes in the network topology occur. When changes occur, they are flooded. 3) Unlimited network size: Operate in both large and small-scale networks. 4) VLSM support 5) Type of Service routing: Supports Layer 4 Quality of Service routing which was not in Routing Information Protocols. 6) Low bandwidth usage: OSPF uses multicast instead of local network broadcasts. 7) Dynamic load balancing and route selection: In OSPF, route desirability is based on link speed. Hence load balancing and fault tolerance is easy.			
	Part C			
III (a)	**Thicknet connectors** Use vampire taps for connection. The tap is connected to an external transceiver that in turn has a 15-pin AUI (Attachment Unit Interface) connector which attach a cable that connects to the station.  **Thinnet connectors**	2 2	8	15

	Use different types of BNC (Bayonet Neill-Concelman) - T connectors. The transceiver is on the network card. Uses BNC terminators to avoid signal bouncing.  	2 2		
III (b)	WiMAX: Worldwide Interoperability for Microwave Access. It is a part of IEEE 802.16 standard (Wireless MAN). The WiMAX standard has the advantage of allowing wireless connections between a *base transceiver station* (BTS) and thousands of subscribers without requiring that they be in a direct line of sight (LOS) with that station. Devices that provide connectivity to a WiMAX network are known as subscriber stations (SS). The term *point-multipoint link* is used for WiMAX's method of communication. Two types of WiMax: Fixed WiMAX (802.16-2004): Provides for a fixed-line connection with an antenna mounted on a rooftop, like a TV antenna. It provides a speed of 75 Mbps and has a range of 10km. Mobile WiMAX (802.16e): Here the clients are mobile devices. It has a speed of 30Mbps and a range of 3.5km	1 3 1 1	6	
IV (a)	1. Coaxial Cable (Coax) Copper is used in this as centre conductor which can be a solid wire or a stranded one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both. Specified by Radio Guide (RG) system. For networking RG-8			

	(thicknet) and RG-58A/U (thinnet) are used. Thicknet was thicker, costly, less flexible, had a maximum segment distance of 500m and was used primarily for network backbones. Thinnet was thinner, less costly, flexible, had a maximum segment distance of 185m and was more often used in a conventional physical bus. 2. Twisted Pair Cable A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together to reduce crosstalk. A cable may have 2 to 4 pair of conductors. The cable can be Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP). STP has an extra layer of braided foil shielding surrounding the wires to decrease electrical interference. UTP is the most common type of telecommunication medium when compared with STP and other forms of cables. TP cables use RJ-11 and RJ-45 connectors. 3. Fibre Optic Cable A fibre-optic cable is made of glass or plastic and transmits signals in the form of light by using the principle of total internal reflection. Electrical signals are converted to light pulses, transmit them over the fibre and converted back to electricals signals at the receiver with the help of media converters. it is immune to electrical interference and to wiretapping. There are two modes of propagating light: **Single mode** (a single source of light, hence longer distance) and **multi mode** (a number of beams in different angles, hence used for shorter distance).	3 3 3	9	15
IV (b)	Wi-Fi (Wireless Fidelity) is a family of radio technologies that is commonly used for the wireless local area networking (WLAN) of devices which is based around the IEEE 802.11 family of standards. All components that can connect into a wireless medium in a network are referred to as stations (STA). All stations are equipped with wireless network interface controllers (WNICs). Wireless stations fall into two categories: wireless access points, and clients. Access points (APs), normally wireless routers, are base stations for the wireless network. Compatible devices can connect to each other through a wireless access point and if it has	6	6	

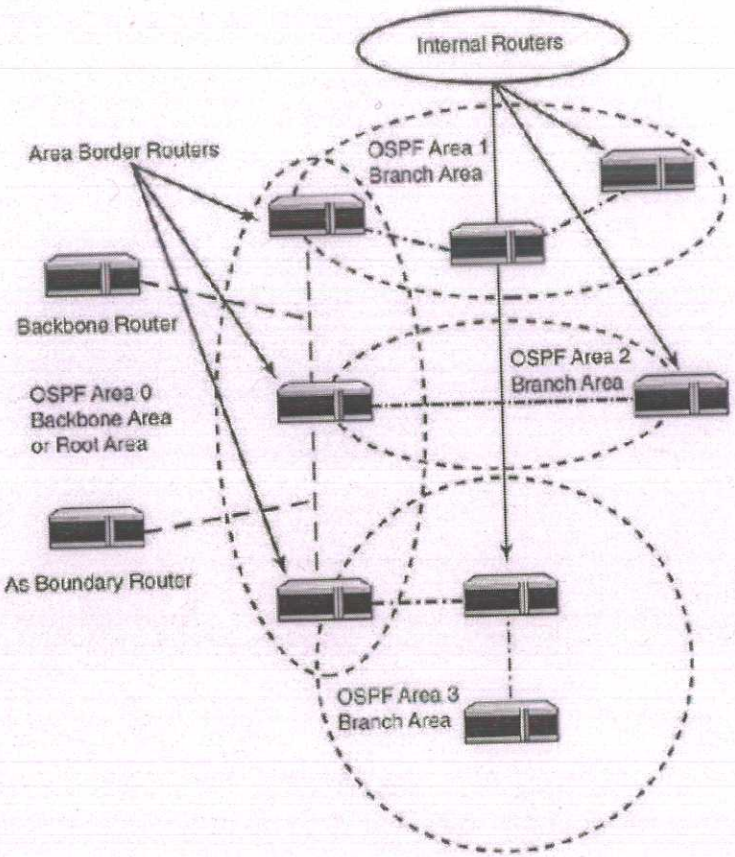
	an internet connectivity the devices can access the Internet too. Wi-Fi most commonly uses the 2.4 gigahertz and 5 gigahertz ISM radio bands. The basic service set (BSS) is a set of all stations that can communicate with each other. The access points of many BSSs connect to form an extended service set (ESS). Wireless Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and WPA2 are commonly used for securing Wi-Fi networks.			
V (a)	Active Directory group is a collection of Active Directory objects including users, computers, other groups and other AD objects. The administrator manages the group as a single object. A group object helps when the same permissions and rights are to be given to a number of users. When a user is moved away from a group, the user loses all rights and permissions assigned to that group. There are two **types** of groups in Active Directory: 1. Security groups: This type of group is used to provide access to resources. For example, when you want to grant a specific group access to files on a shared folder, a security group is used. 2. Distribution groups: This type of group is used to create email distribution lists (usually used in Exchange Servers). An e-mail sent to such a group will reach all users in the group. For each type of group, there are three group **scopes**: 1. Domain local. Used to manage access permissions to resources (files, folders and other types of resources) only in the domain where it was created. 2. Global. This is the default scope. This group type can be used to provide access to resources in the another domain. In this group, you can add only accounts from the same domain in which the group was created. 3. Universal. It is recommended to use it in big Active Directory forests. Using this group scope, you can define roles and manage resources that are distributed across multiple domains.	3 2 3	8	15
V (b)	Machines can understand only IP (numeric) address while people can remember only names. Hence IP addresses are mapped to some names and the whole such information in the network are	4		

	distributed all over the Internet. Any host that needs the mapping from names to IP address can contact the nearby computer that holds this information. This method is called the DOMAIN NAME SYSTEM (DNS) and the computer that holds such mapping information is called a DNS server. The DNS client sends the name to the DNS server which returns the corresponding IP address. The DNS namespace is a collection of names and addresses; both are unique. The names follows a hierarchical order separated by dots.		7	
		3		
VI (a)	With Remote Desktop Connection (or Remote Desktop - RD), it is possible connect to a computer running Windows from another computer running Windows that's connected to the same network or to the Internet. In servers, it helps the administrator to manage the server using his own computer, without going to server room. RD works using Remote Desktop Protocol (RDP). We can use all of the programs, files, and network resources of the remote computer using our home computer, just like sitting in front of the remote one.	4	8	15
	To connect to a remote computer; • That computer must be turned on. • It must have a network connection. • Remote Desktop must be enabled. • Remote Desktop connections are allowed through its firewall. • We must have network access to the remote computer • We must have permission to connect.	4		

VI (b)	OU is an Active Directory container used to organize a network's users and resources into logical administrative units. Contains Active Directory objects, such as user accounts, groups, computer accounts, printers, shared folders, applications, servers, and domain controllers. For example, a corporation might create an OU for each department. OUs can be nested as many levels as necessary. OUs can represent policy boundaries, in which different sets of policies can be applied to objects. A common purpose is delegation of control by the administrator.  	4 3	7	
VII (a)	When a new router is switched on, there will be nothing in the NVRAM and hence ask the user whether to enter the Initial Configuration Mode (yes/no). 'Yes' will help to make a limited configuration and 'No' will enter directly into EXEC mode. User can view the Interfaces (type, slot, and port Information) in the Privileged EXEC mode by; *Router#show ip interface brief* User can set the interfaces at Configuration EXEC mode. To set a local password to control access to various privilege levels, use the enable password command in global configuration mode. To remove the password requirement, use the no form of this command. *enable password abcde* But since this password is stored as plain text in memory, *enable secret* can be used which stores the password in encrypted form. We can set the router name by,	9	9	15

	Router(config)# hostname ABCD *ABCD(config)#* If there is are DNS servers, they can be specified by the command <ip name-server [ip address of the DNS server]> *Router(config)# ip name-server 192.168.12.2* From configuration EXEC mode, it is possible to enter interface modes where interface parameters such as IP addresses can be set for each interface. Router(config)# interface fastethernet 0 Router(config-if)# ip address 192.1.12.51 255.255.255.0 Router(config-if)# no shutdown Static routing tables and dynamic routing tables (RIP - Routing Information Protocol) are stated in Configuration EXEC mode. <u>Static routing syntax:</u> Router(config)# <ip route> <to_network> <to_network_mask> <through_interface_ip> Eg: Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2 <u>Dynamic routing:</u> Eg: Router(config)#router rip Router(config-router)#version 2 Router(config-router)#network 192.168.1.1 <show ip route> command at user or privileged mode will show the routing table.			
VII (b)	To use Syslog logging (trap logging), a syslog server must be defined in the network. Let it be 192.168.1.20 To enable trap logging, the following command is used. *Router(config)#logging 192.168.0.2* Each message has a facility level and severity level associated with it. Based on the severity value, a syslog-defined action can be done. This can be defined in the conf file. The actions are; 1) Log to a file (/usr/log/<filename>) 2) Forward the message to another syslog process on another host (@hostname or @ip address)	3 3	6	

	3) Write the message to a specified user's operator window. (user,username) 4) Write the message to all users' operator windows (*).			
VIII (a)	The easiest method for router IOS upgrading is through TFTP (Trivial File Transfer Protocol). For this, TFTP server must be in the same local network. The new IOS image has to be kept in the TFTP server. Problems occur if the new IOS image is corrupt or any improper IOS version for the model. On RFF (Read From Flash) routers, since the router boots with the flash in read-only mode, the IOS cannot be altered as such. Here to upgrade IOS, the router must be configured to boot from TFTP server. On RFR (Read From RAM) routers, the router's flash is in read/write mode all the time because the IOS is loaded into DRAM at boot. Here the IOS can be upgraded while the router is in operation. For RFF or RFR routers, TFTP booting is the best option to upgrade IOS, just like installing linux in PC after booting in to live linux environment. By default, the IOS uses the first IOS image it finds on the flash filesystem. If TFTP boot is needed, use the command <boot system tftp [IOS_filename] [tftp_server_IP_address]>, and then reboot the router. After the router is up again, the new IOS can be loaded to the flash memory using the <copy> privileged EXEC command: *Router#copy tftp flash*	9	9	15
VIII (b)	Log information is simply status data, such as changes in the router's interface status, modifications to running configuration, and debugging output. It is less useful when everything is smooth. But valuable when a problem comes up. IOS provides four methods for viewing logging information: 1) Console: The router's console port. 2) Monitor: The router's system monitor, a VTY "console" message display. 3) Trap (Syslog logging): Output to a remote syslog server. 4) Buffer: A place to store a list of logging events in the router's DRAM.	2 2	6	

	Messages will have the common format given below. *[seq no:timestamp:] %facility-severity-MNEMONIC:description* IOS uses the syslog level classification to define the severity of logging messages from 0 to 7. Eg: 0 means Emergency, ie System is unusable. 5 means Notifications, ie Normal but significant conditions.	2		
IX (a)	Backbone routers: Maintain complete routing information for all the areas (or domains) that are connected to the backbone. Area border routers: Connect two or more areas (inter-area routing). These routers usually sit on the network backbone and connect the branch areas to the root area. Internal routers: Involved only in routing their internal area (intra-area routing) and only maintain information about the area in which they operate. Autonomous system (AS) boundary routers: These routers have interfaces on the network that are outside the internetwork routing domain.  	1.5x4 3	9	15

IX (b)	1) Hop count: It is the number of intermediate systems (routers) between the router and the destination router. 2) Bandwidth: This metric reflects the interface's ideal throughput. For example, a serial interface on a router has a default bandwidth of 1.544Mbps, and Ethernet has a default bandwidth of 10Mbps. 3) Load: The load metric varies based on the actual usage (traffic). 4) Delay: It is the total time needed to move a packet across the route. The shortest time is the best route. 5) Reliability: Reliability estimates the chance of a link failure and can be set by an administrator or established by the given protocol. 6) Cost: This metric sets the preference for a given route. The lower the cost, the more preferable the route. The interface default cost is directly related to its speed.	6	6	
X (a)	An NMS consists of 1. The network hardware components that need to be managed (router, end-device, etc) 2. A software or firmware-based management interface or agent (on the device itself). 3. A network management protocol (NMP). 4. A network management console (NMC). The hardware components are classified into two categories: managed and unmanaged nodes. Managed nodes have the ability to perform basic testing and diagnostics on themselves and report their operational status to a management entity. Unmanaged nodes are devices that cannot directly support a management agent. They are managed through end-devices/hardware-devices (called proxy) where an NMS is running. An agent is software that runs on the device and provides management functionality by collecting and relaying management data about the device to the management system. The agent can also be used as an interface to the system's proprietary configuration and testing interface, permitting the NMS to perform remote device configuration and testing through the network management entity.	1 2 2	9	15

	NMP defines the structure used by the management agents and the management entities to format, transmit, and exchange management information. There are several experimental, proprietary, and standards based protocols (Eg: SNMP). NMC is a computer that operates one or more management entities. There may several NMCs for large networks. These are the query interfaces that collect information using the NMP. This data is then stored in specialized databases that are used for performance analysis, problem tracking and resolution, trouble ticketing, and inventory control. The data is constantly updated and accessed by NMS.	2 2		
X (b)	Common factors in RIPv1 and RIPv2: • Both uses Distance Vector routing protocol as their basic protocol. • Both support maximum metric (hop count) value of 15. Any router farther than 15 hops away is considered as unreachable. • Both uses port 520 for packet transfer. • Both send routing updates periodically every 30 seconds. Differences:	2 4	6	

RIPv1	RIPv2
• Supports classful addressing only • Information does not contain subnet mask. • Does not support VLSM (Variable Length Subnet Masking). • Sends updates as broadcast to limited broadcast address 255.255.255.255	• Supports classful and classless networks. • RIPv2 has the option for sending network mask in the update to allow classless routing. • Supports VLSM • Sends updates as multicast to 224.0.0.9

	• Does not support authentication of update messages	• Support authentication of RIPv2 update messages confirming that the updates are coming from authorized sources.			