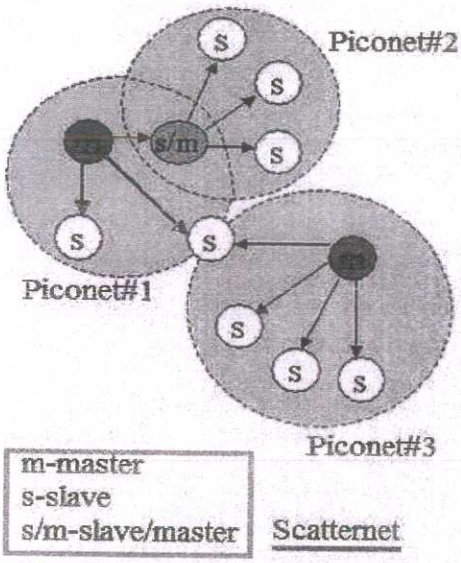
Scoring Indicators

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

Qn. No.	Scoring Indicators	Split up score	Sub Total	Total
	Part A			
I (1)	VPN - Virtual Private Network A secure private network across a probably unsecure public network.	1 1	2	10
I (2)	It is the method of connecting transceivers to Thick Ethernet coaxial cables in order to make a connection to a node system.	2	2	
I (3)	The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory Domain Services (AD DS) forest.	2	2	
I (4)	1. Manually each time the router reboots 2. Automatically using the Network Time Protocol (NTP)	1 1	2	
I (5)	Convergence is the process of bringing all the routing tables of all the routers in the network to a state of consistency.	2	2	
	Part B			
II (1)	Switches are multiport bridges working at data link layer. When powered on, it just act like a hub, ie transmit all packets to all its ports. On receiving each packet at a port, the switch makes an entry (port number, MAC address of the sender) to its MAC address table. On each packet transfer it updates the table. And after some time, it will have the MAC addresses of the devices at all its ports and then it will transfer the packets based on this table in one-to-one mode.	6	6	42
II (2)	1) **Hierarchical organization**: Reflect the organization of the environment where it is used. 2) **Centralized but distributed database**: All network data is centrally located, but it can be distributed among many servers for fast, easy access to information. Automatic replication of information also provides load balancing and fault tolerance. 3) **Scalability**: Advanced indexing technology provides high-performance data access even if there are million objects. 4) **Security**: Uses fine-grained access controls enable administrators to control access to each directory object and its properties. Active Directory also supports secure authentication	1x6	6	

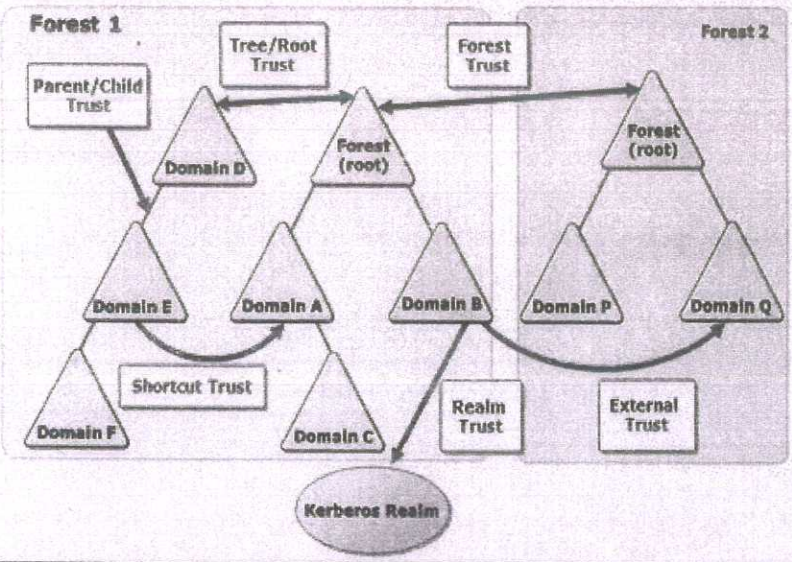
	protocols 5) **Flexibility**: Active Directory is installed with some predefined objects, such as user accounts and groups, but their properties can be modified, and new objects can be added for a customized solution. 6) **Policy-based administration**: Administrators can define policies to ensure a secure and consistent environment for users.			
II (3)	Contains other objects and used to organize and manage users and resources in a network. Also act as administrative and security boundaries or a way to group objects for applying policies. Three types: OU, folder objects, domain objects. Organizational Units (OU): used to organize a network's users and resources into logical administrative units. Folder Objects: When Active Directory is installed, four folder objects are created: Builtin, Computers, Users and ForeignSecurityPrincipals. You can't create new folder objects, nor can you apply group policies to folder objects. Domain Objects: Contain other OUs, leaf objects such as users, groups, etc.	2 4	6	
II (4)	There are two Asynchronous Serial line ports, which are labeled "CONSOLE" and "AUX." Both are configured as data terminal equipment (DTE). **CONSOLE:** This port is the only means of direct access to the router's CLI, and it functions as the router's primary configuration access port when the router is unconfigured. The port can be either RJ-45 or RS232C (9-pin or 25-pin) interface. The console port is also the default output display for all the router's system messages. **AUX:** This port provide a second console port for out-of-band (dial-in) access to the router. It provides remote network access over PPP or SLIP (Serial Line Internet Protocol). It functions as a backup link for a dedicated WAN connection. The AUX port is not used for initial configuration and system messaging. The port can be either RJ-45 or RS232C (9-pin or 25-pin) interface.	1 2.5 2.5	6	
II (5)	Accounting is used to track service abuse and login failures, generate usage statistics, and so on.	1		

	There are two types of IOS accounting: user accounting and operations accounting. User Accounting: IOS provides access information on network sessions (such as PPP) and outbound connections (such as Telnet, rlogin). Operational Accounting: Tracks the Information pertaining to router-centric activities. Operational Accounting can be of two types: <system> accounting—Provides system event information (similar to logging information). <command> accounting—Keeps track of EXEC shell commands usage.	1 2 2	6	
II (6)	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 Cisco 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 default cost of interface is directly related to its speed.	1x6	6	
II (7)	1. Better reliability: OSPF routers construct their own routing table describing network reachability from their perspective form within the network. Hence routing change is easy. 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-	Any 6	6	

	scale networks. 4. VLSM (Variable Length Subnet Masking) support 5. Type of Service routing: Supports Layer 4 Quality of Service routing. 6. Low bandwidth usage: OSPF uses multicast instead of local network broadcasts. 7. Dynamic load balancing and route selection.			
	Part C			
III (a)	(1) Piconet (2) Scatternet **Piconet**: Consists of one primary (master) node and seven active secondary (slave) nodes. There can be only one primary or master station in each piconet. The communication between the primary and the secondary can be one-to-one or one-to-many. Salve-slave communication is not possible. In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state. **Scatternet:** Formed by combining various piconets. A slave in one piconet can act as a master or primary in other piconet. This node is also called bridge slave. A station cannot be a master in two piconets.  	1 3 2 3	9	15
III (b)	Prefer switch. Hub: (1) Physical layer device hence Switch: (1) Data link layer device hence	1		

	does not know MAC address (2) Always performs frame flooding, ie broadcast. (3) Half duplex (4) Non intelligent device (5) Single collision domain, hence less efficient. (6) Only one device can communicate at a time	know the MAC address (2) First flooding, then unicast & multicast as needed. (3) Half/Full duplex (4) Intelligent device (5) Multiple collision domain, hence more efficient. (6) Many device can communicate at a time.	(Any 5 points) 5 marks	6	
IV (a)	1. Straight through crimping Both ends of the cable follow the same standard. Commonly 568B on both sides. Used when dissimilar devices are to be connected (Eg: computer to hub/switch). Such cables are also called patch cables. 2. Crossover crimping Both ends of the cable will be of the opposite standards. Ie, 568A on one side and 568B on the other side or vice versa. Used when similar devices are to be connected (Eg: computer-computer, router-router). 3. Roll over crimping Also called Yost cable. Not used for data transfer. Connect a computer terminal to a router's console port for configuration. Whatever standard is used at one end, the reverse of that colour code will be on the other end. Generally light-blue in colour.		3 3 3	9	15
IV (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. 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.		1 3 1 1	6	

	Mobile WiMAX(802.16e): Here the clients are mobile devices. It has a speed of 30Mbps and a range of 3.5km			
V (a)	The physical structure consists of sites and domain controllers (DC). Site: A site is one or more IP subnets connected by high-speed LAN technology (eg: a small office with no branches). It is a physical location in which domain controllers communicate and replicate information regularly. A business with a branch office in another part of the city connected to the main office through a slow WAN link usually has two sites; but they come under the same domain. Sites have the advantages of controlling the frequency of Active Directory replication and assigning policies based on physical location. Domain controllers (DC): DC is a computer running Windows Server with the Active Directory Domain Services role installed. Active Directory domain can consist of many domain controllers, each domain controller can service only one domain. DC stores a copy of the domain data and replicating changes to that data to all other domain controllers throughout the domain. DC provides data search and retrieval functions for users attempting to locate objects in the directory. DC provides authentication and authorization services for users who log on to the domain and attempt to access network resources.	1 4 4	9	15
V (b)	1. Open industry standard: 2. Transparency: IPSec exists below the transport layer, making it transparent to applications and users. 3. Authentication: 4. Confidentiality: 5. Data origin authentication and integrity: Data origin authentication and integrity is provided by a hashed message authentication code (HMAC) value, which is	Any 6 x 1	6	

	included in every packet. 6. Dynamic re-keying: Occurs during ongoing communications eliminates manual reconfiguration of secret keys and helps protect against secret key determination. 7. Secure links end to end: 8. Centralized management: Network administrators use IPSec policies to provide appropriate levels of security, based on user, work group, or other criteria. 9. Flexibility: Can be applied enterprise-wide or to a single workstation.			
VI (a)	1) Tree-root trust 2) Parent-child trust 3) Shortcut trust 4) Realm trust 5) External trust 6) Forest trust 	Any 3 with explanation X 2 3	9	15
VI (b)	1. Packet filtering firewall: Simply filters (forwards or denies) the packets from and to the network based on a set of rules. 2. Stateful inspection firewall: Tightens the packet filtering by keeping records of each incoming and outgoing TCP connections. 3. Application proxy firewall (application-level gateway): It acts as a proxy between the user and the remote host. But actual connection is between the user and the remote host. Ie, a single TCP connection between the two.	4 x 1.5 marks	6	

	4. Circuit-level proxy firewall (circuit-level gateway): It acts as a proxy between the user and the remote host. But the user is communicating with the proxy only, and the proxy is communicating with the remote host. There are two distinct TCP connections.			
VII (a)	User EXEC, Privileged EXEC and Configuration EXEC modes. User EXEC mode: It is the Initial mode; distinguished by a > prompt. It has the security level 0. It basically allows the user to establish connections from the EXEC shell to other TCP/IP hosts (such as Telnet or rlogin) or start up a network transport session (PPP, etc). The <ping> and <traceroute> applications are also available in user EXEC. To enter the privileged EXEC mode, use the <enable> user EXEC command. Privileged EXEC Mode: Enables complete control over the router. It is distinguished by # prompt. Commonly called enable mode because it is invoked with the user EXEC command <enable>. Highest IOS security level (15) by default; just like the root or the administrator. This mode should be password protected, but it is not by default. IOS allows multiple privileged EXEC levels to be defined with different security levels to control the access to specific commands. Most useful command in this mode is the show command, which is used to show different parameter/configurations in the router. Configuration EXEC mode: Only for creating and modifying the router's configuration files. It is entered from a privileged EXEC mode with a security level of 1 or higher. All configuration changes are active changes, so when a change is made, they are in effect. When changes occur, they are made to the running configuration. Hence if any error occurs, just reboot the router and the startup configuration is reloaded. This mode is also called global configuration mode. Global mode commands are used to set most of the router's global operational parameters and basic network protocol services.	3 3 3	9	15

VII (b)	• While the router is booting, press the pause/break button on the keyboard to enter ROM Monitor ('rommon'). This mode can be identified either by "rommon x >" or simply ">" prompt. (x may be 1,2,3..). • In 2500 series routers, > prompt can be seen. Then type O/R <hex value> to change the config reg value; then press "i" to enter the initialization mode. In most other routers, use the command <confreg hexvalue>. (for recovery 0x2142 is the hex value. This enables the router to boot from flash without using NVRAM contents). • Use the command <reset> to restart the router with the new config-reg value. • The reboot will load IOS skipping the NVRAM. Here we can enter the privileged EXEC and global configuration mode without password and reset the password or give a new password in global configuration mode. • Thus we can recover the router when the password is lost. • Give the default value 0x2102 to the conf register and restart the router to get back to the default mode.	6	6	
VIII (a)	There are four types of memory in router; 1. Read Only Memory (ROM) – for booting the router 2. Flash memory – Stores the IOS. 3. Non-volatile random access memory (NVRAM) – Stores the router's configuration info. 4. Dynamic random access memory (DRAM) – Performs the routing process. ROM handles the routers bootstrap process. In some routers, it contains a limited version of IOS. ROMs have just enough space to load the IOS. Flash memory is rewritable nonvolatile memory. Flash is either mounted on the router's motherboard or installed in a router's PCMCIA slot(s). NVRAM stores the router's configuration information. It does not lose its contents when the power is lost.	1 2 2 2 2	9	15

	DRAM is used for packet processing and IOS operation. DRAM is partitioned into primary and shared memory. Primary memory is loaded with the IOS, data tables and running configuration information. For instance, if IP is being routed, the ARP table and IP route tables are stored in primary memory. The shared memory is used to process datagrams.			
VIII (b)	The configuration register is a 16-bit number, represented in hexadecimal, which controls everything from the way in which a CISCO router boots to whether or not it will process the contents of the startup configuration file. Purposes: The configuration register can be used to change router behavior in several ways, such as: • how the router boots (into ROMmon, NetBoot) • options while booting (ignore configuration, disable boot messages) • console speed (baud rate for a terminal emulation session) • Set and display the configuration register value • Force the router into the ROM monitor (bootstrap program) • Select a boot source and default boot filename • Enable or disable the Break function • Control broadcast addresses • Load operating software from ROM Examples: 1. 0x2102 is the factory-default configuration register value. 2. 0x2142 boots from flash without using NVRAM contents; good for password recovery.	2 Any three x 1 = 3 marks ½ x 2=1 mark	6	
IX (a)	(i) Protocol Analyzers Capture and display network protocol data. It can perform real-time or offline analysis of some or all of the network segment traffic. Collected traffic data can be saved and analyzed later. Through the use of packet filters and triggers, the analyzer can capture data based on application traffic type, Layer 2 or Layer 3 address, transaction type, or specific error. Works in non-intrusive, promiscuous mode. WAN analyzers come with passthrough	3	9	15

	interface cards that sit between the computing device (for example, a router) and the DSU/CSU. (ii) Time Domain Reflectors (TDR) Used for diagnosing cable failure and associated problems. A typical TDR has two components: a TDR scope and a cable terminator. The scope is on one end and the terminator is connected to the other end of the segment. It works by sending a test signal with a specific amplitude and rate into the cable segment and listening for an "echo" or reflection. If no echo is detected, the cable is free of errors. If an echo is detected, the TDR scope can determine the type of problem and the distance where the fault occured based on the type of reflection. (iii) Ping (Packet Internet Groper) Ping is a simple IP-based UNIX tool for testing host reachability. As an IP application, ping functions by sending ICMP echo_request messages at a target destination host. When the target host receives these packets, it responds to the source host with ICMP echo_reply messages.	3 3		
IX (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:	Any 3. 3 marks	6	
	RIPv1: • Supports classful addressing only • Information does not contain subnet mask. • Does not support VLSM RIPv2: • Supports classful and classless networks. • RIPv2 has the option for sending network mask in the update to allow classless routing. • Supports VLSM	Any 3. 3 marks		

	(Variable Length Subnet Masking). • Sends updates as broadcast to limited broadcast address 255.255.255.255 • Does not support authentication of update messages	• Sends updates as multicast to 224.0.0.9 • Support authentication of RIPv2 update messages confirming that the updates are coming from authorized sources.			
X (a)	An autonomous system (AS) is a network or a collection of networks that are all managed and supervised by a single entity or organization. There are three types of AS: 1) Stub: Stub AS reach other networks through one gateway. Routing for stub AS is commonly achieved with static routes. Stub ASs are not common now-a-days. 2) Multihomed nontransit: Large private enterprise networks, with multiple Internet access points, commonly operate as AS. They do not want to have traffic other than their own traversing their network backbone. 3) Multihomed transit: A multihomed transit network allows traffic belonging to other networks to traverse across its network in order to reach its destination.	2 2 2 2	8	15
X (b)	Different parts of a network may use different dynamic routing protocols. Redistribution helps to announce each other's routing information. In static routing, instead of adding static routes on every router on the network, a single router can redistribute a collection of static routes. Bad redistribution may results in routing loops and the difficulty in translation of different routing protocol metrics and distances. To avoid ill-effects of redistribution: 1) If you have only a few networks to redistribute, use static routes or use a single protocol. 2) If possible, avoid redistributing between classless and classful	4 3	7	

	protocols since classful addressing does not use subnet masks in their messages. 3) When using redistribution with multi-gateway networks, it is essential that the gateway routers must select a 'preferable' route.			