

## Scoring Indicators

**Code: 6135**

Qn: No	Scoring Indicators	Split score	Total
I 1	Unbounded medium transport electromagnetic waves without using a physical conductor .(wireless) Eg. Radio waves, waves, Infrared waves(any one)	1+1	2
I 2	IPv4,IPv6	1+1	2
I 3	A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.  A firewall can be hardware, software, or both.	1+1	2
I 4	IOS (Internetwork Operating System) is a proprietary operating system that runs on most Cisco Systems routers and switches to enable data communications between network nodes	1+1	2
I 5	Routing Information Protocols(RIP),Interior Gateway Protocol (IGRP),Open Shortest Path First (OSPF),Exterior Gateway Protocol (EGP	2	2
II 1	<ul style="list-style-type: none"> <li>• A <b>repeater</b> is a device that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal along the next leg of the medium.</li> <li>• In electromagnetic media, repeaters overcome the attenuation caused by free-space electromagnetic-field divergence or cable loss.</li> <li>• A series of repeaters make possible the extension of a signal over a distance.</li> <li>• Repeater remove the unwanted noise in an incoming signal.</li> <li>• A <b>modem (modulator–demodulator)</b> is a network hardware device that modulates one or more carrier wave signals to encode digital information for transmission and demodulates signals to decode the transmitted information.</li> <li>• The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals, from light-emitting diodes to radio.</li> <li>• A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.</li> <li>• Modems are generally classified by the maximum amount of data they can send in a given unit of time, usually expressed in bits per second (symbol bit(s), sometimes abbreviated "bps"), or bytes per second (symbol B(s)).</li> <li>• Modems can also be classified by their symbol rate, measured in baud. The baud unit denotes symbols per second, or the number of times per second the modem sends a new signa</li> </ul>	3+3	6
II 2	<p>Bluetooth</p> <ul style="list-style-type: none"> <li>• Several devices like mobile phones, pdas, headsets, keyboards, mice, medical equipment and even cars now come with this feature.</li> <li>• Due to its low cost, manufacturers are willing to implement this technology in most devices.</li> <li>• It is designed for short range communications with a range of about 10m.</li> <li>• As a result, it consumes less power and are suited for very small battery powered devices and portable devices.</li> <li>• Problems associated when devices communicate via infrared or cables are</li> </ul>	3+3	6

## Scoring Indicators

**Code: 6135**

	<p>removed.</p> <ul style="list-style-type: none"> <li>• Infrared requires a line of sight, bluetooth only needs to be in reasonable vicinity.</li> <li>• As cables are not required, it would be less cumbersome carrying a personal bluetooth device and space would be less cluttered.</li> <li>• As bluetooth devices automatically communicate with each other, it requires very little from the user.</li> <li>• Bluetooth allows for a wireless Personal Area Network (PAN) with it's short range. See chart below for a comparison of these technologies.</li> <li>• For more technical resources and information relating to Bluetooth see the official Bluetooth site.</li> </ul>		
	<p><b>Wi-Fi</b></p> <p>A wireless network uses <u>radio waves</u>, just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens:</p> <ol style="list-style-type: none"> <li>1. A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.</li> <li>2. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.</li> </ol> <p>The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.</p> <ul style="list-style-type: none"> <li>• WiFi or Wireless Fidelity, has a range of about 100m and allows for faster data transfer rate between 10 - 54Mbps.</li> <li>• There are three different wireless standards under WiFi, 802.11a, 802.11b and 802.11g.</li> <li>• 802.11 being the wireless standard set by The Institute of Electrical and Electronic Engineers (IEEE). WiFi is used to create wireless Local Area Networks (WLAN).</li> <li>• The most widely used standard is 802.11b and 802.11g is expected to grow rapidly.</li> <li>• These two standards are relatively inexpensive and can be found providing wireless connectivity in airports, railway stations, cafes, bars, restaurants and other public areas.</li> <li>• The main difference between the two is the speed.</li> <li>• 802.11b has data transfer rate of upto 11Mbps and 802.11g has a rate of upto</li> </ul>		



## Scoring Indicators

**Code: 6135**

	<div style="display: flex; justify-content: space-around; border: 1px solid black; padding: 5px;"> <div style="border: 1px solid black; padding: 2px 10px;">0</div> <div style="border: 1px solid black; padding: 2px 10px;">8</div> <div style="border: 1px solid black; padding: 2px 10px;">16</div> <div style="border: 1px solid black; padding: 2px 10px;">24</div> </div> <p>Class A</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between; border-bottom: 1px solid black; padding-bottom: 5px;"> <span>0 Network</span> <span>Host</span> </div> </div> <p style="text-align: center; margin-top: 20px;">Addresses 1.0.0.0 to 127.255.255.255</p> <p>Class B</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between; border-bottom: 1px solid black; padding-bottom: 5px;"> <span>10 Network</span> <span>Host</span> </div> </div> <p style="text-align: center; margin-top: 20px;">Addresses 128.0.0.0 to 191.255.255.255</p> <p>Class C</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between; border-bottom: 1px solid black; padding-bottom: 5px;"> <span>110 Network</span> <span>Host</span> </div> </div> <p style="text-align: center; margin-top: 20px;">Addresses 192.0.0.0 to 223.255.255.255</p> <p>Class D</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px; text-align: center;">         1110 Multicast address       </div> <p style="text-align: center; margin-top: 20px;">Addresses 224.0.0.0 to 239.255.255.255</p> <p>Class E</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px; text-align: center;">         11110 Reserved for future use       </div> <p style="text-align: center; margin-top: 20px;">Addresses 240.0.0.0 to 255.255.255.25</p>		
II 4	<ul style="list-style-type: none"> <li>• Memory is used to           <ul style="list-style-type: none"> <li>○ boot the router,</li> <li>○ store its operating system,</li> <li>○ perform the routing process,</li> <li>○ and store the router's configuration information.</li> </ul> </li> <li>• To perform these tasks, four types of memory are used:           <ol style="list-style-type: none"> <li>1. Read-only memory (ROM)</li> <li>2. Flash memory</li> <li>3. Non-volatile random access memory (NVRAM)</li> <li>4. Dynamic random access memory (DRAM)</li> </ol> </li> </ul> <p><b>ROM(Read Only Memory)</b></p> <ul style="list-style-type: none"> <li>• ROM is used on the 1600, 2500, 2600, and 3x00 series routers           <ul style="list-style-type: none"> <li>○ to handle the router's bootstrap process,</li> <li>○ to load the OS.</li> </ul> </li> <li>• In 2500, the ROM           <ul style="list-style-type: none"> <li>○ contains a limited version of the router's operating system, called the</li> </ul> </li> </ul>	3+3	6

## Scoring Indicators

**Code: 6135**

	<p style="text-align: center;"><i>Internetwork Operating System (IOS).</i></p> <p><b>Flash memory</b></p> <ul style="list-style-type: none"> <li>• Rewritable nonvolatile memory.</li> <li>• Flash memory is used on all Cisco routers to store the IOS.</li> <li>• By using the bootflash, the bootstrap application can be upgraded without a hardware change.</li> <li>• In the early days of programmable hardware, floppy disks were used to store boot images and configuration files, as flash memory was excessively expensive</li> </ul> <p><b>NVRAM</b></p> <ul style="list-style-type: none"> <li>• similar to flash</li> <li>• It does not lose its contents when power is lost.</li> <li>• It is used to store the router's configuration information.</li> </ul> <p><b>DRAM</b></p> <ul style="list-style-type: none"> <li>• used for packet processing and IOS operation.</li> <li>• used for IOS and routing table storage.</li> <li>• On all router platforms (except the 7x00 series), DRAM is partitioned into             <ul style="list-style-type: none"> <li>○ primary and</li> <li>○ shared memory.</li> </ul> </li> </ul> <p><b>Primary memory</b></p> <ul style="list-style-type: none"> <li>• There are two primary memory architectures used by Cisco routers:             <ul style="list-style-type: none"> <li>○ Read From Flash (RFF)                 <ul style="list-style-type: none"> <li>▪ The Cisco 1600 and 2500 series (and older) routers use an RFF model.</li> <li>▪ The IOS resides on flash, and IOS data structures are loaded into RAM as needed.</li> </ul> </li> <li>○ Read From RAM (RFR)                 <ul style="list-style-type: none"> <li>▪ The 1600-R, 2600, 36'0, 4'00, and 7x00 series routers are RFR routers.</li> </ul> </li> </ul> </li> </ul> <p><b>Shared memory</b></p> <ul style="list-style-type: none"> <li>• used for datagram processing.</li> <li>• By default, the DRAM is partitioned using a 75/25 split of the router's minimum DRAM configuration split.</li> <li>• Memory used for packet processing is on the interface controller or on the switch processor, depending on the router model.</li> <li>• Because the entire operation of the router is dependent on memory, it is essential that the router have enough to operate efficiently.</li> </ul>		
<p><b>II 5</b></p>	<p>To configure the router, perform one or more of these tasks:</p> <ol style="list-style-type: none"> <li>1. Configure Global Parameters</li> <li>2. Configure Fast Ethernet LAN Interfaces</li> <li>3. Configure WAN Interfaces</li> <li>4. Configuring a Loopback Interface</li> <li>5. Configuring Command-Line Access to the Router</li> </ol> <ul style="list-style-type: none"> <li>• Enters global configuration mode, when using the console port-<b>configure terminal</b></li> <li>• Specifies the name for the router.</li> <li>• Specifies an encrypted password to prevent unauthorized access to the router.</li> <li>• Enters the configuration mode for a Fast Ethernet WAN interface on the router.</li> <li>• Sets the IP address and subnet mask for the specified Fast Ethernet interface.</li> <li>• Enables the Ethernet interface, changing its state from administratively down to administratively up.</li> </ul>	<p>2+4</p>	<p>6</p>

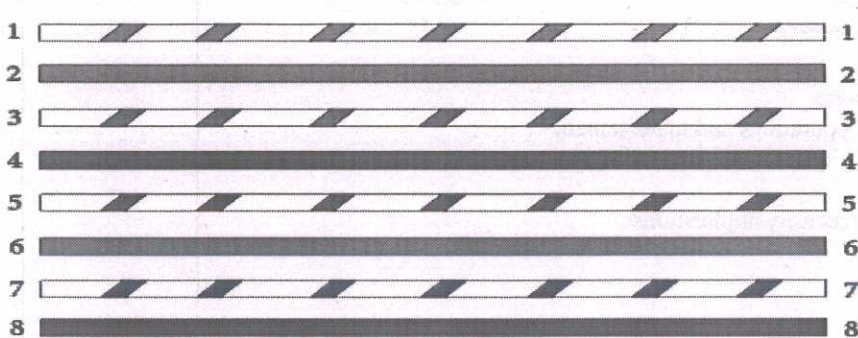
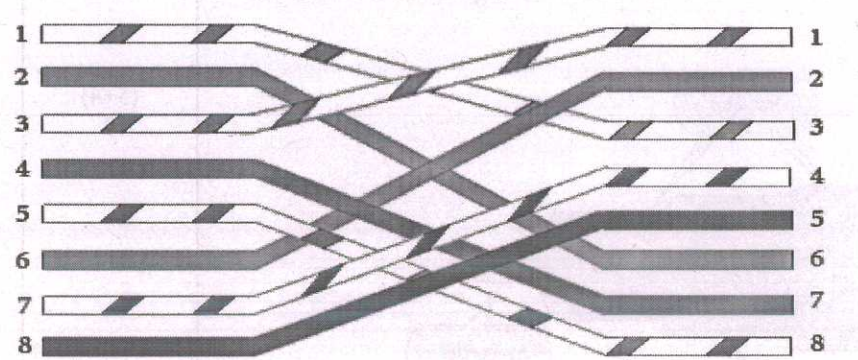
## Scoring Indicators

**Code: 6135**

II 6	BASIS FOR COMPARISON	STATIC ROUTING	DYNAMIC ROUTING	3+3	6																								
	Configuration	Manual	Automatic																										
	Routing table building	Routing locations are hand-typed	Locations are dynamically filled																										
	Routes	User defined	Routes are Updated																										
	Routing algorithms	Doesn't employ complex routing algorithms.	Uses complex																										
	Implemented in	Small networks	Large networks																										
	Link failure	Link failure obstructs the rerouting.	Link failure rerouting.																										
	Routing protocols	No routing protocols are indulged in the process.	Routing protocols such as RIP, EIGRP, etc are involved in the routing process.																										
	Additional resources	Not required	Needs additional resources to store the information.																										
II 7	<ul style="list-style-type: none"> <li>• The router will use all the available sources of reachability information to construct the most accurate and efficient routing table possible, based on the available information.</li> <li>• Each information source is assigned an administrative distance, which is used to determine a route's integrity.</li> </ul> <p><b>IOS Administrative Distances</b></p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Protocol</th> <th style="text-align: left;">Distance</th> </tr> </thead> <tbody> <tr> <td>Connected interface</td> <td>0</td> </tr> <tr> <td>Static route</td> <td>1</td> </tr> <tr> <td>EIGRP summary route</td> <td>5</td> </tr> <tr> <td>BGP (external)</td> <td>20</td> </tr> <tr> <td>EIGRP (internal)</td> <td>90</td> </tr> <tr> <td>IGRP</td> <td>100</td> </tr> <tr> <td>OSPF</td> <td>110</td> </tr> <tr> <td>RIP</td> <td>120</td> </tr> <tr> <td>EIGRP (external)</td> <td>170</td> </tr> <tr> <td>BGP (internal)</td> <td>200</td> </tr> <tr> <td>Unknown</td> <td>255</td> </tr> </tbody> </table> <ul style="list-style-type: none"> <li>• The lower the administrative distance value, the more trusted the</li> </ul>			Protocol	Distance	Connected interface	0	Static route	1	EIGRP summary route	5	BGP (external)	20	EIGRP (internal)	90	IGRP	100	OSPF	110	RIP	120	EIGRP (external)	170	BGP (internal)	200	Unknown	255	6	6
Protocol	Distance																												
Connected interface	0																												
Static route	1																												
EIGRP summary route	5																												
BGP (external)	20																												
EIGRP (internal)	90																												
IGRP	100																												
OSPF	110																												
RIP	120																												
EIGRP (external)	170																												
BGP (internal)	200																												
Unknown	255																												

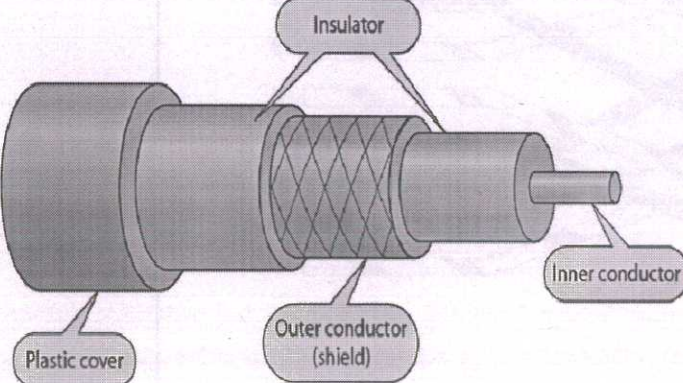
# Scoring Indicators

**Code: 6135**

	<p style="text-align: center;">route.</p> <p>III a Straight-through cables are primarily used for connecting unlike devices. A straight-through cable is typically used in the following situations:</p> <p>Use a straight-through cable when:</p> <ol style="list-style-type: none"> <li>1. Connecting a router to a hub</li> <li>2. Connecting a computer to a switch</li> <li>3. Connecting a LAN port to a switch, hub, or computer</li> </ol> <p style="text-align: center;"><b>Straight Through Wiring Guide 568-B</b></p>  <p>Cross-over cables are used for connecting similar type devices</p> <p>Use a crossover cable when:</p> <ol style="list-style-type: none"> <li>1. Connecting a computer to a router</li> <li>2. Connecting a computer to a computer</li> <li>3. Connecting a router to a router</li> <li>4. Connecting a switch to a switch</li> <li>5. Connecting a hub to a hub</li> </ol> <p style="text-align: center;"><b>Crossover Wiring Guide 568-B</b></p>  <p>Explanation-6marks Diagram-3marks</p>		
		(6+3) 9	15
III b	<ul style="list-style-type: none"> <li>• Network infrastructure is the hardware and software resources of an entire</li> </ul>	(3 +3)	6

## Scoring Indicators

**Code: 6135**

	<p>network that enable network connectivity, communication, operations and management of an enterprise network.</p> <ul style="list-style-type: none"> <li>• It provides the communication path and services between users, processes, applications, services and external networks/the internet.</li> <li>• Network infrastructure is typically part of the IT infrastructure found in most enterprise IT environments.</li> <li>• The entire network infrastructure is interconnected, and can be used for internal communications, external communications or both.</li> </ul> <p>A typical network infrastructure includes:</p> <ul style="list-style-type: none"> <li>• Networking Hardware:             <ul style="list-style-type: none"> <li>○ Routers</li> <li>○ Switches</li> <li>○ LAN cards</li> <li>○ Wireless routers</li> <li>○ Cables</li> </ul> </li> <li>• Networking Software:             <ul style="list-style-type: none"> <li>○ Network operations and management</li> <li>○ Operating systems</li> <li>○ Firewall</li> <li>○ Network security applications</li> </ul> </li> <li>• Network Services:             <ul style="list-style-type: none"> <li>○ T-1 Line</li> <li>○ DSL</li> <li>○ Satellite</li> <li>○ Wireless protocols</li> <li>○ IP addressing</li> </ul> </li> </ul>		
<p>IVa</p>	<p><b>Coaxial cable</b></p> <p>Coaxial cable gets its name because it contains two conductors that are parallel to each other. The center conductor in the cable is usually copper. The copper can be either a solid wire or stranded martial.</p> <p>Outside this central Conductor is a non-conductive material. It is usually white, plastic material used to separate the inner Conductor form the outer Conductor. The other Conductor is a fine mesh made from Copper. It is used to help shield the cable form EMI.Outside the copper mesh is the final protective cover.</p> <div style="text-align: center;">  </div>	<p style="text-align: center;">(5+4) 9</p>	<p style="text-align: center;">15</p>

## Scoring Indicators

Code: 6135

The actual data travels through the center conductor in the cable. EMI interference is caught by outer copper mesh. There are different types of coaxial cable vary by gauge & impedance.

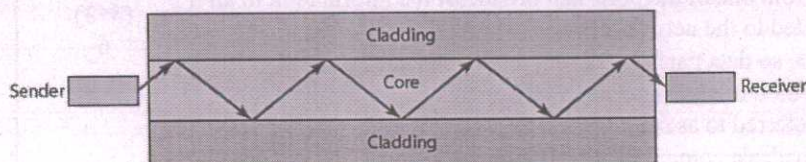
Gauge is the measure of the cable thickness. It is measured by the Radio grade measurement, or RG number. The high the RG number, the thinner the central conductor core, the lower the number the thicker the core

### Advantages of Coaxial Cables

1. It can be used for both analog and digital transmission.
2. It offers higher bandwidth as compared to twisted pair cable and can span longer distances.
3. Because of better shielding in coaxial cable, loss of signal or attenuation is less.
4. Better shielding also offers good noise immunity.
5. It is relatively inexpensive as compared to optical fibers.
6. It has lower error rates as compared to twisted pair.
7. It is not as easy to tap as twisted pair because copper wire is contained in plastic jacket.

### Fibre-optic cable

- A fibre-optic cable is made of glass or plastic and transmits signals in the form of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.
- If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction.
- The below figure shows how a ray of light changes direction when going from a more dense to a less dense substance.
- Optical fibres use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



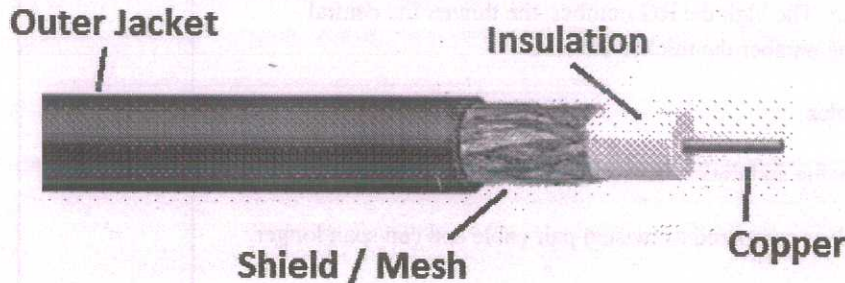
Coaxial cable gets its name because it contains two conductors that are parallel to each

## Scoring Indicators

**Code: 6135**

other. The center conductor in the cable is usually copper. The copper can be either a solid wire or stranded martial.

Outside this central Conductor is a non-conductive material. It is usually white, plastic material used to separate the inner Conductor form the outer Conductor. The other Conductor is a fine mesh made from Copper. It is used to help shield the cable form EMI.Outside the copper mesh is the final protective cover.



The actual data travels through the center conductor in the cable. EMI interference is caught by outer copper mesh. There are different types of coaxial cable vary by gauge & impedance.

Gauge is the measure of the cable thickness. It is measured by the Radio grade measurement, or RG number. The high the RG number, the thinner the central conductor core, the lower the number the thicker the core

Advantages of Coaxial Cables (Any 4 points)

1. It can be used for both analog and digital transmission.
2. It offers higher bandwidth as compared to twisted pair cable and can span longer distances.
3. Because of better shielding in coaxial cable, loss of signal or attenuation is less.
4. Better shielding also offers good noise immunity.
5. It is relatively inexpensive as compared to optical fibers.
6. It has lower error rates as compared to twisted pair.
7. It is not as easy to tap as twisted pair because copper wire is contained in plastic jacket..

Structure-5marks Figure-4marks

IV b

Hub,Switch,Router  
**HUB**

- A hub works in the physical layer of the OSI model.
- A *hub* is a multiport repeater.
- It is basically a non-intelligent device, and has no decision making capability.
- Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.
- It take the input data from one of the ports and broadcast the information to all the other ports connected to the network.
- Hubs cannot filter data, so data packets are sent to all connected devices.
- **Broadcasting** The method of sending data to all systems regardless of the intended recipient is referred to as *broadcasting*.
- On busy networks, broadcast communications can have a significant impact on overall network performance.
- There are two types of hubs:
  1. Active hubs—Where each of the ports is a repeater that amplifies the signal for each connection (CMTA/CD).
    - It regenerate a signal before forwarding it to all the ports on the

(3+3)  
6

## Scoring Indicators

**Code: 6135**

	<p>device and requires a power supply.</p> <ul style="list-style-type: none"> <li>○ Small workgroup hubs normally use an external power adapter, but on larger units the power supply is built in.</li> </ul> <p>2. Passive hubs—</p> <ul style="list-style-type: none"> <li>▪ Do not amplify the signal at all.</li> <li>▪ Do not need power</li> <li>▪ They don't regenerate the data signal</li> </ul> <p><b>Switch</b></p> <ul style="list-style-type: none"> <li>● A switch is multi-port networking device that connects network devices together.</li> <li>● A switch operates at the data link layer (layer 2) of the OSI model. A switch filters and then forwards data packets between networks</li> <li>● Switch Stores MAC address and maintains address.</li> <li>● Used in LAN, MAN, WAN</li> <li>● No. of Ports- 4-48 depending on type of switch</li> <li>● Broadcast, Uni-cast &amp; Multicast.</li> </ul> <p><u>Router</u></p> <ul style="list-style-type: none"> <li>● Directs data in a network. Passes data between home computers, and between computers and the modem.</li> <li>● Store IP address in Routing table and maintain address at its own.</li> <li>● Operates at network layer(layer3)</li> <li>● Can connect to multiple PCs or networking devices via Ethernet or Wi-Fi</li> <li>● Take faster routing decisions</li> </ul>		
V a	<p><b>DHCP (Dynamic Host Configuration Protocol)</b></p> <p>DHCP is a network protocol that is used to assign various network parameters to a device. This greatly simplifies administration, since there is no need to assign static network parameters for each device separately. DHCP is a client-server protocol. A client is a device that is configured to use DHCP to request network parameters from a DHCP server. DHCP server maintains a pool of available IP addresses and assigns one of them to the host. A DHCP server can also provide some other parameters, such as:</p> <ul style="list-style-type: none"> <li>• subnet mask</li> <li>• default gateway</li> <li>• domain name</li> <li>• DNS server</li> </ul> <p>DHCP client goes through the four step process:</p>	7+2	15

## Scoring Indicators

**Code: 6135**

	<div style="text-align: center;"> <pre> sequenceDiagram     participant Client as DHCP client     participant Server as DHCP server     Client-&gt;&gt;Server: 1. DHCP Discover     Server--&gt;&gt;Client: 2. DHCP Offer     Client-&gt;&gt;Server: 3. DHCP Request     Server--&gt;&gt;Client: 4. DHCP Ack             </pre> </div> <p>1: A DHCP client sends a broadcast packet (DHCP Discover) to discover DHCP servers on the LAN segment.</p> <p>2: The DHCP servers receive the DHCP Discover packet and respond with DHCP Offer packets, offering IP addressing information.</p> <p>3: If the client receives the DHCP Offer packets from multiple DHCP servers, the first DHCP Offer packet is accepted. The client responds by broadcasting a DHCP Request packet, requesting network parameters from a single server.</p> <p>4: The DHCP server approves the lease with a DHCP Acknowledgement packet. The packet includes the lease duration and other configuration information.</p> <p style="text-align: center;">Expl-7 Fig-2</p>		
<p><b>V b</b></p>	<p><b>Domain Controller(DC)</b></p> <ul style="list-style-type: none"> <li>• It is a server computer that responds to security authentication requests (logging in, checking permissions, etc.) within a Windows domain.</li> <li>• In the windows domain, the directory resides on computers that are configured as domain controllers.</li> <li>• It manages all security-related aspects between user and domain interactions, centralizing security and administration.</li> <li>• A domain controller is generally suitable for networks with more than 10 PCs.</li> <li>• Their physical location is irrelevant.</li> </ul>	<p>6</p>	
<p><b>VI a</b></p>	<p>Remote desktop is a program or an operating system feature that allows a user to connect to a computer in another location, see that computer's desktop and interact with it as if it were local.</p> <p>People use remote desktop access capabilities to do a variety of things, including the following:</p> <ul style="list-style-type: none"> <li>• Access a workplace computer from home or when traveling.</li> <li>• Access a home computer from other locations.</li> </ul>	<p>7+2</p>	<p>15</p>

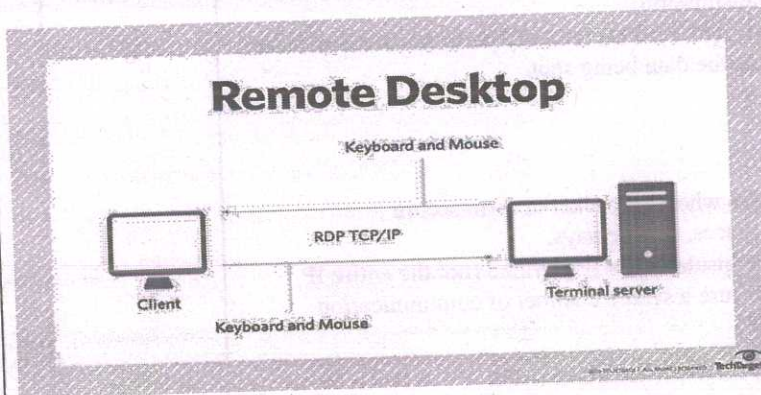
## Scoring Indicators

Code: 6135

- Fix a computer problem.
- Perform administrative tasks.
- Demonstrate something, such as a process or a software application

### Remote desktop protocols

A remote desktop connection relies upon any of a number of protocols, including Remote Desktop Protocol (RDP), virtual network computing (VNC), NX technology and Independent Computing Architecture (ICA).



1. Install AD DS complete the following steps:

Use Server Manager to add the Active Directory Domain Services Role to install the Binaries to support the server becoming a Domain Controller.

1. Launch Server Manager, select the Manage drop down menu, select Add roles and features.
2. Review the Before You Begin page, Click Next.
3. On the Select installation type page ensure Role-based or feature-based installation radial button is selected, click Next.
4. On the Select destination server page Select the desired server from the Server Pool.
5. Click on the Active Directory Domain Services box.
6. he Add features that are required for Active Directory Domain Service dialog box pops up, select Add Features, click Next.
7. Do not add any features on the Select features page, click Next.
8. Review the Active Directory Domain Services information page, click next.
9. The AD DS Binaries are now being installed, click Close to close the Installation progress dialog box.

In Server Manager Title bare click on the yellow triangle to perform post-deployment configuration of promote the server to a Domain Controller.

Click on Promote this server to a domain controller to start the promotion wizard.

4. On the Deployment Configuration page complete the following tasks

- Select the Add a domain to an existing forest radial button.

On the Select domain type drop down box select Child Domain.

Fill in the Parent domain name box with the parent AD DS Domain Name.

## Scoring Indicators

**Code: 6135**

	<p>Fill in the desired New domain name.          Click change to supply the credentials for a member of the Enterprise Admins group.          Verify the entries change if needed, click Next.          On the Domain Controller Options page De-select DNS or GC during this installation,          Enter a desired DSRM Password, click Next.          Note: Because the server's IP Address is in a different site defined in Active Directory Sites and Services, the site name has been pre-selected for that site          Verify the NetBIOS domain name and click Next.          Explanation-7 fig-2</p>		
VI b	<p>Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.</p> <p>Also known as IP Security.</p> <p>IPsec involves two security services:</p> <ul style="list-style-type: none"> <li>• Authentication Header (AH): This authenticates the sender and it discovers any changes in data during transmission.</li> <li>• Encapsulating Security Payload (ESP): This not only performs authentication for the sender but also encrypts the data being sent.</li> </ul> <p>There are two modes of IPsec:</p> <ul style="list-style-type: none"> <li>• Tunnel Mode: This will take the whole IP packet to form secure communication between two places, or gateways.</li> <li>• Transport Mode: This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication</li> </ul>	6	
VII a	<p><b>IOS supports two modes of system authentication:</b></p> <ul style="list-style-type: none"> <li>○ old-mode and</li> <li>○ new-mode.</li> </ul> <p><b>Old-mode</b></p> <ul style="list-style-type: none"> <li>• Old-mode uses a static, locally stored user table or <i>Terminal Access Controller Access Control System</i>(TACACS) for user authentication.</li> <li>• TACACS (introduced in IOS version 10.0) is a security software suite that provides a configurable modular system for providing authentication, accounting, and authorization.</li> <li>• The service is provided by running a service or process daemon on a Windows NT or UNIX system.</li> <li>• The server stores the user authentication and authorization data, and logs user and system accounting events.</li> <li>• There are three versions of TACACS supported by IOS:             <ul style="list-style-type: none"> <li>○ TACACS (CiscoSecure 1.x)</li> <li>○ Extended TACACS (available in old-mode and new-mode)</li> <li>○ TACACS+ (CiscoSecure 2.x) (available only in new-mode and preferred by Cisco)</li> </ul> </li> </ul> <p><b>New-mode</b></p> <ul style="list-style-type: none"> <li>• New-mode is also referred to as AAA (authentication,</li> </ul>	9	15


## Scoring Indicators

Code: 6135

	<ul style="list-style-type: none"> <li>• <i>accounting and authorization</i>).</li> <li>• AAA provides facilities for system and IOS command accounting and authorization.</li> <li>• These additional control facilities allow us to keep accounting logs on user access to the router (a must for dial-in), and, if needed, to configure logged, restricted EXEC command access.</li> <li>• AAA support is essential in access-server environments and can be quite useful in situations where many people are responsible for maintaining then network.</li> </ul> <p>AAA also provides the capability to use Remote Authentication Dial-In User Service (RADIUS) and Kerberos V5 as an alternative to TACACS.</p> <p>There are two types of IOS accounting:</p> <ul style="list-style-type: none"> <li>○ user and</li> <li>○ operations.</li> <li>• IOS provides access information on network sessions(PPP, SLIP, ARA) and outbound connections (such as Telnet, rlogin).</li> </ul> <p>Operational accounting, on the other hand, tracks the information pertaining to router-centric activities.</p>		
VII b	<ul style="list-style-type: none"> <li>• TFTP is the easiest way to upgrade your router's IOS.</li> <li>• It is recommended that you have the TFTP server on the same local segment, if possible.</li> <li>• On RFF routers (1600, 2500 series), the router boots with the flash in read-only mode, and because it reads data structures from the IOS stored in flash, it cannot be altered while the router is using them.</li> <li>• To perform an IOS upgrade, you need to configure the router to load its IOS off the TFTP server instead of using the flash stored image.</li> <li>• On RFR routers (1600-R, 2600, 36x0, 4x00, and 7x00 series), the router's flash is in read/write mode all the time because the IOS is loaded into DRAM at boot.</li> <li>• IOS can be upgraded while the router is in operation.</li> <li>• If the IOS image is corrupt, or if there are incompatibilities between your configuration and the new IOS, you could have some problems.</li> <li>• To play it safe on both RFR and RFF router models, use TFTP to boot the IOS image you plan to upgrade on your router.</li> <li>• Then, upgrade it.</li> </ul>	6	
VIII a	<ul style="list-style-type: none"> <li>• The router's clock can be set either manually each time the router reboots, or by using the Network Time Protocol (NTP) when configuring the router.</li> <li>• IOS uses <i>Universal Time Coordinated (UTC)</i>, more commonly known as <i>Greenwich Mean Time (GMT)</i>.</li> <li>• To set time zone, use the global configuration command:&lt;clock timezone&gt;:             <ul style="list-style-type: none"> <li>○ Router# config terminal</li> <li>○ Enter configuration commands, one per line. End with CNTL/Z.</li> <li>○ Router(config)#clock timezone EST -5</li> <li>○ Router(config)#^Z</li> </ul> </li> <li>• To set the router's system clock, use the privileged EXEC command :             <ul style="list-style-type: none"> <li>○ &lt;clock set&gt;.</li> <li>○ The convention is hour:min:second day month year:</li> </ul> </li> </ul>	9	15

## Scoring Indicators

Code: 6135

	<ul style="list-style-type: none"> <li>○ Router#clock set 12:00:15 14 June 1999</li> <li>• The router's clock must be set every time the router boots (or reboots)</li> </ul>		
VIII b	<ul style="list-style-type: none"> <li>▪ To set up buffered logging, first enable it.</li> <li>▪ Then the local DRAM allocation and logging event history needs to be set.</li> <li>▪ All logging parameters are set in global configuration mode:               <ul style="list-style-type: none"> <li>○ local-AS(config)#logging on</li> <li>○ local-AS(config)#logging buffered 64000</li> <li>○ local-AS(config)#logging history size 250</li> </ul> </li> <li>▪ Here all logging has been enabled, a local buffer of 64K has been allocated, and up to 250 logging messages will be stored in the buffer (the maximum is 500).</li> <li>▪ The buffer log file is a rotating one, so once the message count has reached its limit, it starts to overwrite itself, deleting the last message in the file as new messages are added.</li> <li>▪ To view logging information, use the privileged EXEC command               <ul style="list-style-type: none"> <li>○ &lt;show logging&gt; :</li> <li>○ local-AS#sh logging</li> <li>○ Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)</li> <li>○ Console logging: level informational, 17 messages logged</li> <li>○ Monitor logging: level debugging, 234 messages logged</li> <li>○ Trap logging: level informational, 744 message lines logged</li> <li>○ Logging to 130.140.55.216, 7 message lines logged</li> <li>○ Buffer logging: level debugging, 810 messages logged</li> <li>○ Log Buffer (64000 bytes):00:00:08: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up 00:00:08: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up</li> </ul> </li> </ul>	6	
IX a	<ul style="list-style-type: none"> <li>• Exterior routing protocols (ERPs) are used primarily in Internet backbone networks that connect internetworks.</li> <li>• ERPs send information the same way RIP does:               <ul style="list-style-type: none"> <li>• as a vector (the AS number) and as a distance (the destination network information).</li> <li>• distributing static routes between internetworks.</li> </ul> </li> </ul> <p><b>Autonomous Systems and Exterior Routing</b></p> <ul style="list-style-type: none"> <li>• Routing between autonomous systems or exterior routing is strictly an Internet convention.</li> <li>• ERPs were created to provide a more efficient way to build and manage Internet backbone routing tables.</li> <li>• The difference is that an internetwork uses one or more IGP protocols to exchange routing information within a closed network.</li> <li>• An AS uses both IGP(s) and ERPs to exchange routing information within the context of an open network (like the Internet).</li> <li>• In addition, an AS network is registered with an Internet registration authority (ICANN, AIRN, or RIPE).</li> </ul> <p>The basic job of a <i>dynamic routing protocol</i> is to find the best, most efficient route to forward IP network traffic.</p>		15

## Scoring Indicators

Code: 6135

	<p>The dynamic routing protocol can also find a secondary route in the event that the best route is lost. Enterprise networks commonly use multiple network paths to interconnect segments. Routing protocols provide two main advantages:</p> <ul style="list-style-type: none"> <li>• The capability to balance the traffic load between these paths and keep traffic flowing in the event that a path is lost</li> <li>• The capability to easily add routes (such as new network segments) to the network</li> </ul> <p>IP network routing can be categorized into two distinct types of routing:</p> <ul style="list-style-type: none"> <li>• Intranetwork routing</li> <li>• Internetwork routing</li> </ul> <p><i>Intranetwork routing</i>, or <i>interior routing</i>, exchanges route information between routers within defined routing processes. An intranetwork can have single or multiple routing processes. Protocols that perform intranetwork routing are known as <i>interior gateway protocols (IGPs)</i>. The Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) are popular IGPs.</p> <p><i>Internetwork routing</i> has two dimensions: First, in the context of the global Internet, internetwork routing is the exchange of routing information between large, centrally administered networks known as <i>autonomous systems (ASs)</i>. A particular type of routing protocol known as <i>Exterior Gateway Protocol (EGP)</i> performs this task. EGP was the first protocol created to perform this function. Today, Border Gateway Protocol (BGP) version 4 is the most commonly employed protocol for this task.</p>		
IX b	<ul style="list-style-type: none"> <li>• Before computer networks emerged, there were mainframe time-sharing systems.</li> <li>• These systems were standalone supercomputers that shared memory, processing, and storage resources between a certain number of users.</li> <li>• Users would access the mainframe through dumb terminals that were connected to the server via serial controllers or modems.</li> <li>• This computing model is still used today with some UNIX systems and client/server computing.</li> <li>• But, large mainframe time-sharing systems required more attention and management than most UNIX systems today.</li> <li>• Mainframe management was performed by systems administrators.</li> <li>• These administrators would monitor the mainframe's processor and memory utilization, I/O controllers, line terminals and modems, multiplexers, channel banks, dedicated circuits, disk, tape, and card reading systems.</li> <li>• All these systems required constant monitoring to continue functioning properly and effectively.             <ul style="list-style-type: none"> <li>○ What system resources were over-utilized or under-utilized?</li> <li>○ What was the system's load average and peak load?</li> <li>○ Were the local and remote access lines adequate to meet the access demand?</li> </ul> </li> <li>• The administrators would work with system operators and analysts to resolve system resource failures and reprovisions or add system resources.</li> <li>• In most cases, separate management and configuration systems were required to manage all the different system resources.</li> <li>• When LAN and WAN networks began to emerge in the 1980s with the introduction of the personal computer, similar configuration, management, and monitoring began to appear for computer networks.</li> <li>• These new technologies were proprietary.</li> <li>• Standards bodies, manufacturers, network managers, and network providers realized that there was a need for "universal" standards-based automated network management.</li> </ul>	6	
X a	<p>Network troubleshooting is the collective measures and processes used to identify, diagnose and resolve problems and issues within a computer network.</p>	9	15

## Scoring Indicators

**Code: 6135**

	<ul style="list-style-type: none"> <li>• It is a systematic process that aims to resolve problems and restore normal network operations within the network.</li> <li>• Network troubleshooting is primarily done by network engineers or administrators to repair or optimize a network.</li> <li>• It is generally done to recover and establish network or Internet connections on end nodes/devices.</li> </ul> <p>Network troubleshooting process includes :</p> <ul style="list-style-type: none"> <li>• Finding and resolving problems and establishing Internet/network connection of a computer/device/node</li> <li>• Configuring a router, switch or any network management device</li> <li>• Installing cables or Wi-Fi devices</li> <li>• Updating firmware devices on router switch</li> <li>• Removing viruses</li> <li>• Adding, configuring and reinstalling a network printer             <ul style="list-style-type: none"> <li>• Some individuals are born troubleshooters.</li> <li>• Otherwise, troubleshooting is a skill that is learned.</li> <li>• The development of troubleshooting skills is essential to the success of any network administrator.</li> <li>• The troubleshooting skills are naturally developed by understanding and experience with the different technological aspects of computer networking grow.</li> <li>• technical knowledge is important</li> <li>• ability to ask the right questions when problems arise, and to be able to listen and understand the answers to those questions, is the most important (and often the hardest) troubleshooting skill any technical professional must develop.</li> <li>• identify problems and resolve them before they impact service performance.</li> <li>• to identify the real problem and assist those actually responsible for correcting the problem .</li> </ul> </li> </ul> <p>The following are some guidelines helpful when troubleshooting a problem.</p> <ol style="list-style-type: none"> <li>1. Look at the big picture and then figure out what perspective you have.</li> <li>2. Ask the right questions.             <ul style="list-style-type: none"> <li>• Some examples of the kinds of questions you should ask are as follows:                 <ul style="list-style-type: none"> <li>○ Can you describe the actual problem being experienced? (Be sure to get a list of applications and services used when the problem occurred.)</li> <li>○ Has the problem occurred previously?</li> <li>○ Is it a chronic problem? If so, how long have you been experiencing it?</li> <li>○ If it is chronic, does it occur in along with another event that might or might not be related.</li> </ul> </li> </ul> </li> </ol>		
X b	<p><b>Displaying General Routing Information</b></p> <p>There are several IOS commands used for controlling and displaying information about IP routing.</p> <p>Display commands:</p> <pre>&lt;show ip route&gt; &lt;show ip route connected&gt; &lt;show ip route [address/hostname]&gt; &lt;show arp&gt; &lt;show ip protocol&gt; &lt;show ip masks&gt; &lt;show ip masks [network address]&gt; &lt;tracert&gt;</pre> <p>Control commands:</p> <pre>&lt;clear ip route *&gt; &lt;clear ip route [network] [mask]&gt; <i>&lt;clear arp&gt;</i></pre>	6	