QUESTION 101
You are attempting to properly subnet the IP space of one of the Certkiller location. For the network "200.10.10.0" there is a need for 3 loopback interfaces, 2 point to point links, one Ethernet with 50 stations and one Ethernet with 96 stations. What option below would be the most efficient (for saving IP addresses)?

A. 200.10.10.1/32, 200.10.10.2/32, 200.10.10.3/32
200.10.10.4/30, 200.10.10.8/30
200.10.10.64/26, 200.10.10.128/25
B. 200.10.10.0/32, 200.10.10.1/32, 200.10.10.2/32
200.10.10.4/32, 200.10.10.8/31
200.10.10.64/26, 200.10.10.128/25
C. 200.10.10.1/32, 200.10.10.2/32, 200.10.10.3/32
200.10.10.4/31, 200.10.10.8/32
200.10.10.64/27, 200.10.10.128/27
D. D. 200.10.10.1/31, 200.10.10.2/31, 200.10.10.3/31
200.10.10.4/30, 200.10.10.8/30
200.10.10.64/27, 200.10.10.128/26
E. There is not enough address available on that network for these subnets.

Answer: A

Explanation:
Choice A will provide the necessary subnetting to achieve all of the necessary network/host combinations that are needed at this location. Since each loopback interface is used only as an internal network to the router, no actual hosts are needed so the host subnet mask of a /32 will be sufficient for all three loopback interfaces. Point to point networks commonly use the /30 subnet mask, since in any point to point link, only two hosts are needed (one for the serial interface of the router at each end). Finally, the subnet mask of /26 will provide for 62 useable addresses and the final subnet mask of /25 will provide for 126 useable IP hosts on the second Ethernet network.
Incorrect Answers:
B. This answer includes /32 network masks for the Pt-Pt links, which can not be used for the two point to point links, since they do not provide any useable IP addresses.
C. This answer includes /32 network masks for the Pt-Pt links, which can not be used for the two point to point links, since they do not provide any useable IP addresses. In addition, the subnet mask of /27 provides for only 30 useable IP addresses for the two Ethernet segments.
D. The /27 subnet mask will provide for only 30 useable IP addresses for one of the Ethernet networks, which is insufficient.
Note: Until IOS version 12.2, a /31 address could not be used for point to point links because it does not provide useable IP addresses. However, /31 addressing for point to point links has been an option in Cisco IOS since version 12.2 and is an IEEE standard defined in RFC 3021 http://www.faqs.org/rfcs/rfc3021.html

QUESTION 102
What option is the best way to apply CIDRI if a service provider wants to summarize the following addresses: 200.1.0.0/16, 200.2.0.0/16, 200.3.0.0/16, 200.5.0.0/16, 200.6.0.0/16, 200.7.0.0/16?

A. 200.0.0.0/14, 200.4.0.0/15, 200.6.0.0/16, 200.7.0.0/16
B. 200.0.0.0/16
C. 200.4.0.0/14, 200.2.0.0/15, 200.2.0.0/16, 200.1.0.0/16
D. 200.4.0.0/14, 200.2.0.0/15, 200.1.0.0/16
E. 200.0.0.0/18

Answer: D

Explanation:
The Network 200.4.0.0/14 will encompass the 200.5.0.0, 200.6.0.0 and 200.7.0.0 networks. The second summarization, 200.2.0.0/15 will take care of both the 200.2.0.0 and 200.3.0.0 networks. Finally, the last network is needed in order to include the only remaining network, which is 200.1.0.0/16. This will summarize all 6 networks using only 3 statements.
Incorrect Answers:

A. Although this answer will also fulfill the needs of summarizing all 6 networks, it is not the most efficient way as 4 network entries are needed here, instead of only 3 in answer choice D.
B. This will mean that only the 200.0.0.0/16 network is advertised, which is not even one of the networks that need to be summarized.
C. This is also not the most efficient choice, as the third statement (200.2.0.0/16) is redundant, since this network is already included in the 200.2.0.0/15 summarized route.
E. This network mask would not include all of the needed networks.

QUESTION 103
Which Network Address Translation type describes the internal network that uses private network addresses?

A. Inside local
B. Inside global
C. Outside local
D. Outside global
E. None of the above

Answer: A

Explanation:
Cisco uses the term inside local for the private IP addresses and inside global for the public IP addresses. The enterprise network that uses private addresses, and therefore that needs NAT, is the "inside" part of the network. The Internet side of the NAT function is

the "outside" part of the network. A host that needs NAT has the IP address it uses inside the network, and it needs an IP address to represent it in the outside network.
Incorrect Answers:
B. The inside global address is a legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.
C. The outside local address is the IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.
D. The outside global address the IP address assigned to a host on the outside network by the host's owner. The address is allocated from a globally routable address or network space.

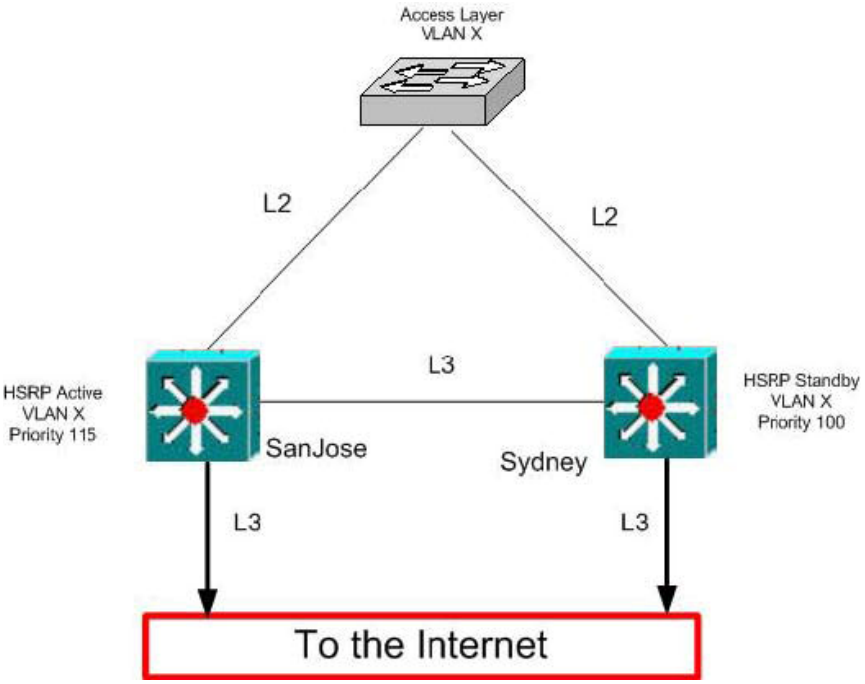
QUESTION 104
A network administrator of Certkiller .com is using a private IP address space for the company network with many to one NAT to allow the users to have access to the Internet. Shortly after this, a web server is added to the network. What must be done to allow outside users access to the web server via the Internet?

A. Use a dynamic mapping with the reverse keyword.
B. Place the server's internal IP address in the external NAT records.
C. There must be a static one to one NAT entry for the web server's address.
D. Nothing more needs to be done as dynamic NAT is automatic.
E. Place the server's IP address into the NAT pool.

Answer: C

Explanation:
Without a static NAT mapping, the server will be NATed out of the NAT pool. Sine many to one NAT (PAT) uses dynamic port mapping, no outside stations will be able to reach the server consistently.

QUESTION 105
The Certkiller LAN is displayed below:



Users in VLAN X behind the Access Layer switch complain that they cannot access the Internet when both layer 3 links in the San Jose switch fail. When only one of the L3 links in San Jose fail, users are still able to get to the Internet. Which command should be used to ensure connectivity to the Internet, even if both L3 San Jose links fail?

A. Standby track
B. Standby timer
C. Standby authentication
D. Standby use-bia
E. Standby priority

Answer: A

Explanation:
Interface tracking allows you to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group.
If the specified interface's line protocol goes down, the HSRP priority of this router is reduced, allowing another HSRP router with higher priority to become active.
Incorrect Answers:
B. Standby timer is used to set the hello time between HSRP routers.
C. Standby authentication is used as a security measure between HSRP routers, using a password authentication process.
D. By default, HSRP uses the preassigned HSRP virtual MAC address on Ethernet and FDDI, or the functional address on Token Ring. To configure HSRP to use the interface's burnt-in address as its virtual MAC address, instead of the default, use the standby usebia command.
E. The priority is used to determine which router will be the active one.

Reference:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm

---

QUESTION 106
A diskless workstation boots up and uses BOOTP to obtain the information it needs from a BOOTP server. How will the diskless client obtain the information it needs from the server?

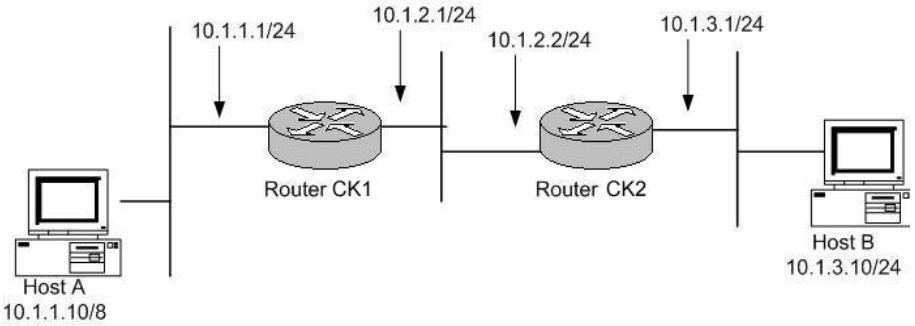
A. The BootP client will use a telnet application to connect to the server, after which the client will use the DHCP server to get hold of the memory image.
B. The BootP client will obtain the memory image after which the client will use a second protocol to gather the necessary information.
C. The BootP client will use a second protocol to gather the necessary information, and then the BootP server will send memory image.
D. The BootP server will gather and provide the client with the information necessary to obtain an image and then the client will use a second protocol to obtain the memory image.
E. None of above.

Answer: D

Explanation:
This RFC describes an IP/UDP bootstrap protocol (BOOTP), which allows a diskless client machine to discover its own IP address, the address of a server host, and the name of a file to be loaded into memory and executed. The bootstrap operation can be thought of as consisting of TWO PHASES. This RFC describes the first phase, which could be labeled `address determination and boot file selection'. After this address and filename information is obtained, control passes to the second phase of the bootstrap where a file transfer occurs. The file transfer will typically use the TFTP protocol, since it is intended that both phases reside in PROM on the client. However BOOTP could also work with other protocols such as SFTP or FTP. This RFC suggests a proposed protocol for the ARPA-Internet community, and requests discussion and suggestions for improvements.
BOOTP procedure summary.
Diskless workstation broadcasts a bootp request on port 67. Server responds to this request on port 68. Server provides the client with two pieces information.
1.IP address of client and Hostname of the Server.
2.File name required by client to boot.
The Client then uses TFTP to obtain this file from the Server and boot.
Incorrect Answers:

A. Telnet is not used.
B. The memory image is the last step, not the first.
C. The client must first receive some basic information before using a second protocol, such as TFTP.

QUESTION 107
You want to ensure that Host A has connectivity with Host B. Host A and Host B are connected via Router CK1 and Router CK2 . A has an 8 bit network mask while Host B has a 24 bit network mask. The Certkiller network is shown in the following exhibit. No routing protocols or static routes are configured on either CK1 or CK2 .



Which of the following is required to enable Host A to send packets to Host B?

A. Host A must have a default gateway address of 10.1.1.1.
B. Host B must have a default gateway address of 10.1.3.1.
C. Proxy ARP must be enabled on Router CK1 .
D. Proxy ARP must be enabled on Router CK2 .
E. Host A will not be able to reach host B until routing is enabled in this network.

Answer: B, C

Explanation:
The default gateway for any host must reside on the same subnet as that host so Host B must have its default gateway set to CK2 . In order for packets to reach host B, then host A must have its default gateway set to CK2 also. This will only work if proxy ARP is enabled on CK1 . This is because Host A will assume that Host B is on the same network statement, because its subnet mask is /8. It will therefore ARP to reach Host B. Because of this, CK1 must have proxy ARP enabled to pass the request on to Host B.
For the return traffic, Host B must use a default gateway, because for it to reach Host A a default gateway must be used since it is on a different network segment.
Incorrect Answers:

A. If host A sets its default gateway to CK1 , then it will not be able to send traffic to host B, since no routing exists. All hosts must have a default gateway that resides on the same LAN subnet.
D. Proxy ARP needs to be enabled on CK1 , not CK2 , to pass the traffic to host B.

QUESTION 108
Which of the following DNS resource records are valid? (Choose all that apply)

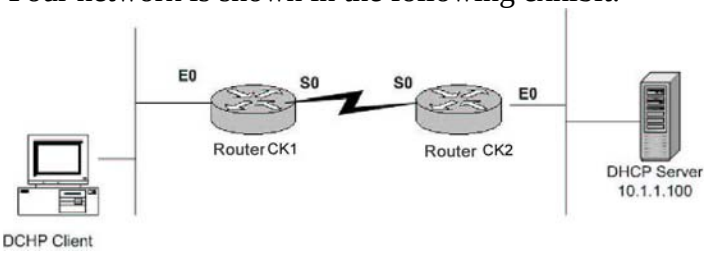
A. NS
B. PTR
C. MX
D. FQDN

E. A
F. None of the above

Answer: A, B, C, E

Explanation:
NS (Name Service), PTR (Pointer), MX (Mail Exchange), and A records are all DNS resource record types.
Incorrect Answers: D
FQDN is Fully Qualified Domain name, for example, www.cisco.com. It has nothing do with DNS Resource Records.

QUESTION 109
Your network is shown in the following exhibit:



You want all PC's at CK1 to be able to obtain their IP address dynamically from the DHCP server that resides at CK2 . Currently, the hosts are not able to obtain an IP address, and they are receiving error messages saying that the DHCP server is busy or is unavailable. What must be done to enable these PC's to obtain dynamic IP addresses.

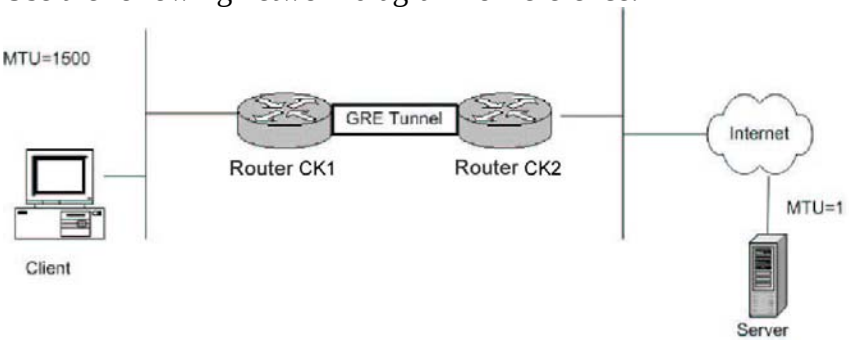
A. Enable the command "ip helper-address 10.1.1.100" under the S0 interface on Router CK1 .
B. Enable the command "ip helper-address 10.1.1.100" under the E0 interface on Router CK1 .
C. Enable the command "ip helper-address 255.255.255.255" under the E0 interface on Router CK1 .
D. Enable the command "ip helper-address 255.255.255.255" under the S0 interface on Router CK2 .
E. Enable the command "ip helper-address 10.1.1.100" in global configuration mode on router CK1 .
F. Enable the command "ip helper-address 10.1.1.100" in global configuration mode on router CK2 .

Answer: B

Explanation:
By default, routers drop all broadcast packets sent through them. Because DHCP clients use BOOTP packets, which are broadcasted to all hosts (255.255.255.255), they will be dropped by router CK1 . The "ip helper-address" command enables the router to forward these BOOTP broadcast packets to a specific host, as specified by the address following

the "ip helper-address" command. Note that this command must be placed on the router's interface that is receiving the broadcast packets from the hosts, which is E0 of the CK1 router.

QUESTION 110
Use the following network diagram for reference:



There is a GRE tunnel between two routers, CK1 and CK2 . Small files can be sent and received through this tunnel, but large files can not. In addition to this, many web pages are not able to be seen.
On CK1 , you issue the "debug ip icmp" command and try to ping the server with IP address 10.1.1.1 and see the following:
ICMP: dst (10.10.10.10) frag. needed and DF set unreachable sent to 10.1.1.1
How can this problem be solved? (Choose all that apply.)

A. Ensure that no filters exist between the tunnel endpoints blocking ICMP.
B. Increase the IP MTU on the tunnel interfaces to 1500.
C. Enable "ip unreachables" on all interfaces on Router CK2 .
D. Decrease the physical interface MTU on the serial interfaces of CK1 and CK2 to less than 1476 bytes.
E. If the physical link between Router CK1 and Router CK2 is able to support a MTU size greater than 1524 bytes, then increase the interface MTU between the tunnel end points to match 1524.

Answer: A, E
Reference:
Refer to "Why Can't I Browse the Internet when Using a GRE Tunnel?"
http://www.cisco.com/warp/public/105/56.html

QUESTION 111
Select the mode that NTP servers can associate with each other:

A. Client and Server
B. Peer
C. Broadcast/Multicast
D. B and C
E. All the above

Answer: B

Explanation:
NTP synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and other time-specific events occur. An NTP association can be a peer association (meaning that this system is willing to either synchronize to the other system or to allow the other system to synchronize to it), or it can be a server association (meaning that only this system will synchronize to the other system, and not the other way around). An NTP server can only be configured as a peer to another NTP server.

QUESTION 112
A customer wants to install a new frame-relay router in their network. One goal is to ensure that the new router has the correct configuration to maintain a consistent time and date, like the other routers in the network. The customer wants to configure the new router to periodically poll a UNIX server that has a very reliable and stable clock for the correct time. This will synchronize the new router's clock with the UNIX server. What command should be configured on the new router to synchronize its clock with a centralized clock service?

A. ntp master
B. ntp server
C. ip ntp clock
D. ntp peer
E. sntp master
F. All of the above

Answer: B

Explanation:
To allow the system clock to be synchronized by a time server, use the ntp server global configuration command.
Incorrect Answers:

A. This command will configure the router to act as the NTP master server, providing time information to other devices.
C. This is an invalid command.
D. Use this command if you want to allow the router to synchronize with an NTP peer, or vice versa.
E. SNTP is a simpler version of NTP used by lower end Cisco devices. If SNTP were to be used, the correct syntax would be "sntp server" and not "sntp master."

QUESTION 113
What should be configured on redundant routers to support the need for a default gateway on LAN network hosts when there are two gateway routers providing

connectivity to the rest of the network?

A. DHCP
B. RIP
C. OSPF
D. HSRP
E. BOOTP

Answer: D

Explanation:
The Hot Standby Router Protocol (HSRP) provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from default gateway failures in the network. It is implemented on networks where there are two or more gateway routers that provide connectivity to the rest of the network with the standby router acting as an automatic failover should the primary router fail.
Incorrect Answers:
A, E: DHCP and BOOTP are used to provide IP addressing, DNS, and default gateway information to end user hosts.
B, C: RIP and OSPF are routing protocols, and will not provide for automatic default gateway redundancy for PC hosts.

QUESTION 114
With regard to the File Transfer Protocol (FTP), which of the following statements are true?

A. FTP always uses one TCP session for both control and data.
B. With passive mode FTP, both the control and data TCP sessions are initiated from the client.
C. With active mode FTP, the server used the "PORT" command to tell the client on which port it wished to send the data.
D. FTP always uses TCP port 20 for the data session and TCP port 21 for the control session.
E. FTP always uses TCP port 20 for the control session and TCP port 21 for the data session.

Answer: B

Explanation:
For a detailed discussion on FTP refer the link below.
Incorrect Answers:

A. FTP always uses two separate TCP sessions, one for control and one for data.
C. In FTP active mode the client (not the server) uses the PORT command to tell the server on which port it expects the server to send the data.
D, E. These statements are too general as FTP behaves differently based on whether the

mode of operation is active or passive.
Reference:
http://www.cisco.com/warp/public/759/ipj_2-3/ipj_2-3_oneb.html

---

QUESTION 115
You use a telnet application to access your Internet router. What statement is true about the telnet application?

A. Telnet does not use a reliable transport protocol.
B. Telnet is a secure protocol because it encrypts every message sent.
C. Telnet sends user names, passwords and every other message in clear text.
D. Telnet encrypts user names, passwords but sends every other message in clear text.
E. Telnet uses UDP as transport protocol.

Answer: C

Explanation:
Telnet is inherently insecure since it sends all data in plain text. This is an important consideration when using telnet across the Internet. For this reason, more secure remote access applications such as SSH have been developed.
Incorrect Answers:
A, E: Telnet uses TCP port 23, which is a reliable protocol.
B, D: No portion of a telnet packet is encrypted or authenticated.

QUESTION 116
What is the method used by SMTP servers on Internet to validate the e-mail address of the message sender?

A. It checks the user address with the MTA sending the message.
B. It validates the domain of the sender address with a DNS server.
C. It does not check the sender address.
D. It checks if the IP address of the MTA sending the message is not spoofed.
E. It checks if the domain of the MTA sending the message matches with the domain of the sender of the message.

Answer: C

Explanation:
When e-mail is handed off today from one organization to another, as a rule no authentication of the sender of the e-mail or the computers delivering it on the sender's behalf takes place.
Due to the spread of SPAM and emails coming from spoofed locations, measures can be taken to minimize their effect. The MTA Authentication Records in DNS Internet Draft describes mechanisms by which a domain owner can publish its set of outgoing Mail Transfer Agents (MTAs), and mechanisms by which SMTP servers can determine what

email address is allegedly responsible for most proximately introducing a message into the Internet mail system, and whether that introduction is authorized by the owner of the domain contained in that email address.
However, as a standard rule today, no SMTP server is required to take any security measures to validate the message sender.

QUESTION 117
Upon which protocol or protocols does TFTP rely on?

A. IP and TCP
B. NFS
C. FTP
D. UDP
E. ICMP and UDP
F. TCP

Answer: D

Explanation:
The Trivial File Transfer Protocol (TFTP) is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password). TFTP uses UDP port 69.

QUESTION 118
Identify the TCP port numbers with their associated programs: 443, 389, 137, 110, and 23 in the proper sequence:

A. BGP, POP3, SNMP, TFTP, Telnet
B. LDAP, SNMP, TFTP, POP3, Telnet
C. HTTPS, SNMP, POP3, DNS, Telnet
D. Finger, DHCP Server, NetBios Name Server, POP3, Telnet
E. HTTPS, LDAP, NetBios Name Server, POP3, Telnet
F. None of the above

Answer: E

Explanation:
The following shows the TCP port numbers used with the associated applications:
HTTPS (secure WWW): 443
LDAP: 389 on the directory server
NetBios Name Server: 137
POP3: 110
Telnet: 23
Incorrect Answers:

A. BGP uses TCP port 179.

B, C. SNMP uses TCP port 161.
D. Finger uses TCP port 79 while DHCP uses 67 (BOOTP)
A complete list of TCP port numbers and their assignments can be found here:
http://www.iana.org/assignments/port-numbers

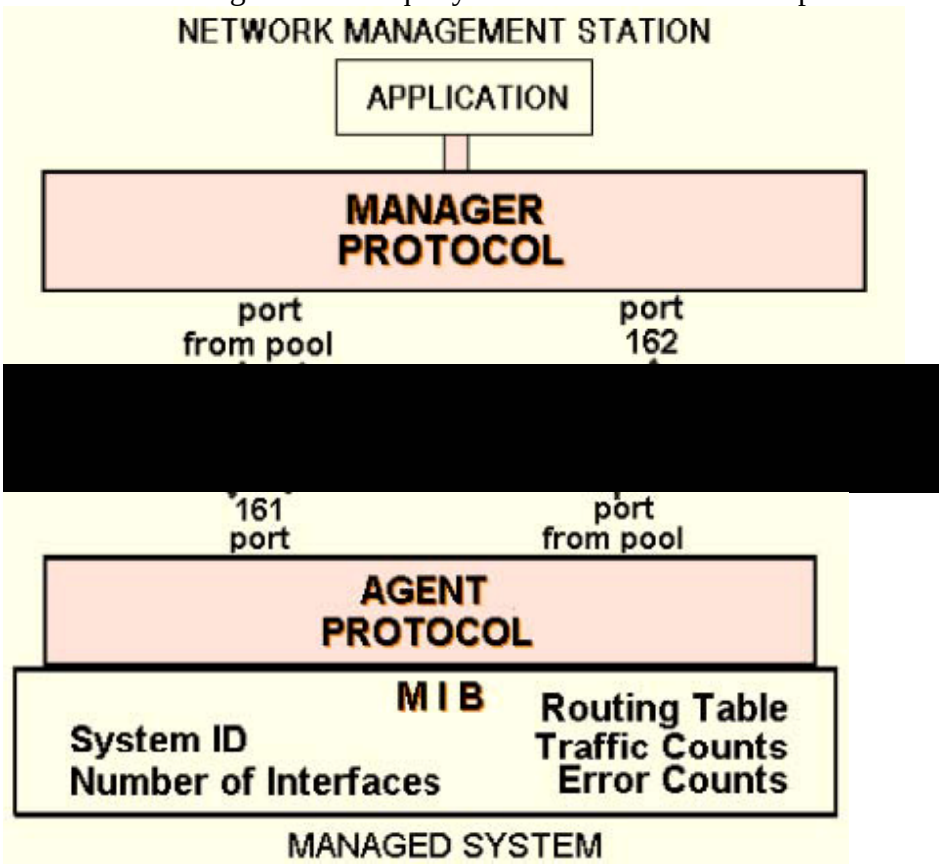
QUESTION 119
On what lower level transport protocol does SNMP rely and why?

A. TCP, because SNMP requires the reliability of TCP, which ensures packets are transmitted reliably, in event that a packet is lost in the network.
B. UDP, because SNMP is an application that does not require the reliability provided by TCP.
C. IP, because SNMP requires the reliability of IP packets, which can detect lost packets and retransmit them if required.
D. UDP, because SNMP is an application that requires the reliability of UDP and UDP's ability to detect lost packets and retransmit them.
E. TCP, because SNMP is an application that does not require detection and retransmission of lost packets.

Answer: B

Explanation:
SNMP uses the User Datagram Protocol (UDP) as the transport protocol for passing data between managers and agents. UDP, defined in RFC 768, was chosen over the Transmission Control Protocol (TCP) because it is connectionless; that is, no end-to-end connection is made between the agent and the NMS when datagrams (packets) are sent back and forth. This aspect of UDP makes it unreliable, since there is no acknowledgment of lost datagrams at the protocol level. It's up to the SNMP application to determine if datagrams are lost and retransmit them if it so desires. This is typically accomplished with a simple timeout. The NMS sends a UDP request to an agent and waits for a response. The length of time the NMS waits depends on how it's configured. If the timeout is reached and the NMS has not heard back from the agent, it assumes the packet was lost and retransmits the request. The number of times the NMS retransmits packets is also configurable.
At least as far as regular information requests are concerned, the unreliable nature of UDP isn't a real problem. At worst, the management station issues a request and never receives a response. For traps, the situation is somewhat different. If an agent sends a trap and the trap never arrives, the NMS has no way of knowing that it was ever sent. The agent doesn't even know that it needs to resend the trap, because the NMS is not required to send a response back to the agent acknowledging receipt of the trap.
The upside to the unreliable nature of UDP is that it requires low overhead, so the impact on your network's performance is reduced. SNMP has been implemented over TCP, but this is more for special-case situations in which someone is developing an agent for a proprietary piece of equipment. In a heavily congested and managed network, SNMP over TCP is a bad idea. It's also worth realizing that TCP isn't magic, and that SNMP is designed for working with networks that are in trouble -- if your network never failed,

you wouldn't need to monitor it. When a network is failing, a protocol that tries to get the data through but gives up if it can't is almost certainly a better design choice than a protocol that will flood the network with retransmissions in its attempt to achieve reliability.
SNMP uses the UDP port 161 for sending and receiving requests, and port 162 for receiving traps from managed devices. Every device that implements SNMP must use these port numbers as the defaults, but some vendors allow you to change the default ports in the agent's configuration. If these defaults are changed, the NMS must be made aware of the changes so it can query the device on the correct ports.



SNMP use of UDP port numbers.

QUESTION 120
In your network, you want the ability to send some traffic around less congested links. To do this, you want to bypass the normal routed hop-by-hop paths. What technology should you implement?
What should you use?

A. Traffic engineering
B. Traffic tunneling
C. Traffic policing
D. Traffic shaping
E. Traffic routing

Answer: A

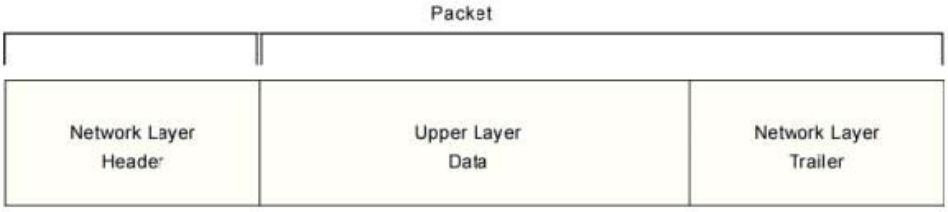
Explanation:
Traffic engineering allows you to bypass the routing protocol information to send traffic over alternative paths.
Incorrect Answers:
B. Using tunnels will not force the traffic over the tunnels to bypass the normal hop by hop routed topology.
C, D. Traffic policing and traffic shaping are methods of QoS.
E. Traffic routing is not a well defined Cisco term.

QUESTION 121
Which of the following are found in a basic Network Layer Packet? (Choose all that apply)

A. Network Layer Trailer
B. Upper Layer Data
C. Network Layer Data
D. Network Layer Header
E. Data Link Layer Header
F. Checksum

Answer: A, B, and D

Explanation:
A packet is an information unit whose source and destination are network-layer entities. A packet is composed of the network-layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the network-layer entity in the destination system. Data from upper-layer entities is encapsulated in the network-layer header and trailer. The figure illustrates the basic components of a network-layer packet.



QUESTION 122
The Certkiller network is shown in the following exhibit:

Host Certkiller 3 sends a message to host Certkiller 4. Which type of delivery is this?

A. Direct delivery
B. Partial delivery
C. Installment delivery
D. Indirect delivery
E. Instant delivery
F. Guarantee delivery

Answer: A.

Explanation:
Direct delivery implies that both the devices are on the same network segment (IP subnet) and no router is required for communication between the two.
Incorrect Answers:
D. In indirect delivery the two devices are on different network segments (IP subnets) and a router will be required for the two to communicate.

QUESTION 123
Real Time Protocol uses which of the following as the transport mechanism?

A. RTCP
B. UDP
C. TCP
D. BRI/ISDN
E. None of the above.

Answer: B

Explanation:
RTP uses UDP for transport.
Incorrect Answers:

A. There is no such thing as RTCP.
C. Since RTP is used for real time traffic, it would not make sense to use TCP for transport, as it provides more overhead that UDP. In addition, the reliable mechanism of TCP is useless for real time traffic such as voice and video traffic, since packets that are resent are too late too late.

QUESTION 124
What should be used to compress Voice over IP packets on a low-speed Frame Relay circuit?

A. TCP header compression
B. FRF.9 payload compression
C. Cisco proprietary payload compression
D. RTP header compression
E. Predictor payload compression

Answer: D

Explanation:
Since VOIP uses the real time protocol (RTP), compressing this type of traffic will be best. RTP is the Internet-standard protocol for the transport of real-time data. It is intended to provide end-to-end network transport functions for applications that support audio, video, or simulation data over multicast or unicast network services.
RTP provides support for real-time conferencing of groups of any size within the Internet. This support includes source identification and support for gateways such as audio and video bridges as well as multicast-to-unicast translators. RTP offers QoS feedback from receivers to the multicast group, as well as support for the synchronization of different media streams.
RTP includes a data portion and a header portion. The data portion of RTP is a thin protocol that provides support for the real-time properties of applications, such as continuous media, including timing reconstruction, loss detection, and content identification.
The header portion of RTP is considerably large. The minimal 12 bytes of the RTP header, combined with 20 bytes of IP header (IPH) and 8 bytes of UDP header, create a 40-byte IP/UDP/RTP header. For compressed-payload audio applications, the RTP packet typically has a 20-byte to 160-byte payload. Given the size of the IP/UDP/RTP header combinations, it is inefficient to transmit the IP/UDP/RTP header without compressing it.
To avoid the unnecessary consumption of available bandwidth, the RTP header compression feature-referred to as CRTP-is used on a link-by-link basis.
RTP can be used over frame relay, HDLC, and PPP links and is meant to be used over slow links (less that 2 Mbps).

QUESTION 125
What best describes the IPv6 Solicited-node Multicast address?

A. For each unicast and anycast addresses configured on an interface of the node or a router, a corresponding solicited-node multicast addresses is automatically enabled.
B. The solicited-node multicast address is scoped at the local link.
C. Since ARP is not used the in IPv6, the solicited-node multicast addresses is used by nodes and router to learn the link layer address of the neighbor nodes and routers on the same local link.
D. Duplicate Address Detection (DAD) is used to verify if the IPv6 address is already in used on it's local link, before it configure it's own IPv6 address with stateless auto-configuration, Solicited-node multicast addresses probe the local link to make sure.
E. All of the above
F. None of the above

Answer: E

Explanation:
In IP version 6, the solicited-node multicast address facilitates efficient querying of network nodes during address resolution. IPv6 uses the Neighbor Solicitation message to perform address resolution. In IPv4, the ARP Request frame is sent to the MAC-level broadcast, disturbing all nodes on the network segment regardless of whether a node is running IPv4. For IPv6, instead of using ARP requests and disturbing all IPv6 nodes on the local link by using the local-link scope all-nodes address, the solicited-node multicast address is used as the Neighbor Solicitation message destination.
The solicited-node multicast address consists of the prefix FF02::1:FF00:0/104 and the last 24-bits of the IPv6 address that is being resolved.
The following steps show an example of how the solicited-node address is handled for the node with the link-local IPv6 address of FE80::2AA:FF:FE28:9C5A, and the corresponding solicited-node address is FF02::1:FF28:9C5A:
1. To resolve the FE80::2AA:FF:FE28:9C5A address to its link layer address, a node sends a Neighbor Solicitation message to the solicited-node address of FF02::1:FF28:9C5A.
2. The node using the address of FE80::2AA:FF:FE28:9C5A is listening for multicast traffic at the solicited-node address FF02::1:FF28:9C5
A. For interfaces
that correspond to a physical network adapter, it has registered the corresponding multicast address with the network adapter.
As shown in this example, by using the solicited-node multicast address, address resolution that commonly occurs on a link can occur without disturbing all network nodes. In fact, very few nodes are disturbed during address resolution. Because of the relationship between the network interface MAC address, the IPv6 interface ID, and the solicited-node address, in practice, the solicited-node address acts as a pseudo-unicast address for efficient address resolution.
Reference: http://msdn.microsoft.com/library/default.asp?url=/library/enus/wcetcpip/html/cmconmulticastipv6addresses.asp

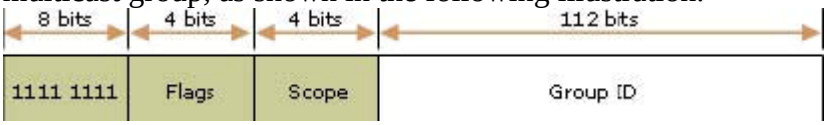
---

QUESTION 126
What is a main difference between the IPv6 and IPv4 multicast?

A. IPv6 has significantly more address space (128 bits), so overlapping addresses are less likely.
B. Multicast Listener Discovery (MLD) replaces IGMP in IPv6 multicasts.
C. MSDP and dense mode multicast is not part of IPv6 multicast.
D. The first 8 bits of Ipv6 Multicast address are always FF (1111 1111).
E. All of the above

Answer: E

Explanation:
A multicast address identifies multiple interfaces, and is used for one-to-many communication. With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address.
IPv6 multicast addresses have the Format Prefix of 1111 1111. An IPv6 address is simple to classify as multicast because it always begins with FF. Multicast addresses cannot be used as source addresses.
Multicast addresses include additional structure to identify their flags, scope, and multicast group, as shown in the following illustration.



MLD is used to exchange membership status information between IPv6 routers that support multicasting and members of multicast groups on a network segment. Membership in a multicast group is reported by individual member hosts, and membership status is periodically polled by multicast routers. MLD is defined in RFC 2710, "Multicast Listener Discovery (MLD) for IPv6." IGMP is not used in IPv6.

QUESTION 127
What best describes the functionality of the Multicast Listener Discovery (MLD)?

A. IPv6 routers use MLD to discover multicast listeners on directly attached links.
B. For each Unicast and Anycast addresses configured on an interface of the node or a router, a corresponding entry is automatically enabled.
C. The MLD addresses is scoped to the local link.
D. Since the ARP is not used in the IPv6, the MLD is used by nodes and routers to learn the link layer address of the neighbor nodes and routers on the same local link.
E. MLD is used to verify if the IPv6 address is already in use on it's local link, before it configure it's own IPv6 address with stateless auto-configuration.

Answer: A

Explanation:

The purpose of Multicast Listener Discovery (MLD) is to enable each IPv6 router to discover the presence of multicast listeners (that is, nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. This information is then provided to whichever multicast routing protocol is being used by the router, in order to ensure that multicast packets are delivered to all links where there are interested receivers.
MLD is an asymmetric protocol, specifying different behaviors for multicast listeners and for routers. For those multicast addresses to which a router itself is listening, the router performs both parts of the protocol, including responding to its own messages.
If a router has more than one interface to the same link, it need perform the router part of MLD over only one of those interfaces. Listeners, on the other hand, must perform the listener part of MLD on all interfaces from which an application or upper-layer protocol has requested reception of multicast packets.

QUESTION 128
Which types of SNMPv1 messages are sent from the NMS (Network Management Station) using SNMP version 1 to the Agent?

A. Trap, Get and Set
B. Get, Set and Getnext
C. Get, Set, Getnext and GetBulk
D. Get, Set and GetBulk
E. Trap only

Answer: B

Explanation:
SNMP itself is a simple request/response protocol, and the SNMPv1 operations used by the NMS are defined as below.
Get: Allows the NMS to retrieve an object variable from the agent.
GetNext: Allows the NMS to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a NMS wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set: Allows the NMS to set values for object variables within an agent.
Incorrect Answers:
A, E. SNMP traps are used by the agent to inform the NMS of some events.
C, D. GetBulk is used in SNMPv2, not version 1. SNMPv2 defines two new operations: GetBulk and Inform. The GetBulk operation is used to efficiently retrieve large blocks of data. The Inform operation allows one NMS to send trap information to another NMS and to then receive a response. In SNMPv2, if the agent responding to GetBulk operations cannot provide values for all the variables in a list, it provides partial results.

QUESTION 129
What is the difference between the community formats of SNMPv1 SNPMv2c?

A. With SNPMv1, communities are sent as clear text and on SNPMv2c they are

encrypted.
B. On SNPMv1 communities are encrypted and on SNPMv2c they are sent as clear text.
C. There is no difference because both versions send encrypted communities.
D. There is no difference because both versions send communities as clear text.
E. SNMPv2c does not use communities.

Answer: D

Explanation:
The original Internet standard Network Management Framework, described in RFCs 1155, 1157, and 1213, is called the SNMP version 1 (SNMPv1) framework. Relevant portions of the proposed framework for version 2C of the Simple Network Management Protocol (SNMPv2C) are described in RFCs 1901 through 1908.
SNMPv1 and SNMPv2c use a community string match for user authentication. Community strings provided a weak form of access control in earlier versions of SNMP. SNMPv3 provides much improved access control using strong authentication and should be preferred over SNMPv1 and SNMPv2c wherever it is supported. Both versions send communities as clear text messages.

QUESTION 130
Network management tools use Management Information Base (MIB) information to monitor and manage networks. Which of the following is NOT part of the MIB-2 specification, as defined in RFC 1213? (Choose all that apply)

A. The System Group
B. The TCP Group
C. The Transmission Group
D. The Enterprises Group
E. The RMON Group
F. The ICMP Group

Answer: D, E

Explanation:
RFC 1213 defines the "Management Information Base for Network Management of TCP/IP-based internets: MIB-II" specification. It defines all of the following groups: System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, EGP, Transmission, and SNMP. The RMON group is not part of RFC 1213, nor is the Enterprises Group

---

QUESTION 131
Which statements are true about the purpose and functionality between SNMP and MIBs? (Select three)

A. A Management Information Base (MIB) is a collection of information that is organized hierarchically.

B. A Management Information Base (MIB) is a collection of network device information that is organized in a bulk transfer mode to the management station.
C. MIBs are accessed using a network-management protocol such as SNMP.
D. MIBs are accessed using a network-management protocol such as TCP.
E. MIBs are comprised of managed objects and are identified by the object identifiers.
F. MIBs are comprised of managed objects and are identified by the lmhosts table.

Answer: A, C, E

Explanation:
The Cisco MIB variables are accessible via the Simple Network Management Protocol (SNMP), which is an application-layer protocol designed to facilitate the exchange of management information between network devices. The SNMP system consists of three parts: SNMP manager, SNMP agent, and MIB.
The MIB structure is logically represented by a tree hierarchy. The root of the tree is unnamed and splits into three main branches: Consultative Committee for International Telegraph and Telephone (CCITT), International Organization for Standardization (ISO), and joint ISO/CCITT.
Finally, each group of MIB variables is accompanied by an illustration that indicates the specific object identifier for each variable.

QUESTION 132
Which options are true regarding the privacy capability using cryptography and the authentication method for SNMPv1, SNMPv2c and SNMPv3? (Choose all that apply)

A. SNMPv1 has no privacy and uses community for authentication.
B. SNMPv2c has privacy and uses community for authentication.
C. SNMPv2c has privacy and uses usernames for authentication.
D. SNMPv3 has privacy and use community for authentication.
E. SNMPv3 has privacy and uses usernames for authentication.

Answer: A, E

Explanation:
SNMPv1 and SNMPv2 use the notion of communities to establish trust between managers and agents. An agent is configured with three community names: read-only, read-write, and trap. The community names are essentially passwords; there's no real difference between a community string and the password you use to access your account on the computer. The three community strings control different kinds of activities. As its name implies, the read-only community string lets you read data values, but doesn't let you modify the data. For example, it allows you to read the number of packets that have been transferred through the ports on your router, but doesn't let you reset the counters. The read-write community is allowed to read and modify data values; with the read-write community string, you can read the counters, reset their values, and even reset the

interfaces or do other things that change the router's configuration. Finally, the trap community string allows you to receive traps (asynchronous notifications) from the agent.
SNMPv3 not only encrypts all transmissions but also enables the responder (usually an SNMP agent) to authenticate the user generating the request, guarantee the integrity of the message using a digital signature, and apply complex and granular access-control rules to each request. It also lets the administrator specify these levels of protection in varied combinations (unsecured, authenticated and authenticated with encryption). In addition, any number of access-control rules can be applied at the SNMP agent or manager. While this level of security was completely impractical in hardware 10 years ago, today's infrastructure devices have enough RAM and CPU cycles to support not only this advanced SNMP security but also full-fledged Web management services--all in firmware.

QUESTION 133
Which security features are defined in SNMPv3? (Select all that apply)

A. Authentication
B. Domain checking
C. Accounting
D. Privacy

Answer: A, D

Explanation:
SNMP Version 3 (SNMPv3) adds security and remote configuration capabilities to the previous versions. The SNMPv3 architecture introduces the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control.
The principal security enhancements defined in SNMP version 3 is authentication, privacy, and access control.
Incorrect Answers:
B, C. SNMP version 3 provides no defines no mechanisms for checking the domain or accounting.

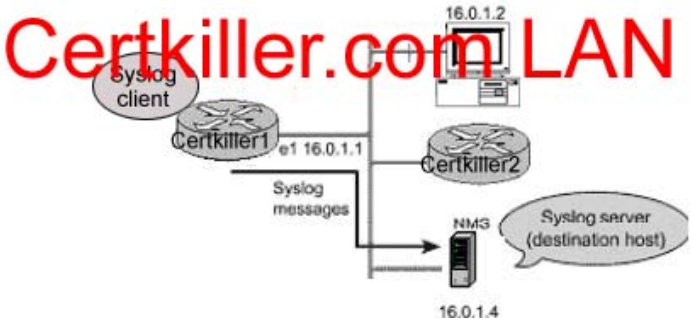
QUESTION 134
What SNMP message type reports events to the NMS reliably?

A. Get
B. Response
C. Inform
D. Trap
E. Get Bulk

Answer: C

Explanation:
SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.
However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform message may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

QUESTION 135
The Certkiller LAN is displayed below:



What should the Cisco IOS commands look like in the Certkiller 1 router to perform the exhibit? Select two.

A. logging source-interface fastethernet 0/0
logging 16.0.1.4
logging facility sys9
logging on
B. logging 16.0.1.4
logging trap debugging
logging facility sys9
logging source-interface serial0
logging on
C. logging 16.0.1.4
logging trap debugging
logging facility sys9
logging source-interface ethernet1
logging on
D. logging 16.0.1.1
logging trap 7
logging source-interface serial 1
logging origin-id ip

Answer: C

Explanation:
In the example displayed above, the syslog server resides at 16.0.1.4 so we will want to send all SNMP traps to this IP address. In addition, the source interface information that should be sent to this server is the ethernet 1 interface, since this is the address used for all messages sent to the server.
Incorrect Answers:

A. In this example the wrong interface source is uses. In addition, the logging level information that should be sent to the server is not specified.
B. Here the wrong interface is configured as the logging source
D. This choice specified the wrong source interface, as well as the wrong IP address of the syslog server.

QUESTION 136
Router CK1 is configured for OSPF. Under the OSPF process, you type in the "area 1 range" command. Which LSA types will be acted upon (summarized) as a result? (Choose all that apply)

A. Type 1
B. Type 2
C. Type 3
D. Type 4
E. Type 5

Answer: A, B

Explanation:
Area range command is used for summarizing routes on the boundary of two OSPF areas. The information to be summarized is contained in two types of LSAs: Type 1 and Type2. Type 1 LSAs are Router LSAs and are generated by each router in an OSPF network. Type 2 LSAs are network LSAs, which are generated by the DR.
Both Type1 and Type 2 LSAs are flooded within the originating area only. Only when the information needs to be conveyed to another area in a summarized form area-range command is used, which acts on the information provided by these two LSAs.
Reference:
CCIE Professional Development Routing TCP/IP Volume I by Jeff Doyle page 471.
Incorrect Answers:
C. Type 3 LSA are the result of type 1 and type 2 summaries that are created by the area range command.
D. Type 4 LSAs are ASBR summary LSAs
E. Type 5 LSAs are AS External LSAs

QUESTION 137
A change in the topology of the Certkiller OSPF network causes the flooding operation. Which OSPF packet types are used in this LSA Flooding?

A. Hello
B. Link State Update
C. Link State Request
D. Database description
E. Link State Acknowledgement

Answer: B, E

Explanation:
A change in the OSPF network topology is represented as a change in one or more of the OSPF Link State Advertisements (LSAs). Flooding is the process by which changed or new LSAs are sent throughout the network, and are used to ensure that the database of every OSPF router is updated and an identical database is maintained. This flooding makes use of two OSPF packet types: Link State Update packets (type 4), and Link State Acknowledgement packets (type 5).
Reference: Jeff Doyle, "Routing TCP/IP volume 1" page 451.

QUESTION 138
Router CK1 is configured for OSPF and is connected to two areas: area 0 and area 1. You then configure area 1 as a stub area. Which LSAs will now operate inside of area 1?

A. Type 7
B. Type 1 and 2
C. Type 1, 2, and 5
D. Type 3 and 4
E. Type 1, 2 and 3

Answer: E

Explanation:
Only type 1, 2, and 3 LSAs will be allowed inside of a stub area.
Incorrect Answers:

A. Type 7 LSAs are used for NSSA, not stubby areas.
B. Network Summary LSAs (Type 3) are also allowed.
Reference:
CCIE Professional Development Routing TCP/IP Volume I by Jeff Doyle page 479.

QUESTION 139
Study the Exhibits below carefully:
The following exhibit is an illustration of the output from an ASBR:
ASBBR#show ip ospf database external
OSPF Router with ID (15.33.4.2) (Process ID 10)
Type-5 AS External Link States

LS age: 15
Options: (No TOS-capability, DC)
LS Type: AS External Link
Link State ID: 10.10.1.0 (External Network Number)
Advertising Router: 15.33.4.2
LS Seq Number: 80000002
Checksum: 0x513
Length: 36
Network Mask: /24
Metric Type: 1 (Comparable directly to link state
metric)
TOS: 0
Metric: 10
Forward Address: 0.0.0.0
External Route Tag: 0
And this exhibit is an illustration from a router in the network:
Router CK1 #show ip ospf border-routers
OSPF Process 10 internal Routing Table
Codes: i-intra-area route, I-Inter-area route
15.33.4.2(2) via 30.0.0.1, Serial0/0, ASBR, Area0, SPF 4
Based on this information what is the total metric for the route to subnet
10.10.1.0/24 on Router CK1 ?

A. 1
B. 8
C. 12
D. 20
E. 22

Answer: C

Explanation:
The metric of the external link shows 10. Then we need to add 2 from the inter-area
metric, for a total of 12.

QUESTION 140
In your OSPF network serial 0 on your router, CK1 , is in area 1. Later, you
configure serial 0 as passive. What is the effect of this configuration change?

A. OSPF will accept the routing updates from neighbors.
B. OSPF will form all the available adjacencies out of that interface.
C. OSPF will not insert any of the learned routes in the local routing table.
D. OSPF will not form any adjacency out of that interface.
E. None of the above.

Answer: D

Explanation:
With passive-interface, an adjacency will never occur out of that interface, as no hello packets are exchanged out of a passive interface.
Incorrect Answers:

A. Normally, defining an interface as passive will accomplish this. No routes will be sent out, but routes can still be received. OSPF differs because link state protocols need information for the entire network topology. Defining an interface as passive with OSPF means that the adjacency will not be established, therefore, no routes will be able to be received on that interface.

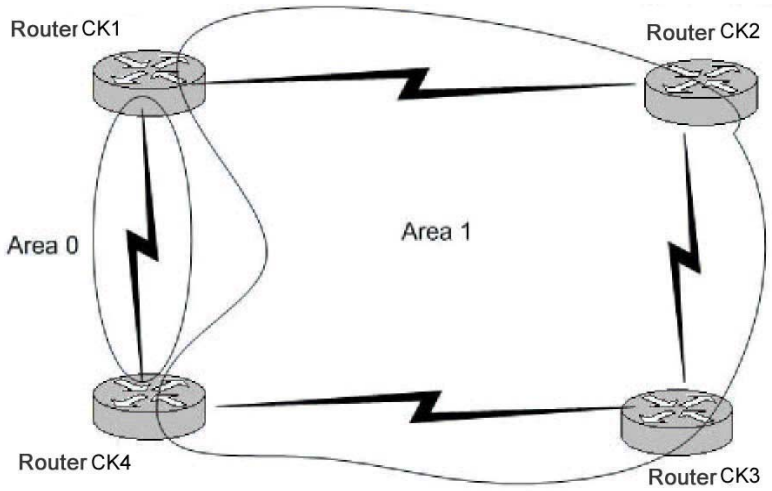
QUESTION 141
You are the network administrator at Certkiller . The Certkiller network contains four Routers named CK1 , CK2 , CK3 , and CK4 . All four routers are connected to a hub via Ethernet interfaces. All four routers have a basic OSPF configuration of a network statement for the Ethernet network. During routine maintenance, you issue the show ip ospf neighbor command on Router CK2 . The output from the show ip ospf neighbor command shows 2WAY/DROTHER for its neighbor, Router CK3 .
What conclusions can you draw from this output? (Choose all that apply)

A. Router CK2 is the DR or BDR.
B. Router CK3 is not a DR or BDR.
C. Router CK2 - Router CK3 adjacency is not yet FULL.
D. Router CK2 is not the DR.
E. Router CK4 is the DR.

Answer: B, D

Explanation:
OSPF routers can have one of three neighbor relationships: Designated Router (DR), Backup Designated Router (BDR), or neither. For neither, the router neighbor relationship will show as 2WAY/DROTHER.
Incorrect Answers:
A, C. 2WAY/DROTHER means that the two routers are neither the DR nor the BDR.
E. Either Router CK1 or Router CK4 is the DR. Based on the information that is provided we cannot be sure which one it is.

QUESTION 142
The following exhibit displays the Certkiller OSPF network:



Router CK2 needs to send a string of packets to router CK4 . How will router CK2 decide the path to take to reach CK4 ?

A. CK2 will select a path after considering the costs inside Area 1 only.
B. CK2 will alternate between Router CK1 and Router CK3 if the costs are equal.
C. CK 2 will always go through Router CK1 with no regard for costs.
D. CK2 will select a path after considering the costs inside both Area 0 and Area 1.
E. None of the above.

Answer: A

Explanation:
OSPF prefers Intra Area Path over Inter Area Paths.
Incorrect Answers:
B. The Answer B is incorrect because OSPF does not conduct ECMP load balancing on multiple paths with equal cost if the respective paths span through more than one area. B is incorrect for several reasons. If a packet has to alternate between two paths that means Per Packet load balancing is in effect. Which is normally in place for links less than 56k. For higher link speeds fast switching (default switching mode) is enabled. In this mode all packets to one destination in a target subnet are sent over one path, since route lookup is not performed for every packet, it is rather performed per flow. So B is totally ruled out.
C. Even though router CK1 is the most direct way to reach area 0, OSPF will always prefer to stay in the same area over traversing multiple areas.
D. OSPF prefers Intra area paths, so only the costs associated with reaching CK4 via area 1 will be considered first.
Reference:
http://www.riverstonenet.com/support/ospf/interface-costs.htm

---

QUESTION 143
Router CK1 is configured for OSPF. Interface serial 0 is configured to be in area 0 and interface serial 1 is configured to be in area 1. Under the OSPF process "area 1 nssa default-information-originate" is configured. Which of the following are true?

(Choose all that apply)

A. CK1 will inject a type 3 default route into area 1.
B. CK1 will inject a type 7 default route into area 1.
C. CK1 will inject a type 7 default route into area 0.
D. CK1 needs a default route in its routing table to inject a default into area 1.
E. CK1 does not need a default route in its routing table to inject a default into area 1.

Answer: B, D

Explanation:
Type 7 routes are injected into OSPF NSSA areas, and the default information originate command will make CK1 inject type 7 default routes into area 1. As a rule, an OSPF router will need a default route itself before injecting a default route into an area, unless the keyword "always" is used in the configuration. For example, "default-information originate always."
Incorrect Answers:

A. In a NSSA area, the NSSA area generates the default route with the "defaultinformation originate" command, but unlike other default routes that use type 3 information, NSSA default routes use type 7.
C. CK1 will inject a type 7 NSSA route into area 1, not area 0. Area 0 can not be an NSSA.
E. Using the command shown in the question above will not create the route, because a previous default route did not already exist within the routing table. A default route would have been injected only if the keyword "always" was inserted.
Reference:
www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a0080094a74.shtml

---

QUESTION 144
Which of the following OSPF routers can generate a type 4 ASBR-summary LSA? (Choose all that apply)

A. ABRs
B. DR
C. BDR
D. ASBRs

Answer: A

Explanation:
Type 4 LSAs are only put out by ABRs and only in two cases: 1. There is an ASBR that the ABR needs to tell the backbone area about. 2. There is a legacy router that is incapable of demand circuits. These last two are indication LSAs and are put out only by

an ABR putting itself in the ASBR position, but it is still not an ASBR. An ASBR would not be responsible for reporting either of these situations.

QUESTION 145
Routers CK1 and CK2 are in the same LAN and both are running OSPF. Which multicast IP address will CK1 and CK2 use for sending routing updates to each other? (Choose all that apply)

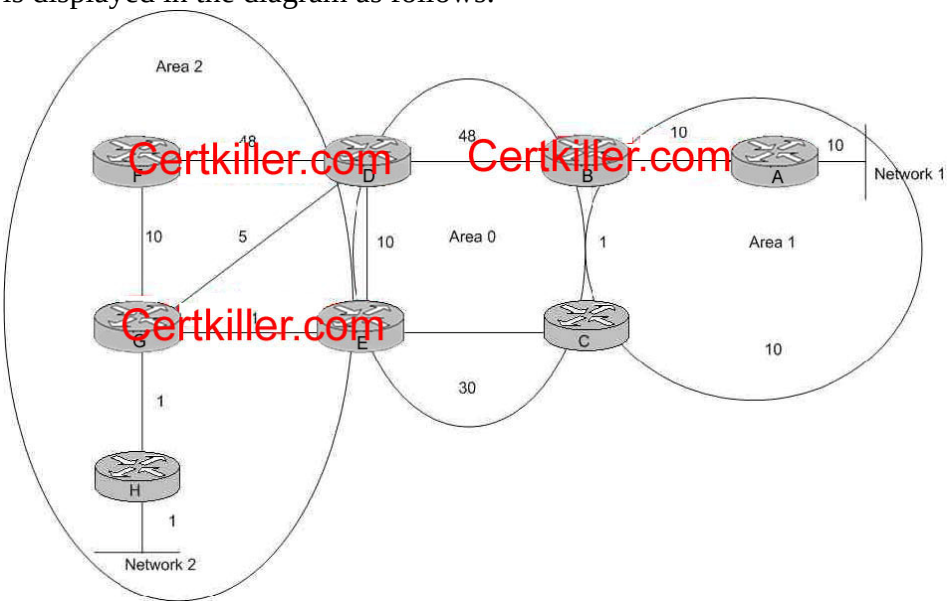
A. 224.0.0.10
B. 224.0.0.1
C. 224.0.0.13
D. 224.0.0.5
E. 224.0.0.9
F. 224.0.0.6

Answer: D, F

Explanation:
224.0.0.5 is the all-OSPF routers multicast and 224.0.0.6 is the Designated Routers multicast address.
Incorrect Answers:

A. 224.0.0.10 is used for IGRP.
B. 224.0.0.1 is reserved for all systems on the subnet.
D. 224.0.0.13 is used by PIM.
E. 224.0.0.9 is reserved for RIP version 2 announcements.

QUESTION 146
The Certkiller WAN utilizes OSPF as shown below. The OSPF metric for each link is displayed in the diagram as follows:



What is the OSPF shortest path from Network 2 to Network 1 with the OSPF link costs shown in the exhibit?

A. H G D B A
B. H G E C B A
C. H G F D B A
D. H G E D B A

Answer: B

Explanation:
Cost of links from Network 2 to Network 1 is:

A. H G D B A = 1+1 +5 +48 +10 = 65
B. H G E C B A = 1+1+1+30+1+10= 44
C. H G F D B A = 1+1+10+48+48+10= 118
D. H G E D B A = 1+1+1+10+48+10= 71
Therefore, the shortest path is the lowest cost path which is option B. It is important to remember that OSPF uses the total cost of the metrics from a source to a given destination, and the number of hop counts is irrelevant.

QUESTION 147
The Certkiller router CK2 is experiencing OSPF problems with a neighbor across a frame relay network. During troubleshooting, OSPF event debugging was issued as shown below:
CK2 #debug ip ospf events
OSPF events debugging is on
CK2 #
00:16:22: OSPF: Rcd hello from 192.168.0.6 area 4 from Ethernet 0/0 16.16.26.6
00:16:22: OSPF: End of hello processing
00:16:22: OSPF: Send hello to 244.0.0.5 area 4 on Ethernet0/0 from 116.16.26.2
CK2 #
00:16:28: OSPF: Rcd hello from 192.168.0.3 area 3 from Serial1/0 116.16.32.1
00:16:28: OSPF: Mismatched hello parameters from 116.16.32.1
00:16:28: OSPF: Dead R 40 C 120, Hello R 10 C 30 Mask R 255.255.255.252 C 255.255.255.252
CK2 :
00:16:32: OSPF: Rcd hello from 192.168.0.6 area 4 from Ethernet0/0 116.16.26.6
00:16:32: OSPF: End of hello processing
00:16:32: OSPF: Send hello to 224.0.0.5 area 4 on Ethernet0/0 from 116.16.26.2

Based on the information above, what is the most likely reason for the OSPF problems across the frame relay link?

A. This router is in area 4 while its neighbor is configured to be in area 3.
B. There is mismatch between the OSPF frame-relay parameters configured on this router and those configured on its neighbor.
C. The OSPF network mode configured on this router is not the same as the mode configured on its neighbor.
D. This router has a frame-relay interface DLCI statement that is using the broadcast mode. While its neighbor is using a point-to-point mode.
E. None of the above.

Answer: C

Explanation:
The default timers for a broadcast network (LAN) are: Hello 10 seconds, Dead 40 seconds
The default timers for an NBMA network (Frame Relay) are: Hello 30 seconds, Dead 120 seconds.
The problem above shows that these timers do not match at each end. The "Dead R 40 C 120, Hello R 10 C 30" means that the configured Dead time is 120 seconds locally on this router, but the received update shows it is configured to be 40 seconds. Similarly, the received hello packet shows that it has a hello time of 10 seconds, where router CK2 is configured for 30 seconds. Although the remote router may have had their timers changed manually within the OSPF process, the most likely cause of the problem is that router CK2 is configured with a network type of NBMA and the other router is configured with a network type of broadcast.
Incorrect Answers:

A. It is common for a router with multiple interfaces to be in different OSPF areas. Each network link must be in the same area, but each router can have multiple interfaces, that each belongs to a different area.
B. The Frame relay parameters do not appear to be misconfigured, just the OSPF timer values.
D. The timers on the local router, CK2 , is 30 seconds for the Hello and 120 seconds for the dead, so this router is configured with a NBMA or pt-pt type, while the remote router is using a broadcast network type.

QUESTION 148
Which of the following statements are true regarding the SPF calculation? (Select three)

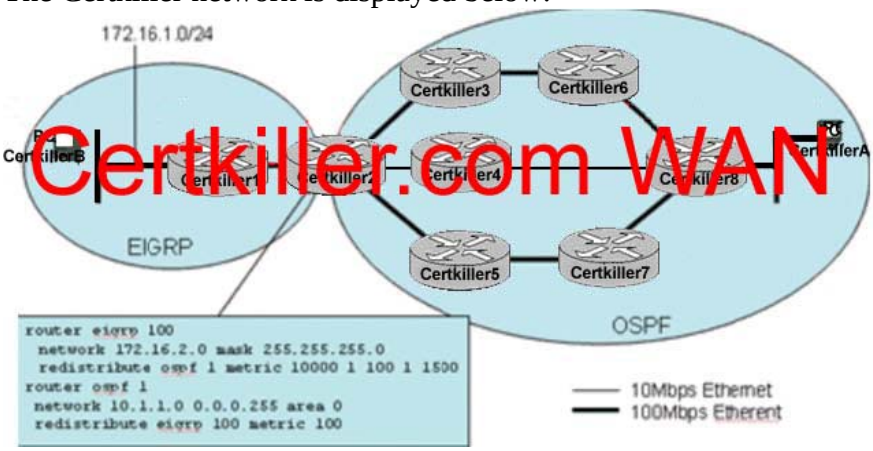
A. The Dijkstra algorithm is run two times.
B. The previous routing table is saved.
C. The present routing table is invalidated.
D. A router calculates the shortest-path cost using their neighbor(s) as the root for the

SPF tree.
E. Cisco routers use a default OSPF cost of 10^7/BW.

Answer: A, B, C

Explanation:
The Dijkstra algorithm code itself is run two times. The first time deals with routers and the second time always deals with networks.
When the Shortest Path First (SPF) algorithm is computed by an OSPF router, the previous routing table is save before the calculation and used in case any problems arise with the new one. It then invalidates the present routing table and performs the calculation using the OSPF neighbors as root in the SPF tree.
Incorrect Answers:
D. The router itself is the root, not the neighbor. A router periodically advertises its status or link state to its adjacencies. Link state advertisements flood throughout an area ensuring that all routers have exactly the same topological database. This database is a collection of the link state advertisements received from each router belonging to an area. From the information in this database, each router can calculate a shortest path tree with itself designated as the root of the tree.
E. The default OSPF cost of any link is 10^8/Bandwidth, or 100,000,000/BW.

QUESTION 149
The Certkiller network is displayed below:



Given the network and OSPF configuration shown above, what statement is true regarding traffic flowing from PC- Certkiller A to PC- Certkiller B?

A. Traffic will only flow on the shortest, low-speed path, PC- Certkiller A - Certkiller 8 - Certkiller 4 - Certkiller 2- Certkiller 1 - PC- Certkiller B.
B. Traffic will flow on both the high speed paths (PC- Certkiller A - Certkiller 8 - Certkiller 6- Certkiller 3 - Certkiller 2 - Certkiller 1 - PC- Certkiller B and PC- Certkiller A - Certkiller 8 - Certkiller 7 - Certkiller 5 - Certkiller 2 - Certkiller 1 - PC- Certkiller B) but not the slow-speed path.
C. Traffic will flow on all three of the paths.
D. Traffic will flow uni-directionally on one of the high-speed paths from PC- Certkiller A to PC- Certkiller B, and uni-directionally on one of the high speed

paths from PC- Certkiller B o PC- Certkiller A.
E. Traffic will flow bi-directionally on only one of the high-speed paths, and the path selected will be based on the OSPF process IDs.

Answer: B

Explanation:
OSPF uses the bandwidth of the links for the metric, and by default the 100 Mbps links will have an OSPF metric of 1 while the low speed links will have a metric of 10 so only the high speed Ethernet links will be used.
By default, OSPF load balances on up to four equal cost paths. Since both high speed paths will have a metric of 3 (1+1+1) from router Certkiller 8 to Certkiller 2 they traffic will load balance over the two paths.

QUESTION 150
What statement is correct regarding OSPF adjacencies and link-state database synchronization?

A. Full adjacency occurs when OSPF routers reach the LOADING state.
B. Adjacency relationship begins in the EXSTART state.
C. All OSPF neighbors establish adjacencies in the FULL state with all other routers on the broadcast network.
D. The INIT state indicates that a router has received a Hello packet from a neighbor and has seen their own ROUTERID in the Hello packet.

Answer: B

Explanation:
The various states in which a neighbor can be are discussed below.
1. Down - the initial state of a neighbor conversation.
2. Attempt - indicates that an attempt should be made to contact the neighbor.
3. Init - hello packet has been received from the neighbor.
4. 2-Way - communication between two routers is bi-directional.
5. ExStart - first step to creating an adjacency between the two neighboring routers.
6. Exchange - the router is sending data description packets to the neighbor.
7. Loading - Link state request packets are sent to the neighbor.
8. Full - the neighboring routers are fully adjacent.
Incorrect Answers:

A. Full adjacency only occurs after the OSPF router has reached a FULL state.
C. In a broadcast network, all routers only become adjacent with the Designated Router (DR).
D. This state specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet. When a router receives a hello packet from a neighbor, it should list the sender's router ID in its hello packet as an acknowledgment that it received a valid hello packet.

QUESTION 151
OAPF is running on the Certkiller network. In OSPF, what LSA type would only cause a partial SPF calculation?

A. Type 1
B. Type 2
C. Type 4
D. Type 7
E. Type 9

Answer: D

Explanation:
OSPF Type 7 LSA's are reserved for Not So Stubby Areas (NSSA). This area accepts Type 7 LSAs which are external route advertisements like Type 5s but they are only flooded within the NSS
A. This is usually used when connecting to a branch office
running an IGP. Normally this would have to be a standard area since a stub area would not import the external routes. If it was a standard area linking the ISP to the branch office then the ISP would receive all the Type 5 LSAs from the branch which it does not want. Because Type 7 LSAs are only flooded to the NSSA the ISP is saved from the external routes whereas the NSSA can still receive them. Therefore, when this LSA is generated, only a partial SPF calculation needs to be performed.

QUESTION 152
OSPF is being used as the routing protocol in the Certkiller network. Which two statements regarding the SPF calculation on these OSPF routers are true? (Select two)

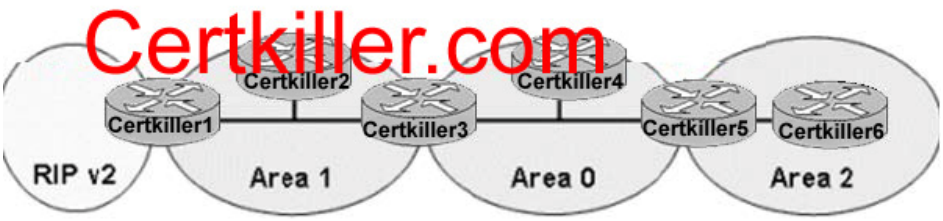
A. The existing routing table is saved so that changes in routing table entries can be identified.
B. The present routing table is invalidated and is built again from scratch.
C. A router calculates the shortest-path cost using their neighbor(s) as the root for the SPF tree.
D. Cisco routers use a default OSPF cost of 10^7/BW.

Answer: A, B

Explanation:
When an OSPF router performs a new SPF calculation, the existing routing table is saved and used as a baseline for changes made to the network topology. When any SPF calculation is made, the OSPF neighbor or neighbors is used as the root of the SPF routing tree.
Incorrect Answers:
C. The root of the SPF tree is always the router itself, not the neighboring router.

D. The default cost for all OSPF links is 10^8/BW, or 100,000,000/ configured bandwidth.

QUESTION 153
The Certkiller OSPF/RIPv2 network is displayed below:



Area 1 is an OSPF Not So Stubby Area (NSSA). What type of LSA will Certkiller 3 send out area 0 to indicate the presence of an ASBR in Area 1?

A. A type 5 because P-bit has been set in the type 4 LSA that was sent from Certkiller 1 to Certkiller 3.
B. A type 4 because the E-bit was set in the type 7 LSA that was sent from Certkiller 1 to Certkiller 3.
C. A type 1 because the B-bit was set in the LSA that was propagated from Certkiller 1 to Certkiller 3.
D. A type 3 because the E-bit was set in the type 1 LSA that was sent from Certkiller 1 to Certkiller 3.

Answer: B

Explanation:
In this case a type 5 LSA would be sent by the ASBR, which is Certkiller 1.
Type 5 Link State advertisements are generated by the ASBR and describe links external to the Autonomous System (AS). This LSAS is flooded to all areas except stub areas.
Here Certkiller 1 is considered to be an ASBR since it is directly connected with the RIP version 2 network.
The E-bit reflects the associated area's External Routing Capability. AS external link advertisements are not flooded into/through OSPF stub areas. The E-bit ensures that all members of a stub area agree on that area's configuration.
LSA type 3 and 4 are summary link advertisements generated by ABRs describing inter-area routes. Type 3 describes routes to networks and is used for summarization. Type 4 describes routes to the ASBR. Since Certkiller 3 needs to advertise the presence of an ASBR, it will send out a type 4 LSA to area 0.
Reference: http://www.cisco.com/warp/public/104/ospfdb6.html

QUESTION 154
What statement is accurate regarding OSPF areas?

A. Redistribution is allowed into all types of OSPF areas.
B. When routes are redistributed into an OSPF stub area, they enter as type-5 LSAs.

C. Redistribution is allowed into an OSPF stub area, but not into an OSPF not-sostubby area.
D. When routes are redistributed into an OSPF not-so-stubby area, they enter as type-5 LSAs.
E. When routes are redistributed into an OSPF not-so-stubby area, they enter as type-7 LSAs.

Answer: E

Explanation:
When routes are redistributed into OSPF, these routes are considered to be external routes. External LSAs are type 5 LSAs. Not so stubby areas allow external routes to be advertised into OSPF network while retaining the charactersistics of a stub area. To do this, the ASBR (the one doing the redistributing) in the NSSA will originate a type 7 LSA to advertise the external destinations.
Reference: Jeff Doyle, Routing TCP/IP volume 1, page 483.
Incorrect Answers:

A. Type 5 LSAs are only allowed into Backbone (area 0) and non backbone, non-stub areas.
B. Type 5 LSAs (external LSAs) are not allowed into stub or totally stub areas.
C. The opposite is true. External LSAs are allowed into NSSA, but not stub areas.
D. Type 5 LSAs are not inserted into NSSA for external routes. Type 7 LSAs are created for this purpose.

QUESTION 155
Within the Certkiller OSPF network, which statement is true regarding the LSA's contained in the link state database? (Choose all that apply).

A. The LSRefreshTime is 30 minutes.
B. LSA's can only be reflooded by the router that originated the LSA.
C. When an LSA reaches its MaxAge the router will send out a purge message to the other routers within its area.
D. All LSAs contained in the LSDB expire at the same time unless they are refreshed.
E. The MaxAge of an LSA is 3600 seconds.

Answer: A, E

Explanation:
Each OSPF LSA has an age, which indicates whether the LSA is still valid. Once the LSA reaches the maximum age (one hour), it is discarded. During the aging process, the originating router sends a refresh packet every 30 minutes to refresh the LS
A. Refresh
packets are sent to keep the LSA from expiring, whether there has been a change in the network topology or not. Checksumming is performed on all LSAs every 10 minutes.

The router keeps track of LSAs it generates and LSAs it receives from other routers. The router refreshes LSAs it generated; it ages the LSAs it received from other routers.
Incorrect Answers:
B. Each LSA gets refreshed when it is 30 minutes old, independent of the other LSAs used by other OSPF routers.
C. Purge messages are not sent to neighboring routers since each router uses its own timers.
D. Global synchronization can be problematic in OSPF networks. This problem is solved by each LSA having its own timer. Each LSA gets refreshed when it is 30 minutes old, independent of other LSAs, so the CPU is used only when necessary.

QUESTION 156
Which of the following is are considered to be attributes of BGP routes? (Choose all that apply)

A. Origin
B. Weight
C. Local Preference
D. Community
E. Cluster List

Answer: A, C, D, and E

Explanation:
Origin, Local Preference, Community, and Cluster List are all BGP attributes.
ORIGIN Well-known mandatory, Type code 1 RFC 1771
LOCAL_PREF Well-Known discretionary, Type code 5 RFC 1771
COMMUNITY Optional transitive, Type 8 RFC 1997
CLUSTER_LIST Optional nontransitive, Type code 10 RFC 1966
Incorrect Answers:
B. Cisco routers do indeed use weight during the BGP route decision making process. In fact, it is the first parameter that is looked at. However, weight is a Cisco-only parameter, and is therefore not considered a BGP attribute.

QUESTION 157
You are the network administrator at Certkiller . You want to advertise the network 190.72.27.0/27 to an EBGP peer.
What command should you use?

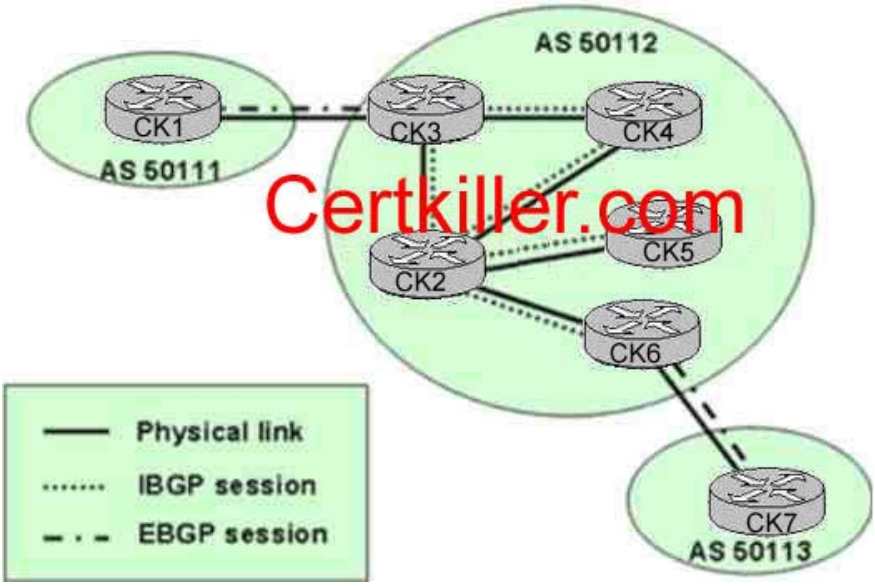
A. network 190.72.27.0
B. network 190.72.27.0 mask 255.255.255.224
C. network 190.72.27.0 mask 255.255.225.240
D. network 190.72.27.0 mask 0.0.0.31.

Answer: B

Explanation:
The correct syntax is: network ip-address mask subnet-mask where ipaddress is the network address and subnet-mask is the subnet mask. In this case the network address is 190.72.27.0. The subnet mask is a 27 bit subnet mask (11111111.11111111.11111111.11100000) that equates to 255.255.255.224.
Incorrect Answers:

A. If no mask is specified, the default class mask is used. In the 190.72.27.0 case it would be a /16.
C. Here the wrong mask is used.
D. This is the inverse mask, which is normally used by OSPF when specifying the network mask, but not by BGP.

QUESTION 158
The Certkiller BGP network consists of AS 50112 as shown in the diagram below:



Based on the physical connectivity and the IBGP peering shown, what router within the Transit AS 501112 should be setup as the route reflector and which routers should be setup as the clients based on the recommended route reflector design rules?

A. CK4 should be the route reflector with CK2 and CK5 as its clients.
B. CK2 should be the route reflector with CK5 and CK6 as its clients.
C. CK3 should be the route reflector with CK2 and CK4 as its clients.
D. CK2 should be the route reflector with CK4 and CK5 as its clients.
E. CK4 should be the route reflector with CK2 and CK3 as its clients.
F. All of the above are valid options.

Answer: B

Explanation:
Within any BGP autonomous system, every IBGP speaker must have a fully meshed

peering arrangement with every other iBGP speaker. This is due to the fact that a BGP speaker will not advertise a route learned via another iBGP speaker to a third iBGP speaker. The use of route reflectors is one way to maintain connectivity throughout the AS without having a fully meshed peering arrangement. By relaxing this restriction a bit and by providing additional control, we can allow a router to advertise (reflect) iBGP learned routes to other iBGP speakers.
When using route reflectors, the clients need only peer to the route reflector. In the example above, if router CK2 is configured as the route reflector, with routers CK5 and CK6 set up as clients, then 5 and 6 need only peer with CK2 . In doing this, all other routers are fully meshed. No other answer choices will allow us to maintain a fully meshed iBGP configuration.

QUESTION 159
Routers CK1 and CK2 are configured for BGP. Both routers reside in AS 65234. Routes from Router CK2 show up in the BGP table on Router CK1 , but not in the IP routing table.
What could be the cause of this problem?

A. Synchronization is off.
B. The BGP peers are down.
C. BGP multi-hop is disabled on Router CK1 .
D. Router CK1 is not receiving the same routes via an internal protocol.

Answer: D

Explanation:
BGP Synchronization says: "If your autonomous system is passing traffic from another AS to a third AS, BGP should not advertise a route before all routers in your AS have learned about the route via IGP." Therefore, we can assume that synchronization is on and that the BGP routes have not yet been learned by an IGP.
Incorrect Answers:

A. If synchronization is off the routes would show up in the IP routing table on CK1 .
B. If the BGP peers were down, then the routers would not be sending and receiving BGP route information to each other.
C. BGP multi-hop is only useful for EBGP peers, not IBGP peers.

QUESTION 160
You have a router running BGP for the Internet connections as well as IGRP for use internally. You configure the network backdoor command on this router under the BGP process. What will this do?

A. It will change the distance of an iBGP route to 20.
B. It will change the distance of an eBGP route to 200.
C. It will change the distance of an IGRP route to 20.
D. It will not change the distance of the route.

Answer: B

Explanation:
Backdoor only makes the IGP learned route the preferred route. To specify a backdoor route to a BGP border router that will provide better information about the network, use the network backdoor router configuration command. To remove an address from the list, use the no form of this command.
By definition, eBGP updates have a distance of 20 that is lower than the IGP distances. Default distance is 120 for RIP, 100 for IGRP, 90 for EIGRP, and 110 for OSPF.
By default, BGP has the following distances, but that could be changed by the distance command:
distance bgp external-distance internal-distance local-distance
external-distance:20
internal-distance:200
local-distance:200
If we want RTA to learn about 160.10.0.0 via RTB (IGP), then we have two options:
• Change eBGP's external distance or IGP's distance, which is not recommended.
• Use BGP backdoor.
BGP backdoor makes the IGP route the preferred route
RTA learns 160.10.0.0 from RTB via EIGRP with distance 90, and also learns it from RTC via eBGP with distance 20. Normally eBGP is preferred, but because of the backdoor command EIGRP is preferred
References:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_command_summary_chapter09186a00800d9c5b.html#xtocid197442
http://www.cisco.com/en/US/tech/ CK3 65/ CK8 0/technologies_tech_note09186a00800c95bb.shtml#bgpbackdoor

---

QUESTION 161
You have two routers running BGP to two different ISP's. You wish to influence the way that traffic comes into your network from the Internet, but your company policy prohibits the use of BGP communities. What is the best way to influence this traffic?

A. Adjust the cost of your routers.
B. Use MED values.
C. Increase the weight value on one of your routers.
D. Decrease the local preference value on one of your routers.
E. Use AS-path prepending.
F. Use Metrics.

Answer: E

Explanation:
When influencing incoming traffic from the Internet, the two most widely used methods

are AS Path Prepending and Multi-Exit Discriminators (MED). AS Path prepending works by adding AS paths to certain network ranges, making them appear to the Internet to be further away than they really are. MEDs are used to advertise metrics to the neighbor AS to influence the incoming path that traffic should take to reach certain destinations. In this case, AS Path Prepending is preferred over the use of MEDs because AS path prepending information is distributed to all networks within the Internet. MEDs are only used between neighboring Autnomous Systems. Another advantage to path prepending is that the AS path information is ranked higher in the BGP decision process than the MED information. IN fact, MED information is one of the last things considered in the BGP path decision algorithm.
Note: Although one method of using AS Path prepending requires the use of communities, it is not required to use communities for simply sending prepending information.
Incorrect Answers:
A, C, D, F. These are all methods for influencing traffic going out to the Internet, not coming in.
E. This would be an acceptable way to influence traffic, but would not be the best way.

QUESTION 162
Your router is multi-homed to three different ISP's for Internet access. You then configure "bgp deterministic-med" under the BGP routing process configuration of your router. What effect does this change have on your network?

A. It configures BGP to compare MEDs between different ASs.
B. It makes the default metric count the worst possible metric.
C. It makes the default metric count the best possible metric.
D. It configures BGP to reorder the entries by neighbor AS.
E. It configures BGP to reorder the entries by MED.

Answer: D

Explanation:
There is sometimes confusion between the two Border Gateway Protocol (BGP) configuration commands bgp deterministic-med and bgp always-compare-med. Enabling the bgp deterministic-med command ensures the comparison of the MED variable when choosing routes advertised by different peers in the same autonomous system. Enabling the bgp always-compare-med command ensures the comparison of the MED for paths from neighbors in different autonomous systems. The bgp alwayscompare-med command is useful when multiple service providers or enterprises agree on a uniform policy for setting MED. Thus, for network X, if Internet Service Provider A (ISP A) sets the MED to 10, and ISP B sets the MED to 20, both ISPs agree that ISP A has the better performing path to X.
When BGP receives multiple routes to a particular destination, it lists them in the reverse order that they were received, from the newest to the oldest. BGP then compares the routes in pairs, starting with the newest entry and moving toward the oldest entry (starting at top of the list and moving down). For example, entry1 and entry2 are

compared. The better of these two is then compared to entry3, and so on. The bgp always-compare-med command reorders the entries by neighbor AS.
Incorrect Answers:

A. The router would compare MEDs between different AS numbers if the "bgp alwayscomapre-med" was configured, not the bgp deterministic-med command.
B, C. This command does not affect the default BGP metric.
E. This command reorders the entries based on AS number, not MED.
Reference:http://www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a00800 94925.shtml

---

QUESTION 163
Which of the following attributes are "well known" BGP attributes? (Choose all that apply)

A. Atomic-aggregate
B. MED
C. Next-hop
D. AS-path
E. Origin
F. Weight
G. Aggregator

Answer: A, C, D, E

Explanation:
The following BGP attributes are all well known:
Well Known, Mandatory attributes: AS_PATH, NEXT-HOP and ORIGIN
Well Known, Discretionary attributes: LOCAL_PREF and ATOMIC_AGGREGATE
Incorrect Answers:
B, E, F. The optional, transitive attributes are AGGREGATOR and COMMUNITY. The optional non-transitive attributes include MULTI_EXIT_DISC (MED, the ORIGINATOR_ID. and CLUSTER_LIST.
Reference:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm

---

QUESTION 164
In BGP routing, what does the rule of synchronization mean?

A. It means that a BGP router can only advertise an iBGP-learned route provided that the route is in the only in the BGP table.
B. It means that a BGP router can only advertise an eBGP-learned route provided that the route is an IGP route in the routing table.
C. It means that a BGP router can only advertise an iBGP-learned route provided that the route is in the routing table of all its iBGP neighbors.
D. It means that a BGP router can only advertise an eBGP-learned route provided

that the route is metric 0 in the BGP table.
E. It means that a BGP router can only advertise an iBGP-learned route provided that the route is an IGP route in the routing table.

Answer: E

Explanation:
The BGP rule of synchronization states that a BGP router should not advertise to external neighbors destinations learned from IBGP neighbors unless those destinations are also known via an IGP.
Incorrect Answers:
B, D. Synchronization is used to ensure that you don't develop black holes by advertising local routes to the rest of the world, when the local routers don't even know how to get to the route in question. That's why synchronization with the IGP is not a concern when you either create a full iBGP mesh, or implement route reflectors, confederations, or both. Therefore, synchronization is implemented only for IBGP routes, not EBGP.
C. The route needs only be in the routing table of its own router, not every neighboring router.
Reference:
"Internet Routing Architectures" Sam Halabi page 143, Cisco Press.

QUESTION 165
What is the correct sequence order that BGP routers use when determining the best route to any given destination?

A. MED, Local preference, AS-path, Weight, Origin Code
B. Origin Code, MED, Weight, AS Path, Local Preference
C. Weight, Local Preference, AS-path, Origin Code, MED
D. Weight, Local Preference, MED, AS-Path, Origin Code
E. MED, Weight, Local Preference, Origin Code, AS Path

Answer: C

Explanation:
How the Best Path Algorithm Works
BGP assigns the first valid path as the current best path. It then compares the best path with the next path in list, until it reaches the end of the list of valid paths. Following is a list of rules used to determine the best path:
1. Prefer the path with the largest WEIGHT. Note: WEIGHT is a Cisco-specific parameter, local to the router on which it's configured.
2. Prefer the path with the largest LOCAL_PREF.
3. Prefer the path that was locally originated via a network or aggregate BGP subcommand, or through redistribution from an IGP. Local paths sourced by network/redistribute commands are preferred over local aggregates sourced by the aggregate-address command.
4. Prefer the path with the shortest AS_PATH. Note the following:

o This step is skipped if bgp bestpath as-path ignore is configured.
o An AS_SET counts as 1, no matter how many ASs are in the set.
o The AS_CONFED_SEQUENCE is not included in the AS_PATH length.
5. Prefer the path with the lowest origin type: IGP is lower than EGP, and EGP is lower than INCOMPLETE.
6. Prefer the path with the lowest multi-exit discriminator (MED).

QUESTION 166
You are setting up BGP on router CK1 and you wish to simplify the configuration file through the use of BGP peer groups. Which of the following best describes the proper use of BGP peer groups?

A. They should be used for peers with common community values
B. They should be used for peers with common inbound announcement policies
C. They should be used for peers with common outbound announcement policies
D. They should be sued to combine MED inbound policies
E. They should be used to peers with common transitive AS policies

Answer: C

Explanation:
The major benefit of specifying a BGP peer group is that it reduces the amount of system resources (CPU and memory) used in an update generation, and it also simplifies the BGP configuration. It reduces the load on system resources by allowing the routing table to be checked only once, and updates to be replicated to all peer group members instead of being done individually for each peer in the peer group. Depending on the number of peer group members, the number of prefixes in the table, and the number of prefixes advertised, this can significantly reduce the load. Cisco recommends that you group together peers with identical outbound announcement policies.

QUESTION 167
Router CK1 is being configured for as both an IBGP peer to the other routers within the Certkiller network, and as an EBGP peer to the ISP. Select the BGP attributes that are required to be sent to these BGP neighbors from CK1 :

A. AS_PATH
B. MED
C. NEXT_HOP
D. LOCAL_PREF
E. ORIGIN
F. ROUTER_ID

Answer: A, C, E

Explanation:
AS-PATH, NEXT-HOP, and ORIGIN are all well known, mandatory BGP attributes,

which is defined below:
Well known mandatory attributes: These attributes must be recognized by all BGP speakers, and must be included in all update messages. Almost all of the attributes impacting the path decision process, described in the next section, are well known mandatory attributes.
Origin Code
The ORIGIN is a well known mandatory attribute that indicates the origin of the prefix, or rather, the way in which the prefix was injected into BGP. There are three origin codes, listed in order or preference:
• IGP, meaning the prefix was originated from information learned from an interior gateway protocol
• EGP, meaning the prefix originated from the EGP protocol, which BGP replaced
• INCOMPLETE, meaning the prefix originated from some unknown source
AS Path
The AS_PATH is a well-known mandatory attribute and is the list of all autonomous systems the prefixes contained in this update have passed through. The local autonomous system number is added by a BGP speaker when advertising a prefix to an eBGP peer.
Next Hop
The BGP NEXT_HOP is a well-known mandatory attribute. The Next Hop attribute is set when a BGP speaker advertises a prefix to a BGP speaker outside its local autonomous system (it may also be set when advertising routes within an AS, this will be discussed in later sections). The Next Hop attribute may also serve as a way to direct traffic to another speaker, rather than the speaker advertising the route itself.
Incorrect Answers:
B. The MUTLI_EXIT_DISC (MED) is an optional non-transitive attribute that provides a mechanism for the network administrator to convey to adjacent autonomous systems to optimal entry point in the local AS.
D. The LOCAL_PREF attribute is a well-known attribute that represents the network operator's degree of preference for a route within the entire AS. It is not a mandatory attribute and it is not applied to all BGP updates.
F. The router ID is not a well known, mandatory BGP attribute.

QUESTION 168
Assume the following routes are in the BGP routing table.
172.16.0.0/24
172.16.1.0/24
172.16.2.0/24
172.16.3.0/24
also assume the following commands have been configured:
router bgp 1
neighbor 10.1.1.1 remote-as 2
aggregate-address 172.16.0.0 255.255.252.0 suppress-map specific
access-list 1 permit 172.16.2.0 0.0.0.3.255
route-map specific permit 10
match ip-address 1
Which routes will BGP advertise?

A. 172.16.0.0/22
B. 172.16.0.0/22, 172.16.2.0/24, 172.16.3.0/24
C. 172.16.0.0/22, 172.16.0.0/24, 172.16.1.0/24
D. 172.16.2.0/24 and 172.16.3.0/24
E. 172.16.0.0/22 and 172.16.1.0/24

Answer: A

Explanation:
BGP allows the aggregation of specific routes into one route using the aggregate-address address mask command. Aggregation applies to routes that exist in the BGP routing table. This is in contrast to the network command, which applies to the routes that exists in IP routing table. Aggregation can be performed if at least one or more of the specific routes of the aggregate address exist in the BGP routing table. In this specific example, the router will summarize the routes into 172.16.0.0/22, as long as at least one of the more specific 172.16 assumed routes actually exist in the routing table. Normally, aggregate addresses are advertised in addition to the more specific subnets. However, in this case the suppress map will filter the more specific routes, advertising only the 172.16.0.0/22 route.

QUESTION 169
A BGP router in the Certkiller network called P1R3 is configured as shown below:
!
hostname P1R3
!
! Output omitted
!
router bgp 50001
synchronization
bgp log-neighbor-changes
neighbor 10.200.200.11 remote-as 50001
neighbor 10.200.200.11 update-source loopback0
neighbor 10.200.200.12 remote-as 20001
neighbor 10.200.200.12 update-source Loopback0
neighbor 10.200.200.14 remote-as 50001
neighbor 10.200.200.14 update-source Loopback0
no auto-summary
PIR3#show ip bgp summary
BGP router identifier 10.200.200.13, local As number 50001
BGP table version is 1, main routing table version 1
6 network entries using 606 bytes of memory
7 path entires using 336 bytes of memory
4 BGP path attribute entries using 240 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory

0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1254 total bytes of memory
BGP activity 6/0 prefixes, 7/2 paths, scan interval 60 secs
Neighbor V AS MsgRcvd MsqSent TblVer InO OutO
Up/Down State/Pfxrcd

10.200.200.11	4	50001	9	4	1	0	0 00:00: 14	6
10.200.200.12	4	50001	9	4	1	0	0 00:00: 14	6
10.200.200.14	4	50001	4	4	1	0	0 00:00: 14	0

PIR#show ip bgp
BGP table version is 1, local router: ID is 10.200.200.13
Status Codes: s suppressed, d damped, h history, * valid, > best, I - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* i10.0.0.0	10.200.200.12	0	100	0	i
* i	10.200.200.11	0	100	0	i
* i192.168.11.0	10.200.200.12	0	100	0	50998 50222 50223 i
* i	10.200.200.11	0	100	0	50998 50222 50223 i
* i192.168.12.0	10.200.200.12	0	100	0	50998 50222 50223 i
* i	10.200.200.11	0	100	0	50998 50222 50223 i
* i192.168.13.0	10.200.200.12	0	100	0	50998 50222 50223 i
* i	10.200.200.11	0	100	0	50998 50222 50223 i
* i192.168.14.0	10.200.200.11	0	100	0	50998 50222 50223 i
* i	10.200.200.11	0	100	0	50998 50222 50223 i

<output omitted>
PIR#show ip route
Codes: C - connected, s - static, I IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, 0 - OSPF< IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - is-is, su - IS-IS summary, L1 - IS-IS leval-1, L2 - IS-IS level - 2
Ia - IS-IS inter area, * - candidate default, U - per-user static route
O - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
o 10.200.200.11/32 [110/11] via 10.1.1.1, 00:06:38, Ethernet0/0
o 10.200.200.14/32 [110/65] via 10.1.3.4, 00:06:38, Seriall/0
o 10.200.200.12/32 [110/75] via 10.1.1.1, 00:06:38, Ethernet0/0
c 10.200.200.13/32 is directly connected, Loopback0
c 10.1.3.0/24 is directly connected, Seriall/0
o 10.1.2.0/72 [110/74] via 10.1.3.4, 00:06:38, Seriall/0
c 10.1.1.0/24 is directly connected, Ethernet0/0
c 10.1.0.0/24 [110/74] via 10.1.1.1, 00:06:38, Ethernet 0/0
Router PIR3 is running an IBGP full-mesh with its IBGP neighbors (10.200.200.11, 10.200.200.12, and 10.200.200.14). Based on the BGP configuration and the show command outputs above, why are BGP routes not being selected in the BGP table and placed into the IP routing table?

A. Because the 10.200.200.11 and 10.200.200.12 neighbors are setting the Weight to
B. Because the 10.200.200.11 and 10.200.200.12 neighbors are setting the MED to 0
C. Because the 10.200.200.11 and 10.200.200.12 neighbors are not using next-hopself
D. Because synchronization is enabled on PIR 3
E. Because there are no routes to reach the next-hops

Answer: D

Explanation:
A BGP router with synchronization enabled will not advertise iBGP-learned routes to other eBGP peers if it is not able to validate those routes in its IGP. Assuming that IGP has a route to iBGP-learned routes, the router will announce the iBGP routes to eBGP peers. Otherwise the router treats the route as not being synchronized with IGP and does not advertise it. Disabling synchronization using the no synchronization command under router BGP prevents BGP from validating iBGP routes in IGP. By default, synchronization is enabled on all BGP routers.

QUESTION 170
With regards to BGP and the administrative distance in a routed environment, which statement is correct?

A. The administrative distance of all BGP routes is 20, which explains why BGP routes are preferred over any IGP (such as OSPF).
B. BGP is a path vector protocol, and thus does not employ the concept of administrative distance.
C. BGP dynamically adjusts its administrative distance to match that of the IGP within the AS to eliminate routing confusion.
D. BGP actually employs two different administrative distance values: IBGP is 20, while EBGP is 200.
E. BGP actually employs two different administrative distance values: IBGP is 200, while EBGP is 20.

Answer: E

Explanation:
BGP employs the use of two separate administrative distances, based on the type of BGP route. (Internal or External)
The table below lists the administrative distance default values of the protocols that Cisco supports:

Route Source	Default Distance Values
Connected interface	0
Static route*	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown**	255

Incorrect Answers:

A. Only external BGP routes have an AD of 20. Internal BGP routes are given a high AD to prevent these routes from overriding the routes from the IGP routing protocols, such as OSPF, EIGRP, RIP, etc.
B. BGP is indeed considered a path vector routing protocol, but it does also use the concept of AD, as shown in the table above.
C. The AD of BGP routes is static, with the default values shown in the table. These values can be configured to use different values, but they will still be considered static and will not change dynamically.
D. BGP does indeed use two different values, but the values used are the reverse. EBGP is 20 while IBGP is 200.

QUESTION 171
You are configuring the Certkiller Internet router as a BGP peer to your ISP's router. After doing this, which BGP attributes will be carried in every BGP update (both IBGP and EBGP)?

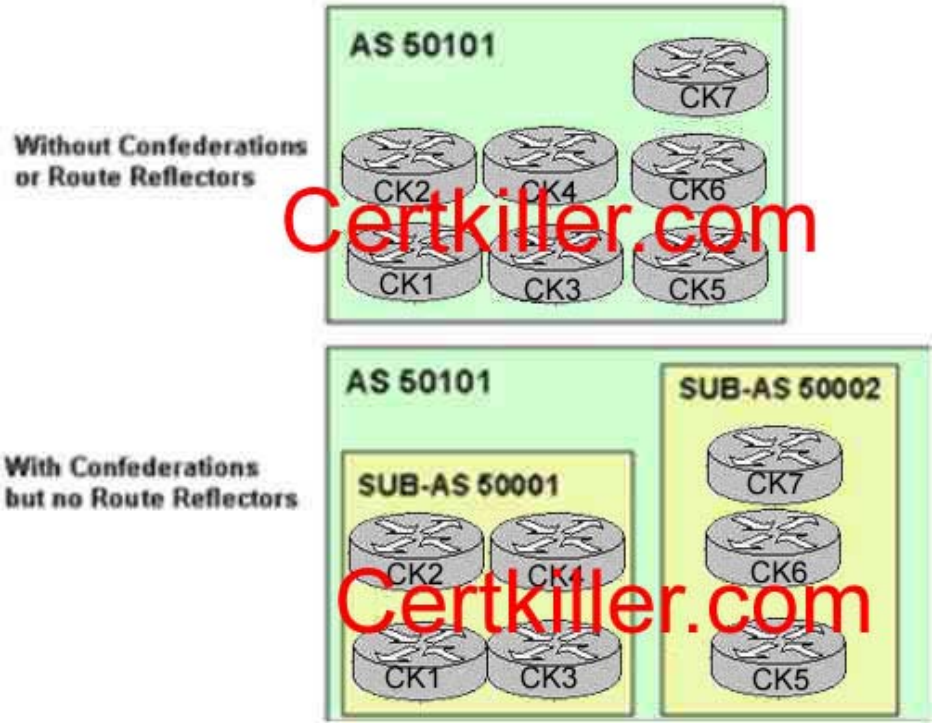
A. Origin, AS-Path, Next Hop
B. Origin, local preference, AS-Path

C. Router-ID, Origin, AS-Path
D. Router-ID, Local-Preference, Next-Hop
E. AS-Path, Local Preference, Next-Hop

Answer: A

Explanation:
Origin, AS-PATH, and Next-Hop are all well known, mandatory BGP attributes, which is defined below:
Well known mandatory attributes: These attributes must be recognized by all BGP speakers, and must be included in all update messages. Almost all of the attributes impacting the path decision process, described in the next section, are well known mandatory attributes.
Origin Code
The ORIGIN is a well known mandatory attribute that indicates the origin of the prefix, or rather, the way in which the prefix was injected into BGP. There are three origin codes, listed in order or preference:
• IGP, meaning the prefix was originated from information learned from an interior gateway protocol
• EGP, meaning the prefix originated from the EGP protocol, which BGP replaced
• INCOMPLETE, meaning the prefix originated from some unknown source
AS Path
The AS_PATH is a well-known mandatory attribute and is the list of all autonomous systems the prefixes contained in this update have passed through. The local autonomous system number is added by a BGP speaker when advertising a prefix to an eBGP peer.
Next Hop
The BGP NEXT_HOP is a well-known mandatory attribute. The Next Hop attribute is set when a BGP speaker advertises a prefix to a BGP speaker outside its local autonomous system (it may also be set when advertising routes within an AS, this will be discussed in later sections). The Next Hop attribute may also serve as a way to direct traffic to another speaker, rather than the speaker advertising the route itself.
Incorrect Answers:
B, D, E. The LOCAL_PREF attribute is a well-known attribute that represents the network operator's degree of preference for a route within the entire AS. It is not a mandatory attribute that is applied to all BGP updates.
C, D. The router ID is not a well known, mandatory BGP attribute.

QUESTION 172
The Certkiller BGP network has been assigned AS number 50101 as shown below:



The Certkiller AS 50101 network is split into two AS numbers (Sub-AS 50001 and Sub-AS 50002) using Confederations without any route reflectors. Sub-AS 50001 contains 4 routers and sub-AS 50002 contains the other 3 routers. Based on this information, how many IBGP sessions are required?

A. 9 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.
B. 11 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.
C. 18 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.
D. 21 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.
E. 25 IBGP sessions using Confederations with two sub-ASs where one of the sub-AS contains 4 routers and the other sub-As contains the other 3 routes.

Answer: A

Explanation:
The advantage of confederations is that they sharply reduce the number of IBGP peering sessions. IBGP is used normally within each member AS, but a special version of EBGP known as confederations. EBGP is run between the autonomous systems.
Confederations are another way of scaling IBGP. Defined in RFC 3065, this feature introduces a divide-and-conquer approach to remove the full mesh requirement.
Using confederations an AS is split into multiple sub-ASs, but the network still appears as one AS to the outside world. Each sub-AS number is stripped from AS path at the confederation border. A full IBGP mesh is only required within each sub-AS, which is

usually a manageable number of routers. In very large networks, you can even configure route reflection within a sub-AS. Typically private ASs are assigned for each sub-AS number.
With IBGP, all routers are to be configured as a fully meshed topology. The number of connections needed for any fully meshed configuration can be found by the formula:
N (N-1)
2
There are 4 Sub-AS peers in 5001 so that makes 4*3 / 2 = 6 peer sessions.
Similarly, there are 3 peers in Sub-As 5002, so we have 3*2 / 2 = 3 peer sessions
Therefore, the total number of peering sessions is 9(6+3).
Reference: Jeff Doyle, "Routing TCP/IP" Vol. II page 287

QUESTION 173
Router CK1 is used as the Certkiller Internet router and is configured for BGP. The Ip BGP information of this router is displayed below:
CK1 # show ip bgp
BGP table version is 12, local router ID is 172.16.1.2
Status code: s supported, d damped, h history, * valid, > best,
i - internal Origin codes: i IGP, e - EGP ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 192.168.0.0/16 172.16.1.1 0 0 50 103 {50101, 50102} i
Given above information, why does the 192.168.0.0/16 prefix contain an AS-PATH of 50 103 { 50101, 50102}

A. Because AS 50101 and AS 50102 are Transit AS's
B. Because AS 50103 is using BGP confederations with two sub-ASs (sub-AS 50101 and sub-AS 50102)
C. Because it is an aggregate route and the more specific routes have passed through AS 50101 and AS 50102
D. Because AS 50103 is using AS-Path pre-pending to influence the return traffic
E. Because AS 50103 is performing route summarization using the network 192.168.0.0. mask 255.255.0.0 command

Answer: C

Explanation:
In this example, the 192.168.0.0/16 route includes the SET {50101, 50102}. This indicates that aggregate route of 192.168.0.0 actually summarizes routes that have passed through AS 50101 and AS 50102. The AS-SET information is preserved because it becomes important in avoiding loops as it maintains an indication of where the route has been.
Incorrect Answers:

A. Transit AS numbers are displayed normally in the IP BGP table.
B. Confederations are seen as only one single AS to the rest of the Internet, so they will not appear as an AS-SET to EBGP peers.

D. AS Path prepending is displayed normally, and if this were the case then you would see multiple entries in a row for the same AS number.
E. Summarized routes only appear in an AS SET when the more specific routes have passed through multiple different AS numbers.
Reference: Bassam Halabi, "Internet Routing Architectures" Cisco Press, page 359.

QUESTION 174
The IP BGP information for a specific network on router CK1 is displayed below:
CK1 #show ip bgp 10.254.0.0
BGP routing table entry for 10.254.0.0/24, version 8
Paths: (2 available, best #1, table Default-IP-Routing-
Table, not advertised
Advertised to non peer-group peers:
10.1.0.2 10.200.200.13 10.200.200.14
50998
172.31.1.3 from 172.31.1.3 (172.31.1.3)
Origin IGP, metric 0, localpref 100, valid, external,
best Community: 50998:1 no-export
50998
172.31.1.3 from 10.1.0.2 (10.200.200.12)
Origin IGP, metric 0, localpref 100, valid, internal
Router CK1 , which is in Transit AS 50001, is not propagating the 10.254.0.0/24 prefix to its neighboring ASs. Based the "show IP BGP 10.254.0.0" output shown, determine a possible cause of this problem.

A. Because the 10.254.0.0/24 prefix is tagged with the no-export community
B. Because the best path chosen by BGP is the IBGP learned path
C. Because the best path chosen by BGP is the EBGP learned path
D. Because the 10.254.0.0/24 prefix has a MED of 0
E. Because of the EBGP split horizon rule

Answer: A

Explanation:
From the output shown above, the 10.254.0.0 route is indeed tagged with the BGP community of no-export. The Well Known BGP community of NO EXPORT means that the route can be advertised to other IBGP peers, but it is not to be passed to EBGP peers. If the BGP community of NO ADVERTISE was used instead, then this route would not be forwarded to both IBGP as well as EBGP peers.
Incorrect Answers:
B, C. Regardless of the path that the BGP route was learned, the default behavior is to forward the route to EBGP peers.
D. The metric 0 shown in the example above is the normal behavior for IBGP learned routes.
E. BGP does not use the split horizon rule. This rule applies to distance vector interior routing protocols. BGP is considered to be a path vector external routing protocol.

QUESTION 175
The Certkiller network is using BGP for Internet routing, and part of the router configuration is shown below:

```
router bgp 50101
neighbor 10.1.1.1 remote-as 50102
neighbor 10.2.2.2 remote-as 50103
neighbor 10.2.2.2 route-map test2 out
neighbor 10.1.1.1 route-map test out
!
ip as-path access-list 1 permit _50104$
ip as-path access-list 2 permit .*
!
route-map test permit 10
match as-path 1
set metric 140
!
route-map test permit 20
match as-path 2
!
route-map test2 permit 10
set metric 100
```

Based on the configuration above, which statement is correct?

A. All prefixes originating in AS 50104 will be advertised to the 10.1.1.1 neighbor with a MED of 150.
B. All prefixes not originating in AS 50104 will be advertised to the 10.1.1.1 neighbor with a MED of 0.
C. All prefixes not originating in AS 50104 will be advertised to the 10.1.1.1 neighbor.
D. All prefixes will be advertised to the neighbor with a MED of 100.
E. All prefixes originating in AS 50104 will be advertised to the 10.2.2.2 and the 10.1.1.1 neighbor with a MED of 100.

Answer: B

Explanation:
For the 10.1.1.1 BGP peer, route-map "test" is being applied. This route map has two statement entries. The first states that all traffic originating from AS 50104 (as shown by the "ip as-path access-list 1 permit _50104$" command statement)
should have the MED set to 140. The regular expression ".*" matches everything else, so all other traffic is to be routed normally. Since the default MED value is 0, all other traffic not originating in AS will be advertised to the 10.1.1.1 peer with a MED of 0.
Incorrect Answers:

A. The MED value advertised to the 10.1.1.1 peer that originated from AS 50104 will

have the MED value set to 140, not 150.
C. All prefixes, even the one originating from AS 50104 will be advertised to the 10.1.1.1 neighbor. The only difference with traffic originating from AS 50104 is that the MED values will be changed.
D, E. The default MED value is 0, not 100. The default local preference value is 100.

QUESTION 176
Assume that a BGP router has learned prefix 63.0.0.0/8 from two different BGP neighbors. Which statement regarding the BGP route selection process and how this route will be installed is correct?

A. The update from the neighbor that has the highest weight and the highest local preference becomes the preferred path.
B. The update from the neighbor that has the shortest AS path becomes the preferred path.
C. The update from the neighbor that has the highest local preference and the highest MED becomes the preferred path.
D. The update from the neighbor that has the lowest local preference becomes the preferred path.
E. The update from the neighbor that has the highest MED becomes the preferred path.

Answer: A

Explanation:
BGP selects only one path as the best path. When the path is selected, BGP puts the selected path in its routing table and propagates the path to its neighbors. BGP uses the following criteria, in the order presented, to select a path for a destination:
1. If the path specifies a next hop that is inaccessible, drop the update.
2. Prefer the path with the largest weight.
3. If the weights are the same, prefer the path with the largest local preference.
4. If the local preferences are the same, prefer the path that was originated by BGP running on this router.
5. If no route was originated, prefer the route that has the shortest AS_path.
6. If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than Incomplete).
7. If the origin codes are the same, prefer the path with the lowest MED attribute.
8. If the paths have the same MED, prefer the external path over the internal path.
9. If the paths are still the same, prefer the path through the closest IGP neighbor.
10. Prefer the path with the lowest IP address, as specified by the BGP router ID.
Incorrect Answers:
B: Although this statement is correct, the weight and local preference values have a higher precedence than the AS path length.
C, E: The lowest MED is preferred, not the highest.
D: A higher local preference is preferred over a lower one.

QUESTION 177
The Certkiller network is using BGP for external routing. If a BGP router has more than one route to the same IP prefix, in what order are BGP attributes examined in making a best path route selection?

A. LOCAL_PREF, MED, AS_PATH, WEIGHT, ORIGIN
B. WEIGHT, LOCAL_PREF, ORIGIN, AS_PATH; MED
C. WEIGHT, LOCAL_PREF, AS_PATH, ORIGIN, MED
D. WEIGHT; LOCAL_PREF, AS_PATH, MED, ORIGIN
E. MED, LOCAL_PREF, WEIGHT, ORIGIN, AS_PATH

Answer: C

Explanation:
BGP assigns the first valid path as the current best path. It then compares the best path with the next path in list, until it reaches the end of the list of valid paths. The following is a list of rules used to determine the best path.
1. Prefer the path with the highest WEIGHT.
Note: WEIGHT is a Cisco-specific parameter, local to the router on which it's configured.
2. Prefer the path with the highest LOCAL_PREF. Note the following:
3. Prefer the path that was locally originated via a network or aggregate BGP subcommand, or through redistribution from an IGP.
4. Prefer the path with the shortest AS_PATH.
5. Prefer the path with the lowest ORIGIN type: IGP is lower than EGP, and EGP is lower than INCOMPLETE.
6. Prefer the path with the lowest multi-exit discriminator (MED). Note the following:
7. Prefer external (eBGP) over internal (iBGP) paths. If bestpath is selected, go to Step 9 (multipath).
8. Prefer the path with the lowest IGP metric to the BGP next hop. Continue, even if bestpath is already selected.
9. Check if multiple paths need to be installed in the routing table for BGP Multipath. Continue, if bestpath is not selected yet.
o When both paths are external, prefer the path that was received first (the oldest one).
10. Prefer the route coming from the BGP router with the lowest router ID. The router ID is the highest IP address on the router, with preference given to loopback addresses. It can also be set manually using the bgp router-id command.
11. If the originator or router ID is the same for multiple paths, prefer the path with the minimum cluster list length. This will only be present in BGP route-reflector environments. It allows clients to peer with RRs or clients in other clusters. In this scenario, the client must be aware of the RR-specific BGP attribute.
12. Prefer the path coming from the lowest neighbor address. This is the IP address used in the BGP neighbor configuration, and corresponds to the remote peer used in the TCP connection with the local router

Reference:
www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a0080094431.shtml

---

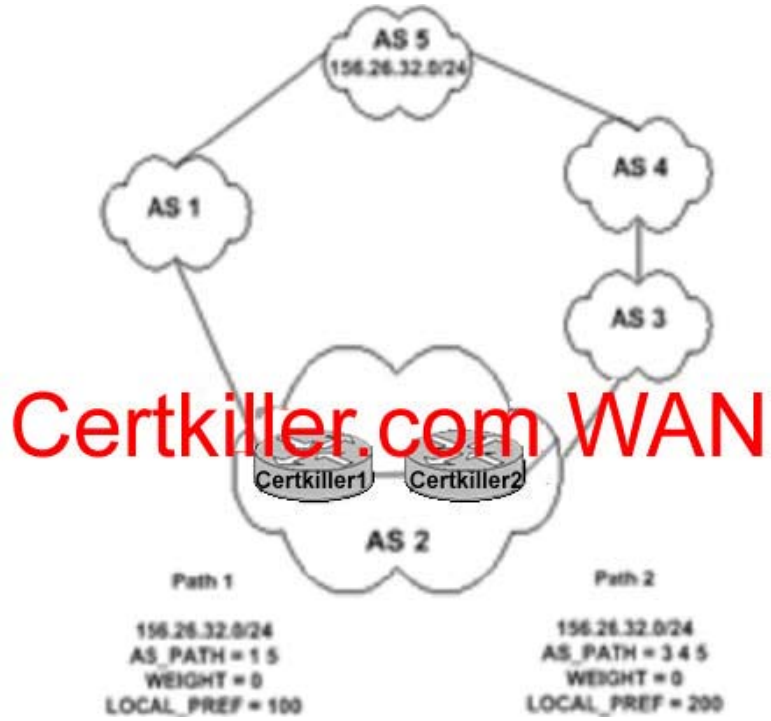
QUESTION 178
The router CK1 is being configured for BGP, and the configuration will contain both IBGP and EBGP peers. Which statements regarding IBGP and EBGP neighbors are correct? (Select three)

A. BGP updates from an IBGP peer are propagated to other IBGP and EBGP peers.
B. BGP updates from an EBGP peer are propagated to other IBGP and EBGP pees.
C. IBGP peers must be directly connected. If not, the IBGP-multihop option must be configured.
D. EBGP peers must be directly connected; otherwise, the EBGP-multihop option must be configured.
E. IBGP neighbors peering can be established using the loopback interface.
F. EBGP neighbor peering must use the physical interface address to establish peering

Answer: B, D, E

Explanation:
When a BGP router receives a BGP routing update from an EBGP neighbor, the update is propagated to all IBGP neighbors. It is important to note that the same is not true for routing updates received via an IBGP neighbor, as these updates are not passed on to all IBGP peers. This is why IBGP speakers must be configured in a full mesh.
For EBGP peers, the best method is to use the directly connected interfaces as the peering IP addresses. If not, then EBGP multihop must be used. Multihop is used only in EBGP, not in IBGP.
It is recommended to use the loopback interface when configuring IBGP peers, since this interface is always up. For IBGP, the peering IP address needs to only be reachable via the IGP, so they do not need to be directly connected.

QUESTION 179
The Certkiller network is running BGP as displayed in the diagram below:



What path will routers Certkiller 1 and Certkiller 2 take to reach the 156.36.32.0/24 network in AS 5?

A. Both will use the path through AS 1 due to Certkiller 1 having the shortest AS_PATH attributre.
B. Certkiller 1 will use the path through AS 1 and Certkiller 2 will use the path through AS 3.
C. Both will use the path through AS 1 due to Certkiller 1 having a lower LOCAL_PREF value.
D. Both Certkiller 1 and Certkiller 2 will use the path through AS 3 due to Certkiller 2 having a higher LOCA_PREF value.

Answer: D

Explanation:
BGP uses the following criteria, in the order presented, to select a path for a destination:
1. If the path specifies a next hop that is inaccessible, drop the update.
2. Prefer the path with the largest weight.
3. If the weights are the same, prefer the path with the largest local preference.
4. If the local preferences are the same, prefer the path that was originated by BGP running on this router.
5. If no route was originated, prefer the route that has the shortest AS_path.
6. If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than Incomplete).
7. If the origin codes are the same, prefer the path with the lowest MED attribute.
8. If the paths have the same MED, prefer the external path over the internal path.
9. If the paths are still the same, prefer the path through the closest IGP neighbor.

10. Prefer the path with the lowest IP address, as specified by the BGP router ID.
Based on the information above, the value of the Local Preference is considered before the length of the AS Path. When comparing the Local Preference value, the higher one is preferred.

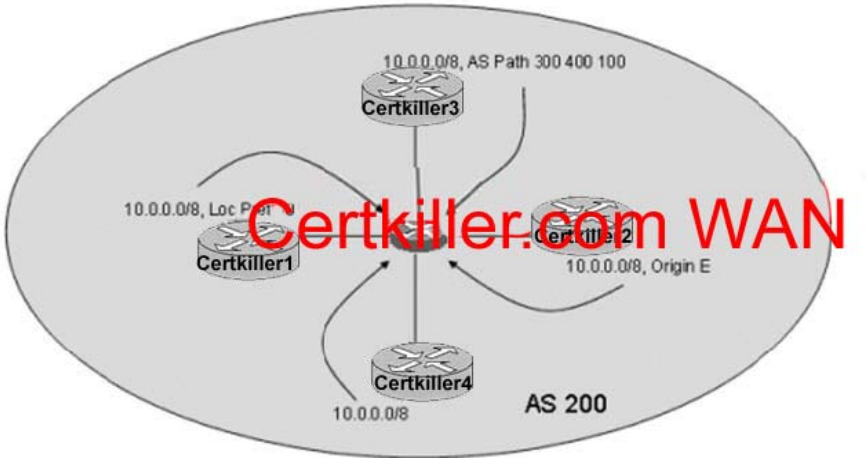
QUESTION 180
Router CK 1 and CK2 are IBGP peers. Which BGP attributes are carried in all IBGP routing updates? (Select 3)

A. MED
B. Local Preference
C. Weight
D. Community
E. AS-path
F. Cost
G. Origin

Answer: B, E, G

Explanation:
There are three well-known mandatory attributes. These must be included in updates propagated to all peers (both INGP and EBGP) and includes AS-PATH, NEXT-HOP and ORIGIN.
In addition to these three, all IBGP speakers must also carry the Local Preference information. The Local Preference is relevant when there is more than one path to a network outside of the current AS for instance if your network is connected to more than one ISP. Each of the routers that link to outside the AS can set a preference value for routes advertised into the AS, and this value indicates the router's preference for these routes. Only IBGP routers share the local preference values it does not leave the AS. The higher the value the more preferable the route is so if there are multiple paths to this network the route with the highest Local Preference is chosen and all traffic destined for the network is sent this way.

QUESTION 181
The Certkiller network resides in AS 200 as shown in the diagram below:



A BGP router receives updates for prefix 10.0.0.0/8 sourced from AS 100 from four different BGP neighbors. Certkiller 1 has the Local Preference of the prefix set to 50, while the other three neighbors do nothing with Loc Pref. Neighbor Certkiller 2 advertises the prefix with an AS path length of 3, while all other neighbors have an AS Path length of 2. The advertisement from neighbor Certkiller 3 has the origin code set to E, while the other have it set to I. And Neighbor Certkiller 4 does nothing to any of the attributes. What statement is true?

A. Neighbor Certkiller 1 is the preferred path to prefix 10.0.0.0/8, since a higher local preference is better, and local preference is compared before the others.
B. Neighbor Certkiller 2 is the preferred path to prefix 10.0.0.0/8, since a longer AS Path is better, and AS path is compared before the others.
C. Neighbor Certkiller 3 is the preferred path to prefix 10.0.0.0/8, since an origin code of E is better than I, and origin code is compared before the others.
D. Neighbor Certkiller 4 is the preferred path to prefix 10.0.0.0/8 only after neighbor Certkiller 2 dies.
E. Neighbor Certkiller 3 is the preferred path to prefix 10.0.0.0/8 only after neighbor Certkiller 4 dies.

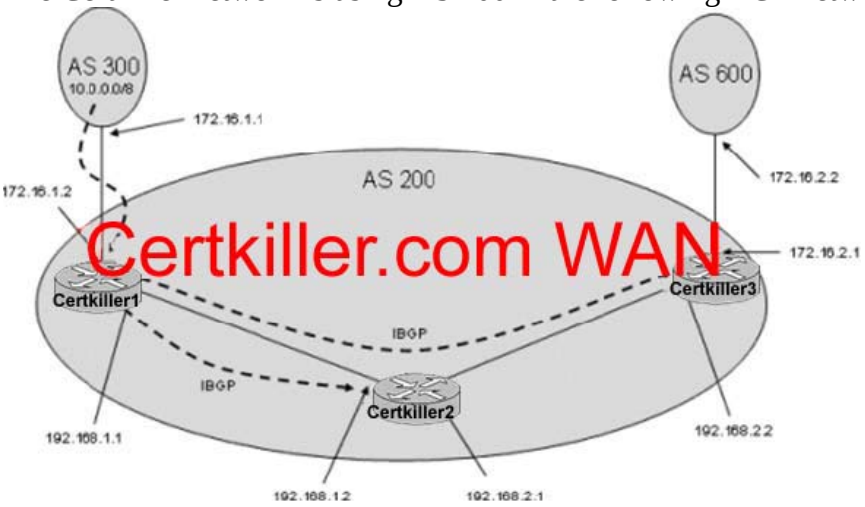
Answer: E

Explanation:
Based on the information provided, the route for 10.0.0.0/8 will be preferred from the following routers, in order:
1. Certkiller 4
2. Certkiller 3
3. Certkiller 2
4. Certkiller 1
BGP uses the following criteria, in the order presented, to select a path for a destination:
1. If the path specifies a next hop that is inaccessible, drop the update.
2. Prefer the path with the largest weight.
3. If the weights are the same, prefer the path with the largest local preference.
4. If the local preferences are the same, prefer the path that was originated by BGP running on this router.

5. If no route was originated, prefer the route that has the shortest AS_path.
6. If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP; and EGP is lower than Incomplete).
7. If the origin codes are the same, prefer the path with the lowest MED attribute.
Incorrect Answers:

A. The default local preference value is 100, so router Certkiller 1 will be the last router used because its local preference was set to 50.
B. A shorter AS path is preferred over a longer one.
C. An origin code of I (Internal) is preferred over an origin code of E (External).
D. Using the information given here, router Certkiller 4 will be preferred over all the others, and router Certkiller 2 will be used only if routers Certkiller 4 and Certkiller 3 both fail.

QUESTION 182
The Certkiller network is using AS 200 in the following BGP network:



Router Certkiller1 Configuration:

```
Certkiller1 (config)# router bgp 200
Certkiller1 (config-bgp)# neighbor 192.168.1.2 remote-as 200
Certkiller1 (config-bgp)# neighbor 192.168.1.2 next-hop-self
Certkiller1 (config-bgp)# neighbor 192.168.2.2 remote-as 200
```

Router Certkiller 1 receives an EBGP update containing 10.0.0.0/8 sourced from AS 300. Router Certkiller 1 then advertises 10.0.0.0/8 to routers Certkiller 2 and Certkiller 3 via IBGP. What does router Certkiller 3 use as a BGP next hop to reach network 10.0.0.0/8?

A. 172.16.1.1
B. 172.16.1.2
C. 192.168.1.1
D. 192.168.1.2
E. 192.168.2.1

Answer: A

Explanation:
The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers. For IBGP, the EBGP next-hop address is carried into the local AS, as illustrated in Figure 39-6.
Figure 39-5 BGP AS-path Attribute

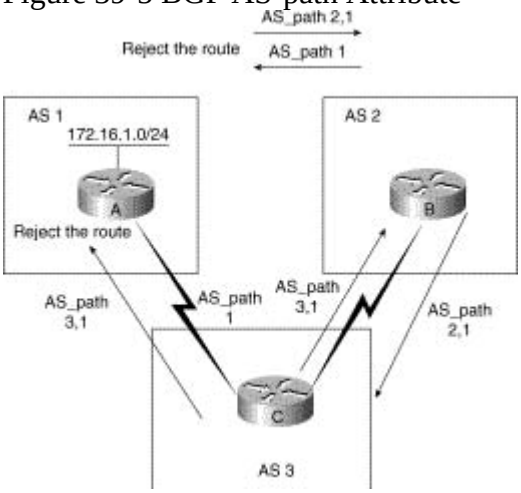
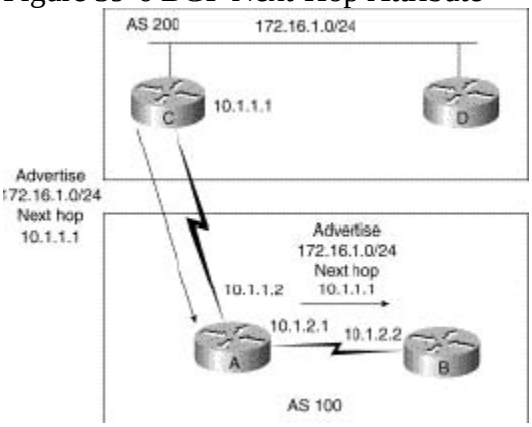


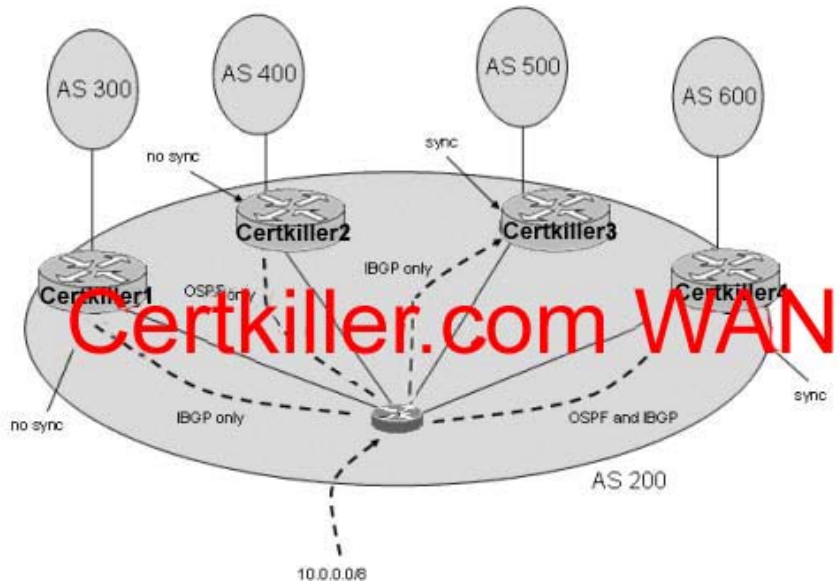
Figure 39-6 BGP Next-Hop Attribute



Router C advertises network 172.16.1.0 with a next hop of 10.1.1.1. When Router A propagates this route within its own AS, the EBGP next-hop information is preserved. If Router B does not have routing information regarding the next hop, the route will be discarded. Therefore, it is important to have an IGP running in the AS to propagate nexthop routing information.
Reference: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm

---

QUESTION 183
The Certkiller BGP network is using AS 200 as shown in the diagram below:



A router receives an EBGP update with prefix 10.0.0.0/8. This update is then forwarded to all BGP neighbors within its AS.
Which neighbors advertise 10.0.0.0/8 with EBGP updates of their own?

A. Only router Certkiller 1 advertises 10.0.0.0/8 into AS 300.
B. Both router Certkiller 1 and router Certkiller 2 advertise 10.0.0.0/8 into their respective neighbor ASs.
C. Both router Certkiller 1 and router Certkiller 4 advertise 10.0.0.0/8 into their respective neighbor ASs.
D. Both router Certkiller 2 and router Certkiller 4 advertise 10.0.0.0/8 into their respective neighbor ASs.
E. Routers Certkiller 1, Certkiller 2, and Certkiller 4 advertise 10.0.0.0/8 into their respective neighbor ASs.

Answer: C

Explanation:
A BGP router with synchronization enabled will not advertise iBGP-learned routes to other eBGP peers if it is not able to validate those routes in its IGP. Assuming that IGP has a route to iBGP-learned routes, the router will announce the iBGP routes to eBGP peers. Otherwise the router treats the route as not being synchronized with IGP and does not advertise it. Disabling synchronization using the no synchronization command under router BGP prevents BGP from validating iBGP routes in IGP. By default, synchronization is on for all BGP routers.
In this example, Certkiller 1 will advertise this route to its EBGP peer due to the fact that synchronization is disabled. Although synchronization is enabled on router Certkiller 4, it will advertise the route because it is running both OSPF and BGP, so this route will match the corresponding route within the OSPF table and be advertised.
Incorrect Answers:

A. Both Certkiller 1 and Certkiller 4 will advertise this route.

B, C, D. Certkiller 2 will not advertise this route. Since it is not an IBGP peer, it will not receive the routing update in the first place so it will not be able to forward this route on to the other AS.

QUESTION 184
The Certkiller 1 BGP routing routes are displayed below:

```
Certkiller1 #show ip route bgp
B    192.168.12.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.13.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.14.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.15.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.16.0/24 [200/0] via 2.2.2.2, 00:53:00
B    192.168.20.0/24 [200/0] via 2.2.2.2, 00:52:57
B    192.168.21.0/24 [200/0] via 2.2.2.2, 00:52:57
B    192.168.22.0/24 [200/0] via 2.2.2.2, 00:52:57
B    192.168.23.0/24 [200/0] via 2.2.2.2, 00:52:57
B    192.168.24.0/24 [200/0] via 2.2.2.2, 00:52:57

Certkiller1 #show run
!
! Partial show run output

router bgp 65101
 aggregate-address 192.168.12.0 255.255.252.0 summary-only
 aggregate-address 192.168.20.0 255.255.252.0 as-set
 neighbor 2.2.2.2 remote-as 65101
 neighbor 2.2.2.2 update-source loopback0
 neighbor 2.2.2.2 next-hop-self
 neighbor 10.1.1.1 remote-as 65104
```

Based on the show ip route bgp output and the partial show run output shown, which BGP prefixes will be advertised by Certkiller 1 to the 10.1.1.1 neighbor?

A. 192.168.12.0/22, 192.168.16.0/24, 192.168.20.0/22, 192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/22, 192.168.23.0/24, 192.168.24.0/24
B. 192.168.12.0/22, 192.168.20.0/22, 192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/22, 192.168.23.0/24, 192.168.24.0/24
C. 192.168.12.0/22, 192.168.20.0/22, 192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/22, 192.168.23.0/24
D. 192.168.12.0/22, 192.168.20.0/22, 192.168.20.0/24
E. 192.168.12.0/22, 192.168.20.0/22
F. All routes will be advertised, since there are no route filters in place.

Answer: A

Explanation:
When the aggregate-address command is used within BGP routing, the aggregated address is advertised, along with the more specific routes. The exception to this rule is through the use of the summary-only command. The "summary-only" keyword suppresses the more specific routes and announces only the summarized route.
Using the as-set argument creates an aggregate address with a mathematical set of

autonomous systems (AS). This as-set summarizes the AS_PATH attributes of the all of the individual routes. This can be useful to avoid routing loops while aggregating routes. Again, unless the "summary-only" keyword is used with the as-set command the summary route is advertised along with the more specific routes.
In the example above, the 192.168.12.0, 192.168.13.0, 192.168.14.0, and 192.168.15.0 networks will be summarized into the only 192.168.12/22 route, which will be advertised. Along with this one route, the others will also be advertised, as well as one additional 192.168.20.0/22 route. In total, 8 different routes will be advertised.

QUESTION 185
Many of the Certkiller BGP routers are configured using peer groups. Which of the following correctly display the common properties of BGP peer groups?

A. Community values
B. Inbound policies
C. Outbound policies
D. MED inbound policies
E. Transitive AS policies
F. None of the above

Answer: C

Explanation:
BGP neighbors who share the same outbound policies can be grouped together in what is called a BGP peer group. Instead of configuring each neighbor with the same policy individually, Peer group allows to group the policies which can be applied to individual peer thus making efficient update calculation along with simplified configuration.
Reference:
www.cisco.com/en/US/tech/ CK3 65/technologies_tech_note09186a0080093fb7.shtml

---

QUESTION 186
While verifying the BGP configuration of router Certkiller 1, you issue the following command:

```
Certkiller1#show route-map setweight
route-map test, permit, sequence 10
  Match clauses:
    ip address prefix-lists: filter
    as-path (as-path filter): 1 2
  Set clauses:
    weight 200
  Policy routing matches: 0 packets, 0 bytes
```


Based upon the show route-map setweight output shown above, which matching routes will be set to a weight of 200?

A. Routes that match the prefix-list named filter
AND
also match either the as-path filter 1 OR 2
B. Routes that match the prefix-list named filter
OR
also match either the as-path filter 1 AND 2
C. Routes that match the prefix-list named filter
AND
also match either the as-path filter 1 AND 2
D. Routes that match the prefix-list named filter
OR
also match either the as-path filter 1 OR 2

Answer: A

Explanation:
When the match clauses are shown on different lines, then all of the match conditions must be met. In this example, both the IP prefix list named "filter" and the AS path filter must match in order to set the weight to 200 as shown. However, in this configuration, there are two AS path filters configured, numbered 1 and 2. In this case, only one of the two filters needs to be matched. If all three of the criteria had needed to be met, then there would be three distinct lines listed under the match clauses.

QUESTION 187
An EIGRP multicast flow timer is defined as which of the following?

A. The timeout timer after which EIGRP retransmits to the neighbor in non CR mode, through unicasts.
B. The time interval that EIGRP hello packets are sent.
C. The timer after which EIGRP will not forward multicast data traffic.
D. The timer interval between consecutive transmitted EIGRP hello intervals.
E. The timeout timer after which EIGRP retransmits to the neighbor in CR mode, through unicasts.
F. None of the above.

Answer: E

Explanation:
After pair of routers become neighbors, they will send routing updates (and other packets) to one another using a reliable multicast scheme. For example, if router one has a series of packets which must be transmitted to routers two, three, and four such as a routing table update, it will send the first packet to the EIGRP multicast address, 224.0.0.10, and wait for an acknowledgment from each of its neighbors on its Ethernet interface (in this case, routers two, three and four). Let's assume that routers two and four do answer, but router three does not.
Router one will wait until the multicast flow timer expires on the Ethernet interface, then

send out a special packet, a sequence TLV, telling router three not to listen to any further multicast packets from router one, then it will continue transmitting the remainder of the update packets as multicast to all other routers on the network. The sequence TLV indicates an out-of-sequence multicast packet. Those routers not listed in the packet enter Conditional Receive (CR) mode, and continue listening to multicast. While there are some routers in this mode, the Conditional Receive bit will be set in multicast packets. In this case, router one will send out a sequence TLV with router three listed, so routers two and four will continue listening to further multicast updates.

QUESTION 188
Which components are factored in by default when an EIGRP metric is calculated? (Choose all that apply)

A. MTU
B. Delay
C. Load
D. Bandwidth
E. Reliability

Answer: B, D

Explanation:
By default, EIGRP uses only bandwidth and Delay when calculating the metric. EIGRP uses these scaled values to determine the total metric to the network:
• metric = [K1 * bandwidth + (K2 * bandwidth) / (256 - load) + K3 * delay] * [K5 / (reliability + K4)]
The default values for K are:
• K1 = 1
• K2 = 0
• K3 = 1
• K4 = 0
• K5 = 0
For default behavior, you can simplify the formula as: Metric = Bandwidth + Delay
Incorrect Answers:

A. The MTU is tracked but never used in calculating the metric for IGRP or EIGRP at any time.
C, E. Although Load and Reliability are K values that can indeed be factored into the metric, by default their K value is 0 so they are not used.
Reference:
http://www.cisco.com/warp/public/103/eigrp-toc.html#eigrpmetrics

---

QUESTION 189
The topology of a network changes causing an EIGRP router to go into the active state. The DUAL process shows a new route that meets the EIGRP Feasibility Condition. In regards to this specific route, which of the following is true?

A. The Feasible Distance of the new route must be equal to one.
B. The Feasible Distance of the new route must be higher than one.
C. The Reported Distance of the new route must be equal to Feasible Distance.
D. The Reported Distance of the new route must be higher than Feasible Distance.
E. The Reported Distance of the new route must be lower than Feasible Distance.

Answer: E

Explanation:
The following are some terms relating to EIGRP:
1. Feasible Distance: The lowest calculated metric to each destination
2. Feasibility Condition: A condition that is met if a neighbor's advertised distance to a destination is lower that the router's Feasible Distance to that same destination.
3. Successor: The neighbor that has been selected as the next hop for a given destination based on the Feasibility Condition.
Reference:
Jeff Doyle, Routing TCP/IP, Volume I, Chapter 8: Enhanced Interior Gateway Routing Protocol (EIGRP), p.336-337, Cisco Press, (ISBN 1-57870-041-8)
Incorrect Answers:
A: The metric of the new route needs only to be less than the current metric to the destination (feasible distance), and does not necessarily need to equal one.
B: It is feasible that the new metric to the destination could equal one, and also be lower than the current metric.
C, D: The reported distance must be lower than the feasible distance.
Additional info:
The Feasible Condition is met when the receiving router has a Feasible Distance (FD) to a particular network and it receives an update from a neighbor with a lower advertised or Reported Distance (RD) to that network. The neighbor then becomes a Feasible Successor (FS) for that route because it is one hop closer to the destination network. There may be a number of Feasible Successors in a meshed network environment.
The RD for a neighbor to reach a particular network must always be less than the FD for the local router to reach that same network. In this way EIGRP avoids routing loops. This is why routes that have RD larger than the FD are not entered into the Topology table.
Reference:
Ravi Malhotra, IP Routing, Chapter 4: Enhanced Interior Gateway Routing Protocol (EIGRP), O'Reilly Press, January 2002 (ISBN 0-596-00275-0)

QUESTION 190
Which of the following EIGRP packets require an acknowledgement? (Choose all that apply)

A. Hello
B. Query
C. Reply
D. Update

E. Ack
F. None of the above

Answer: B, C, and D

Explanation:
Updates are used to convey reachability of destinations. When a new neighbor is discovered, update packets are sent so the neighbor can build up its topology table. In this case, update packets are unicast. In other cases, such as a link cost change, updates are multicast. Updates are always transmitted reliably.
Queries and replies are sent when destinations go into Active state. Queries are always multicast unless they are sent in response to a received query. In this case, it is unicast back to the successor that originated the query. Replies are always sent in response to queries to indicate to the originator that it does not need to go into Active state because it has feasible successors. Replies are unicast to the originator of the query. Both queries and replies are transmitted reliably.
EIGRP reliable packets are: Update, Query and Reply.
EIGRP unreliable packets are: Hello and Ack.
Incorrect Answers:
A, E. Hellos are multicast for neighbor discovery/recovery. They do not require acknowledgment. A hello with no data is also used as an acknowledgment (ack). Acks are always sent using a unicast address and contain a non-zero acknowledgment number.
Reference: Cisco BSCN version 1.0 study guide, pages 6-18.

QUESTION 191
Which of the following types of EIGRP packets contain the Init flag?

A. Hello/Ack
B. Query
C. Reply
D. Update
E. None of the above

Answer: D

Explanation:
In EIGRP header there is an 8-bit flag value. The rightmost bit is init.
Which when set to 0x00000001 indicates that the enclosed route entries are the first in a new neighbor relationship.
Also the route entries are carried in update packet not hello packet.
Additional Info:
The following debug output displays the Init Sequence increasing only with the update packet.
Router# debug eigrp packet
EIGRP: Sending HELLO on Ethernet0/1
AS 109, Flags 0x0, Seq 0, Ack 0

EIGRP: Sending HELLO on Ethernet0/1
AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
AS 109, Flags 0x1, Seq 1, Ack 0
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
AS 109, Flags 0x0, Seq 2, Ack 0
Incorrect Answers:

A. Hellos are multicast for neighbor discovery/recovery. They do not require acknowledgment. A hello with no data is also used as an acknowledgment (ack). Acks are always sent using a unicast address and contain a non-zero acknowledgment number.
B, C. Queries and replies are sent when destinations go into Active state. Replies are always sent in response to queries to indicate to the originator that it does not need to go into Active state because it has feasible successors. Replies are unicast to the originator of the query. Both queries and replies are transmitted reliably.
Reference: "Routing TCP/IP" Jeff Doyle Pg364

QUESTION 192
In your EIGRP network you notice that the neighbor relationship between two of your routers was recently restarted. Which of the following could have occurred to have caused this? (Choose all that apply)

A. The clear ip route command was issued.
B. The ARP cache was cleared.
C. The IP cache was cleared.
D. An update packet with Init flag set from a known, already established neighbor relationship was received by one of the routers.
E. The IP EIGRP neighbor relationship was cleared manually.

Answer: D, E

Explanation:
D as well as E will result in EIGRP relationship to be restarted.
The reason for D: If a router receives an update packet with the init flag set it clearly implies that this packet is the first after a new neighbor relationship has been established.
The reason for E: If we clear the IP EIGRP neighbor relationship it will automatically result in EIGRP neighbor relationship to be restarted.
Incorrect Answers:

A. This will clear the IP routing table, but will not have any affect on the EIGRP

neighbor relationship.
B. This will only clear the MAC address learned ARP cache.
C. This also will not have any affect on the EIGRP neighbor relationship.

QUESTION 193
The Certkiller EIGRP network has a router named Router CK2 . Router CK2 is connected to an EIGRP neighbor, CK1 . CK1 is defined as a stub. With regard to this network, which of the following are true?

A. Router CK1 will not advertise any network routes to CK2 .
B. Router CK2 will send only summary routes to CK1 .
C. Router CK2 will not query CK1 about any internal route.
D. Router CK2 will not query CK1 about any external route.
E. Router CK2 will not query CK1 about any route.
F. None of the above.

Answer: E

Explanation:
E is the best choice, as an EIGRP router will not query a stub neighbor about any route.
Incorrect Answers:

A. CK1 will still be required to advertise its network routes to the neighbor, even though it is configured as a stub.
B. CK2 still sends all routes to CK1 .
C, D. Although both of these are true, since CK2 will not query CK1 about any route, E is a better choice.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/eigrpstb.htm

---

QUESTION 194
The Certkiller network uses EIGRP as the routing protocol and has an ISDN connection that is used as a backup to their frame relay network. The ISDN link successfully comes up when the frame relay network fails, but no routing traffic will pass over the ISDN link. What could be the cause of this problem?

A. The dialer-list is blocking EIGRP.
B. The EIGRP configuration is incorrect.
C. The encapsulation is different on the opposite ends of the link.
D. There is a network type mismatch.
E. The broadcast keyword is missing from the dialer-map.

Answer: E

Explanation:

For routing protocol traffic to pass over the ISDN link, the broadcast keyword must be present in the dialer map.
Incorrect Answers:

A. Although the dialer list may indeed be blocking EIGRP updates, so that these updates do not initiate ISDN calls, one the ISDN link is up, all traffic will be able to traverse this link, and not just the traffic that is defined as interesting.
C, D. If this were the case, there would be a problem with the ISDN link connecting in the first place.

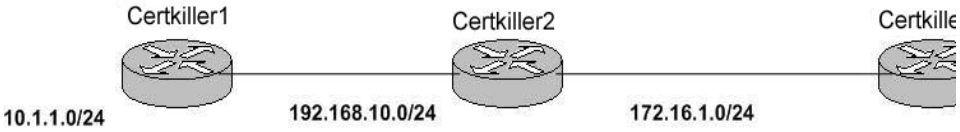
QUESTION 195
How is the metric for a summarized route derived when the interface summary command for EIGRP is used?

A. It is derived from the route that has the biggest metric.
B. It is derived from the route that has the smallest metric.
C. It is derived from the interface that has the summary command configured on it.
D. It is derived from the route that has the shortest matching mask.
E. It is derived from the default-metric.

Answer: B

Explanation:
According to Cisco's EIGRP design guide, "The metric is the best metric from among the summarized routes."
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfeigrp.htm#1001078
"...EIGRP will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes."

QUESTION 196
Routers Certkiller 1, Certkiller 2, and Certkiller 3 are all configured for EIGRP as shown below:



Certkiller 1 has the following configuration:
Router eigrp 1
Network 192.168.10.0
Redistribute connected
Which routes would show up in the routing table of Certkiller 3 as EIGRP routes? (Choose all that apply)

A. 10.1.0.0/16
B. 10.0.0.0/24

C. 10.0.0.0/8
D. 10.1.1.0/24
E. 192.168.10.0/24

Answer: C, E

Explanation:
EIGRP will perform auto-summarization of External Routes. Since the 10.1.1.0 network was redistributed into EIGRP via a connected network, this will automatically make this route external to EIGRP. The 192.168.10.0 network will also show up in the routing table as an EIGRP route through the normal EIGRP process.
Additional Info:
Auto-Summarization
EIGRP performs an auto-summarization
each time it crosses a border between two different major networks.
For example, in Figure 13, Router Two advertises only the 10.0.0.0/8 network to Router One, because the interface Router Two uses to reach Router One is in a different major network.

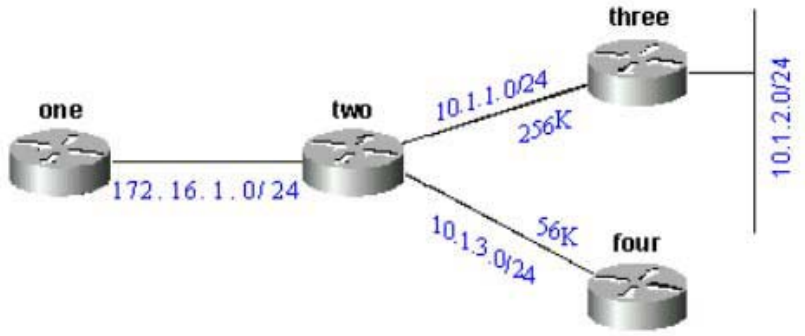
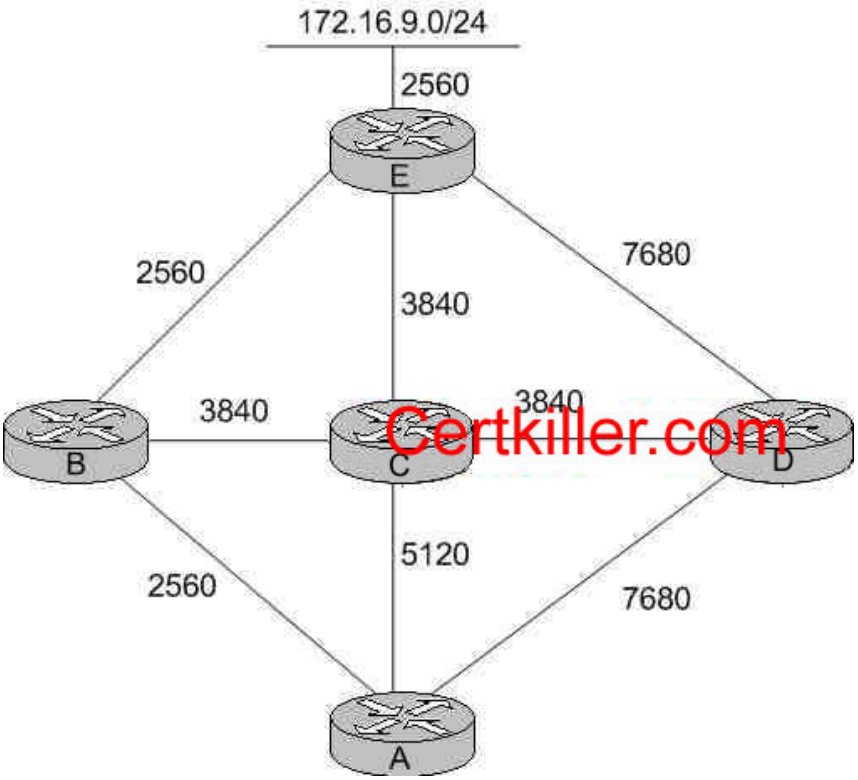


Figure 13

On Router One, this looks like the following:
one#show ip eigrp topology 10.0.0.0
IP-EIGRP topology entry for 10.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 11023872
Routing Descriptor Blocks:
172.16.1.1 (Serial0), from 172.16.1.2, Send flag is 0x0
Composite metric is (11023872/10511872), Route is Internal
Vector metric:
Minimum bandwidth is 256 Kbit
Total delay is 40000 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 1
This route is not marked as a summary route in any way; it looks like an internal route. The metric is the best metric from among the summarized routes. Note that the minimum bandwidth

on this route is 256k; although there are links in the 10.0.0.0 network that have a bandwidth of 56k.
On the router doing the summarization, a route is built to null0 for the summarized address:
two#show ip route 10.0.0.0
Routing entry for 10.0.0.0/8, 4 known subnets
Attached (2 connections)
Variably subnetted with 2 masks
Redistributing via eigrp 2000
C 10.1.3.0/24 is directly connected, Serial2
D 10.1.2.0/24 [90/10537472] via 10.1.1.2, 00:23:24, Serial1
D 10.0.0.0/8 is a summary, 00:23:20, Null0
C 10.1.1.0/24 is directly connected, Serial1
The route to 10.0.0.0/8 is marked as a summary through Null0. The topology table entry for this summary route looks like the following:
two#show ip eigrp topology 10.0.0.0
IP-EIGRP topology entry for 10.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 10511872
Routing Descriptor Blocks:
0.0.0.0 (Null0), from 0.0.0.0, Send flag is 0x0
(note: the 0.0.0.0 here means this route is originated by this router)
Composite metric is (10511872/0), Route is Internal
Vector metric:
Minimum bandwidth is 256 Kbit
Total delay is 20000 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 0
Incorrect Answers:
A, B, D. Any more specific routes in the 10.0.0.0 network will be summarized into one 10.0.0.0/8 network. Again, since the 10.0.0.0 network was learned by EIGRP only via redistribution, it is external as far as EIGRP is concerned.

QUESTION 197
The Certkiller EIGRP network topology is displayed below, along with the EIGRP metric values for each link:



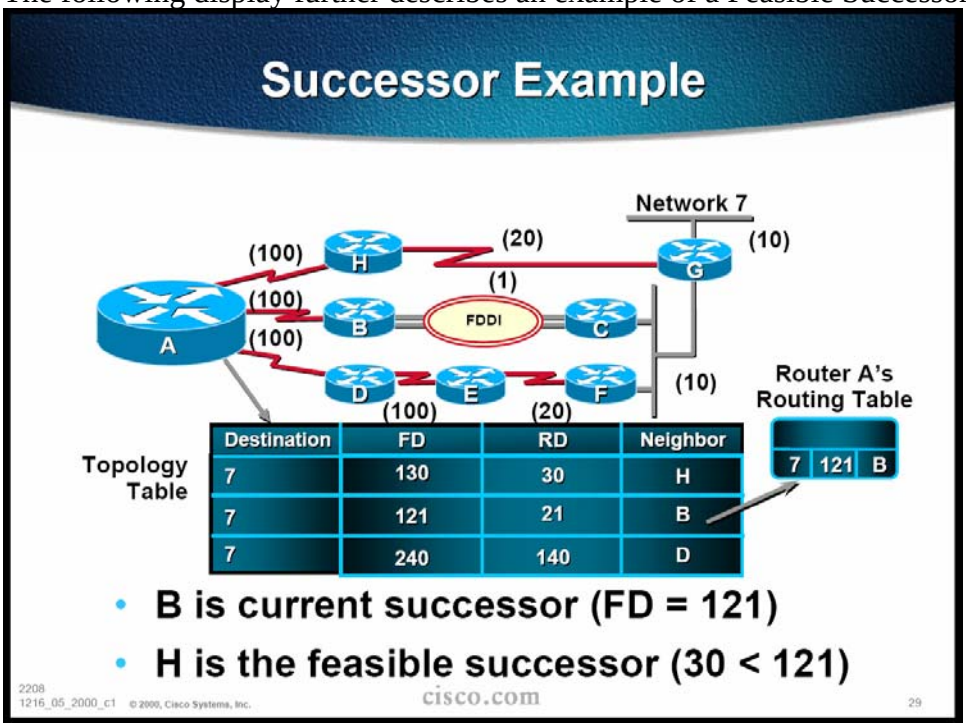
From the perspective of router A shown above, which of the following routers would be considered the successor and the feasible successors to the 172.16.9.0/24 network? (Select two choices below)

A. B is the successor
B. C is the successor
C. D is the successor
D. B is a feasible successor
E. C is a feasible successor
F. D is a feasible successor.
G. E is a feasible successor

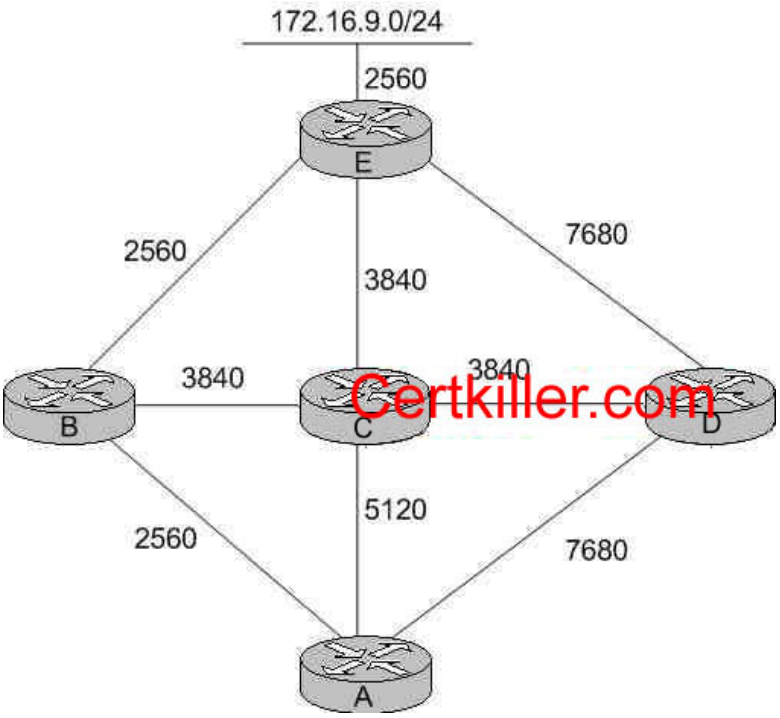
Answer: A, E

Explanation:
The following are some terms relating to EIGRP:
1. Feasible Distance: The lowest calculated metric to each destination
2. Feasibility Condition: A condition that is met if a neighbor's advertised distance to a destination is lower that the router's Feasible Distance to that same destination.
3. Successor: The neighbor that has been selected as the next hop for a given destination based on the Feasibility Condition.
4. Feasible Successor: A neighbor whose Reported Distance (RD) is less than the Feasible Distance (FD).
The Feasible Condition is met when the receiving router has a Feasible Distance (FD) to a particular network and it receives an update from a neighbor with a lower advertised or

Reported Distance (RD) to that network. The neighbor then becomes a Feasible Successor (FS) for that route because it is one hop closer to the destination network. There may be a number of Feasible Successors in a meshed network environment. The RD for a neighbor to reach a particular network must always be less than the FD for the local router to reach that same network. In this way EIGRP avoids routing loops. This is why routes that have RD larger than the FD are not entered into the Topology table. In this example, Router B would be the successor, with a feasible distance of 7680 (2560+2560+2560). Therefore, only routers with an AD of less than 7680 will become successors. In this case, router C will have an Advertised Distance of 6400 so it is a FS. Router D has a RD of 10240, and since it must be less than the current FD, it will not become a FS.
Reference:
Jeff Doyle, Routing TCP/IP, Volume I, Chapter 8: Enhanced Interior Gateway Routing Protocol (EIGRP), p.336-337, Cisco Press, (ISBN 1-57870-041-8)
The following display further describes an example of a Feasible Successor:



QUESTION 198
The Certkiller EIGRP network is displayed in the following diagram:



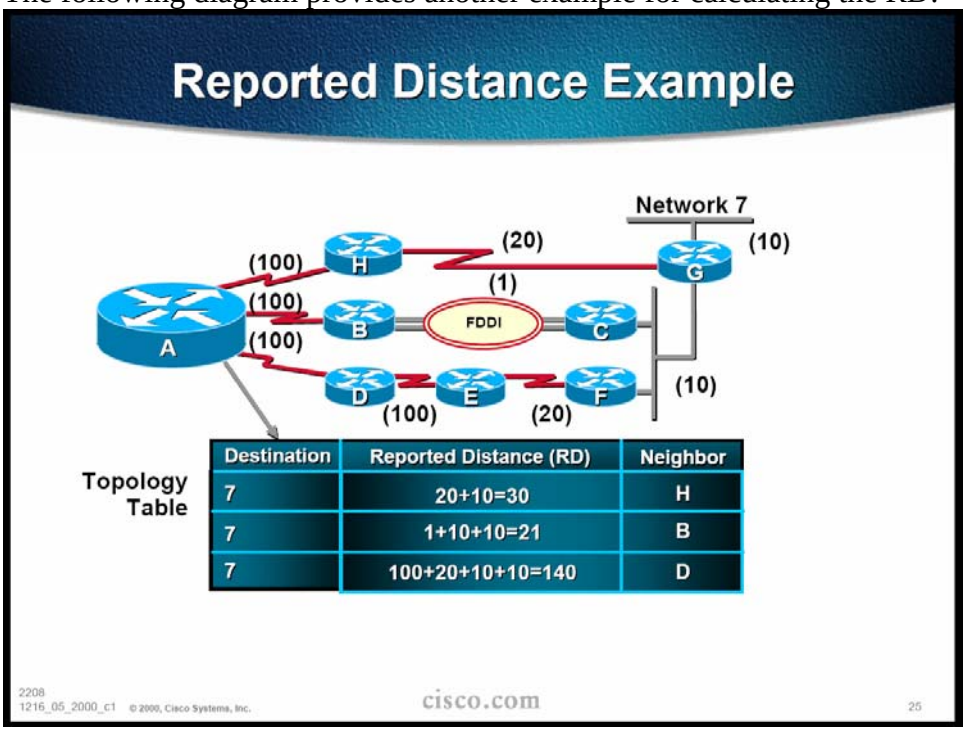
The associated EIGRP metric is listed as shown above for each of the links. Based on this information, what is the reported distance to network 172.16.9.0/24 from router C to router A?

A. 5120
B. 6400
C. 17,920
D. 10,240
E. 11,520
F. 2560
G. None of the above

Answer: B

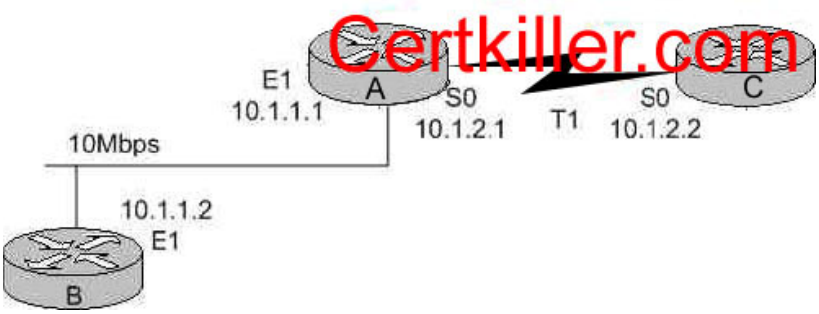
Explanation:
The following are some terms relating to EIGRP:
1. Feasible Distance: The lowest calculated metric to each destination
2. Feasibility Condition: A condition that is met if a neighbor's advertised distance to a destination is lower that the router's Feasible Distance to that same destination.
3. Successor: The neighbor that has been selected as the next hop for a given destination based on the Feasibility Condition.
4. Feasible Successor: A neighbor whose Reported Distance (RD) is less than the Feasible Distance (FD).
In the example above, the Feasible Distance to network 172.16.9.0/24 from C to A would be the distance that this network is from router C. In this case, the distance is 2560+3840=6400, so Choice B is correct.

The following diagram provides another example for calculating the RD:



QUESTION 199

The Certkiller EIGRP network is displayed in the exhibit below:



The "Show IP EIGRP neighbor" command is issued on the router
A. Router A is
configured with the default EIGRP settings. After issuing this command, which of the following answer choices correctly describe the expected output?

A. routerA#show ip eigrp neighbor
IP-EIGRP neighbors for process 1

H	Address	Interface	Hold (Sec)	Uptime	SRTT (ms)	RTO	Q	Seq
1	10.1.1.2	Et1	13	12:00:53	12	300	0	620
0	10.1.2.2	S0	174	12:00:56	17	200	0	645

B. routerA#show ip eigrp neighbor
IP-EIGRP neighbors for process 1

H	Address	Interface	Hold (Sec)	Uptime	SRTT (ms)	RTO	Q	Seq Cnt Num
1	10.1.1.2	Et1	20	12:00:53	12	300	0	620
0	10.1.2.2	S0	190	12:00:56	17	200	0	645

C. routerA#show ip eigrp neighbor
IP-EIGRP neighbors for process 1

H	Address	Interface	Hold (Sec)	Uptime	SRTT (ms)	RTO	Q	Seq Cnt Num
1	10.1.1.2	Et1	174	12:00:53	12	300	0	620
0	10.1.2.2	S0	13	12:00:56	17	200	0	645

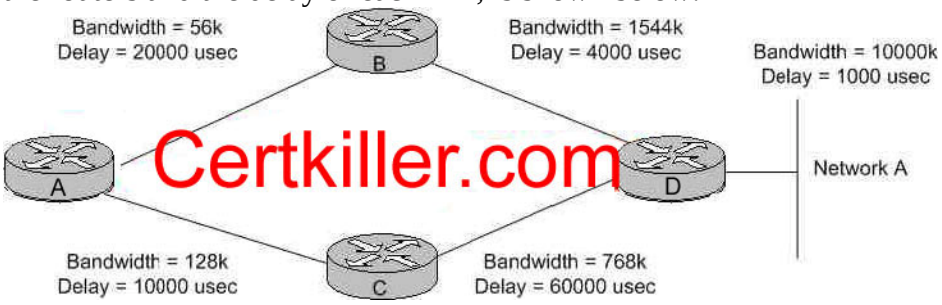
D. routerA#show ip eigrp neighbor
IP-EIGRP neighbors for process 1

H	Address	Interface	Hold	Uptime (Sec)	SRTT (ms)	RTO	Q	Seq Cnt Num
1	10.1.1.2	Et1	185	12:00:53 19	12	300	0	620
0	10.1.2.2	S0		12:00:56	17	200	0	645

Answer: A

Explanation:
The value in the Hold column of the command output should never exceed the hold time, and should never be less than the hold time minus the hello interval (unless, of course, you are losing hello packets). If the Hold column usually ranges between 10 and 15 seconds, the hello interval is 5 seconds and the hold time is 15 seconds. If the Hold column usually has a wider range - between 120 and 180 seconds - the hello interval is 60 seconds and the hold time is 180 seconds.
The EIGRP default timer settings are:
Hello Interval: 5 seconds for all high speed links
60 seconds for low speed links (T1 or less)
The default hold timer is less 3 times the hello interval. Since this question tells us that the default values are used, the Router A would have a value of not more than 15 seconds for the Ethernet peer and 180 seconds for the serial peer, so choice A is correct.
Incorrect Answers:
B, D. The timers for both the Ethernet and serial peers are above the maximum theoretical values for a working EIGRP network, assuming that the default timers are being used.
C. The timer values in this choice is wrong. High speed links such as ethernet use a shorter hello interval than low speed T1 links.

QUESTION 200
The Certkiller EIGRP network, along with the configured bandwidth statements of the routers and the delay of each link, is shown below:



Assuming that all EIGRP routers are all using default configurations, what path would router A choose to route packets to network A?

A. Router A takes the path through router B.
B. Router A takes the path through router C.
C. Router A would load balance to both router B and router C.
D. Neither path would be chosen as there is a loop in the network.
E. The metrics shown are too large, and the route to network A would be considered unreachable.

Answer: B

Explanation:
When all 5 of the K values are set to the default values, the EIGRP metric calculation for each link is found by the default formula of (Bandwidth + Delay) x 256. The metric calculation is the same as IGRP, but the result is multiplied by 256 for finer granularity. In this case, the bandwidth component is found in the same was as the OSPF metric, which is 10,000,000/bandwidth. It is important to note that only the minimum outgoing bandwidth is used, so along any path from A to Z, the slowest link among all the hops is used as the chosen metric for the bandwidth portion. This is true for both IGRP and EIGRP (See Routing TCP/IP by Jeff Doyle, page 243-244). The delay metric is found by adding the total delay of the path (in microseconds) and dividing by 10.
For this question, the shortest path can be found by comparing the two different choices that we really have (through router B or router C). For the path through router B the bandwidth metric is:
(10 million/56) + (24000/10) x 256 = (178571 + 2400) x 256 = 46328683.
For the path going through router C:
(10 million/128) + (70000/10) x 256 = (78125 + 7000) x 256 = 21792000.
Note that only the lowest bandwidth metric was used along the entire path, where as the delay was added at each hop. Also note that the calculation for the path from router D to network A was omitted, since this value would be simply added to the metrics above would not change the answer.
Incorrect Answers:

A. The path through this router has a higher metric and so would not be used.
C. By default, EIGRP would load balance over equal cost paths. Although these paths

are not equally valued, load balancing could occur despite this if the "variance" EIGRP feature was used. However, the variance command is not enabled by default.
D. Although a loop does exist, EIGRP routers maintain loop avoidance techniques, including keeping track of hop counts used. For IGRP and EIGRP, there is a maximum hop count of 100 hops.
E. Both of the metric listed above are well within the maximum limits set by EIGRP.