Cisco 200-120
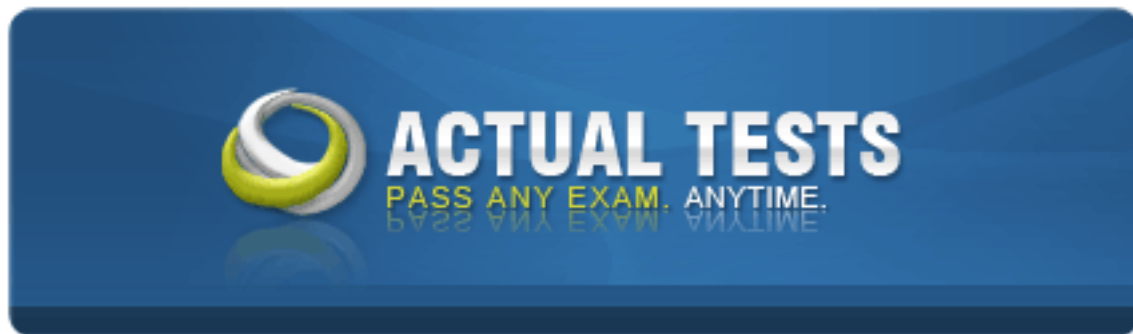

CCNA Cisco Certified Network Associate CCNA
Version: 18.1

Topic 1, Operation of IP Data Networks

QUESTION NO: 1

Refer to the exhibit:

```
Router1# show ip arp
Protocol   Address        Age(min)   Hardware Adddr   Type   Interface
Internet   192.168.20.5      9        0000.0c07.f892   ARPA   FastEthernet0/0
Internet   192.168.60.5      8        0000.0c07.ac00   ARPA   FastEthernet0/1
Internet   192.168.20.1      -        0000.0c63.ae45   ARPA   FastEthernet0/0
Internet   192.168.40.5      9        0000.0c07.4320   ARPA   FastEthernet0/2
Internet   192.168.60.1      -        0000.0c63.1300   ARPA   FastEthernet0/1
Internet   192.168.40.1      -        0000.0c36.6965   ARPA   FastEthernet0/2
```

Data Frame:

Source MAC	Source IP	Destination MAC	Destination IP
0000.0c07.f892	192.168.20.5	0000.0c63.ae45	192.138.40.5

What will Router1 do when it receives the data frame shown? (Choose three.)

A. Router1 will strip off the source MAC address and replace it with the MAC address 0000.0c36.6965.
B. Router1 will strip off the source IP address and replace it with the IP address 192.168.40.1.
C. Router1 will strip off the destination MAC address and replace it with the MAC address 0000.0c07.4320.
D. Router1 will strip off the destination IP address and replace it with the IP address of 192.168.40.1.
E. Router1 will forward the data packet out interface FastEthernet0/1.
F. Router1 will forward the data packet out interface FastEthernet0/2.
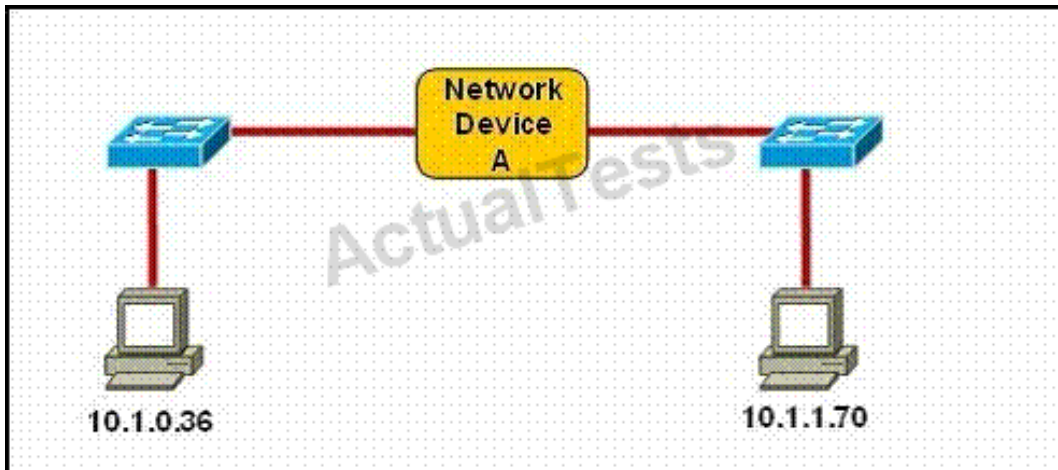
Answer: A,C,F
Explanation:
Remember, the source and destination MAC changes as each router hop along with the TTL being decremented but the source and destination IP address remain the same from source to destination.

QUESTION NO: 2

Refer to the exhibit.

Which three statements correctly describe Network Device A? (Choose three.)

A. With a network wide mask of 255.255.255.128, each interface does not require an IP address.
B. With a network wide mask of 255.255.255.128, each interface does require an IP address on a unique IP subnet.
C. With a network wide mask of 255.255.255.0, must be a Layer 2 device for the PCs to communicate with each other.
D. With a network wide mask of 255.255.255.0, must be a Layer 3 device for the PCs to communicate with each other.
E. With a network wide mask of 255.255.254.0, each interface does not require an IP address.

Answer: B,D,E
Explanation:
If Subnet Mask is 255.255.255.128 the hosts vary from x.x.x.0 - x.x.x.127 & x.x.x.128- x.x.x.255,so the IP Addresses of 2 hosts fall in different subnets so each interface needs an IP an address so that they can communicate each other.

If Subnet Mask is 255.255.255.0 the 2 specified hosts fall in different subnets so they need a Layer 3 device to communicate.

If Subnet Mask is 255.255.254.0 the 2 specified hosts are in same subnet so are in network address and can be accommodated in same Layer 2 domain and can communicate with each other directly using the Layer 2 address.

QUESTION NO: 3

Which layer in the OSI reference model is responsible for determining the availability of the receiving program and checking to see if enough resources exist for that communication?

A. transport
B. network
C. presentation
D. session
E. application

Answer: E
Explanation:
This question is to examine the OSI reference model.
The Application layer is responsible for identifying and establishing the availability of the intended communication partner and determining whether sufficient resources for the intended communication exist.

QUESTION NO: 4

Which of the following describes the roles of devices in a WAN? (Choose three.)

A. A CSU/DSU terminates a digital local loop.
B. A modem terminates a digital local loop.
C. A CSU/DSU terminates an analog local loop.
D. A modem terminates an analog local loop.
E. A router is commonly considered a DTE device.
F. A router is commonly considered a DCE device.

Answer: A,D,E
Explanation:
The idea behind a WAN is to be able to connect two DTE networks together through a DCE network. The network's DCE device (includes CSU/DSU) provides clocking to the DTE-connected interface (the router's serial interface).
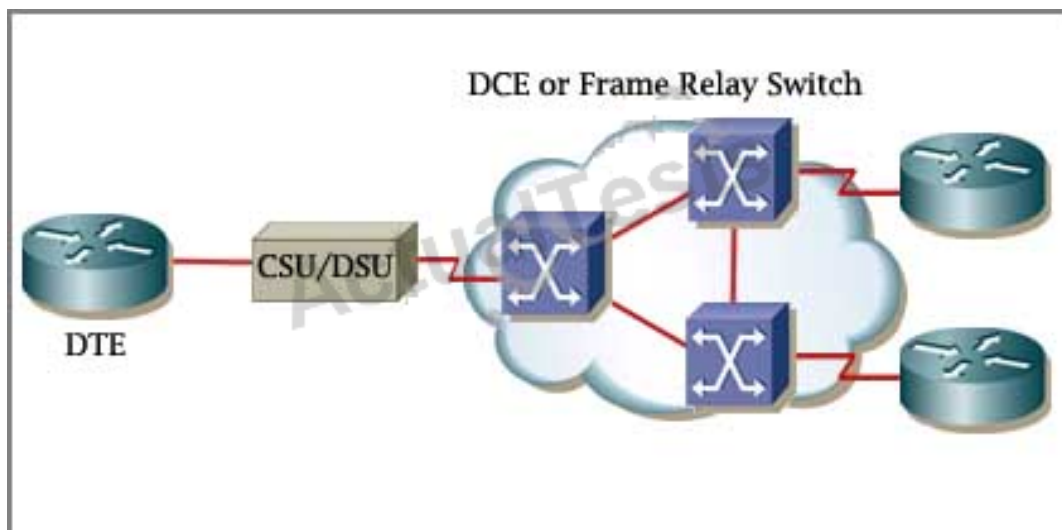
A modem modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device. A CSU/DSU is used between two digital lines -

For more explanation of answer D, in telephony the **local loop** (also referred to as a subscriber line) is the physical link or circuit that connects from the demarcation point of the customer premises to the edge of the carrier or telecommunications service provider's network. Therefore a modem terminates an analog local loop is correct.

QUESTION NO: 5

Refer to the exhibit.
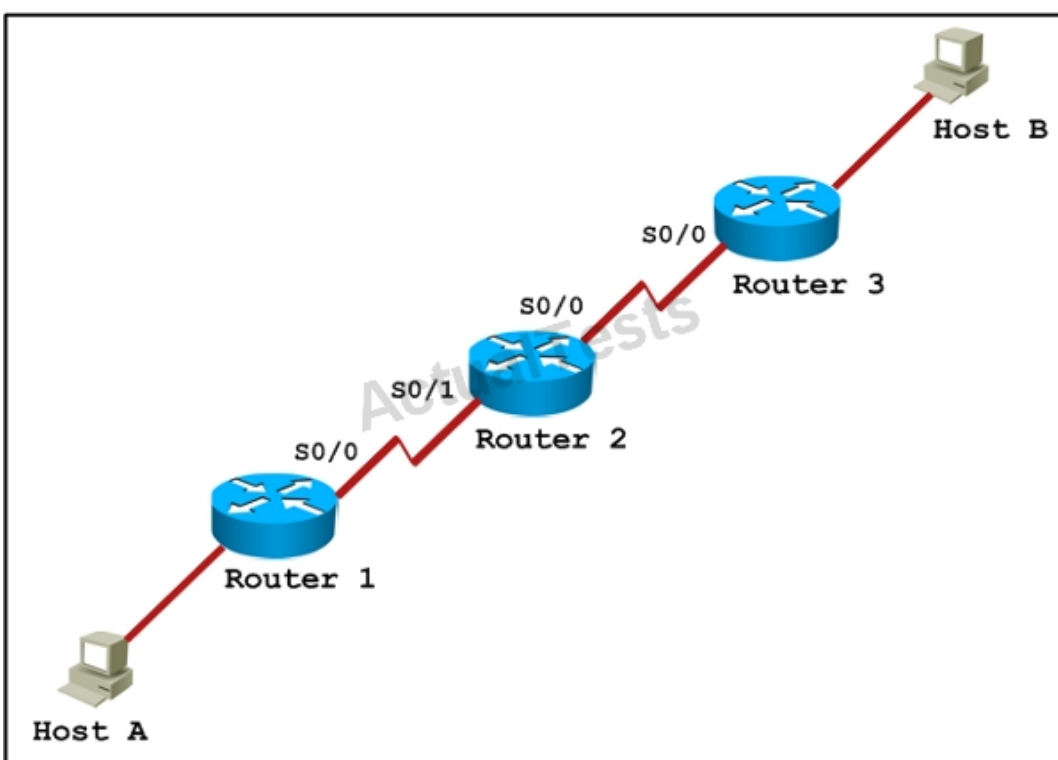
Host A pings interface S0/0 on router 3. What is the TTL value for that ping?

A. 252
B. 253
C. 254
D. 255

Answer: B

Explanation: Explanation

From the CCNA ICND2 Exam book: "Routers decrement the TTL by 1 every time they forward a packet; if a router decrements the TTL to 0, it throws away the packet. This prevents packets from rotating forever." I want to make it clear that before the router forwards a packet, the TTL is still remain the same. For example in the topology above, pings to S0/1 and S0/0 of Router 2 have the same TTL.

The picture below shows TTL values for each interface of each router and for Host B. Notice that Host A initializes ICMP packet with a TTL of 255:
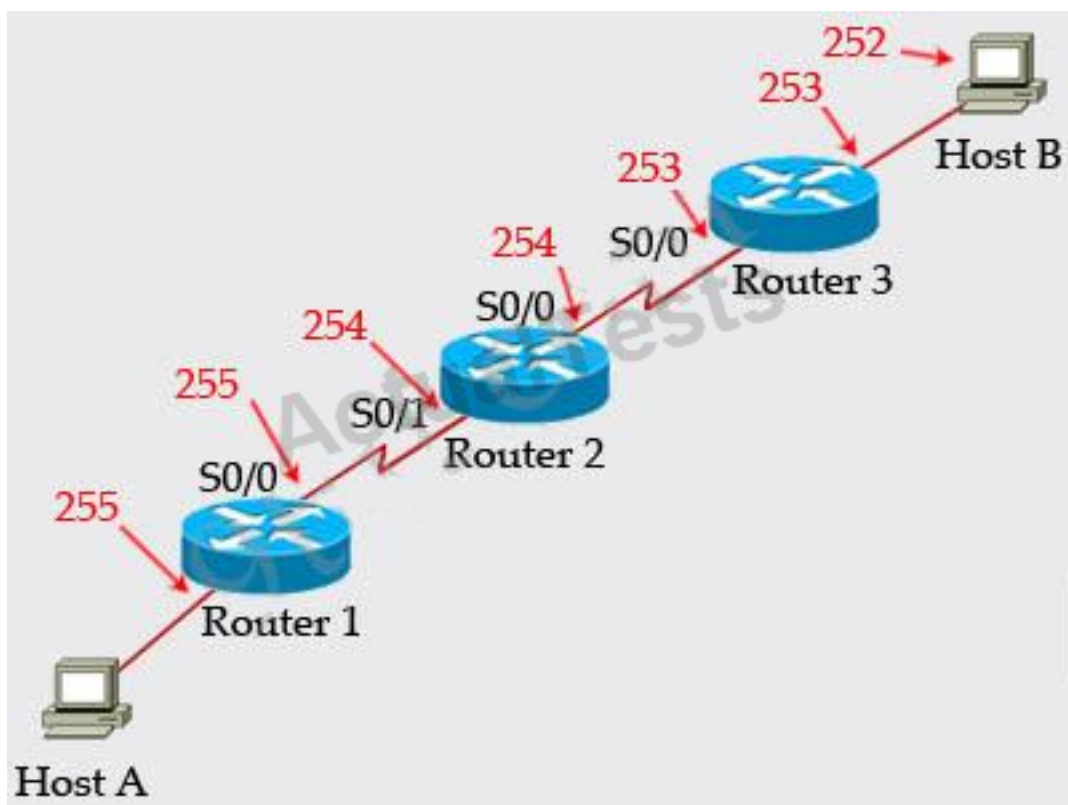
QUESTION NO: 6

A network administrator is verifying the configuration of a newly installed host by establishing an

FTP connection to a remote server. What is the highest layer of the protocol stack that the network administrator is using for this operation?

A. application
B. presentation
C. session
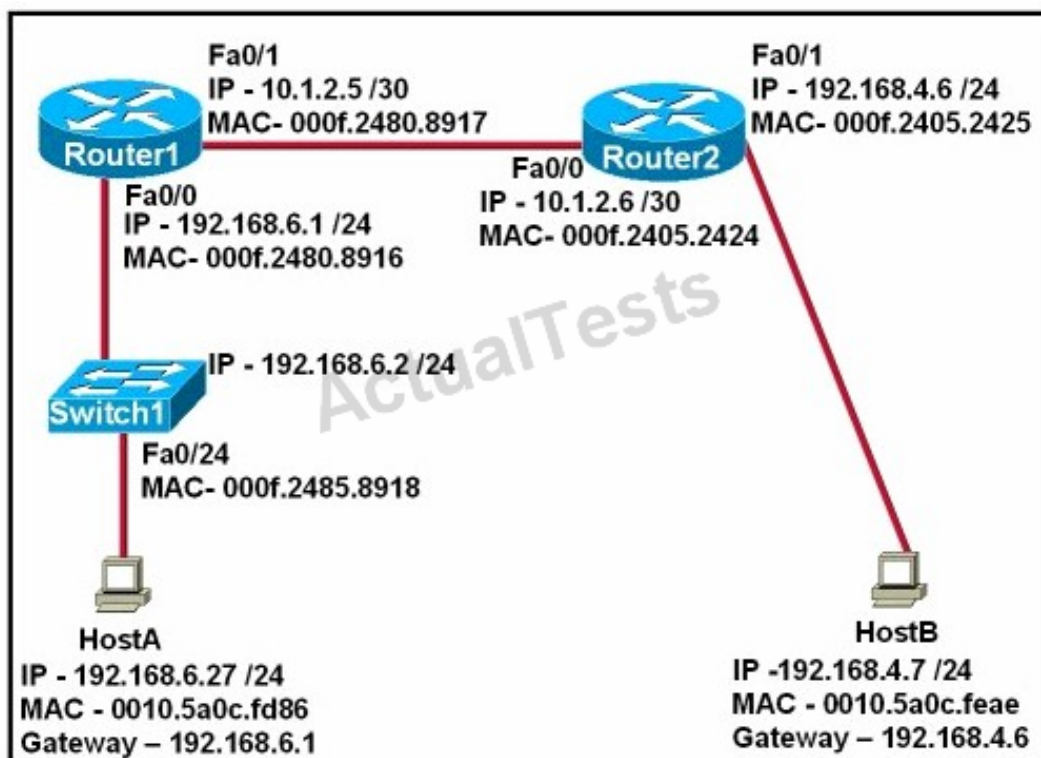**D.** transport
E. internet
F. data link

Answer: A

Explanation: Explanation

FTP belongs to Application layer and it is also the highest layer of the OSI model.

QUESTION NO: 7

Refer to the exhibit.

After HostA pings HostB, which entry will be in the ARP cache of HostA to support this transmission?

A.

Interface Address	Physical Address	Type
192.168.4.7	000f.2480.8916	dynamic

B.

Interface Address	Physical Address	Type
192.168.4.7	0010.5a0c.feae	dynamic

C.

Interface Address	Physical Address	Type
192.168.6.1	0010.5a0c.feae	dynamic

D.

Interface Address	Physical Address	Type
192.168.6.1	000f.2480.8916	dynamic

E.

Interface Address	Physical Address	Type
192.168.6.2	0010.5a0c.feae	dynamic

F.

Interface Address	Physical Address	Type
192.168.6.2	000f.2485.8918	dynamic

A. Exhibit A
B. Exhibit B
C. Exhibit C
D. Exhibit D
E. Exhibit E
F. Exhibit F

Answer: A

Explanation:

When a host needs to reach a device on another subnet, the ARP cache entry will be that of the Ethernet address of the local router (default gateway) for the physical MAC address. The destination IP address will not change, and will be that of the remote host (HostB).

QUESTION NO: 8

A network interface port has collision detection and carrier sensing enabled on a shared twisted pair network. From this statement, what is known about the network interface port?

A. This is a 10 Mb/s switch port.
B. This is a 100 Mb/s switch port.
C. This is an Ethernet port operating at half duplex.
D. This is an Ethernet port operating at full duplex.
E. This is a port on a network interface card in a PC.

Answer: C

Explanation:

Modern Ethernet networks built with switches and full-duplex connections no longer utilize CSMA/CD. CSMA/CD is only used in obsolete shared media Ethernet (which uses repeater or hub).

QUESTION NO: 9

A receiving host computes the checksum on a frame and determines that the frame is damaged. The frame is then discarded. At which OSI layer did this happen?

A. session
B. transport
C. network
D. data link
E. physical

Answer: D

Explanation:

The Data Link layer provides the physical transmission of the data and handles error notification, network topology, and flow control. The Data Link layer formats the message into pieces, each called a data frame, and adds a customized header containing the hardware destination and source address. Protocols Data Unit (PDU) on Datalink layer is called frame. According to this question the frame is damaged and discarded which will happen at the Data Link layer.

QUESTION NO: 10

Which of the following correctly describe steps in the OSI data encapsulation process? (Choose two.)

A. The transport layer divides a data stream into segments and may add reliability and flow control information.

B. The data link layer adds physical source and destination addresses and an FCS to the segment.
C. Packets are created when the network layer encapsulates a frame with source and destination host addresses and protocol-related control information.
D. Packets are created when the network layer adds Layer 3 addresses and control information to a segment.
E. The presentation layer translates bits into voltages for transmission across the physical link.

Answer: A,D
Explanation:
The Application Layer (Layer 7) refers to communications services to applications and is the interface between the network and the application. Examples include. Telnet, HTTP, FTP, Internet browsers, NFS, SMTP gateways, SNMP, X.400 mail, and FTAM.

The Presentation Layer (Layer 6) defining data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption also is defined as a presentation layer service. Examples include. JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, MPEG, and MIDI.

The Session Layer (Layer 5) defines how to start, control, and end communication sessions. This includes the control and management of multiple bidirectional messages so that the application can be notified if only some of a series of messages are completed. This allows the presentation layer to have a seamless view of an incoming stream of data. The presentation layer can be presented with data if all flows occur in some cases. Examples include. RPC, SQL, NFS, NetBios names, AppleTalk ASP, and DECnet SCP

The Transport Layer (Layer 4) defines several functions, including the choice of protocols. The most important Layer 4 functions are error recovery and flow control. The transport layer may provide for retransmission, i.e., error recovery, and may use flow control to prevent unnecessary congestion by attempting to send data at a rate that the network can accommodate, or it might not, depending on the choice of protocols. Multiplexing of incoming data for different flows to applications on the same host is also performed. Reordering of the incoming data stream when packets arrive out of order is included. Examples include. TCP, UDP, and SPX.

The Network Layer (Layer 3) defines end-to-end delivery of packets and defines logical addressing to accomplish this. It also defines how routing works and how routes are learned; and how to fragment a packet into smaller packets to accommodate media with smaller maximum transmission unit sizes. Examples include. IP, IPX, AppleTalk DDP, and ICMP. Both IP and IPX define logical addressing, routing, the learning of routing information, and end-to-end delivery rules. The IP and IPX protocols most closely match the OSI network layer (Layer 3) and are called Layer 3 protocols because their functions most closely match OSI's Layer 3.
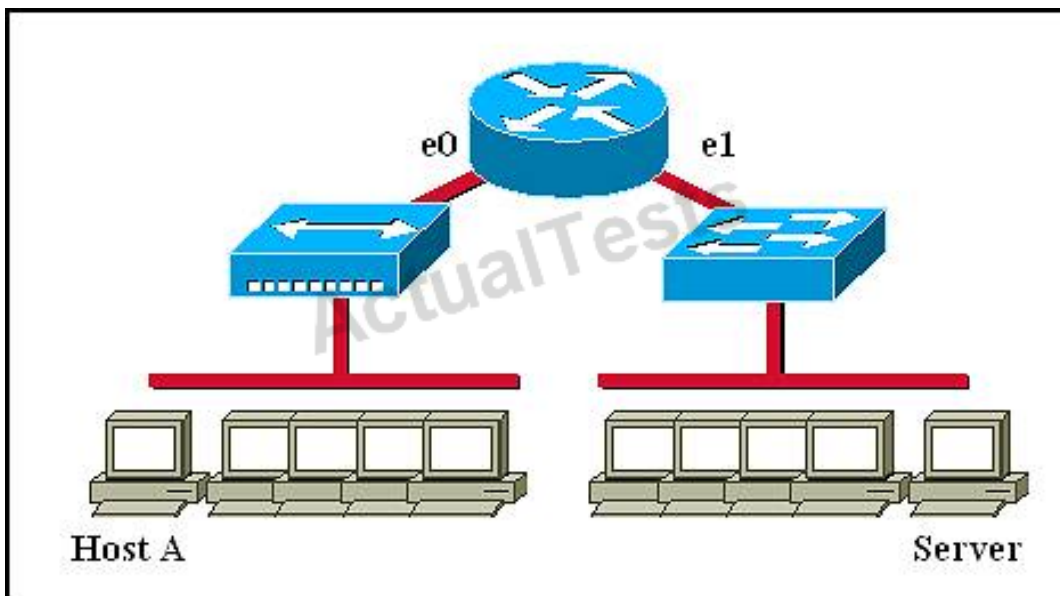
The Data Link Layer (Layer 2) is concerned with getting data across one particular link or medium.

The data link protocols define delivery across an individual link. These protocols are necessarily concerned with the type of media in use. Examples includE. IEEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, ATM, and IEEE 802.5/802.2.

QUESTION NO: 11

Refer to the graphic.

Host A is communicating with the server. What will be the source MAC address of the frames received by Host A from the server?

A. the MAC address of router interface e0
B. the MAC address of router interface e1
C. the MAC address of the server network interface
**D.** the MAC address of host A

Answer: A
Explanation:
Whereas switches can only examine and forward packets based on the contents of the MAC header, routers can look further into the packet to discover the network for which a packet is destined. Routers make forwarding decisions based on the packet's network-layer header (such as an IPX header or IP header). These network-layer headers contain source and destination network addresses. Local devices address packets to the router's MAC address in the MAC header. After receiving the packets, the router must perform the following steps:

1. Check the incoming packet for corruption, and remove the MAC header . The router checks the packet for MAC-layer errors. The router then strips off the MAC header and examines the network-layer header to determine what to do with the packet.

2. Examine the age of the packet. The router must ensure that the packet has not come too far to be forwarded. For example, IPX headers contain a hop count. By default, 15 hops is the maximum number of hops (or routers) that a packet can cross. If a packet has a hop count of 15, the router discards the packet. IP headers contain a Time to Live (TTL) value. Unlike the IPX hop count, which increments as the packet is forwarded through each router, the IP TTL value decrements as the IP packet is forwarded through each router. If an IP packet has a TTL value of 1, the router discards the packet. A router cannot decrement the TTL value to 1 and then forward the packet.

3. Determine the route to the destination. Routers maintain a routing table that lists available networks, the direction to the desired network (the outgoing interface number), and the distance to those networks. After determining which direction to forward the packet, the router must build a new header. (If you want to read the IP routing tables on a Windows 95/98 workstation, type ROUTE PRINT in the DOS box.)

4. Build the new MAC header and forward the packet. Finally, the router builds a new MAC header for the packet. The MAC header includes the router's MAC address and the final destination's MAC address or the MAC address of the next router in the path.

QUESTION NO: 12

Refer to the exhibit.
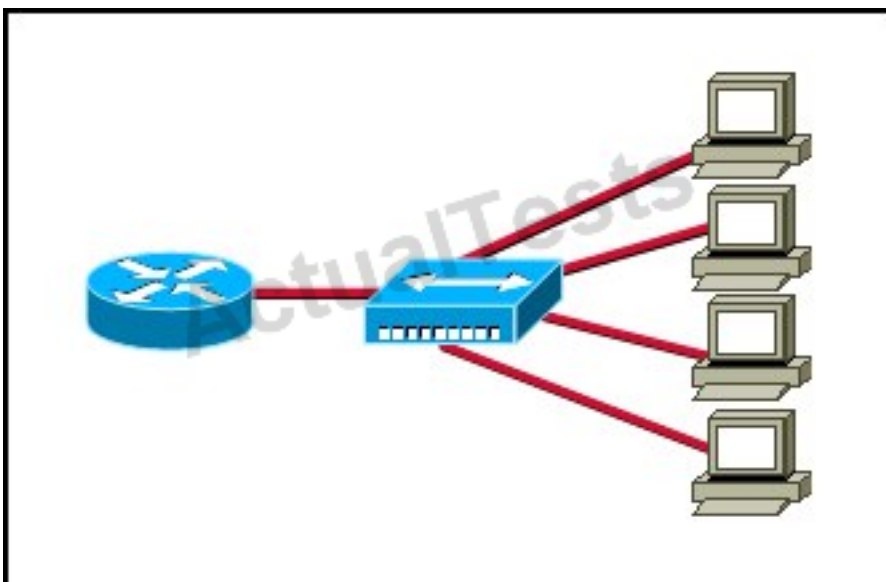
What two results would occur if the hub were to be replaced with a switch that is configured with one Ethernet VLAN? (Choose two.)

A. The number of collision domains would remain the same.
B. The number of collision domains would decrease.
C. The number of collision domains would increase.
D. The number of broadcast domains would remain the same.
E. The number of broadcast domains would decrease.
F. The number of broadcast domains would increase.

Answer: C,D
Explanation:
Basically, a collision domain is a network segment that allows normal network traffic to flow back and forth. In the old days of hubs, this meant you had a lot of collisions, and the old CSMA/CD would be working overtime to try to get those packets re-sent every time there was a collision on the wire (since ethernet allows only one host to be transmitting at once without there being a traffic jam). With switches, you break up collision domains by switching packets bound for other collision domains. These days, since we mostly use switches to connect computers to the network, you generally have one collision domain to a PC.

Broadcast domains are exactly what they imply: they are network segments that allow broadcasts to be sent across them. Since switches and bridges allow for broadcast traffic to go unswitched, broadcasts can traverse collision domains freely. Routers, however, don't allow broadcasts through by default, so when a broadcast hits a router (or the perimeter of a VLAN), it doesn't get forwarded. The simple way to look at it is this way: switches break up collision domains, while routers (and VLANs) break up collision domains and broadcast domains. Also, a broadcast domain can contain multiple collision domains, but a collision domain can never have more than one broadcast domain associated with it.

Collision Domain: A group of Ethernet or Fast Ethernet devices in a CSMA/CD LAN that are connected by repeaters and compete for access on the network. Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network in order to avoid data collisions. A collision domain is sometimes referred to as an Ethernet segment.

Broadcast Domain: Broadcasting sends a message to everyone on the local network (subnet). An example for Broadcasting would be DHCP Request from a Client PC. The Client is asking for a IP Address, but the client does not know how to reach the DHCP Server. So the client sends a DHCP Discover packet to EVERY PC in the local subnet (Broadcast). But only the DHCP Server will answer to the Request.

How to count them?

Broadcast Domain:

No matter how many hosts or devices are connected together, if they are connected with a repeater, hub, switch or bridge, all these devices are in ONE Broadcast domain (assuming a single VLAN). A Router is used to separate Broadcast-Domains (we could also call them Subnets - or call them VLANs).

So, if a router stands between all these devices, we have TWO broadcast domains.

Collision Domain:

Each connection from a single PC to a Layer 2 switch is ONE Collision domain. For example, if 5 PCs are connected with separate cables to a switch, we have 5 Collision domains. If this switch is connected to another switch or a router, we have one collision domain more.

If 5 Devices are connected to a Hub, this is ONE Collision Domain. Each device that is connected to a Layer 1 device (repeater, hub) will reside in ONE single collision domain.

QUESTION NO: 13

Which three statements accurately describe Layer 2 Ethernet switches? (Choose three.)

A. Spanning Tree Protocol allows switches to automatically share VLAN information.
B. Establishing VLANs increases the number of broadcast domains.
C. Switches that are configured with VLANs make forwarding decisions based on both Layer 2 and Layer 3 address information.
D. Microsegmentation decreases the number of collisions on the network.
E. In a properly functioning network with redundant switched paths, each switched segment will contain one root bridge with all its ports in the forwarding state. All other switches in that broadcast domain will have only one root port.
F. If a switch receives a frame for an unknown destination, it uses ARP to resolve the address.

Answer: B,D,E
Explanation: Explanation
Microsegmentation is a network design (functionality) where each workstation or device on a network gets its own dedicated segment (collision domain) to the switch. Each network device gets the full bandwidth of the segment and does not have to share the segment with other devices. Microsegmentation reduces and can even eliminate collisions because each segment is its own collision domain -> .
Note: Microsegmentation decreases the number of collisions but it increases the number of collision domains.
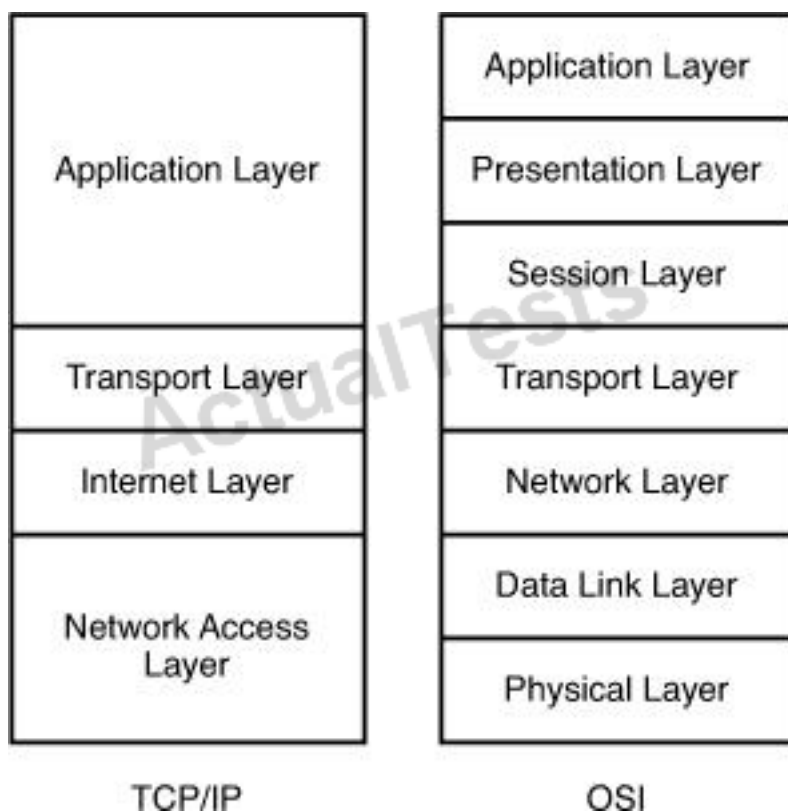
QUESTION NO: 14

Where does routing occur within the DoD TCP/IP reference model?

A. application
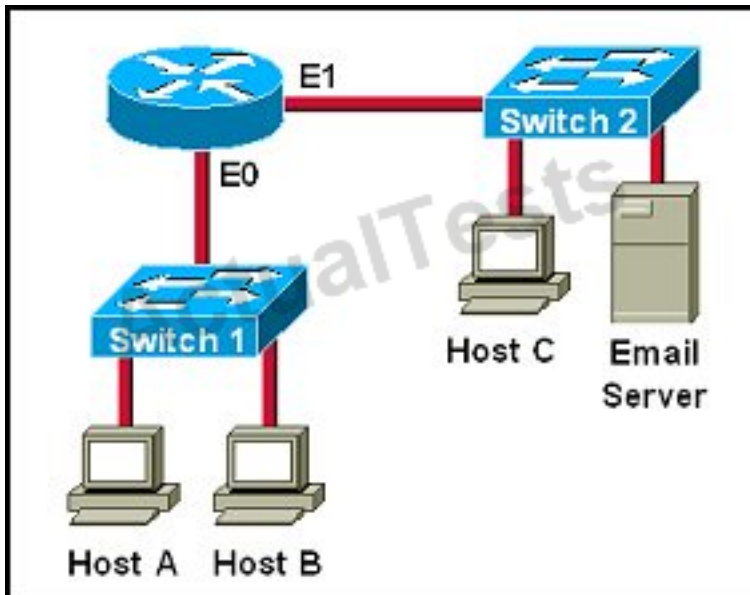**B.** internet
C. network
D. transport

Answer: B

Explanation:

The picture below shows the comparison between TCP/IP model & OSI model. Notice that the Internet Layer of TCP/IP is equivalent to the Network Layer which is responsible for routing decision.

TCP/IP	OSI
	Application Layer
Application Layer	Presentation Layer
	Session Layer
Transport Layer	Transport Layer
Internet Layer	Network Layer
Network Access Layer	Data Link Layer
	Physical Layer

QUESTION NO: 15

Refer to exhibit:

Which destination addresses will be used by Host A to send data to Host C? (Choose two.)

A. the IP address of Switch 1
B. the MAC address of Switch 1
C. the IP address of Host C
D. the MAC address of Host C
E. the IP address of the router's E0 interface
F. the MAC address of the router's E0 interface

Answer: C,F

Explanation: Explanation

While transferring data through many different networks, the source and destination IP addresses are not changed. Only the source and destination MAC addresses are changed. So in this case Host A will use the IP address of Host C and the MAC address of E0 interface to send data. When the router receives this data, it replaces the source MAC address with it own E1 interface's MAC address and replaces the destination MAC address with Host C's MAC address before sending to Host C .

QUESTION NO: 16

For what two purposes does the Ethernet protocol use physical addresses? (Choose two.)

A. to uniquely identify devices at Layer 2
B. to allow communication with devices on a different network
C. to differentiate a Layer 2 frame from a Layer 3 packet

D. to establish a priority system to determine which device gets to transmit first
E. to allow communication between different devices on the same network
F. to allow detection of a remote device when its physical address is unknown

Answer: A,E
Explanation:
Physical addresses or MAC addresses are used to identify devices at layer 2.

MAC addresses are only used to communicate on the same network. To communicate on different network we have to use Layer 3 addresses (IP addresses) -> B is not correct.
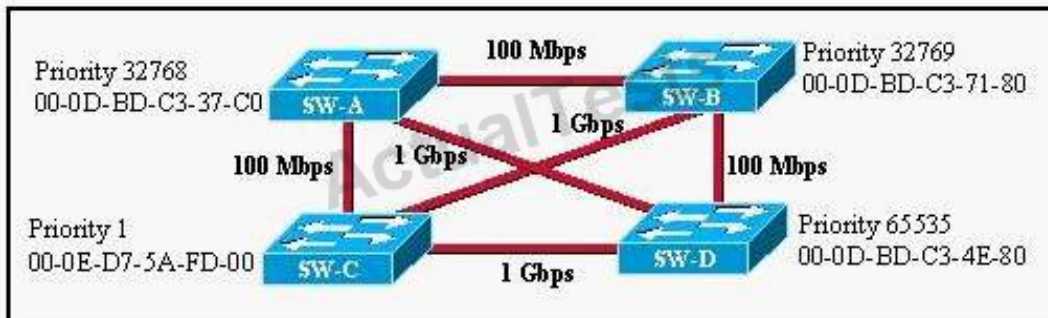
Layer 2 frame and Layer 3 packet can be recognized via headers. Layer 3 packet also contains physical address ->

On Ethernet, each frame has the same priority to transmit by default ->
All devices need a physical address to identify itself. If not, they can not communicate ->

QUESTION NO: 17

Refer to the exhibit.

Based on the information given, which switch will be elected root bridge and why?

A. Switch A, because it has the lowest MAC address
B. Switch A, because it is the most centrally located switch
C. Switch B, because it has the highest MAC address
D. Switch C, because it is the most centrally located switch
E. Switch C, because it has the lowest priority
**F.** Switch D, because it has the highest priority

Answer: E

Explanation:

To elect the root bridge in the LAN, first check the priority value. The switch having the lowest priority will win the election process. If Priority Value is the same then it checks the MAC Address; the switch having the lowest MAC Address will become the root bridge. In this case, switch C has the lowest MAC Address so it becomes the root bridge.

QUESTION NO: 18

Which of the following statements describe the network shown in the graphic? (Choose two.)
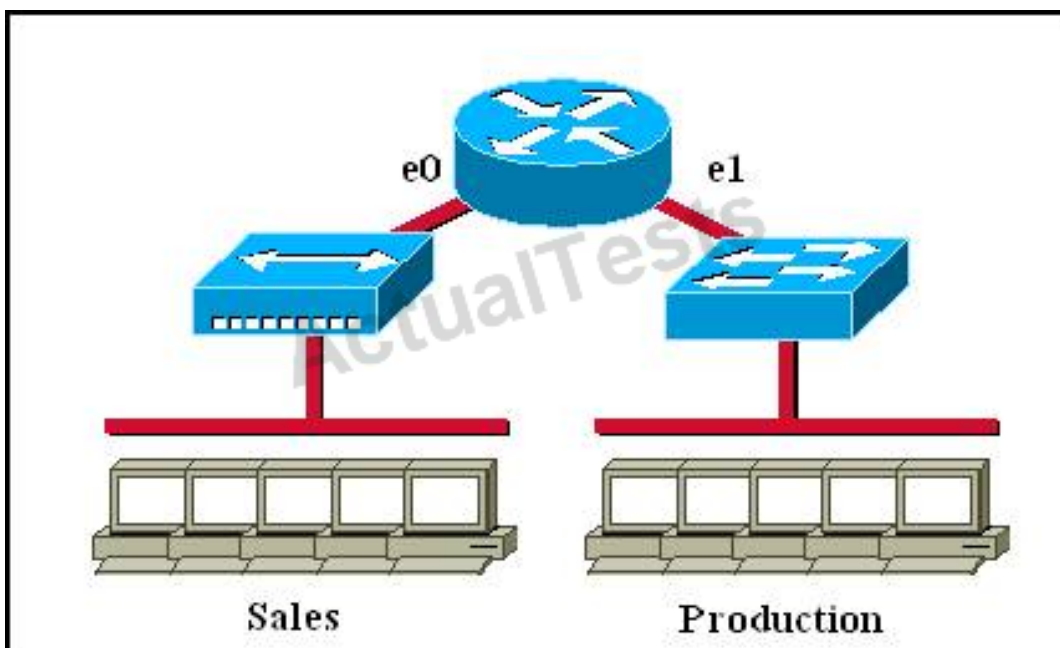
A. There are two broadcast domains in the network.
B. There are four broadcast domains in the network.
C. There are six broadcast domains in the network.
D. There are four collision domains in the network.
E. There are five collision domains in the network.
F. There are seven collision domains in the network.

Answer: A,F
Explanation:
Only router can break up broadcast domains so in the exhibit there are 2 broadcast domains: from e0 interface to the left is a broadcast domain and from e1 interface to the right is another broadcast domain ->.
Both router and switch can break up collision domains so there is only 1 collision domain on the left of the router (because hub doesn't break up collision domain) and there are 6 collision

domains on the right of the router (1 collision domain from e1 interface to the switch + 5 collision domains for 5 PCs in Production) ->

QUESTION NO: 19

In an Ethernet network, under what two scenarios can devices transmit? (Choose two.)

A. when they receive a special token
B. when there is a carrier
C. when they detect no other devices are sending
D. when the medium is idle
E. when the server grants access

Answer: C,D
Explanation: Explanation
Ethernet network is a shared environment so all devices have the right to access to the medium. If more than one device transmits simultaneously, the signals collide and can not reach the destination.

If a device detects another device is sending, it will wait for a specified amount of time before attempting to transmit.

When there is no traffic detected, a device will transmit its message. While this transmission is occurring, the device continues to listen for traffic or collisions on the LAN. After the message is sent, the device returns to its default listening mode.

QUESTION NO: 20

A router has two Fast Ethernet interfaces and needs to connect to four VLANs in the local network. How can you accomplish this task, using the fewest physical interfaces and without decreasing network performance?

A. Use a hub to connect the four VLANS with a Fast Ethernet interface on the router.
B. Add a second router to handle the VLAN traffic.
C. Add two more Fast Ethernet interfaces.

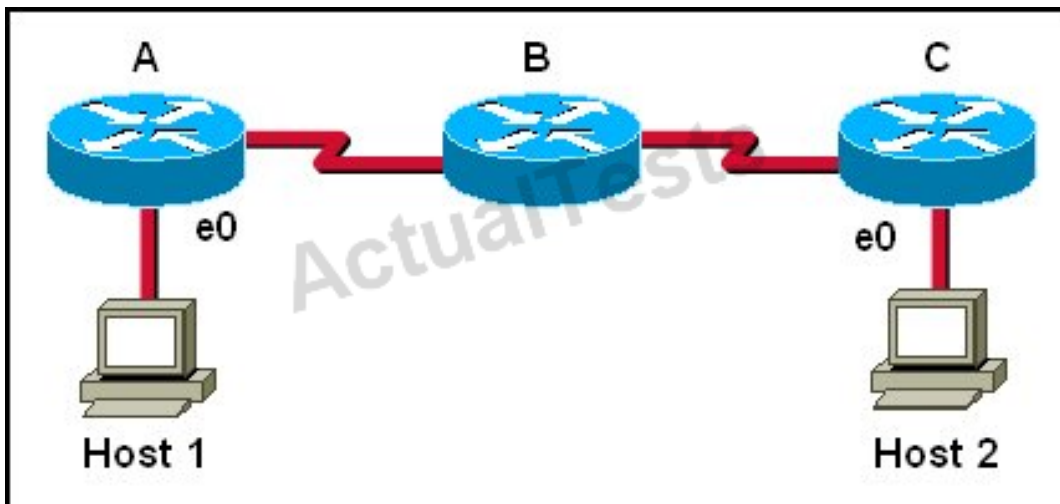**D.** Implement a router-on-a-stick configuration.

Answer: D
Explanation:
A router on a stick allows you to use sub-interfaces to create multiple logical networks on a single physical interface.

QUESTION NO: 21

Host 1 is trying to communicate with Host 2. The e0 interface on Router C is down.

Which of the following are true? (Choose two.)

A. Router C will use ICMP to inform Host 1 that Host 2 cannot be reached.
B. Router C will use ICMP to inform Router B that Host 2 cannot be reached.
C. Router C will use ICMP to inform Host 1, Router A, and Router B that Host 2 cannot be reached.
D. Router C will send a Destination Unreachable message type.
E. Router C will send a Router Selection message type.
F. Router C will send a Source Quench message type.

Answer: A,D
Explanation:
Host 1 is trying to communicate with Host 2. The e0 interface on Router C is down. Router C will send ICMP packets to inform Host 1 that Host 2 cannot be reached.

QUESTION NO: 22

What is the difference between a CSU/DSU and a modem?

A. A CSU/DSU converts analog signals from a router to a leased line; a modem converts analog signals from a router to a leased line.
B. A CSU/DSU converts analog signals from a router to a phone line; a modem converts digital signals from a router to a leased line.
C. A CSU/DSU converts digital signals from a router to a phone line; a modem converts analog signals from a router to a phone line.
D. A CSU/DSU converts digital signals from a router to a leased line; a modem converts digital signals from a router to a phone line.

Answer: D
Explanation:
CSU/DSU is used to convert digital signals from a router to a network circuit such as a T1, while a modem is used to convert digital signals over a regular POTS line.

QUESTION NO: 23 DRAG DROP

Drag the cable type on the left to the purpose for which it is best suited on the right. (Not all options are used.)	
crossover	switch access port to router
null modem	switch to switch
straight-through	PC COM port to switch
rollover	
9-25 pin serial	

Answer:

Drag the cable type on the left to the purpose for which it is best suited on the right. (Not all options are used.)	
crossover	straight-through
null modem	crossover
straight-through	rollover
rollover	
9-25 pin serial	

Explanation:

straight-through
crossover
rollover

To remember which type of cable you should use, follow these tips:

- To connect **two serial interfaces** of 2 routers we use **serial cable**– To specify when we use crossover cable or straight-through cable, we should remember:**Group 1:** Router, Host, Server **Group 2:** Hub, SwitchOne device in group 1 + One device in group 2: use **straight-through cable** Two devices in the same group: use **crossover cable**

For example: we use straight-through cable to connect switch to router, switch to host, hub to host, hub to server… and we use crossover cable to connect switch to switch, switch to hub, router to router, host to host…)

QUESTION NO: 24 DRAG DROP

Match the terms on the left with the appropriate OSI layer on the right. (Not all options are used.)	
frames	**Network Layer**
packets	
UDP	
IP addresses	
segments	**Transport Layer**
MAC addresses	
windowing	
routing	

Answer:

Match the terms on the left with the appropriate OSI layer on the right. (Not all options are used.)

| frames |
| packets |
| UDP |
| IP addresses |
| segments |
| MAC addresses |
| windowing |
| routing |

Network Layer
| packets |
| IP addresses |
| routing |

Transport Layer
| UDP |
| segments |
| windowing |

Explanation:

Network Layer

| packets |

| IP addresses |

| routing |

Transport Layer

| UDP |

| segments |

| windowing |

QUESTION NO: 25 DRAG DROP

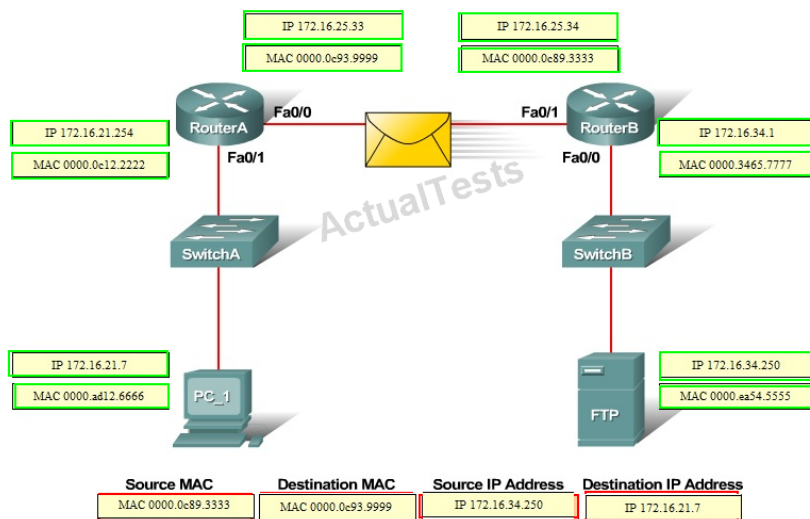Refer to the exhibit. PC_1 is exchanging packets with the FTP server. Consider the packets as they leave RouterB interface Fa0/1 towards RouterA. Drag the correct frame and packet addresses to their place in the table.

IP 172.16.25.33
MAC 0000.0c93.9999

IP 172.16.25.34
MAC 0000.0c89.3333

RouterA Fa0/0   Fa0/1 RouterB
IP 172.16.21.254   IP 172.16.34.1
MAC 0000.0c12.2222   Fa0/1   Fa0/0   MAC 0000.3465.7777

ActualTests

SwitchA   SwitchB

IP 172.16.21.7   IP 172.16.34.250
MAC 0000.ad12.6666   PC_1   FTP   MAC 0000.ea54.5555

Source MAC	Destination MAC	Source IP Address	Destination IP Address
Target	Target	Target	Target

Answer:

Refer to the exhibit. PC_1 is exchanging packets with the FTP server. Consider the packets as they leave RouterB interface Fa0/1 towards RouterA. Drag the correct frame and packet addresses to their place in the table.

IP 172.16.25.33
MAC 0000.0c93.9999

IP 172.16.25.34
MAC 0000.0c89.3333

RouterA Fa0/0   Fa0/1 RouterB
IP 172.16.21.254   IP 172.16.34.1
MAC 0000.0c12.2222   Fa0/1   Fa0/0   MAC 0000.3465.7777

ActualTests

SwitchA   SwitchB

IP 172.16.21.7   IP 172.16.34.250
MAC 0000.ad12.6666   PC_1   FTP   MAC 0000.ea54.5555

Source MAC	Destination MAC	Source IP Address	Destination IP Address
MAC 0000.0c89.3333	MAC 0000.0c93.9999	IP 172.16.34.250	IP 172.16.21.7

Explanation:

Source Mac Address Destination Mac Address Source IP address Destination MAC address
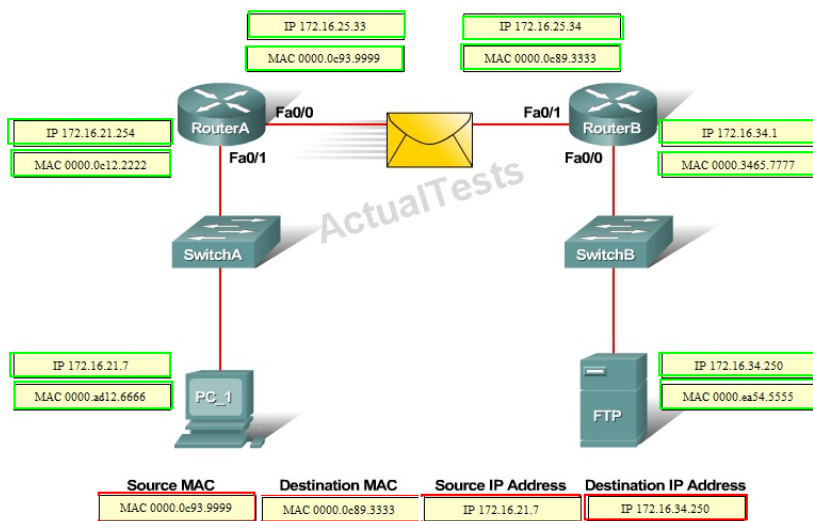MAC 0000.0c89.3333 MAC 0000.0c89.9999 IP 172.16.34.250 IP 172.16.21.7

QUESTION NO: 26 DRAG DROP

Refer to the exhibit. PC_1 is sending packets to the FTP server. Consider the packets as they leave RouterA interface Fa0/0 towards RouterB. Drag the correct frame and packet address to their place in the table.
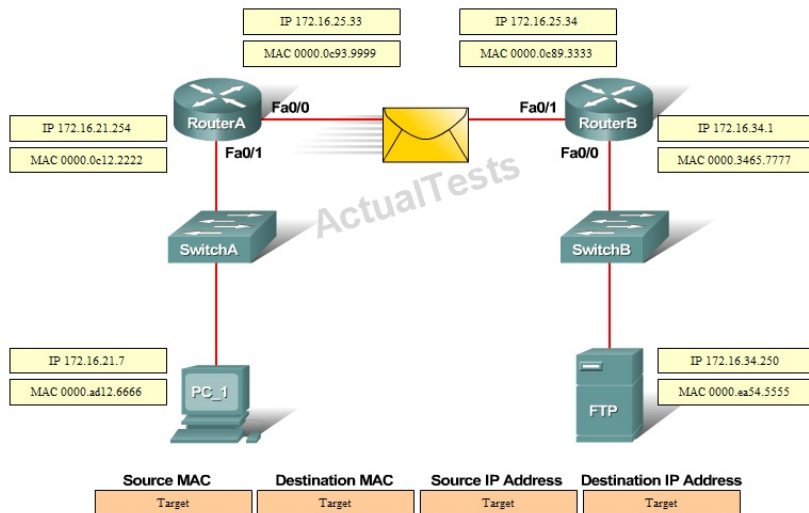
Answer:

Refer to the exhibit. PC_1 is sending packets to the FTP server. Consider the packets as they leave RouterA interface Fa0/0 towards RouterB. Drag the correct frame and packet address to their place in the table.
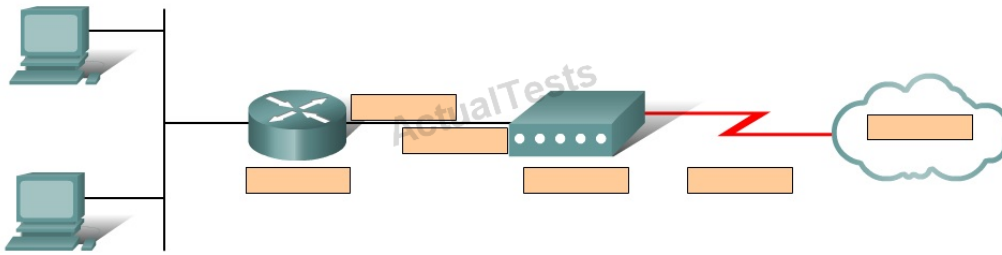

Explanation:

| Source MAC	Destination MAC	Source IP Address	Destination IP Address
MAC 0000.0c93.9999	MAC 0000.0c89.3333	IP 172.16.21.7	IP 172.16.34.250

QUESTION NO: 27 DRAG DROP

Refer to the exhibit. Complete this network diagram by dragging the correct device name or description to the correct location. Not all the names or descriptions will be used.

| Digital Line | CSU/DSU Synchronous | Analog Modem Asynchronous | WAN Service Provider Network | Router | Switch | DTE | DCE |

Answer:

Refer to the exhibit. Complete this network diagram by dragging the correct device name or description to the correct location. Not all the names or descriptions will be used.
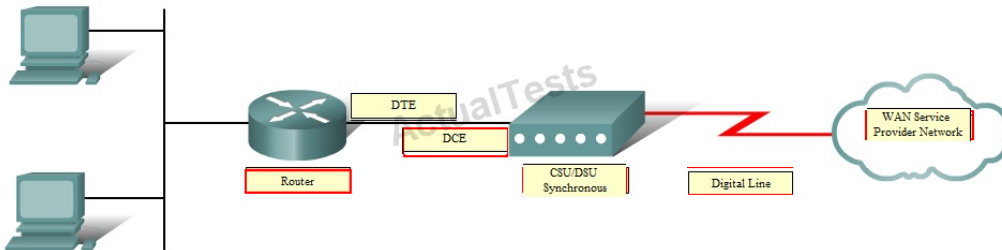
| Digital Line | CSU/DSU Synchronous | Analog Modem Asynchronous | WAN Service Provider Network | Router | Switch | DTE | DCE |

Explanation:
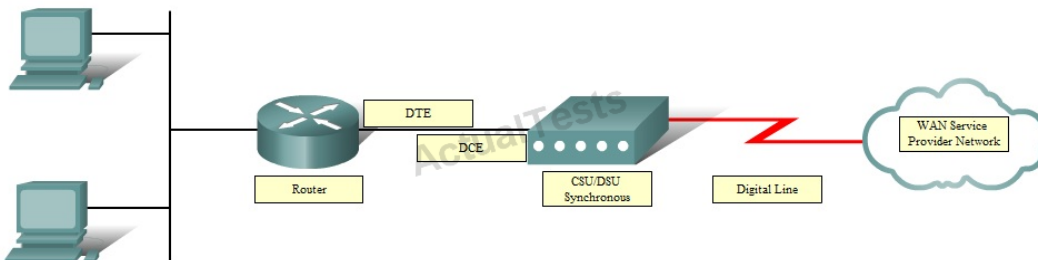
Topic 2, LAN Switching Technologies

QUESTION NO: 28

Refer to the exhibit.

```
ALSwitch1# show running-config
«output omitted»
interface FastEthernet0/24 no ip address
«output omitted»
ALSwitch1# show interfaces FastEthernet0/24 switchport
Name: Fa0/24
Switchport: Enable
Administrative Mode: static access
Operation Mode: static access
Administrative Trunking Encapsulation: dot1q
Operation Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operation private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false

Voice VLAN: none (Inactive)
Aplliance trust: none
```

Switch port FastEthernet 0/24 on ALSwitch1 will be used to create an IEEE 802.1Q-compliant trunk to another switch. Based on the output shown, what is the reason the trunk does not form, even though the proper cabling has been attached?

A. VLANs have not been created yet.
B. An IP address must be configured for the port.

C. The port is currently configured for access mode.

D. The correct encapsulation type has not been configured.

E. The "no shutdown" command has not been entered for the port.

Answer: C

Explanation:

According to the output shown the switchport (layer 2 Switching) is enabled and the port is in access mode. To make a trunk link the port should configured as a trunk port, not an access port, by using the following command: (Config-if)#switchport mode trunk

QUESTION NO: 29

Which port state is introduced by Rapid-PVST?

A. learning

B. listening

C. discarding

D. forwarding

Answer: C

Explanation:

PVST+ is based on IEEE802.1D Spanning Tree Protocol (STP). But PVST+ has only 3 port states (discarding, learning and forwarding) while STP has 5 port states (blocking, listening, learning, forwarding and disabled). So discarding is a new port state in PVST+.

QUESTION NO: 30

VLAN 3 is not yet configured on your switch. What happens if you set the switchport access vlan 3 command in interface configuration mode?

A. The command is rejected.

B. The port turns amber.

C. The command is accepted and the respective VLAN is added to vlan.dat.

D. The command is accepted and you must configure the VLAN manually.

Answer: C

Explanation:

The "switchport access vlan 3" will put that interface as belonging to VLAN 3 while also updated the VLAN database automatically to include VLAN 3.

QUESTION NO: 31

What value is primarily used to determine which port becomes the root port on each nonroot switch in a spanning-tree topology?

A. path cost
B. lowest port MAC address
C. VTP revision number
D. highest port priority number
E. port priority number and MAC address

Answer: A
Explanation: The path cost to the root bridge is the most important value to determine which port will become the root port on each non-root switch. In particular, the port with lowest cost to the root bridge will become root port (on non-root switch).

QUESTION NO: 32

In a switched environment, what does the IEEE 802.1Q standard describe?

A. the operation of VTP
B. a method of VLAN trunking
C. an approach to wireless LAN communication
D. the process for root bridge selection
E. VLAN pruning

Answer: B
Explanation:
A broadcast domain must sometimes exist on more than one switch in the network. To accomplish this, one switch must send frames to another switch and indicate which VLAN a particular frame belongs to. On Cisco switches, a trunk link is created to accomplish this VLAN identification. ISL and IEEE 802.1Q are different methods of putting a VLAN identifier in a Layer 2 frame.
The IEEE 802.1Q protocol interconnects VLANs between multiple switches, routers, and servers. With 802.1Q, a network administrator can define a VLAN topology to span multiple physical devices.
Cisco switches support IEEE 802.1Q for FastEthernet and Gigabit Ethernet interfaces. An 802.1Q

trunk link provides VLAN identification by adding a 4-byte tag to an Ethernet Frame as it leaves a trunk port.

QUESTION NO: 33

Refer to the exhibit.

```
Switch-1# show mac address-table
Dynamic Addresses Count:                3
Secure Addresses (User-defined) Count:  0
Static Addresses (User-defined) Count:  0
System Self Addresses Count:           41
Total Mac addresses:                   50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  ----------------
0010.0de0.e289       Dynamic       1     FastEthernet0/1
0010.7b00.1540       Dynamic       2     FastEthernet0/3
0010.7b00.1545       Dynamic       2     FastEthernet0/2
```

Switch-1 needs to send data to a host with a MAC address of 00b0.d056.efa4. What will Switch-1 do with this data?

A. Switch-1 will drop the data because it does not have an entry for that MAC address.
B. Switch-1 will flood the data out all of its ports except the port from which the data originated.
C. Switch-1 will send an ARP request out all its ports except the port from which the data originated.
D. Switch-1 will forward the data to its default gateway.

Answer: B
Explanation:
This question tests the operating principles of the Layer 2 switch. Check the MAC address table of Switch1 and find that the MAC address of the host does not exist in the table. Switch1 will flood the data out all of its ports except the port from which the data originated to determine which port the host is located in.

Switches work as follows:

In output there is no MAC address of give host so switch floods to all ports except the source port.

QUESTION NO: 34

What is the function of the command switchport trunk native vlan 999 on a Cisco Catalyst switch?

A. It creates a VLAN 999 interface.
B. It designates VLAN 999 for untagged traffic.
C. It blocks VLAN 999 traffic from passing on the trunk.
D. It designates VLAN 999 as the default for all unknown tagged traffic.

Answer: B
Explanation:
Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

QUESTION NO: 35

Which two protocols are used by bridges and/or switches to prevent loops in a layer 2 network? (Choose two.)

A. 802.1d
B. VTP
C. 802.1q
D. STP
E. SAP

Answer: A,D
Explanation:
This question is to examine the STP protocol.
STP (802.1d) is used to prevent Layer 2 loops.
802.1q is a Frame Relay protocol which belongs to VLAN.
SAP is a concept of the OSI model.

QUESTION NO: 36

Which switch would STP choose to become the root bridge in the selection process?

A. 32768: 11-22-33-44-55-66
B. 32768: 22-33-44-55-66-77
C. 32769: 11-22-33-44-55-65
D. 32769: 22-33-44-55-66-78

Answer: A

Explanation:

The root bridge of the spanning tree is the bridge with the smallest (lowest) bridge ID. Each bridge has a configurable priority number and a MAC Address; the bridge ID contains both numbers combined together - Bridge priority + MAC (32768.0200.0000.1111). The Bridge priority default is 32768 and can only be configured in multiples of 4096(Spanning tree uses the 12 bits extended system ID). To compare two bridge IDs, the priority is compared first, as if looking at a real number anything less than 32768...will become the target of being the root. If two bridges have equal priority then the MAC addresses are compared; for example, if switches A (MAC=0200.0000.1111) and B (MAC=0200.0000.2222) both have a priority of 32768 then switch A will be selected as the root bridge.
In this case, 32768: 11-22-33-44-55-66 would be the bridge because it has a lower priority and MAC address.

QUESTION NO: 37

A switch is configured with all ports assigned to VLAN 2 with full duplex FastEthernet to segment existing departmental traffic. What is the effect of adding switch ports to a new VLAN on the switch?

A. More collision domains will be created.
B. IP address utilization will be more efficient.
C. More bandwidth will be required than was needed previously.
D. An additional broadcast domain will be created.

Answer: D

Explanation:

Each VLAN creates its own broadcast domain. Since this is a full duplex switch, each port is a separate collision domain.

QUESTION NO: 38

What are three benefits of implementing VLANs? (Choose three.)

A. A higher level of network security can be reached by separating sensitive data traffic from other network traffic.
B. A more efficient use of bandwidth can be achieved allowing many physical groups to use the same network infrastructure.
C. A more efficient use of bandwidth can be achieved allowing many logical networks to use the same network infrastructure.
D. Broadcast storms can be mitigated by increasing the number of broadcast domains, thus reducing their size.
E. Broadcast storms can be mitigated by decreasing the number of broadcast domains, thus increasing their size.
F. VLANs make it easier for IT staff to configure new logical groups, because the VLANs all belong to the same broadcast domain.
G. Port-based VLANs increase switch-port use efficiency, thanks to 802.1Q trunks.

Answer: A,C,D
Explanation:
Benefits of VLANs
VLAN is a network structure which allows users to communicate while in different locations by sharing one multicast domain and a single broadcast. They provide numerous networking benefits and have become popular in the market. For instance, it helps reduce administrative costs when users are geographically dispersed.

1. Inexpensive
The popularity of VLANs is due to the fact that changes, adds, and moves can be attained simply by making necessary configurations on the VLAN port. Time-consuming, re-addressing, and host reconfigurations is now a thing of the past, because network configuration can be made at ease when need arises.

2. Better management
A VLAN typically solve the scalability issues that exist in a large network by breaking the main domain into several VLAN groups or smaller broadcast configurations, thereby encourage better control of multicast traffic as well as broadcast domains.

3. Improves network security
High-security can be positioned in different VLAN groups to ensure that non-members cannot receive their broadcasts. On the other hand, a router is added and workgroups relocated into

centralized locations.

4. Enhances performance

A more efficient use of bandwidth can be achieved allowing many logical networks to use the same network infrastructure.

5. Segment multiple networks

VLANs are typically used to achieve multiple purposes. They are popularly used to reduce broadcast traffic. Each VLAN creates a separate, smaller broadcast domain.

6. Better administration

VLANs facilitate grouping of multiple geographical stations. When VLAN users move to another physical location, the network does not have to be configured.

QUESTION NO: 39

Which IEEE standard protocol is initiated as a result of successful DTP completion in a switch over Fast Ethernet?

A. 802.3ad
B. 802.1w
C. 802.1D
D. 802.1Q

Answer: D

Explanation: Explanation

Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q) to be used.

QUESTION NO: 40

Which of the following are benefits of VLANs? (Choose three.)

A. They increase the size of collision domains.
B. They allow logical grouping of users by function.
C. They can enhance network security.
D. They increase the size of broadcast domains while decreasing the number of collision domains.
E. They increase the number of broadcast domains while decreasing the size of the broadcast domains.

F. They simplify switch administration.

Answer: B,C,E

Explanation: Explanation

When using VLAN the number and size of collision domains remain the same ->

VLANs allow to group users by function, not by location or geography -> .

VLANs help minimize the incorrect configuration of VLANs so it enhances the security of the network -> .

VLAN increases the size of broadcast domains but does not decrease the number of collision domains ->

VLANs increase the number of broadcast domains while decreasing the size of the broadcast domains which increase the utilization of the links. It is also a big advantage of VLAN -> .

VLANs are useful but they are more complex and need more administration ->

QUESTION NO: 41

Refer to the exhibit.
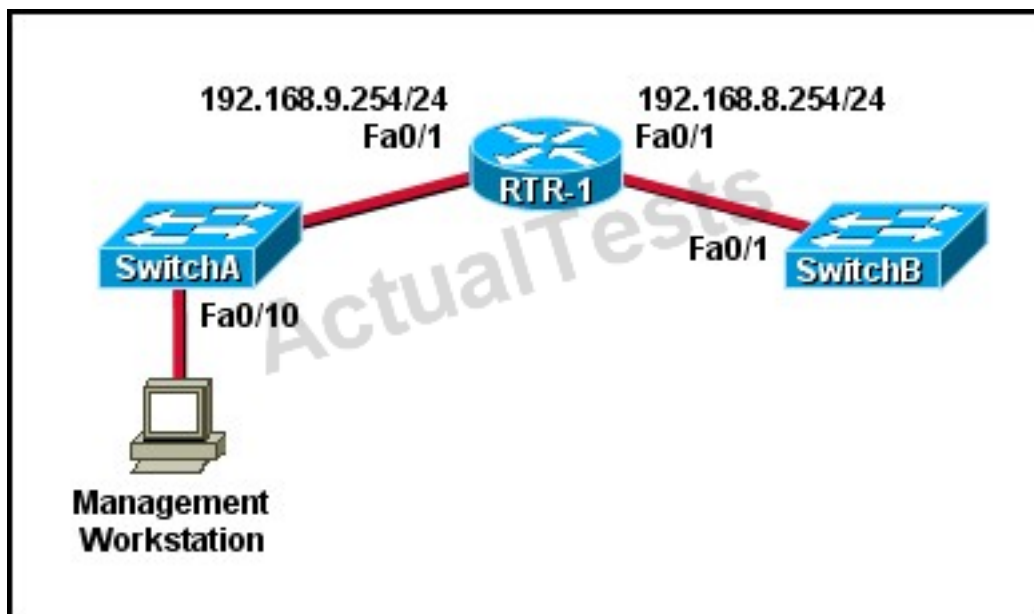
A technician has installed SwitchB and needs to configure it for remote access from the management workstation connected to SwitchA. Which set of commands is required to accomplish this task?

A. SwitchB(config)# interface FastEthernet 0/1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown

B. SwitchB(config)# interface vlan 1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# ip default-gateway 192.168.8.254 255.255.255.0
SwitchB(config-if)# no shutdown
C. SwitchB(config)# ip default-gateway 192.168.8.254
SwitchB(config)# interface vlan 1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown
D. SwitchB(config)# ip default-network 192.168.8.254
SwitchB(config)# interface vlan 1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown
E. SwitchB(config)# ip route 192.168.8.254 255.255.255.0
SwitchB(config)# interface FastEthernet 0/1
SwitchB(config-if)# ip address 192.168.8.252 255.255.255.0
SwitchB(config-if)# no shutdown

Answer: C

Explanation: Explanation

To remote access to SwitchB, it must have a management IP address on a VLAN on that switch.
Traditionally, we often use VLAN 1 as the management VLAN (but in fact it is not secure).
In the exhibit, we can recognize that the Management Workstation is in a different subnet from the
SwitchB. For intersubnetwork communication to occur, you must configure at least one default
gateway. This default gateway is used to forward traffic originating from the switch only, not to
forward traffic sent by devices connected to the switch.

QUESTION NO: 42

Which two states are the port states when RSTP has converged? (Choose two.)

A. discarding
B. listening
C. learning
D. forwarding
E. disabled

Answer: A,D

Explanation:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml
#states

QUESTION NO: 43

Which two commands can be used to verify a trunk link configuration status on a given Cisco switch interface? (Choose two.)

A. show interface trunk
B. show interface interface
C. show ip interface brief
D. show interface vlan
E. show interface switchport

Answer: A,E

Explanation:

Example output from these two commands:

SW3#show interface trunk

Port Mode Encapsulation Status Native vlanFa0/19 auto n-802.1q trunking 1Fa0/20 auto n-802.1q trunking 1Fa0/21 auto n-802.1q trunking 1Fa0/22 auto n-802.1q trunking 1

Port Vlans allowed on trunkFa0/19 1-4094Fa0/20 1-4094Fa0/21 1-4094Fa0/22 1-4094

SW1#show interface fast 0/2 switchportName: Fa0/2Switchport: EnabledAdministrative Mode: dynamic desirableOperational Mode: downAdministrative Trunking Encapsulation: dot1qNegotiation of TrunkinG. OnAccess Mode VLAN: 1 (default)Trunking Native Mode VLAN: 1 (default)Voice VLAN: none

QUESTION NO: 44

Which command enables RSTP on a switch?

A. spanning-tree uplinkfast
B. spanning-tree mode rapid-pvst
C. spanning-tree backbonefast
D. spanning-tree mode mst

**Answer: B**

Explanation:

Rapid Spanning Tree Protocol (RSTP) is an enhancement of the original STP 802.1D protocol. The RSTP 802.1w protocol is an IEEE open implementation. Cisco has its own proprietary

implementation of RSTP, that includes the benefits of its Per-VLAN spanning tree protocols, called Rapid-PVST+.

To activate the Rapid-PVST+ protocol: switch(config)#spanning-tree mode rapid-pvst

QUESTION NO: 45

Refer to the exhibit.
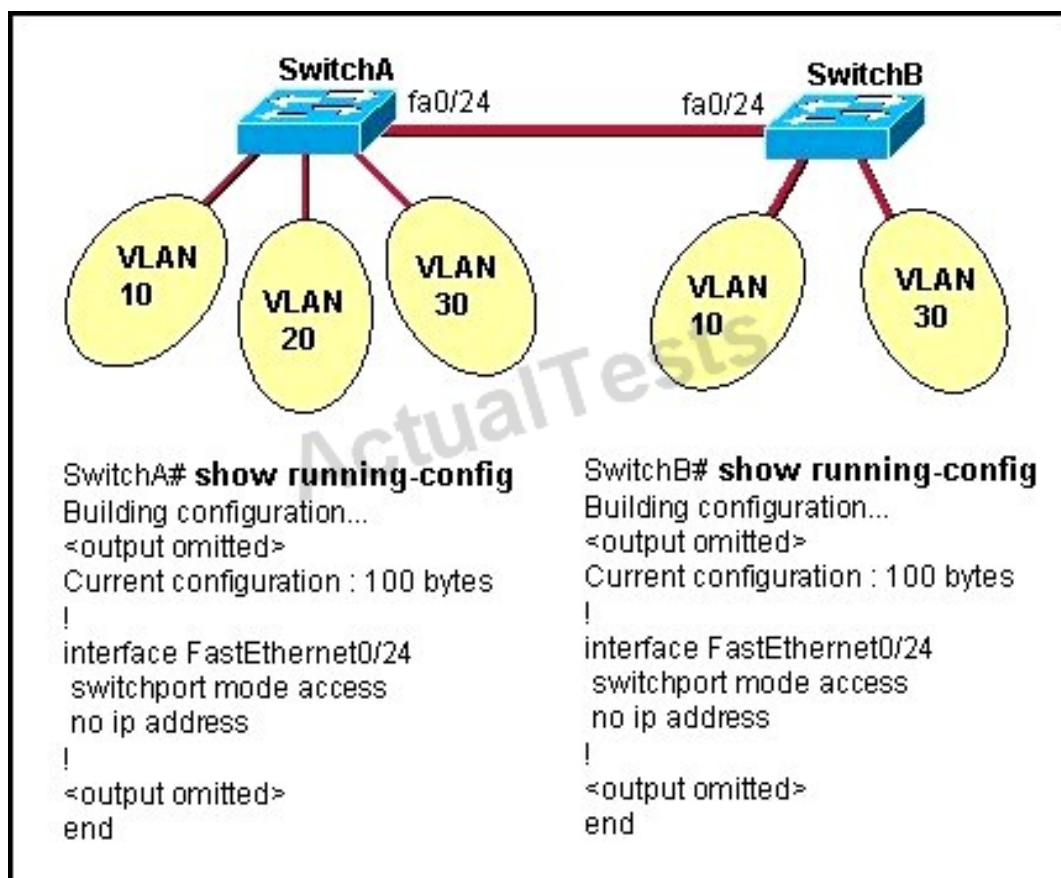
All switch ports are assigned to the correct VLANs, but none of the hosts connected to SwitchA can communicate with hosts in the same VLAN connected to SwitchB. Based on the output shown, what is the most likely problem?

A. The access link needs to be configured in multiple VLANs.
B. The link between the switches is configured in the wrong VLAN.
C. The link between the switches needs to be configured as a trunk.
D. VTP is not configured to carry VLAN information between the switches.
E. Switch IP addresses must be configured in order for traffic to be forwarded between the switches.

Answer: C

Explanation:

In order to pass traffic from VLANs on different switches, the connections between the switches must be configured as trunk ports.

QUESTION NO: 46

Refer to the exhibit.

```
RouterA#show interface pos8/0/0
POS8/0/0 is up, line protocol is up
  Hardware is Packet over Sonet
  Keepalive set (10 sec)
  Scramble disabled
  LMI enq sent  2474988, LMI stat recvd 2474969, LMI upd recvd 0, DTE LMI up
  Broadcast queue 0/256, broadcasts sent/dropped 25760668/0, interface broadcasts 25348176
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 40w6d
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 39000 bits/sec, 60 packets/sec
     63153396 packets input, 4389121455 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
             0 parity
     44773 input errors, 39138 CRC, 0 frame, 0 overrun, 0 ignored, 27 abort
     945596253 packets output, 62753244360 bytes, 0 underruns
     0 output errors, 0 applique, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Which WAN protocol is being used?

A. ATM
B. HDLC
C. Frame Relay
D. PPP

Answer: C

Explanation:

This question is to examine the show int command.

According to the information provided in the exhibit, we can know that the data link protocol used in this network is the Frame Relay protocol.

"LMI enq sent…"

QUESTION NO: 47

Refer to the exhibit.

```
Switch# show spanning-tree interface fastethernet 0/10
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
VLAN0001         Root FWD 19        128.1    P2p
VLAN0002         Altn BLK 19        128.2    P2p
VLAN0003         Root FWD 19        128.2    P2p
```

Given the output shown from this Cisco Catalyst 2950, what is the reason that interface FastEthernet 0/10 is not the root port for VLAN 2?

A. This switch has more than one interface connected to the root network segment in VLAN 2.
B. This switch is running RSTP while the elected designated switch is running 802.1d Spanning Tree.
C. This switch interface has a higher path cost to the root bridge than another in the topology.
D. This switch has a lower bridge ID for VLAN 2 than the elected designated switch.

Answer: C

Explanation:

Since the port is in the blocked status, we must assume that there is a shorter path to the root bridge elsewhere.

QUESTION NO: 48

Why will a switch never learn a broadcast address?

A. Broadcasts only use network layer addressing.
B. A broadcast frame is never forwarded by a switch.
C. A broadcast address will never be the source address of a frame.
D. Broadcast addresses use an incorrect format for the switching table.
E. Broadcast frames are never sent to switches.

Answer: C

Explanation:

Switches dynamically learn MAC addresses based on the source MAC addresses that it sees, and since a broadcast is never the source, it will never learn the broadcast address.

QUESTION NO: 49

Refer to the exhibit.

```
Switch# show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    20481
             Address     0008.217a.5800
             Cost        38
             Port        1 (FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0008.205e.6600
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300


Interface         Role Sts Cost      Prio.Nbr Type
----------------  ---- --- --------- -------- --------------------------------
Fa0/1             Root FWD 19        128.1    P2p
Fa0/4             Desg FWD 38        128.1    P2p
Fa0/11            Altn BLK 57        128.1    P2p
Fa0/13            Desg FWD 38        128.1    P2p
```

Why has this switch not been elected the root bridge for VLAN1?

A. It has more than one interface that is connected to the root network segment.
B. It is running RSTP while the elected root bridge is running 802.1d spanning tree.
C. It has a higher MAC address than the elected root bridge.
D. It has a higher bridge ID than the elected root bridge.

Answer: D

Explanation:

The root bridge is determined by the lowest bridge ID, and this switch has a bridge ID priority of

32768, which is higher than the roots priority of 20481.

QUESTION NO: 50

Which two link protocols are used to carry multiple VLANs over a single link? (Choose two.)

A. VTP
B. 802.1q
C. IGP
D. ISL
E. 802.3u

Answer: B,D

Explanation:

Cisco switches can use two different encapsulation types for trunks, the industry standard 802.1q or the Cisco proprietary ISL. Generally, most network engineers prefer to use 802.1q since it is standards based and will interoperate with other vendors.

QUESTION NO: 51

Assuming the default switch configuration, which VLAN range can be added, modified, and removed on a Cisco switch?

A. 1 through 1001
B. 2 through 1001
C. 1 through 1002
D. 2 through 1005

Answer: B

Explanation: Explanation

VLAN 1 is the default VLAN on Cisco switch. It always exists and can not be added, modified or removed.

VLANs 1002-1005 are default VLANs for FDDI & Token Ring and they can't be deleted or used for Ethernet.

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig1/1, Gig1/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

QUESTION NO: 52

Which statement about VLAN operation on Cisco Catalyst switches is true?

A. When a packet is received from an 802.1Q trunk, the VLAN ID can be determined from the source MAC address and the MAC address table.
B. Unknown unicast frames are retransmitted only to the ports that belong to the same VLAN.
C. Broadcast and multicast frames are retransmitted to ports that are configured on different VLAN.
D. Ports between switches should be configured in access mode so that VLANs can span across the ports.

Answer: B
Explanation:
Each VLAN resides in its own broadcast domain, so incoming frames with unknown destinations are only transmitted to ports that reside in the same VLAN as the incoming frame.

QUESTION NO: 53

Refer to the topology shown in the exhibit.
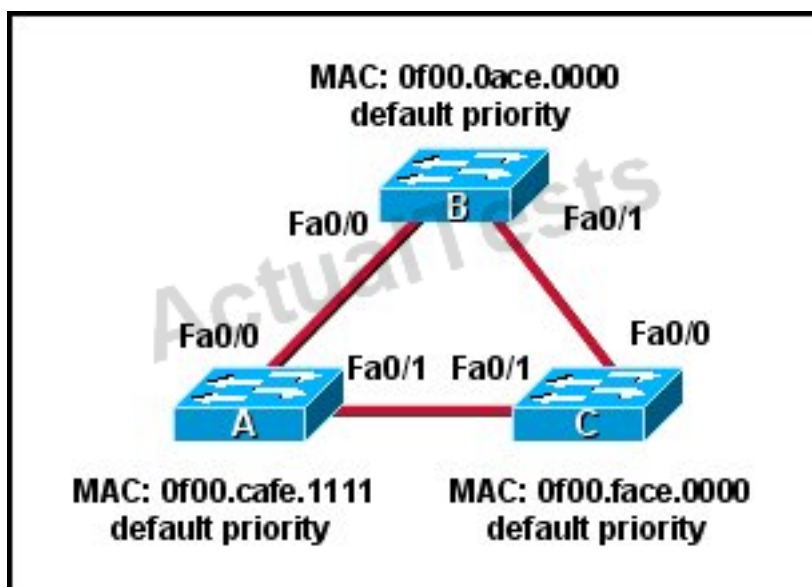
Which ports will be STP designated ports if all the links are operating at the same bandwidth?

(Choose three.)

A. Switch A - Fa0/0
B. Switch A - Fa0/1
C. Switch B - Fa0/0
D. Switch B - Fa0/1
E. Switch C - Fa0/0
F. Switch C - Fa0/1

Answer: B,C,D

Explanation:

This question is to check the spanning tree election problem.

1. First, select the root bridge, which can be accomplished by comparing the bridge ID, the smallest will be selected. Bridge-id= bridge priority + MAC address. The three switches in the figure all have the default priority, so we should compare the MAC address, it is easy to find that SwitchB is the root bridge.

2. Select the root port on the non-root bridge, which can be completed through comparing root path cost. The smallest will be selected as the root port.

3. Next, select the Designated Port. First, compare the path cost, if the costs happen to be the same, then compare the BID, still the smallest will be selected. Each link has a DP. Based on the exhibit above, we can find DP on each link. The DP on the link between SwitchA and SwitchC is SwitchA'Fa0/1, because it has the smallest MAC address.

QUESTION NO: 54

Refer to the exhibit.
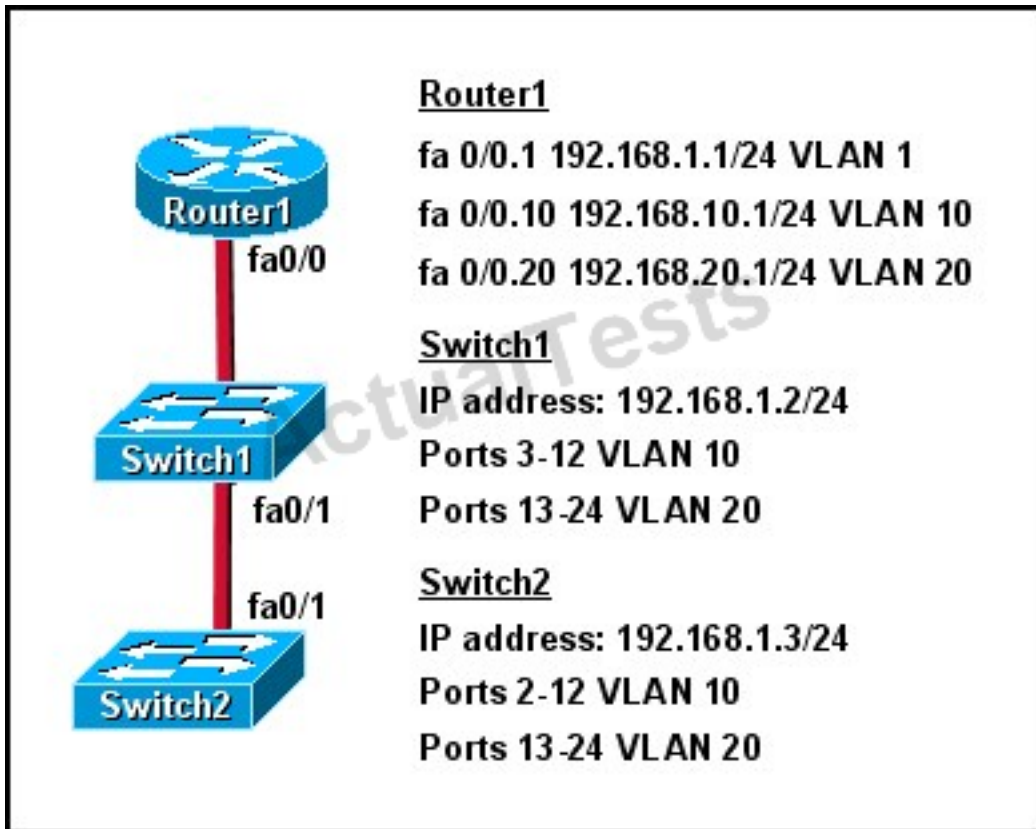
How should the FastEthernet0/1 ports on the 2950 model switches that are shown in the exhibit be configured to allow connectivity between all devices?

A. The ports only need to be connected by a crossover cable.
B. SwitchX(config)# interface fastethernet 0/1
SwitchX(config-if)# switchport mode trunk
C. SwitchX(config)# interface fastethernet 0/1
SwitchX(config-if)# switchport mode access
SwitchX(config-if)# switchport access vlan 1
D. SwitchX(config)# interface fastethernet 0/1
SwitchX(config-if)# switchport mode trunk
SwitchX(config-if)# switchport trunk vlan 1
SwitchX(config-if)# switchport trunk vlan 10
SwitchX(config-if)# switchport trunk vlan 20

Answer: B
Explanation:
IN order for multiple VLANs to cross switches, the connection between the switches must be a trunk. The "switchport mode trunk" command is all that is needed, the individual VLANs should not be listed over that trunk interface.

QUESTION NO: 55

Refer to the exhibit.
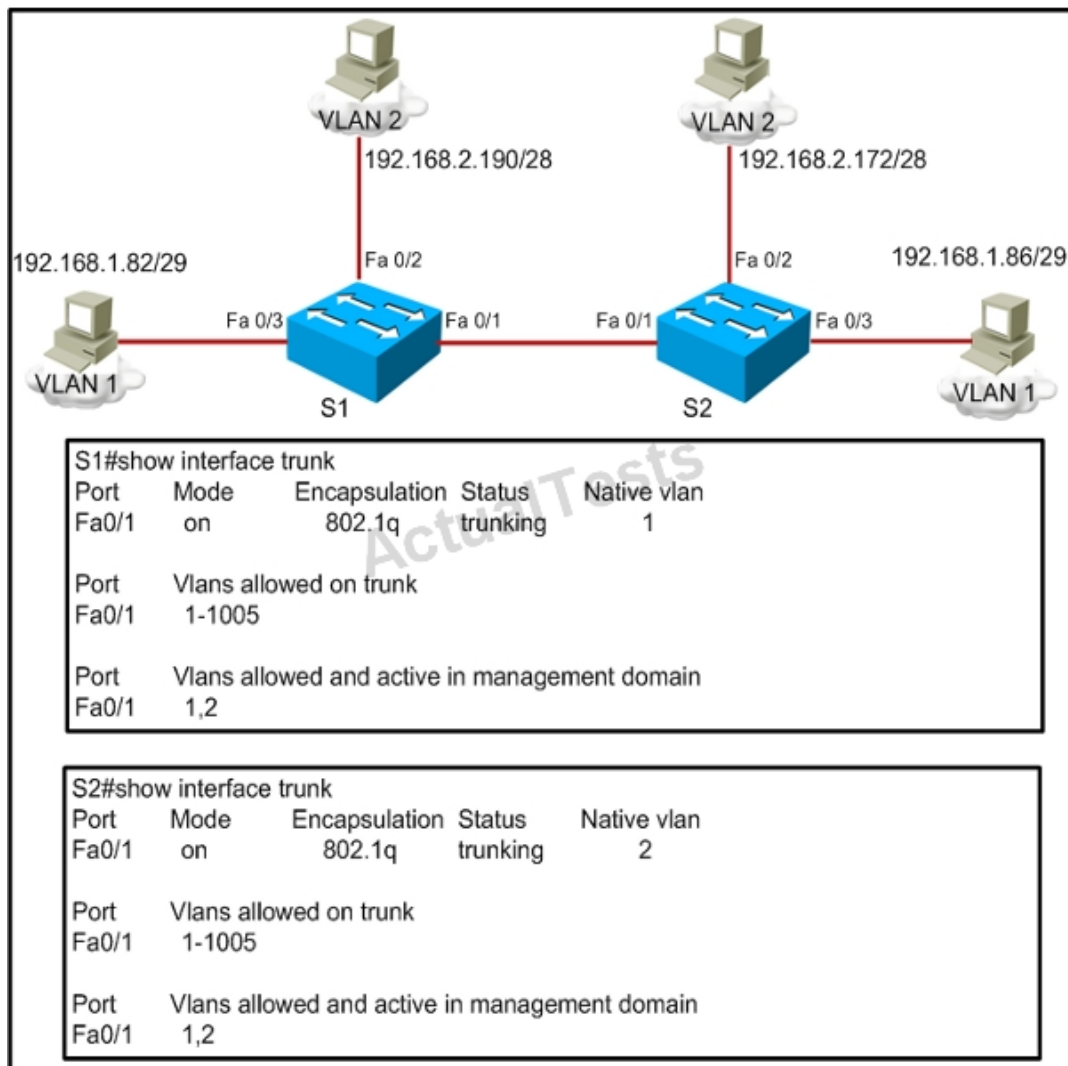
A frame on VLAN 1 on switch S1 is sent to switch S2 where the frame is received on VLAN 2. What causes this behavior?

A. trunk mode mismatches
B. allowing only VLAN 2 on the destination
C. native VLAN mismatches
D. VLANs that do not correspond to a unique IP subnet

Answer: C

Explanation:

Untagged frames are encapsulated with the native VLAN. In this case, the native VLANs are different so although S1 will tag it as VLAN 1 it will be received by S2.

QUESTION NO: 56

Which three statements about RSTP are true? (Choose three.)

A. RSTP significantly reduces topology reconverging time after a link failure.
B. RSTP expands the STP port roles by adding the alternate and backup roles.
C. RSTP port states are blocking, discarding, learning, or forwarding.
D. RSTP provides a faster transition to the forwarding state on point-to-point links than STP does.
E. RSTP also uses the STP proposal-agreement sequence.
F. RSTP uses the same timer-based process as STP on point-to-point links.

Answer: A,B,D

Explanation:

One big disadvantage of STP is the low convergence which is very important in switched network. To overcome this problem, in 2001, the IEEE with document 802.1w introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), which significantly reduces the convergence time after a topology change occurs in the network. While STP can take 30 to 50 seconds to transit from a blocking state to a forwarding state, RSTP is typically able to respond less than 10 seconds of a physical link failure.

RSTP works by adding an alternative port and a backup port compared to STP. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge.

RSTP bridge port roles:

* **Root port** – A forwarding port that is the closest to the root bridge in terms of path cost*
Designated port – A forwarding port for every LAN segment* **Alternate port** – A best alternate path to the root bridge. This path is different than using the root port. The alternative port moves to the forwarding state if there is a failure on the designated port for the segment.* **Backup port** – A backup/redundant path to a segment where another bridge port already connects. The backup port applies only when a single switch has two links to the same segment (collision domain). To have two links to the same collision domain, the switch must be attached to a hub.* **Disabled port** – Not strictly part of STP, a network administrator can manually disable a port

QUESTION NO: 57

At which layer of the OSI model is RSTP used to prevent loops?

A. physical
B. data link
C. network
D. transport

Answer: B
Explanation: Explanation
RSTP and STP operate on switches and are based on the exchange of Bridge Protocol Data Units (BPDUs) between switches. One of the most important fields in BPDUs is the Bridge Priority in which the MAC address is used to elect the Root Bridge -> RSTP operates at Layer 2 – Data Link layer -> .

QUESTION NO: 58

What does a Layer 2 switch use to decide where to forward a received frame?

A. source MAC address
B. source IP address
C. source switch port
D. destination IP address
E. destination port address
F. destination MAC address

Answer: F
Explanation:
When a frame is received, the switch looks at the destination hardware address and finds the interface if it is in its MAC address table. If the address is unknown, the frame is broadcast on all interfaces except the one it was received on.

QUESTION NO: 59

Refer to the exhibit.

```
SwitchA# show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     0017.596d.2a00
             Cost        38
             Port        11 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     0017.596d.1580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface          Role Sts Cost       Prio.Nbr Type
---------------- ---- --- --------- -------- ---------
Fa0/11             Root FWD 19         128.11   P2p
Fa0/12             Altn BLK 19         128.12   P2p
```

Which statement is true?

A. The Fa0/11 role confirms that SwitchA is the root bridge for VLAN 20.
B. VLAN 20 is running the Per VLAN Spanning Tree Protocol.
C. The MAC address of the root bridge is 0017.596d.1580.
D. SwitchA is not the root bridge, because not all of the interface roles are designated.

Answer: D

Explanation: Explanation

Only non-root bridge can have root port. Fa0/11 is the root port so we can confirm this switch is not the root bridge ->

From the output we learn this switch is running Rapid STP, not PVST ->

0017.596d.1580 is the MAC address of this switch, not of the root bridge. The MAC address of the root bridge is 0017.596d.2a00 ->

All of the interface roles of the root bridge are designated. SwitchA has one Root port and 1 Alternative port so it is not the root bridge.

QUESTION NO: 60

Which two benefits are provided by creating VLANs? (Choose two.)

A. added security
B. dedicated bandwidth
C. provides segmentation

D. allows switches to route traffic between subinterfaces
E. contains collisions

Answer: A,C
Explanation:
A VLAN is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis.
Security:
VLANs also improve security by isolating groups. High-security users can be grouped into a VLAN, possible on the same physical segment, and no users outside that VLAN can communicate with them
LAN Segmentation

VLANs allow logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. By containing traffic originating on a particular LAN only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth.

QUESTION NO: 61

Which command can be used from a PC to verify the connectivity between hosts that connect through a switch in the same LAN?

A. ping address
B. tracert address
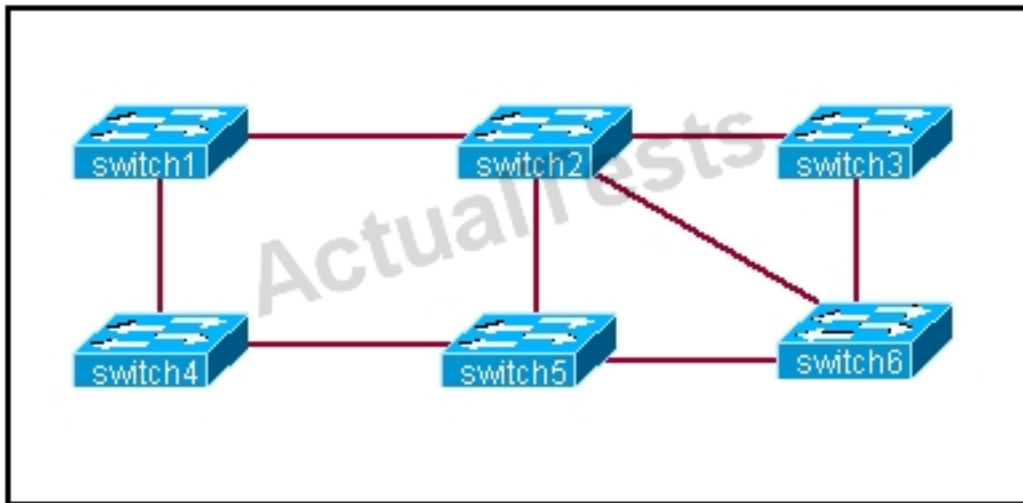**C.** traceroute address
D. arp address

Answer: A
Explanation:
ICMP pings are used to verify connectivity between two IP hosts. Traceroute is used to verify the router hop path traffic will take but in this case since the hosts are in the same LAN there will be no router hops involved.

QUESTION NO: 62

Based on the network shown in the graphic

Which option contains both the potential networking problem and the protocol or setting that should be used to prevent the problem?

A. routing loops, hold down timers
B. switching loops, split horizon
C. routing loops, split horizon
D. switching loops, VTP
E. routing loops, STP
F. switching loops, STP

Answer: F

Explanation: The Spanning-Tree Protocol (STP) prevents loops from being formed when switches or bridges are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is one and only one active path between two network devices.

QUESTION NO: 63

Refer to the exhibit.
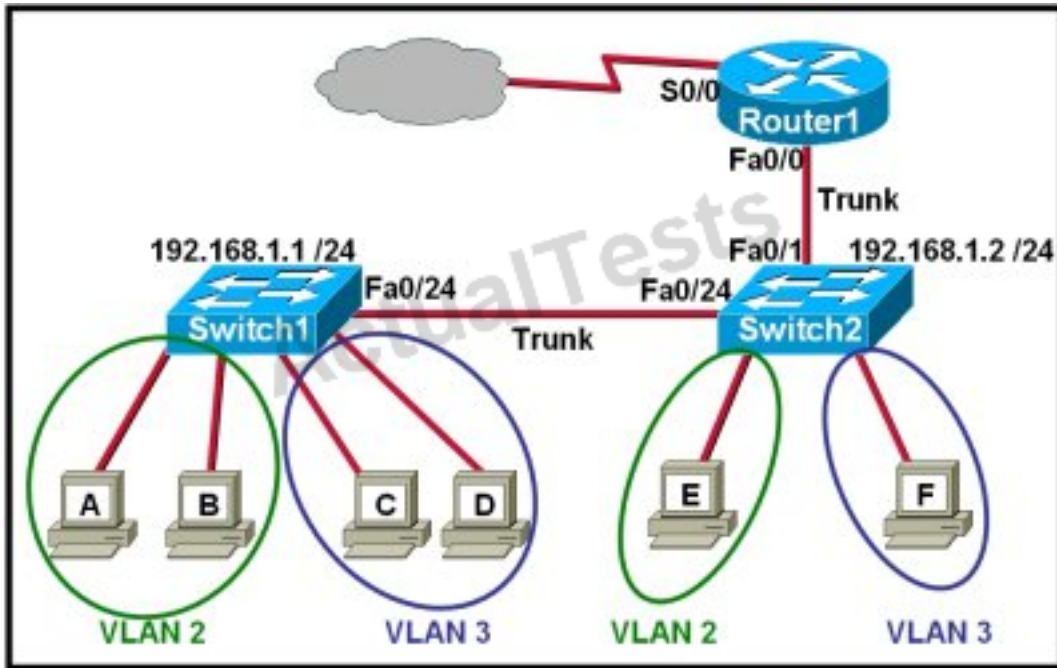
Which two statements are true about interVLAN routing in the topology that is shown in the exhibit? (Choose two.)

A. Host E and host F use the same IP gateway address.
B. Router1 and Switch2 should be connected via a crossover cable.
C. Router1 will not play a role in communications between host A and host D.
D. The FastEthernet 0/0 interface on Router1 must be configured with subinterfaces.
E. Router1 needs more LAN interfaces to accommodate the VLANs that are shown in the exhibit.
F. The FastEthernet 0/0 interface on Router1 and the FastEthernet 0/1 interface on Switch2 trunk ports must be configured using the same encapsulation type.

Answer: D,F
Explanation:
In order for multiple VLANs to connect to a single physical interface on a Cisco router, subinterfaces must be used, one for each VLAN. This is known as the router on a stick configuration. Also, for any trunk to be formed, both ends of the trunk must agree on the encapsulation type, so each one must be configured for 802.1q or ISL.

QUESTION NO: 64

Which two of these are characteristics of the 802.1Q protocol? (Choose two.)

A. It is used exclusively for tagging VLAN frames and does not address network reconvergence following switched network topology changes.

B. It modifies the 802.3 frame header, and thus requires that the FCS be recomputed.
C. It is a Layer 2 messaging protocol which maintains VLAN configurations across networks.
D. It includes an 8-bit field which specifies the priority of a frame.
**E.** It is a trunking protocol capable of carrying untagged frames.

Answer: B,E
Explanation:
802.1Q protocol, or Virtual Bridged Local Area Networks protocol, mainly stipulates the realization of the VLAN. 802.1Q is a standardized relay method that inserts 4 bytes field into the original Ethernet frame and re-calculate the FCS. 802.1Q frame relay supports two types of frame: marked and non-marked. Non-marked frame carries no VLAN identification information.

QUESTION NO: 65

Refer to the exhibit.
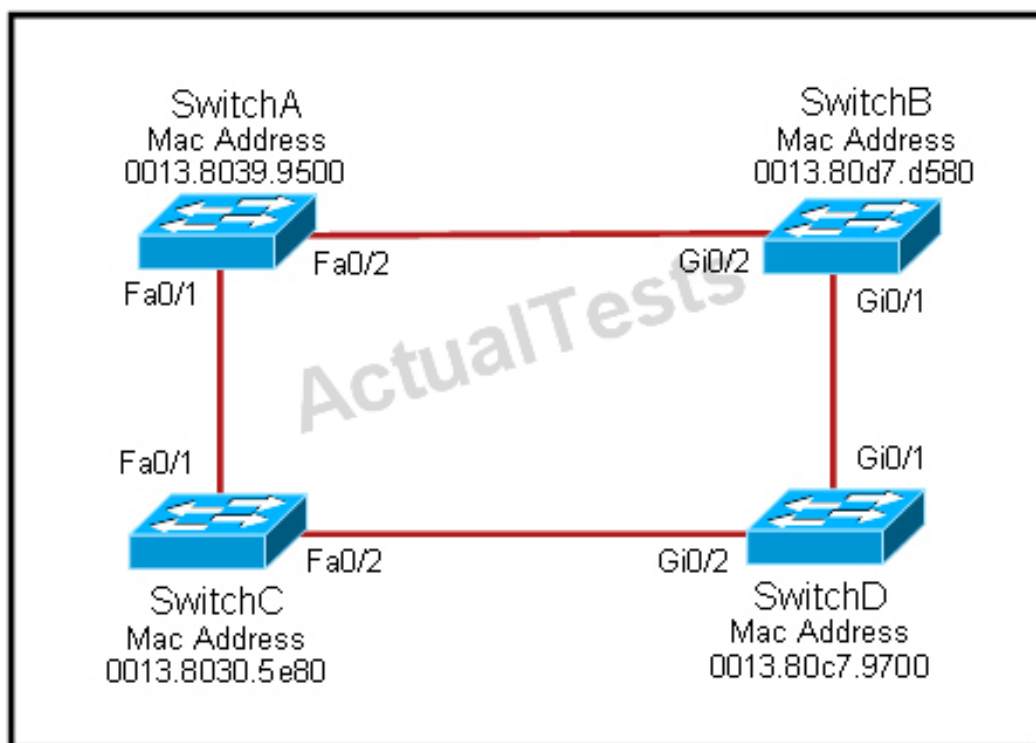
Each of these four switches has been configured with a hostname, as well as being configured to run RSTP. No other configuration changes have been made. Which three of these show the correct RSTP port roles for the indicated switches and interfaces? (Choose three.)

A. SwitchA, Fa0/2, designated
B. SwitchA, Fa0/1, root

C. SwitchB, Gi0/2, root

D. SwitchB, Gi0/1, designated

E. SwitchC, Fa0/2, root

F. SwitchD, Gi0/2, root

Answer: A,B,F

Explanation: Explanation

The question says "no other configuration changes have been made" so we can understand these switches have the same bridge priority. Switch C has lowest MAC address so it will become root bridge and 2 of its ports (Fa0/1 & Fa0/2) will be designated ports.

Because SwitchC is the root bridge so the 2 ports nearest SwitchC on SwitchA (Fa0/1) and SwitchD (Gi0/2) will be root ports..

Now we come to the most difficult part of this question: SwitchB must have a root port so which port will it choose? To answer this question we need to know about STP cost and port cost.

In general, "cost" is calculated based on bandwidth of the link. The higher the bandwidth on a link, the lower the value of its cost. Below are the cost values you should memorize:

Link speed	Cost
10Mbps	100
100Mbps	19
1 Gbps	4

SwitchB will choose the interface with lower cost to the root bridge as the root port so we must calculate the cost on interface Gi0/1 & Gi0/2 of SwitchB to the root bridge. This can be calculated from the "cost to the root bridge" of each switch because **a switch always advertises its cost to the root bridge** in its BPDU. The receiving switch will **add its local port cost value to the cost** in the BPDU.

One more thing to notice is that a root bridge always advertises the cost to the root bridge (itself) with an initial value of 0.

Now let's have a look at the topology again
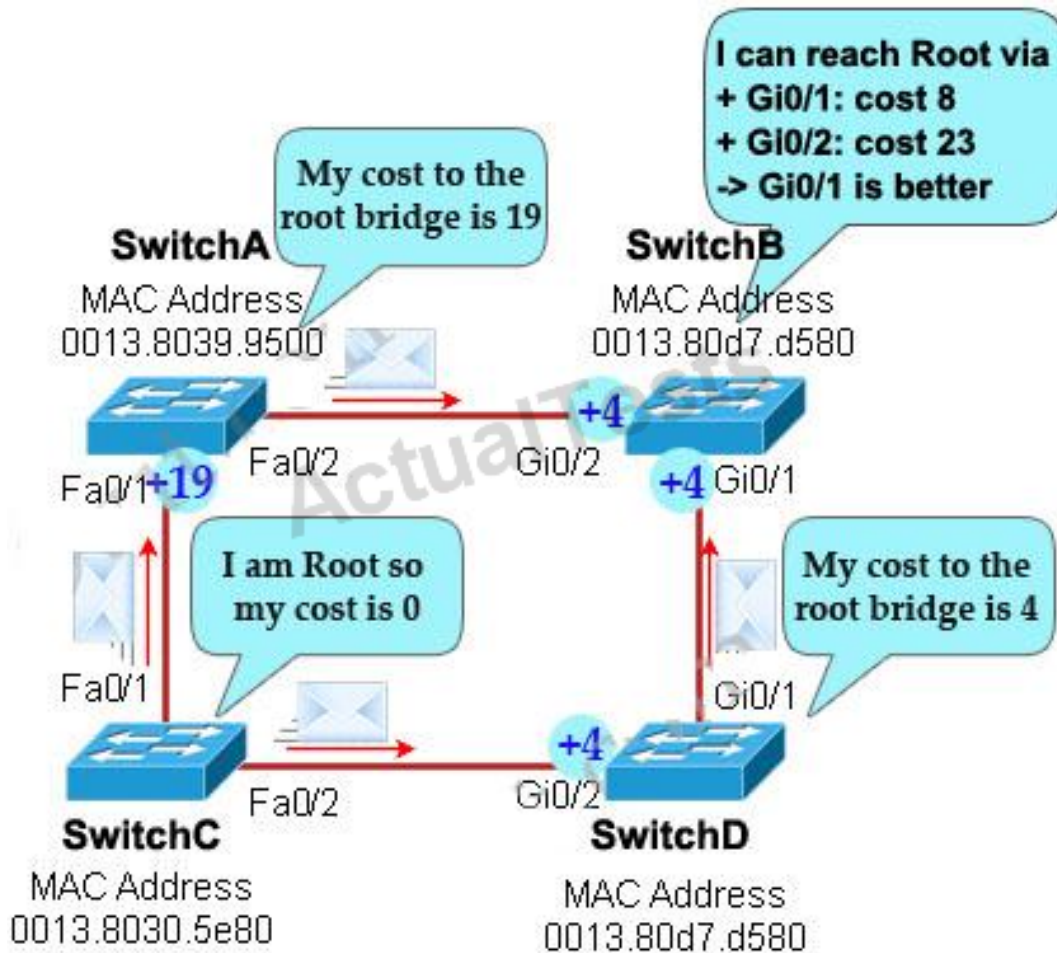
SwitchC advertises its cost to the root bridge with a value of 0. Switch D adds 4 (the cost value of 1Gbps link) and advertises this value (4) to SwitchB. SwitchB adds another 4 and learns that it can reach SwitchC via Gi0/1 port with a total cost of 8. The same process happens for SwitchA and SwitchB learns that it can reach SwitchC via Gi0/2 with a total cost of 23 -> Switch B chooses Gi0/1 as its root port ->

Now our last task is to identify the port roles of the ports between SwitchA & SwitchB. It is rather easy as the MAC address of SwitchA is lower than that of SwitchB so Fa0/2 of SwitchA will be designated port while Gi0/2 of SwitchB will be alternative port.
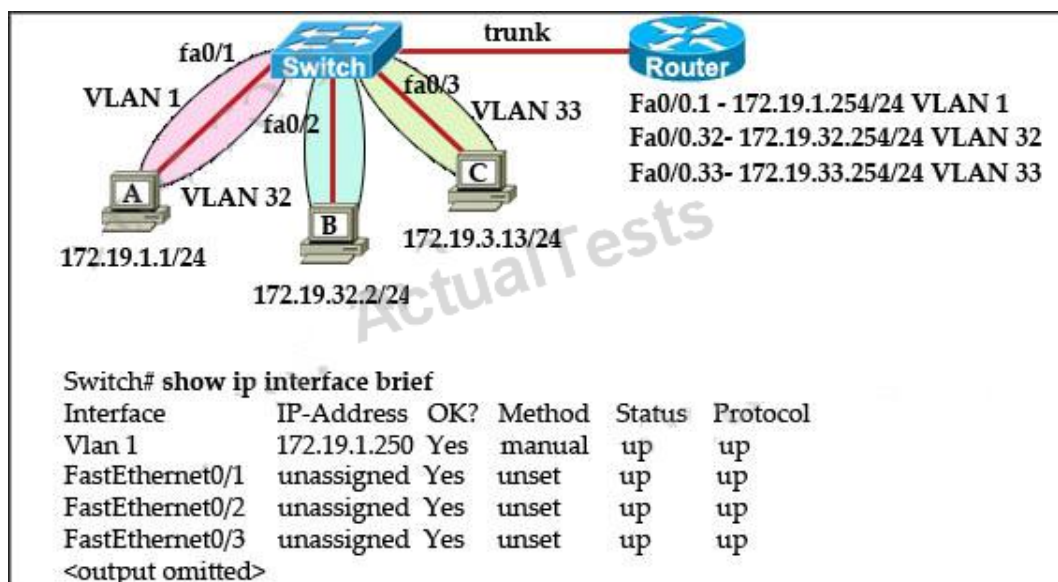
Below summaries all the port roles of these switches:
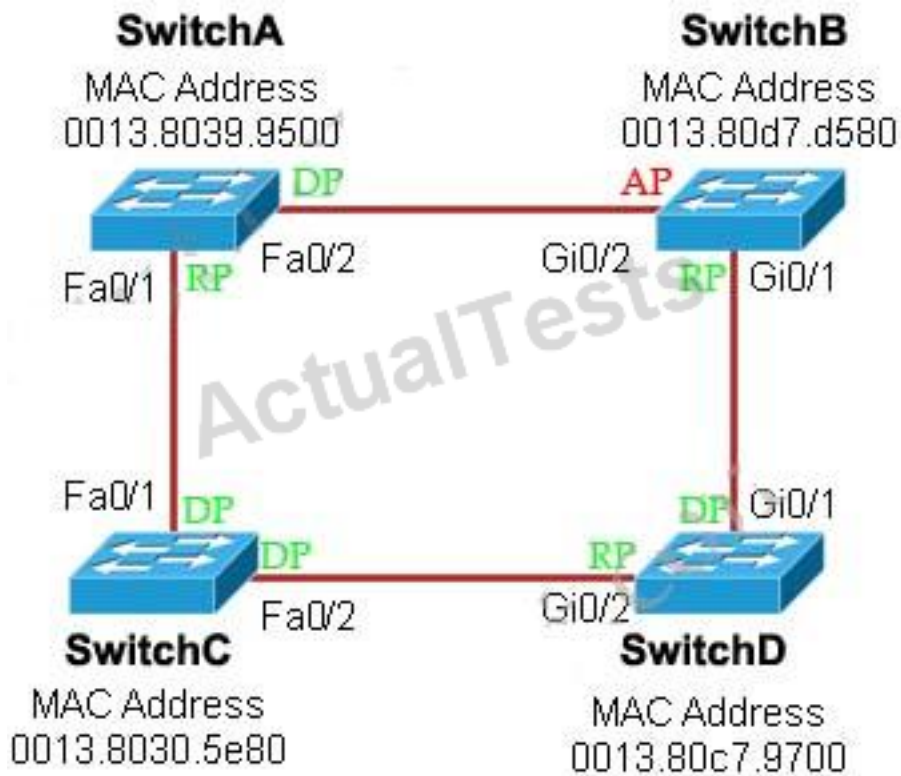
+ DP: Designated Port (forwarding state)
+ RP: Root Port (forwarding state)
+ AP: Alternative Port (blocking state)

QUESTION NO: 66

Refer to the exhibit.

The network administrator normally establishes a Telnet session with the switch from host A. However, host A is unavailable. The administrator's attempt to telnet to the switch from host B fails, but pings to the other two hosts are successful. What is the issue?

A. Host B and the switch need to be in the same subnet.
B. The switch interface connected to the router is down.
C. Host B needs to be assigned an IP address in VLAN 1.
D. The switch needs an appropriate default gateway assigned.
**E.** The switch interfaces need the appropriate IP addresses assigned.

Answer: D

Explanation:

Ping was successful form host B to other hosts because of intervlan routing configured on router. But to manage switch via telnet the VLAN32 on the switch needs to be configured interface vlan32 along with ip address and its appropriate default-gateway address.

Since VLAN1 interface is already configure on switch Host A was able to telnet switch.

QUESTION NO: 67

Refer to the exhibit.
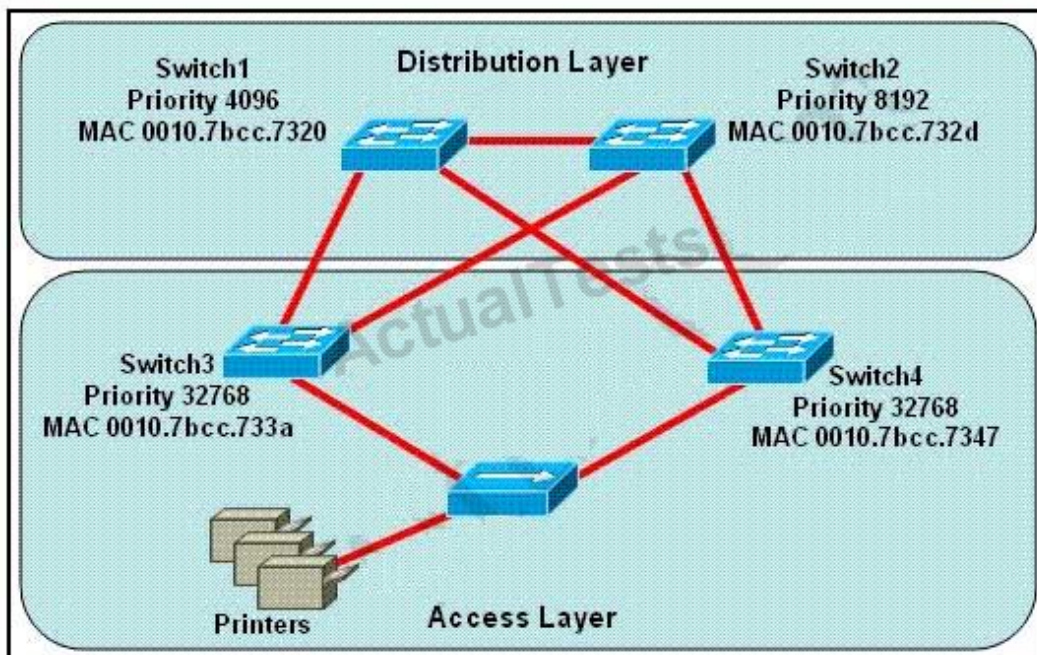
Which switch provides the spanning-tree designated port role for the network segment that services the printers?

A. Switch1
B. Switch2
C. Switch3
D. Switch4

Answer: C

Explanation:

Printers are connected by hubs. Decide the switch that provides the spanning-tree designated port role between Switch3 and Switch4. They have the same priority 32768. Compare their MAC addresses. Switch3 with a smaller MAC address will provide a designated port for printers.

QUESTION NO: 68

What is one benefit of PVST+?

A. PVST+ supports Layer 3 load balancing without loops.
B. PVST+ reduces the CPU cycles for all the switches in the network.
C. PVST+ allows the root switch location to be optimized per VLAN.
D. PVST+ automatically selects the root bridge location, to provide optimized bandwidth usage.

Answer: C

Explanation:

The PVST+ provides Layer 2 load-balancing for the VLAN on which it runs. You can create different logical topologies by using the VLANs on your network to ensure that all of your links are used but that no one link is oversubscribed. Each instance of PVST+ on a VLAN has a single root switch. This root switch propagates the spanning-tree information associated with that VLAN to all other switches in the network. Because each switch has the same information about the network, this process ensures that the network topology is maintained and optimized per VLAN.
Reference:
http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_55_se/configuration/guide/swstp.html

QUESTION NO: 69

Which are valid modes for a switch port used as a VLAN trunk? (Choose three.)

A. transparent
B. auto

C. on

D. desirable
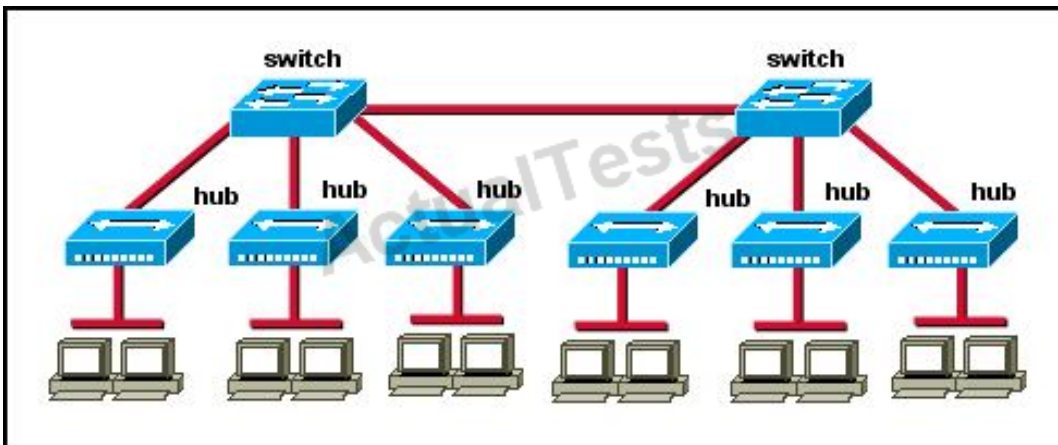
E. blocking

F. forwarding

Answer: B,C,D

Explanation:

These are the different types of trunk modes:

QUESTION NO: 70

Refer to Exhibit:

How many broadcast domains are shown in the graphic assuming only the default VLAN is configured on the switches?

A. one

B. two

C. six

D. twelve

Answer: A

Explanation: Explanation

Only router can break up broadcast domains but in this exhibit no router is used so there is only 1 broadcast domain.

For your information, there are 7 collision domains in this exhibit (6 collision domains between hubs & switches + 1 collision between the two switches).

QUESTION NO: 71

Which three of these statements regarding 802.1Q trunking are correct? (Choose three.)

A. 802.1Q native VLAN frames are untagged by default.
B. 802.1Q trunking ports can also be secure ports.
C. 802.1Q trunks can use 10 Mb/s Ethernet interfaces.
D. 802.1Q trunks require full-duplex, point-to-point connectivity.
E. 802.1Q trunks should have native VLANs that are the same at both ends.

Answer: A,C,E
Explanation:
By default, 802.1Q trunk defined Native VLAN in order to forward unmarked frame. Switches can forward Layer 2 frame from Native VLAN on unmarked trunks port. Receiver switches will transmit all unmarked packets to Native VLAN. Native VLAN is the default VLAN configuration of port. Note for the 802.1Q trunk ports between two devices, the same Native VLAN configuration is required on both sides of the link. If the Native VLAN in 802.1Q trunk ports on same trunk link is properly configured, it could lead to layer 2 loops. The 802.1Q trunk link transmits VLAN information through Ethernet.

QUESTION NO: 72

Refer to the exhibit.

```
Switch# show spanning-tree vlan 30
VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 24606
Address 00d0.047b.2800
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 24606 (priority 24576 sys-id-ext 30)
Address 00d0.047b.2800
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface      Role  Sts    Cost    Prio.Nbr     Type
---------      ----  ---    ----    --------     ----- ----------
Fa1/1          Desg  FWD    4       128.1        p2p
Fa1/2          Desg  FWD    4       128.2        p2p
Fa5/1          Desg  FWD    4       128.257      p2p
```

The output that is shown is generated at a switch. Which three statements are true? (Choose three.)

A. All ports will be in a state of discarding, learning, or forwarding.
B. Thirty VLANs have been configured on this switch.
C. The bridge priority is lower than the default value for spanning tree.
D. All interfaces that are shown are on shared media.
E. All designated ports are in a forwarding state.
F. This switch must be the root bridge for all VLANs on this switch.

Answer: A,C,E

Explanation: Explanation

From the output, we see that all ports are in designated role (forwarding state).

The command "show spanning-tree vlan 30 only shows us information about VLAN 30. We don't know how many VLAN exists in this switch ->

The bridge priority of this switch is 24606 which is lower than the default value bridge priority 32768.

All three interfaces on this switch have the connection type "p2p", which means Point-to-point environment – not a shared media.

The only thing we can specify is this switch is the root bridge for VLAN 3o but we can not guarantee it is also the root bridge for other VLANs.

QUESTION NO: 73

Refer to the exhibit.
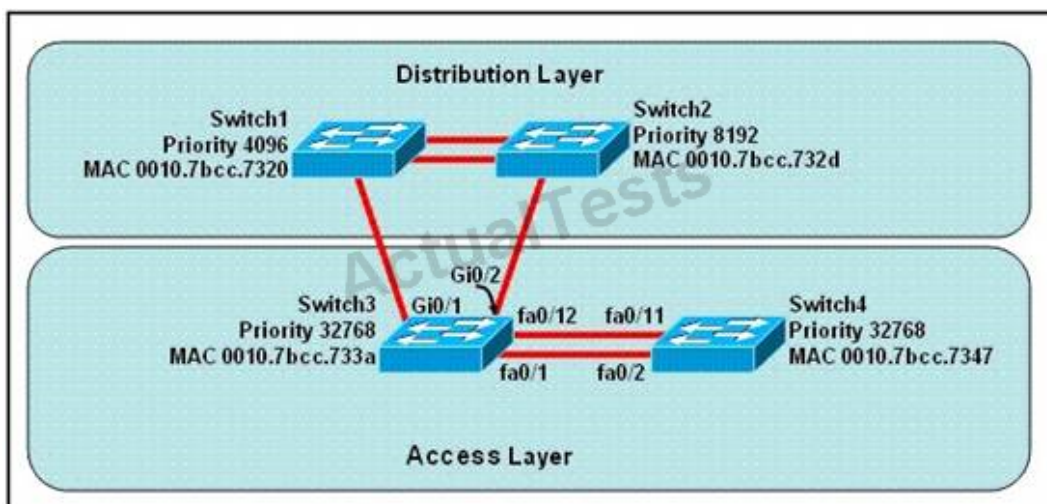
At the end of an RSTP election process, which access layer switch port will assume the discarding

role?

A. Switch3, port fa0/1
B. Switch3, port fa0/12
C. Switch4, port fa0/11
D. Switch4, port fa0/2
E. Switch3, port Gi0/1
F. Switch3, port Gi0/2

Answer: C

Explanation: Explanation

In this question, we only care about the Access Layer switches (Switch3 & 4). Switch 3 has a lower bridge ID than Switch 4 (because the MAC of Switch3 is smaller than that of Switch4) so both ports of Switch3 will be in forwarding state. The alternative port will surely belong to Switch4. Switch4 will need to block one of its ports to avoid a bridging loop between the two switches. But how does Switch4 select its blocked port? Well, the answer is based on the BPDUs it receives from Switch3. A BPDU is superior to another if it has:

1. A lower Root Bridge ID
2. A lower path cost to the Root
3. A lower Sending Bridge ID
4. A lower Sending Port ID

These four parameters are examined in order. In this specific case, all the BPDUs sent by Switch3 have the same Root Bridge ID, the same path cost to the Root and the same Sending Bridge ID. The only parameter left to select the best one is the Sending Port ID (Port ID = port priority + port index). In this case the port priorities are equal because they use the default value, so Switch4 will compare port index values, which are unique to each port on the switch, and because Fa0/12 is inferior to Fa0/1, Switch4 will select the port connected with Fa0/1 (of Switch3) as its root port and block the other port -> Port fa0/11 of Switch4 will be blocked (discarding role).

QUESTION NO: 74

Which term describes a spanning-tree network that has all switch ports in either the blocking or fowarding state?

A. converged
B. redundant
C. provisioned
D. spanned

Answer: A

Explanation: Explanation

Spanning Tree Protocol convergence (Layer 2 convergence) happens when bridges and switches have transitioned to either the forwarding or blocking state. When layer 2 is converged, root bridge is elected and all port roles (Root, Designated and Non-Designated) in all switches are selected.

QUESTION NO: 75

What are the possible trunking modes for a switch port? (Choose three.)

A. transparent
B. auto
C. on
D. desirable
E. client
F. forwarding

Answer: B,C,D

Explanation:

These are the different types of trunk modes:

QUESTION NO: 76

Which two of these statements regarding RSTP are correct? (Choose two.)

A. RSTP cannot operate with PVST+.
B. RSTP defines new port roles.
C. RSTP defines no new port states.
D. RSTP is a proprietary implementation of IEEE 802.1D STP.
E. RSTP is compatible with the original IEEE 802.1D STP.

Answer: B,E

Explanation:

When network topology changes, rapid spanning tree protocol (IEEE802.1W, referred to as RSTP) will speed up significantly the speed to re-calculate spanning tree. RSTP not only defines the role of other ports: alternative port and backup port, but also defines status of 3 ports: discarding

status, learning status, forwarding status.

RSTP is 802.1D standard evolution, not revolution. It retains most of the parameters, and makes no changes.

QUESTION NO: 77

Refer to the exhibit.

```
Switch1# show mac-address-table
Dynamic Addresses Count: 19
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count: 41
Total MAC addresses: 50
Non-static Address Table:
Destination Address     AddressType     VLAN    Destination Port
-------------------     -----------     ----    ----------------
0010.0de0.e289          Dynamic         1       FastEthernet0/1
0010.7b00.1540          Dynamic         2       FastEthernet0/5
0010.7b00.1545          Dynamic         2       FastEthernet0/5
0060.5cf4.0076          Dynamic         1       FastEthernet0/1
0060.5cf4.0077          Dynamic         3       FastEthernet0/1
0060.5cf4.1315          Dynamic         1       FastEthernet0/1
0060.70cb.f301          Dynamic         2       FastEthernet0/1
0060.70cb.3f01          Dynamic         5       FastEthernet0/2
00e0.1e42.9978          Dynamic         4       FastEthernet0/1
00e0.1e9f.3900          Dynamic         3       FastEthernet0/1
0060.70cb.33f1          Dynamic         6       FastEthernet0/3
0060.70cb.103f          Dynamic         6       FastEthernet0/4

<output omitted>

Switch1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID       Local Intrfce   Holdtime   Capability   Platform   Port ID
Switch2         Fas 0/1         157          S          2950-12    Fas 0/1
Switch3         Fas 0/2         143          S          2950-12    Fas 0/5

Switch1#
```

Which two statements are true of the interfaces on Switch1? (Choose two.)

A. Multiple devices are connected directly to FastEthernet0/1.
B. A hub is connected directly to FastEthernet0/5.
C. FastEthernet0/1 is connected to a host with multiple network interface cards.
D. FastEthernet0/5 has statically assigned MAC addresses.
E. FastEthernet0/1 is configured as a trunk link.
F. Interface FastEthernet0/2 has been disabled.

Answer: B,E

Explanation:

Carefully observe the information given after command show. Fa0/1 is connected to Switch2, seven MAC addresses correspond to Fa0/1, and these MAC are in different VLAN. From this we know that Fa0/1 is the trunk interface.

From the information given by show cdp neighbors we find that there is no Fa0/5 in CDP neighbor. However, F0/5 corresponds to two MAC addresses in the same VLAN. Thus we know that Fa0/5 is connected to a Hub.

Based on the output shown, there are multiple MAC addresses from different VLANs attached to the FastEthernet 0/1 interface. Only trunks are able to pass information from devices in multiple VLANs.

QUESTION NO: 78

Three switches are connected to one another via trunk ports. Assuming the default switch configuration, which switch is elected as the root bridge for the spanning-tree instance of VLAN 1?

A. the switch with the highest MAC address
B. the switch with the lowest MAC address
C. the switch with the highest IP address
D. the switch with the lowest IP address

Answer: B

Explanation:

Each switch in your network will have a Bridge ID Priority value, more commonly referred to as a BID. This BID is a combination of a default priority value and the switch's MAC address, with the priority value listed first. The lowest BID will win the election process.

For example, if a Cisco switch has the default priority value of 32,768 and a MAC address of 11-22-33-44-55-66, the BID would be 32768:11-22-33-44-55-66. Therefore, if the switch priority is left at the default, the MAC address is the deciding factor in the root bridge election.

QUESTION NO: 79

What are three advantages of VLANs? (Choose three.)

A. VLANs establish broadcast domains in switched networks.

B. VLANs utilize packet filtering to enhance network security.

C. VLANs provide a method of conserving IP addresses in large networks.

D. VLANs provide a low-latency internetworking alternative to routed networks.

E. VLANs allow access to network services based on department, not physical location.

F. VLANs can greatly simplify adding, moving, or changing hosts on the network.

Answer: A,E,F

Explanation:

VLAN technology is often used in practice, because it can better control layer2 broadcast to improve network security. This makes network more flexible and scalable.

Packet filtering is a function of firewall instead of VLAN.

QUESTION NO: 80

Cisco Catalyst switches CAT1 and CAT2 have a connection between them using ports FA0/13. An 802.1Q trunk is configured between the two switches. On CAT1, VLAN 10 is chosen as native, but on CAT2 the native VLAN is not specified.

What will happen in this scenario?

A. 802.1Q giants frames could saturate the link.

B. VLAN 10 on CAT1 and VLAN 1 on CAT2 will send untagged frames.

C. A native VLAN mismatch error message will appear.

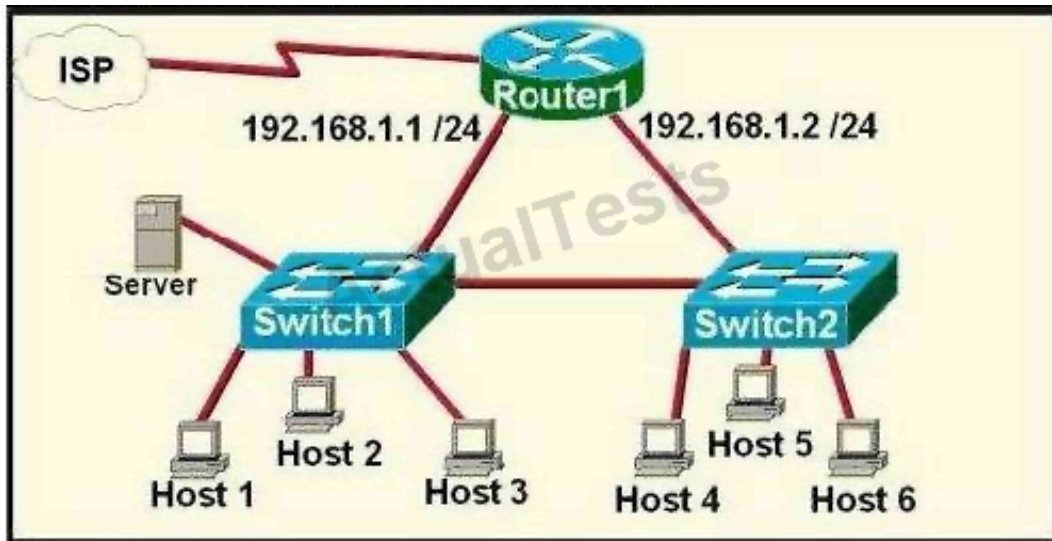**D.** VLAN 10 on CAT1 and VLAN 1 on CAT2 will send tagged frames.

Answer: C

Explanation: Explanation

A "native VLAN mismatch" error will appear by CDP if there is a native VLAN mismatch on an 802.1Q link. "VLAN mismatch" can cause traffic from one vlan to leak into another vlan.

QUESTION NO: 81

Refer to the exhibit.

A network technician is asked to design a small network with redundancy. The exhibit represents this design, with all hosts configured in the same VLAN. What conclusions can be made about this design?

A. This design will function as intended.
B. Spanning-tree will need to be used.
C. The router will not accept the addressing scheme.
D. The connection between switches should be a trunk.
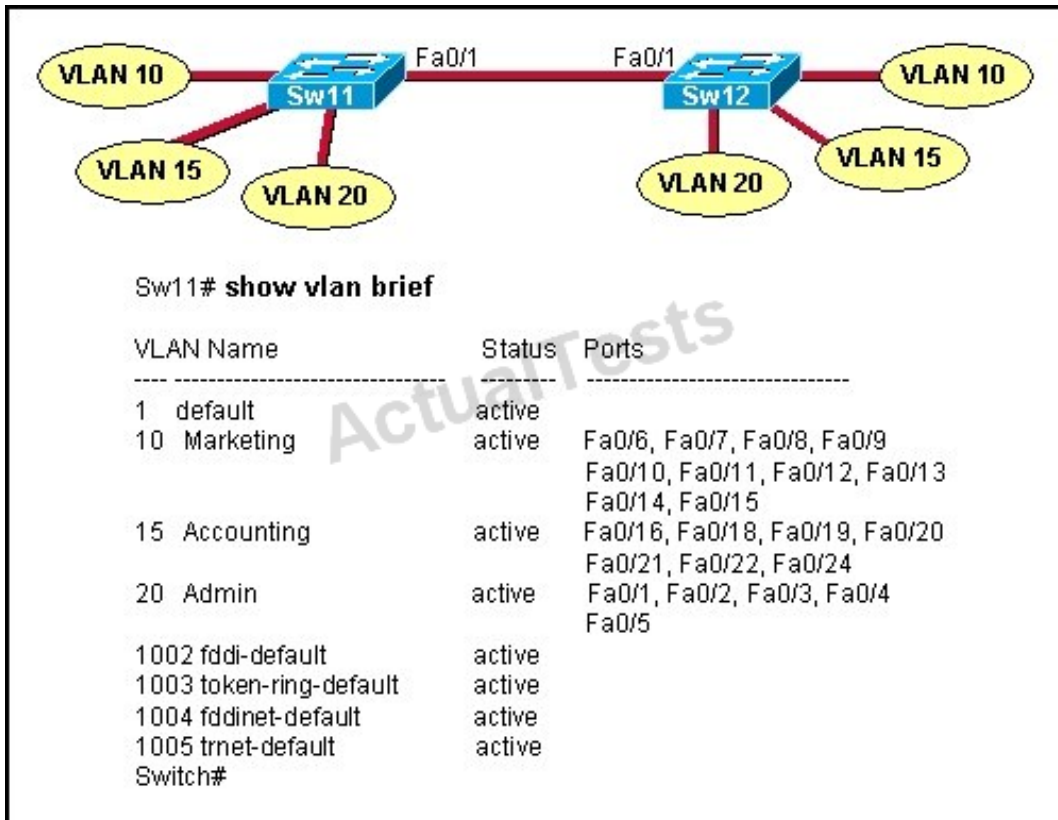**E.** The router interfaces must be encapsulated with the 802.1Q protocol.

Answer: C

Explanation: Explanation

Each interface on a router must be in a different network. If two interfaces are in the same

network, the router will not accept it and show error when the administrator assigns it.

QUESTION NO: 82

Refer to the exhibit.

```
Sw11# show vlan brief

VLAN Name                    Status   Ports
---- ------------------------  --------  ------------------------------
1    default                  active
10   Marketing                active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                        Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                        Fa0/14, Fa0/15
15   Accounting               active    Fa0/16, Fa0/18, Fa0/19, Fa0/20
                                        Fa0/21, Fa0/22, Fa0/24
20   Admin                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                        Fa0/5
1002 fddi-default             active
1003 token-ring-default       active
1004 fddinet-default          active
1005 trnet-default            active
Switch#
```

A technician is troubleshooting host connectivity issues on the switches. The hosts in VLANs 10 and 15 on Sw11 are unable to communicate with hosts in the same VLANs on Sw12. Hosts in the Admin VLAN are able to communicate. The port-to-VLAN assignments are identical on the two switches. What could be the problem?

A. The Fa0/1 port is not operational on one of the switches.
B. The link connecting the switches has not been configured as a trunk.
C. At least one port needs to be configured in VLAN 1 for VLANs 10 and 15 to be able to communicate.
D. Port FastEthernet 0/1 needs to be configured as an access link on both switches.
E. A router is required for hosts on SW11 in VLANs 10 and 15 to communicate with hosts in the same VLAN on Sw12.
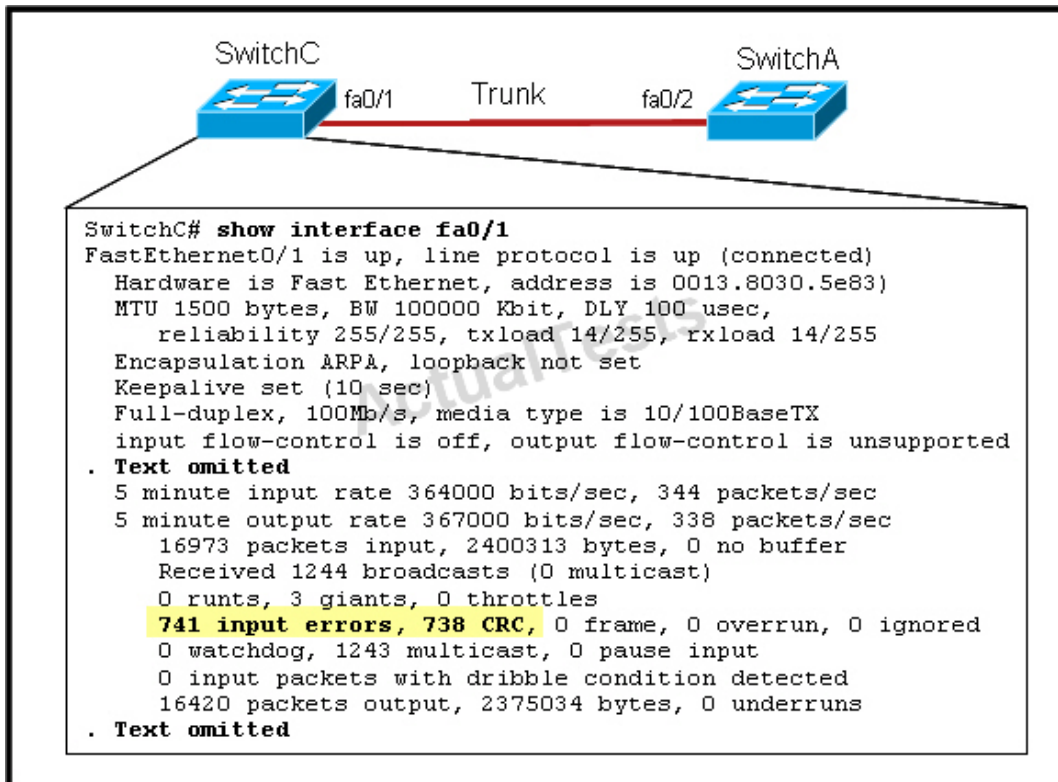
Answer: B
Explanation:
In order for hosts in the same VLAN to communicate with each other over multiple switches, those switches need to be configured as trunks on their connected interfaces so that they can pass traffic from multiple VLANs.

QUESTION NO: 83
Refer to the exhibit.

```
SwitchC# show interface fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0013.8030.5e83)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
      reliability 255/255, txload 14/255, rxload 14/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
. Text omitted
  5 minute input rate 364000 bits/sec, 344 packets/sec
  5 minute output rate 367000 bits/sec, 338 packets/sec
      16973 packets input, 2400313 bytes, 0 no buffer
      Received 1244 broadcasts (0 multicast)
      0 runts, 3 giants, 0 throttles
      741 input errors, 738 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 1243 multicast, 0 pause input
      0 input packets with dribble condition detected
      16420 packets output, 2375034 bytes, 0 underruns
. Text omitted
```

Given this output for SwitchC, what should the network administrator's next action be?

A. Check the trunk encapsulation mode for SwitchC's fa0/1 port.
B. Check the duplex mode for SwitchC's fa0/1 port.
C. Check the duplex mode for SwitchA's fa0/2 port.
D. Check the trunk encapsulation mode for SwitchA's fa0/2 port.

Answer: C

Explanation:

Here we can see that this port is configured for full duplex, so the next step would be to check the duplex setting of the port on the other switch. A mismatched trunk encapsulation would not result in input errors and CRC errors.

Topic 3, IP addressing (IPv4 / IPv6)

QUESTION NO: 84

You have been asked to come up with a subnet mask that will allow all three web servers to be on

the same network while providing the maximum number of subnets. Which network address and subnet mask meet this requirement?

A. 192.168.252.0 255.255.255.252
B. 192.168.252.8 255.255.255.248
C. 192.168.252.8 255.255.255.252
D. 192.168.252.16 255.255.255.240
E. 192.168.252.16 255.255.255.252

Answer: B
Explanation:

A subnet mask of 255.255.255.248 will allow for up to 6 hosts to reside in this network. A subnet mask of 255.255.255.252 will allow for only 2 usable IP addresses, since we can not use the network or broadcast address.

QUESTION NO: 85

Given an IP address 172.16.28.252 with a subnet mask of 255.255.240.0, what is the correct network address?

A. 172.16.16.0
B. 172.16.0.0
C. 172.16.24.0
D. 172.16.28.0

Answer: A
Explanation:

For this example, the network range is 172.16.16.1 - 172.16.31.254, the network address is 172.16.16.0 and the broadcast IP address is 172.16.31.255.

QUESTION NO: 86

Which IPv6 address is the equivalent of the IPv4 interface loopback address 127.0.0.1?

A. ::1
B. ::
C. 2000::/3
D. 0::/10

Answer: A
Explanation:

In IPv6 the loopback address is written as,

1

This is a 128bit number, with the first 127 bits being '0' and the 128th bit being '1'. It's just a single address, so could also be written as ::1/128.

QUESTION NO: 87

You are working in a data center environment and are assigned the address range 10.188.31.0/23. You are asked to develop an IP addressing plan to allow the maximum number of subnets with as many as 30 hosts each. Which IP address range meets these requirements?

A. 10.188.31.0/26
B. 10.188.31.0/25
C. 10.188.31.0/28
D. 10.188.31.0/27
E. 10.188.31.0/29

Answer: D
Explanation: Explanation

Each subnet has 30 hosts < 32 = 25 so we need a subnet mask which has at least 5 bit 0s -> /27. Also the question requires the maximum number of subnets (which minimum the number of hosts-per-subnet) so /27 is the best choice.

QUESTION NO: 88

What are three features of the IPv6 protocol?

(Choose three.)

A. optional IPsec
B. autoconfiguration
C. no broadcasts
D. complicated header
E. plug-and-play
F. checksums

Answer: B,C,E

Explanation:

An important feature of IPv6 is that it allows plug and play option to the network devices by allowing them to configure themselves independently. It is possible to plug a node into an IPv6 network without requiring any human intervention. This feature was critical to allow network connectivity to an increasing number of mobile devices. This is accomplished by autoconfiguration.

IPv6 does not implement traditional IP broadcast, i.e. the transmission of a packet to all hosts on the attached link using a special broadcast address, and therefore does not define broadcast addresses. In IPv6, the same result can be achieved by sending a packet to the link-local all nodes multicast group at address ff02::1, which is analogous to IPv4 multicast to address 224.0.0.1.

QUESTION NO: 89

Which command enables IPv6 forwarding on a Cisco router?

A. ipv6 local
B. ipv6 host
C. ipv6 unicast-routing
D. ipv6 neighbor

Answer: C

Explanation:

to enable IPv6 routing on the Cisco router use the following command:

ipv6 unicast-routing

If this command is not recognized, your version of IOS does not support IPv6.

QUESTION NO: 90

What is known as "one-to-nearest" addressing in IPv6?

A. global unicast
B. anycast
C. multicast
D. unspecified address

Answer: B
Explanation:
IPv6 Anycast addresses are used for one-to-nearest communication, meaning an Anycast address is used by a device to send data to one specific recipient (interface) that is the closest out of a group of recipients (interfaces).

QUESTION NO: 91

What is the first 24 bits in a MAC address called?

A. NIC
B. BIA
C. OUI
D. VAI

Answer: C
Explanation:
An Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization globally or worldwide.
They are used as the first 24 nits of the MAC address to uniquely identify a particular piece of equipment.

QUESTION NO: 92

Refer to the exhibit.
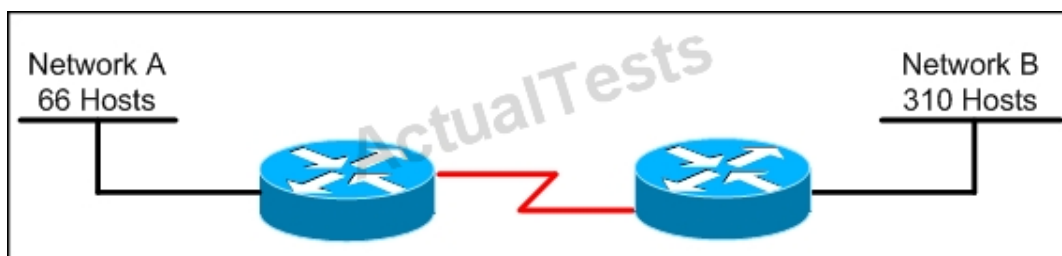
Which subnet mask will place all hosts on Network B in the same subnet with the least amount of wasted addresses?

A. 255.255.255.0
B. 255.255.254.0
C. 255.255.252.0
D. 255.255.248.0

Answer: B

Explanation: Explanation

310 hosts < 512 = 29 -> We need a subnet mask of 9 bits 0 -> 1111 1111.1111 1111.1111 1110.0000 0000 -> 255.255.254.0

QUESTION NO: 93

Refer to the exhibit.
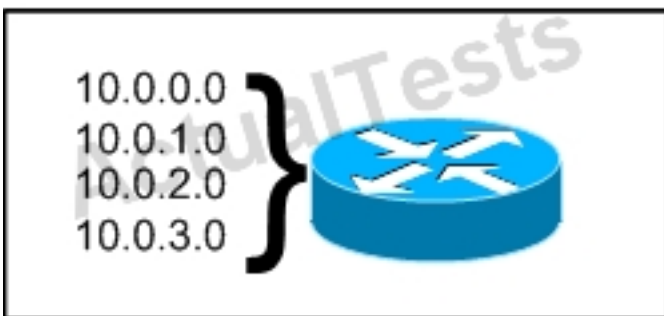
What is the most appropriate summarization for these routes?

A. 10.0.0.0 /21
B. 10.0.0.0 /22
C. 10.0.0.0 /23
D. 10.0.0.0 /24

Answer: B
Explanation:
The 10.0.0.0/22 subnet mask will include the 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0 networks, and only those four networks.

QUESTION NO: 94

Which two are features of IPv6? (Choose two.)

A. anycast
B. broadcast
C. multicast
D. podcast
E. allcast

Answer: A,C
Explanation:
IPv6 addresses are classified by the primary addressing and routing methodologies common in networkinG. unicast addressing, anycast addressing, and multicast addressing.

QUESTION NO: 95

Which two of these statements are true of IPv6 address representation? (Choose two.)

A. There are four types of IPv6 addresses: unicast, multicast, anycast, and broadcast.
B. A single interface may be assigned multiple IPv6 addresses of any type.
C. Every IPv6 interface contains at least one loopback address.
D. The first 64 bits represent the dynamically created interface ID.
E. Leading zeros in an IPv6 16 bit hexadecimal field are mandatory.

Answer: B,C
Explanation:
Leading zeros in IPv6 are optional do that 05C7 equals 5C7 and 0000 equals 0 -> D is not correct.

QUESTION NO: 96

Refer to the exhibit.
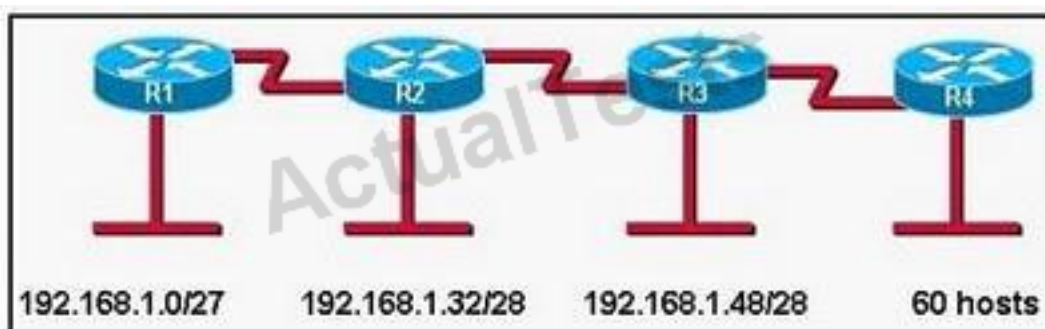
A new subnet with 60 hosts has been added to the network. Which subnet address should this network use to provide enough usable addresses while wasting the fewest addresses?

A. 192.168.1.56/26
B. 192.168.1.56/27
C. 192.168.1.64/26
D. 192.168.1.64/27

Answer: C

Explanation:

A subnet with 60 host is 2*2*2*2*2*2 = 64 -2 == 62

6 bits needed for hosts part. Therefore subnet bits are 2 bits (8-6) in fourth octet.

8bits+ 8bits+ 8bits + 2bits = /26

/26 bits subnet is 24bits + 11000000 = 24bits + 192

256 – 192 = 64

0 -63

64 – 127

QUESTION NO: 97

Refer to the exhibit.
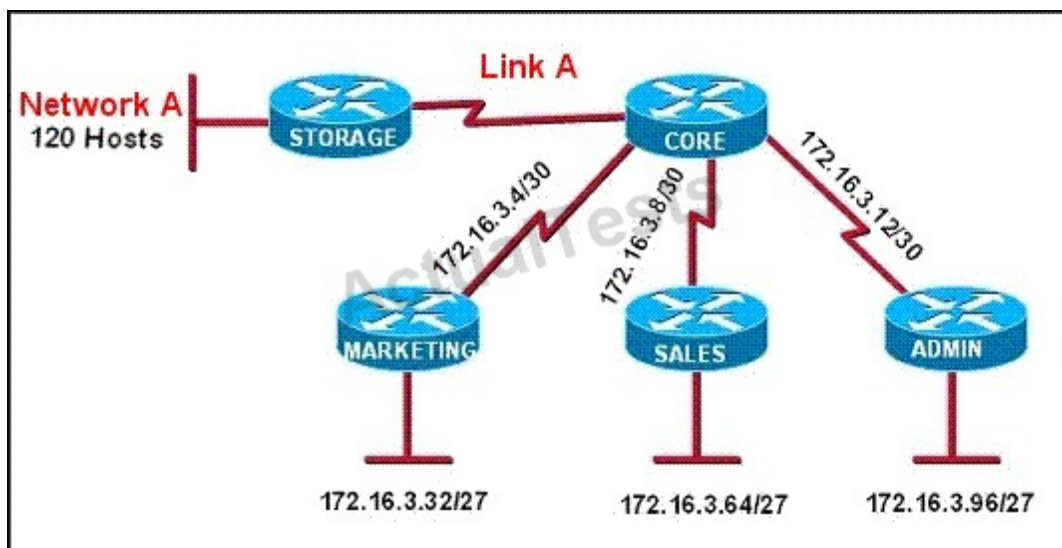
All of the routers in the network are configured with the ip subnet-zero command. Which network addresses should be used for Link A and Network A? (Choose two.)

A. Network A - 172.16.3.48/26

B. Network A - 172.16.3.128/25
C. Network A - 172.16.3.192/26
D. Link A - 172.16.3.0/30
E. Link A - 172.16.3.40/30
F. Link A - 172.16.3.112/30

Answer: B,D
Explanation:
Only a /30 is needed for the point to point link and sine the use of the ip subnet-zero was used, 172.16.3.0/30 is valid. Also, a /25 is required for 120 hosts and again 172.16.3.128/25 is the best, valid option.

QUESTION NO: 98

The network administrator needs to address seven LANs. RIP version 1 is the only routing protocol in use on the network and subnet 0 is not being used. What is the maximum number of usable IP addresses that can be supported on each LAN if the organization is using one class C address block?

A. 8
B. 6
C. 30
D. 32
E. 14
F. 16

Answer: C
Explanation:
Since there is one class C network that means 256 total IP addresses. Since we need 7 LAN blocks and we can not use the first one (subnet 0) we take 256/8=32 hosts. However, since we need to reserve the network and broadcast addresses for each of these subnets, only 30 total IP addresses are usable.

QUESTION NO: 99

What will happen if a private IP address is assigned to a public interface connected to an ISP?

A. Addresses in a private range will be not be routed on the Internet backbone.

B. Only the ISP router will have the capability to access the public network.

C. The NAT process will be used to translate this address to a valid IP address.

D. A conflict of IP addresses happens, because other public routers can use the same range.

Answer: A

Explanation:

Private RFC 1918 IP addresses are meant to be used by organizations locally within their own network only, and can not be used globally for Internet use.

QUESTION NO: 100

Which two benefits are provided by using a hierarchical addressing network addressing scheme? (Choose two.)

A. reduces routing table entries

B. auto-negotiation of media rates

C. efficient utilization of MAC addresses

D. dedicated communications between devices

E. ease of management and troubleshooting

Answer: A,E

Explanation:

Here are some of the benefits of hierarchical addressing:
Reference: http://www.ciscopress.com/articles/article.asp?p=174107

QUESTION NO: 101

What is the alternative notation for the IPv6 address
B514:82C3:0000:0000:0029:EC7A:0000:EC72?

A. B514 : 82C3 : 0029 : EC7A : EC72

B. B514 : 82C3 :: 0029 : EC7A : EC72

C. B514 : 82C3 : 0029 :: EC7A : 0000 : EC72

D. B514 : 82C3 :: 0029 : EC7A : 0 : EC72

Answer: D

Explanation:

There are two ways that an IPv6 address can be additionally compressed: compressing leading

zeros and substituting a group of consecutive zeros with a single double colon (::). Both of these can be used in any number of combinations to notate the same address. It is important to note that the double colon (::) can only be used once within a single IPv6 address notation. So, the extra 0's can only be compressed once.

QUESTION NO: 102

Refer to the diagram.
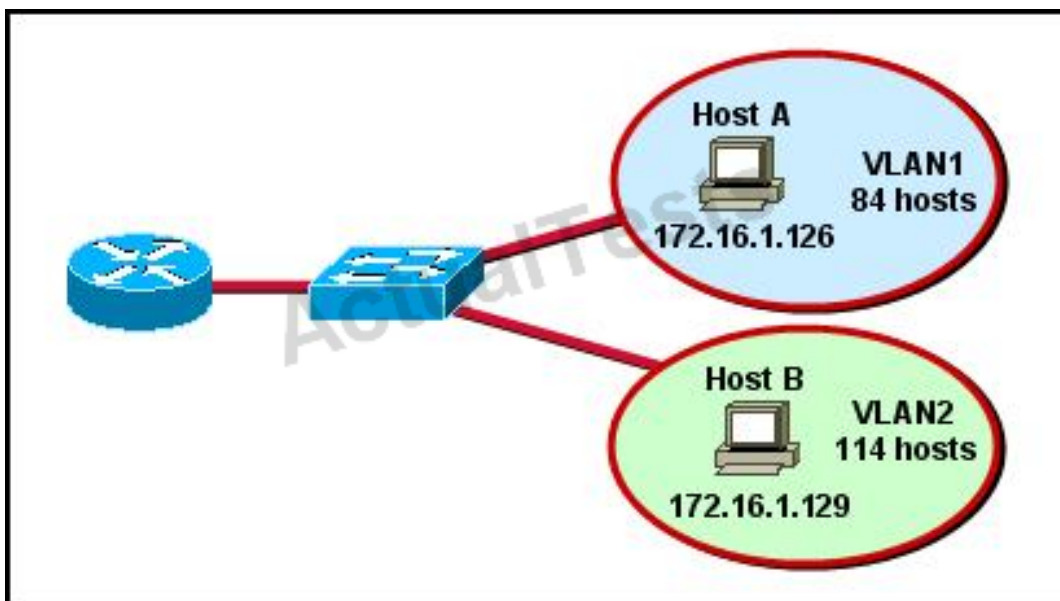
All hosts have connectivity with one another. Which statements describe the addressing scheme that is in use in the network? (Choose three.)

A. The subnet mask in use is 255.255.255.192.
B. The subnet mask in use is 255.255.255.128.
C. The IP address 172.16.1.25 can be assigned to hosts in VLAN1
D. The IP address 172.16.1.205 can be assigned to hosts in VLAN1
E. The LAN interface of the router is configured with one IP address.
F. The LAN interface of the router is configured with multiple IP addresses.

Answer: B,C,F
Explanation:
The subnet mask in use is 255.255.255.128: This is subnet mask will support up to 126 hosts, which is needed.
The IP address 172.16.1.25 can be assigned to hosts in VLAN1: The usable host range in this subnet is 172.16.1.1-172.16.1.126

The LAN interface of the router is configured with multiple IP addresses: The router will need 2 subinterfaces for the single physical interface, one with an IP address that belongs in each VLAN.

QUESTION NO: 103

Which two statements describe characteristics of IPv6 unicast addressing? (Choose two.)

A. Global addresses start with 2000::/3.
B. Link-local addresses start with FE00:/12.
C. Link-local addresses start with FF00::/10.
D. There is only one loopback address and it is ::1.
E. If a global address is assigned to an interface, then that is the only allowable address for the interface.

Answer: A,D
Explanation:
Below is the list of common kinds of IPv6 addresses:

Loopback address	::1
Link-local address	FE80::/10
Site-local address	FEC0::/10
Global address	2000::/3
Multicast address	FF00::/8

QUESTION NO: 104

The network administrator has been asked to give reasons for moving from IPv4 to IPv6. What are two valid reasons for adopting IPv6 over IPv4? (Choose two.)

A. no broadcast
B. change of source address in the IPv6 header
C. change of destination address in the IPv6 header
D. Telnet access does not require a password
E. autoconfiguration
F. NAT

Answer: A,E

Explanation:

IPv6 does not use broadcasts, and autoconfiguration is a feature of IPV6 that allows for hosts to automatically obtain an IPv6 address.

QUESTION NO: 105

An administrator must assign static IP addresses to the servers in a network. For network 192.168.20.24/29, the router is assigned the first usable host address while the sales server is given the last usable host address. Which of the following should be entered into the IP properties box for the sales server?

A. IP address: 192.168.20.14
Subnet Mask: 255.255.255.248
Default Gateway: 192.168.20.9
B. IP address: 192.168.20.254
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.20.1
C. IP address: 192.168.20.30
Subnet Mask: 255.255.255.248
Default Gateway: 192.168.20.25
D. IP address: 192.168.20.30
Subnet Mask: 255.255.255.240
Default Gateway: 192.168.20.17
E. IP address: 192.168.20.30
Subnet Mask: 255.255.255.240
Default Gateway: 192.168.20.25

Answer: C

Explanation:

For the 192.168.20.24/29 network, the usable hosts are 192.168.24.25 (router) – 192.168.24.30 (used for the sales server).

QUESTION NO: 106

Which subnet mask would be appropriate for a network address range to be subnetted for up to eight LANs, with each LAN containing 5 to 26 hosts?

A. 0.0.0.240
B. 255.255.255.252
C. 255.255.255.0
D. 255.255.255.224
E. 255.255.255.240

Answer: D
Explanation:
For a class C network, a mask of 255.255.255.224 will allow for up to 8 networks with 32 IP addresses each (30 usable).

QUESTION NO: 107

How many bits are contained in each field of an IPv6 address?

A. 24
B. 4
C. 8
D. 16

Answer: D
Explanation:
An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:). An example of an IPv6 address is 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

QUESTION NO: 108

What are three approaches that are used when migrating from an IPv4 addressing scheme to an IPv6 scheme. (Choose three.)

A. enable dual-stack routing
B. configure IPv6 directly
C. configure IPv4 tunnels between IPv6 islands
D. use proxying and translation to translate IPv6 packets into IPv4 packets
E. statically map IPv4 addresses to IPv6 addresses
F. use DHCPv6 to map IPv4 addresses to IPv6 addresses

Answer: A,C,D

Explanation:

Several methods are used terms of migration including tunneling, translators, and dual stack. Tunnels are used to carry one protocol inside another, while translators simply translate IPv6 packets into IPv4 packets. Dual stack uses a combination of both native IPv4 and IPv6. With dual stack, devices are able to run IPv4 and IPv6 together and if IPv6 communication is possible that is the preferred protocol. Hosts can simultaneously reach IPv4 and IPv6 content.

QUESTION NO: 109

Refer to the exhibit.
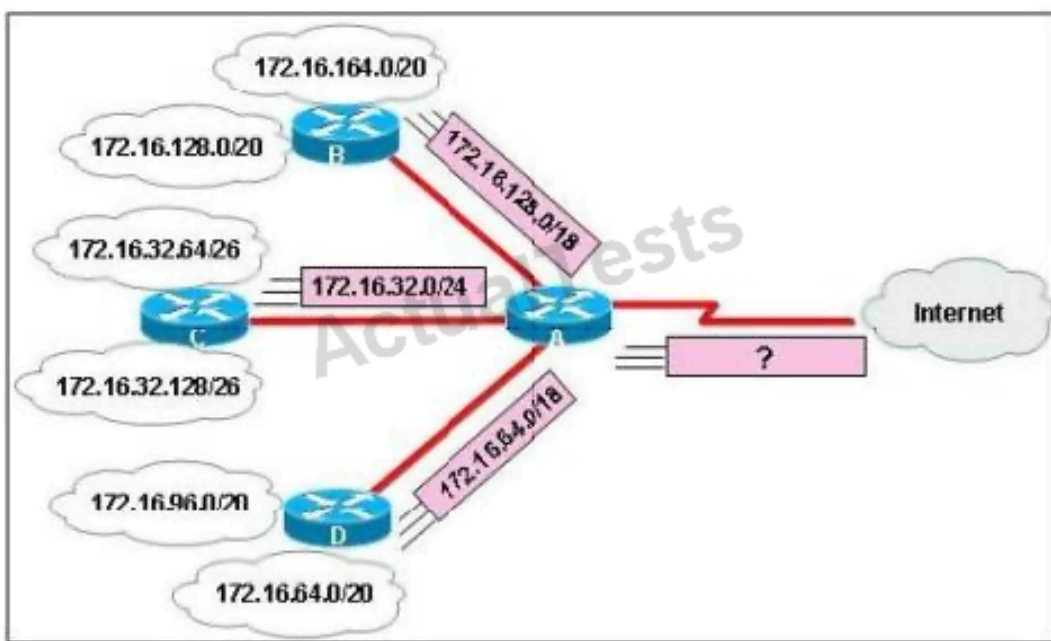
In this VLSM addressing scheme, what summary address would be sent from router A?

A. 172.16.0.0 /16
B. 172.16.0.0 /20
C. 172.16.0.0 /24
D. 172.32.0.0 /16
E. 172.32.0.0 /17
F. 172.64.0.0 /16

Answer: A

Explanation: Explanation

Router A receives 3 subnets: 172.16.64.0/18, 172.16.32.0/24 and 172.16.128.0/18.

All these 3 subnets have the same form of 172.16.x.x so our summarized subnet must be also in that form -> Only A, B or .

The smallest subnet mask of these 3 subnets is /18 so our summarized subnet must also have its subnet mask equal or smaller than /18.

-> Only answer A has these 2 conditions -> .

QUESTION NO: 110

How is an EUI-64 format interface ID created from a 48-bit MAC address?

A. by appending 0xFF to the MAC address
B. by prefixing the MAC address with 0xFFEE
C. by prefixing the MAC address with 0xFF and appending 0xFF to it
D. by inserting 0xFFFE between the upper three bytes and the lower three bytes of the MAC address
E. by prefixing the MAC address with 0xF and inserting 0xF after each of its first three bytes

Answer: D
Explanation:
The modified EUI-64 format interface identifier is derived from the 48-bit link-layer (MAC) address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower three bytes (serial number) of the link layer address.

QUESTION NO: 111

Refer to the exhibit.
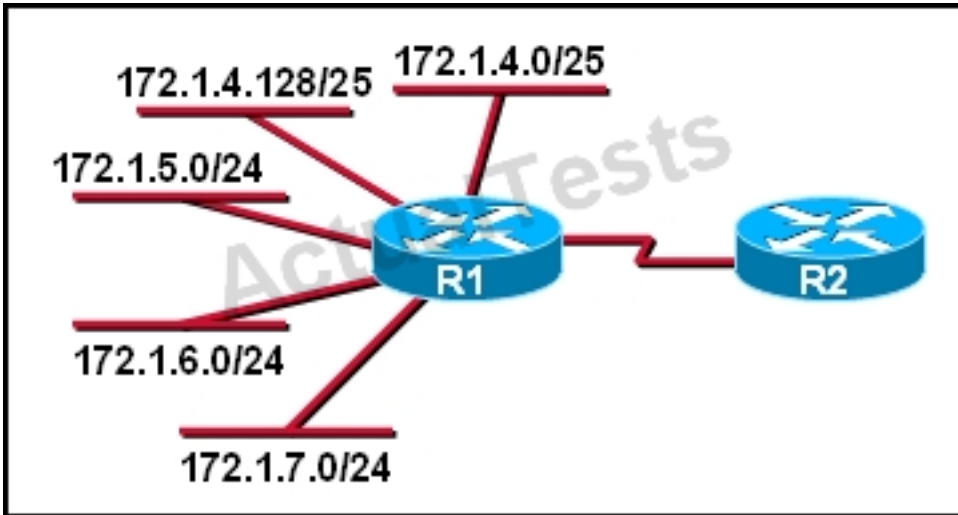
What is the most efficient summarization that R1 can use to advertise its networks to R2?

A. 172.1.0.0/22
B. 172.1.0.0/21
C. 172.1.4.0/22
D. 172.1.4.0/24
172.1.5.0/24
172.1.6.0/24
172.1.7.0/24
E. 172.1.4.0/25
172.1.4.128/25
172.1.5.0/24
172.1.6.0/24
172.1.7.0/24

Answer: C
Explanation:
The 172.1.4.0/22 subnet encompasses all routes from the IP range 172.1.4.0 – 172.1.7.255.

QUESTION NO: 112

Which option is a valid IPv6 address?

A. 2001:0000:130F::099a::12a
B. 2002:7654:A1AD:61:81AF:CCC1
C. FEC0:ABCD:WXYZ:0067::2A4
D. 2004:1:25A4:886F::1

Answer: D

Explanation:

An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:). An example of an IPv6 address is 2001:0db8:85a3:0000:0000:8a2e:0370:7334. The leading 0's in a group can be collapsed using ::, but this can only be done once in an IP address.

QUESTION NO: 113

Which three are characteristics of an IPv6 anycast address? (Choose three.)

A. one-to-many communication model
B. one-to-nearest communication model
C. any-to-many communication model
D. a unique IPv6 address for each device in the group
E. the same address for multiple devices in the group
F. delivery of packets to the group interface that is closest to the sending device

Answer: B,E,F

Explanation:

A new address type made specifically for IPv6 is called the Anycast Address. These IPv6 addresses are global addresses, these addresses can be assigned to more than one interface unlike an IPv6 unicast address. Anycast is designed to send a packet to the nearest interface that is apart of that anycast group.

The sender creates a packet and forwards the packet to the anycast address as the destination address which goes to the nearest router. The nearest router or interface is found by using the metric of a routing protocol currently running on the network. However in a LAN setting the nearest interface is found depending on the order the neighbors were learned. The anycast packet in a LAN setting forwards the packet to the neighbor it learned about first.

QUESTION NO: 114

A national retail chain needs to design an IP addressing scheme to support a nationwide network. The company needs a minimum of 300 sub-networks and a maximum of 50 host addresses per subnet. Working with only one Class B address, which of the following subnet masks will support an appropriate addressing scheme? (Choose two.)

A. 255.255.255.0
B. 255.255.255.128
C. 255.255.252.0
D. 255.255.255.224
**E.** 255.255.255.192
F. 255.255.248.0

Answer: B,E

Explanation:

Subnetting is used to break the network into smaller more efficient subnets to prevent excessive rates of Ethernet packet collision in a large network. Such subnets can be arranged hierarchically, with the organization's network address space (see also Autonomous System) partitioned into a tree-like structure. Routers are used to manage traffic and constitute borders between subnets.
A routing prefix is the sequence of leading bits of an IP address that precede the portion of the address used as host identifier. In IPv4 networks, the routing prefix is often expressed as a "subnet mask", which is a bit mask covering the number of bits used in the prefix. An IPv4 subnet mask is frequently expressed in quad-dotted decimal representation, e.g., 255.255.255.0 is the subnet mask for the 192.168.1.0 network with a 24-bit routing prefix (192.168.1.0/24).

QUESTION NO: 115

Refer to the exhibit.
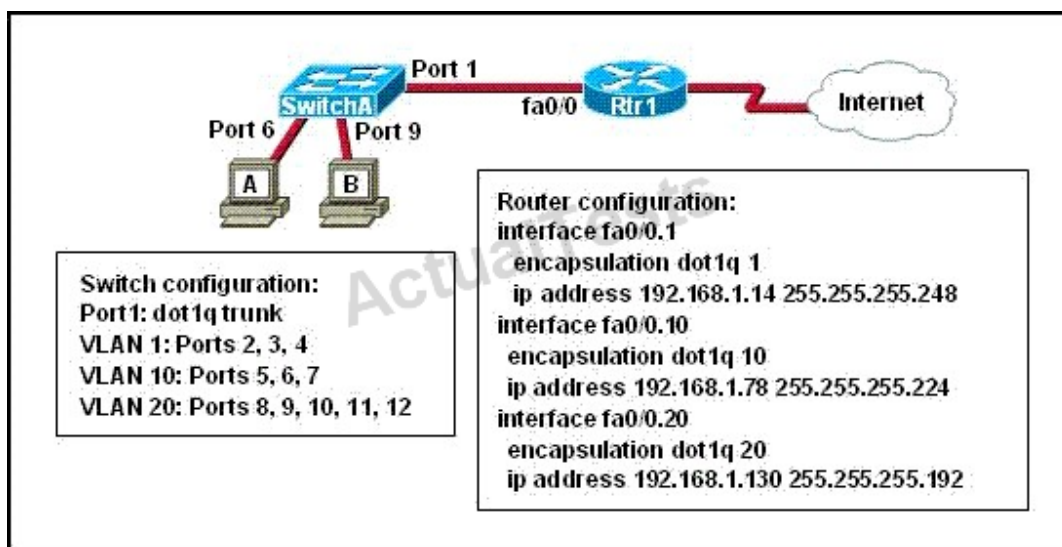
A network administrator is adding two new hosts to SwitchA. Which three values could be used for the configuration of these hosts? (Choose three.)

A. host A IP address: 192.168.1.79
B. host A IP address: 192.168.1.64
C. host A default gateway: 192.168.1.78
D. host B IP address: 192.168.1.128
E. host B default gateway: 192.168.1.129
F. host B IP address: 192.168.1.190

Answer: A,C,F
Explanation:

QUESTION NO: 116

Which IPv6 address is the all-router multicast group?

A. FF02::1
B. FF02::2
C. FF02::3
D. FF02::4

Answer: B
Explanation:
Well-known IPv6 multicast addresses:
Address
Description
ff02::1
All nodes on the local network segment
ff02::2
All routers on the local network segment

QUESTION NO: 117

Refer to the exhibit.
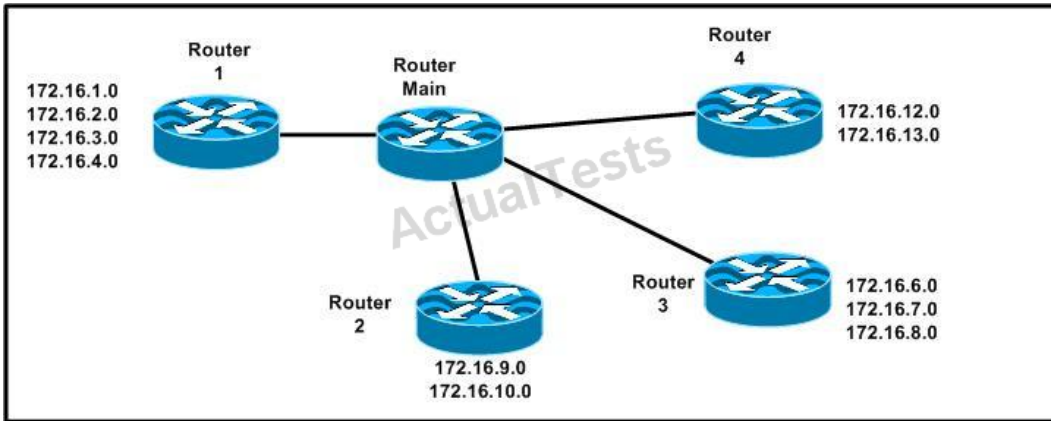
Which address range efficiently summarizes the routing table of the addresses for router Main?

A. 172.16.0.0./21
B. 172.16.0.0./20
C. 172.16.0.0./16
D. 172.16.0.0/18

Answer: B

Explanation:

The 172.16.0.0./20 network is the best option as it includes all networks from 172.16.0.0 –
172.16.16.0 and does it more efficiently than the /16 and /18 subnets. The /21 subnet will not
include all the other subnets in this one single summarized address.

QUESTION NO: 118

Which IPv6 address is valid?

A. 2001:0db8:0000:130F:0000:0000:08GC:140B
B. 2001:0db8:0:130H::87C:140B
C. 2031::130F::9C0:876A:130B
D. 2031:0:130F::9C0:876A:130B

Answer: D

Explanation:

An IPv6 address is represented as eight groups of four hexadecimal digits, each group
representing 16 bits (two octets). The groups are separated by colons (:). An example of an IPv6
address is 2001:0db8:85a3:0000:0000:8a2e:0370:7334. The leading 0's in a group can be
collapsed using ::, but this can only be done once in an IP address.

QUESTION NO: 119

Which command can you use to manually assign a static IPv6 address to a router interface?

A. ipv6 autoconfig 2001:db8:2222:7272::72/64
B. ipv6 address 2001:db8:2222:7272::72/64
C. ipv6 address PREFIX_1 ::1/64
D. ipv6 autoconfig

Answer: B
Explanation:
To assign an IPv6 address to an interface, use the "ipv6 address" command and specify the IP address you wish to use.

QUESTION NO: 120

Which of these represents an IPv6 link-local address?

A. FE80::380e:611a:e14f:3d69
B. FE81::280f:512b:e14f:3d69
C. FEFE:0345:5f1b::e14d:3d69
D. FE08::280e:611:a:f14f:3d69

Answer: A
Explanation:
In the Internet Protocol Version 6 (IPv6), the address block fe80::/10 has been reserved for link-local unicast addressing. The actual link local addresses are assigned with the prefix fe80::/64. They may be assigned by automatic (stateless) or stateful (e.g. manual) mechanisms.

QUESTION NO: 121

The network administrator is asked to configure 113 point-to-point links. Which IP addressing scheme defines the address range and subnet mask that meet the requirement and waste the fewest subnet and host addresses?

A. 10.10.0.0/16 subnetted with mask 255.255.255.252
B. 10.10.0.0/18 subnetted with mask 255.255.255.252
C. 10.10.1.0/24 subnetted with mask 255.255.255.252
D. 10.10.0.0/23 subnetted with mask 255.255.255.252
E. 10.10.1.0/25 subnetted with mask 255.255.255.252

Answer: D

Explanation: Explanation

We need 113 point-to-point links which equal to 113 sub-networks < 128 so we need to borrow 7 bits (because 2^7 = 128).

The network used for point-to-point connection should be /30.

So our initial network should be 30 – 7 = 23.

So 10.10.0.0/23 is the correct answer.

You can understand it more clearly when writing it in binary form:

/23 = 1111 1111.1111 1110.0000 0000

/30 = 1111 1111.1111 1111.1111 1100 (borrow 7 bits)

Topic 4, IP Routing Technologies

QUESTION NO: 122 DRAG DROP

Drag each definition on the left to the matching term on the right.		
the number of point-to-point links in a transmission path		cost
the data capacity of a link		load
the amount of time required to move a packet from source to destination		bandwidth
the amount of activity on a network resource		hop count
usually refers to the bit error rate of each network link		reliability
a configurable value based by default on the bandwidth of the interface		delay

Answer:

Drag each definition on the left to the matching term on the right.

the number of point-to-point links in a transmission path	a configurable value based by default on the bandwidth of the interface
the data capacity of a link	the amount of activity on a network resource
the amount of time required to move a packet from source to destination	the data capacity of a link
the amount of activity on a network resource	the number of point-to-point links in a transmission path
usually refers to the bit error rate of each network link	usually refers to the bit error rate of each network link
a configurable value based by default on the bandwidth of the interface	the amount of time required to move a packet from source to destination

Explanation:

a configurable value based by default on the bandwidth of the interface

the amount of activity on a network resource

the data capacity of a link

the number of point-to-point links in a transmission path

usually refers to the bit error rate of each network link

the amount of time required to move a packet from source to destination

QUESTION NO: 123 DRAG DROP

Drag the Cisco default administrative distance to the appropriate routing protocol or route. (Not all options are used.)

0	RIP
1	OSPF
20	static route referencing IP address of next hop
90	internal EIGRP route
100	directly connected network
110	
120	
130	

Answer:

Drag the Cisco default administrative distance to the appropriate routing protocol or route. (Not all options are used.)

0	120
1	110
20	1
90	90
100	0
110	
120	
130	

Explanation:

120
110
1
90
0

QUESTION NO: 124 DRAG DROP

Routing has been configured on the local router with these commands:
Local(config)# **ip route 0.0.0.0 0.0.0.0 192.168.1.1**
Local(config)# **ip route 10.1.0.0 255.255.255.0 192.168.2.2**
Local(config)# **ip route 10.1.0.0 255.255.0.0 192.168.3.3**
Drag each destination IP address on the left to its correct next hop address on the right.

10.1.1.10		Next hop 192.168.1.1
10.1.0.14		
10.2.1.3		
10.1.4.6		Next hop 192.168.2.2
10.1.0.123		
10.6.8.4		
		Next hop 192.168.3.3

Answer:

Routing has been configured on the local router with these commands:
Local(config)# **ip route 0.0.0.0 0.0.0.0 192.168.1.1**
Local(config)# **ip route 10.1.0.0 255.255.255.0 192.168.2.2**
Local(config)# **ip route 10.1.0.0 255.255.0.0 192.168.3.3**
Drag each destination IP address on the left to its correct next hop address on the right.

10.1.1.10		Next hop 192.168.1.1
10.1.0.14		10.2.1.3
10.2.1.3		10.6.8.4
10.1.4.6		Next hop 192.168.2.2
10.1.0.123		10.1.0.14
10.6.8.4		10.1.0.123
		Next hop 192.168.3.3
		10.1.1.10
		10.1.4.6

Explanation:

Next hop 192.168.1.1
10.2.1.3
10.6.8.4

Next hop 192.168.2.2
10.1.0.14
10.1.0.123

Next hop 192.168.3.3
10.1.1.10
10.1.4.6

Explanation

If we have many entries matching for next hop ip address then the router will choose the one with most specific path to send the packet. This is called the "longest match" rule, the route with the most bits in the mask set to "1 will be chosen to route packet.

QUESTION NO: 125

Which parameter or parameters are used to calculate OSPF cost in Cisco routers?

A. Bandwidth
B. Bandwidth and Delay
C. Bandwidth, Delay, and MTU
D. Bandwidth, MTU, Reliability, Delay, and Load

Answer: A
Explanation: The well-known formula to calculate OSPF cost is
Cost = 108 / Bandwidth

QUESTION NO: 126

Why do large OSPF networks use a hierarchical design? (Choose three.)

A. to decrease latency by increasing bandwidth
B. to reduce routing overhead
C. to speed up convergence
D. to confine network instability to single areas of the network
E. to reduce the complexity of router configuration
F. to lower costs by replacing routers with distribution layer switches

Answer: B,C,D

Explanation:

OSPF implements a two-tier hierarchical routing model that uses a core or backbone tier known as area zero (0). Attached to that backbone via area border routers (ABRs) are a number of secondary tier areas. The hierarchical approach is used to achieve the following:

•

Rapid convergence because of link and/or switch failures

•

Deterministic traffic recovery

•

Scalable and manageable routing hierarchy, reduced routing overhead.

QUESTION NO: 127

Which command encrypts all plaintext passwords?

A. Router# service password-encryption
B. Router(config)# password-encryption
C. Router(config)# service password-encryption
D. Router# password-encryption

Answer: C

Explanation:

Command

The "service password-encryption" command allows you to encrypt all passwords on your router so they can not be easily guessed from your running-config. This command uses a very weak encryption because the router has to be very quickly decode the passwords for its operation.

It is meant to prevent someone from looking over your shoulder and seeing the password, that is all. This is configured in global configuration mode.

QUESTION NO: 128

Which two are advantages of static routing when compared to dynamic routing? (Choose two.)

A. Configuration complexity decreases as network size increases.
B. Security increases because only the network administrator may change the routing table.
C. Route summarization is computed automatically by the router.
D. Routing tables adapt automatically to topology changes.
E. An efficient algorithm is used to build routing tables, using automatic updates.
F. Routing updates are automatically sent to neighbors.
G. Routing traffic load is reduced when used in stub network links.

Answer: B,G
Explanation:
Since static routing is a manual process, it can be argued that it is more secure (and more prone to human errors) since the network administrator will need to make changes to the routing table directly. Also, in stub networks where there is only a single uplink connection, the load is reduced as stub routers just need a single static default route, instead of many routes that all have the same next hop IP address.

QUESTION NO: 129

A network administrator needs to allow only one Telnet connection to a router. For anyone viewing the configuration and issuing the show run command, the password for Telnet access should be encrypted. Which set of commands will accomplish this task?

A. service password-encryption
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 4
login
password cisco
access-class 1
B. enable password secret
line vty 0
login

password cisco
C. service password-encryption
line vty 1
login
password cisco
D. service password-encryption
line vty 0 4
login
password cisco

Answer: C
Explanation:
Only one VTY connection is allowed which is exactly what's requested.
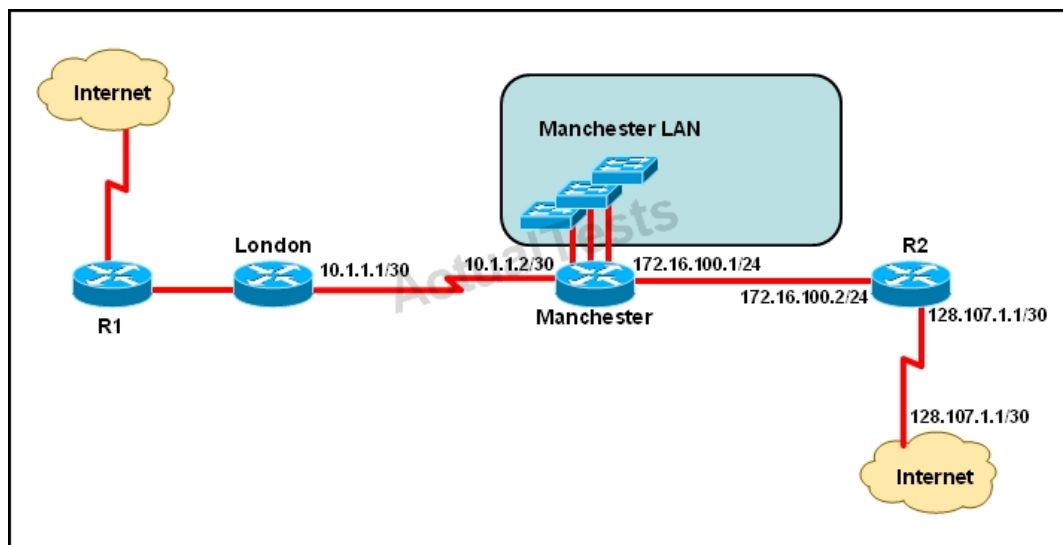Incorrect answer: command.
line vty0 4
would enable all 5 vty connections.

QUESTION NO: 130

Refer to the exhibit.

The speed of all serial links is E1 and the speed of all Ethernet links is 100 Mb/s. A static route will be established on the Manchester router to direct traffic toward the Internet over the most direct path available. What configuration on the Manchester router will establish a route toward the Internet for traffic that originates from workstations on the Manchester LAN?

A. ip route 0.0.0.0 255.255.255.0 172.16.100.2

B. ip route 0.0.0.0 0.0.0.0 128.107.1.1
C. ip route 0.0.0.0 255.255.255.252 128.107.1.1
D. ip route 0.0.0.0 0.0.0.0 172.16.100.1
E. ip route 0.0.0.0 0.0.0.0 172.16.100.2
F. ip route 0.0.0.0 255.255.255.255 172.16.100.2

Answer: E
Explanation:
We use default routing to send packets with a remote destination network not in the routing table to the next-hop router. You should generally only use default routing on stub networks—those with only one exit path out of the network.

According to exhibit, all traffic towards Internet that originates from workstations should forward to Router R1.

Syntax for default route is:
ip route <Remote_Network> <Netmask> <Next_Hop_Address>.

QUESTION NO: 131

Refer to the exhibit.
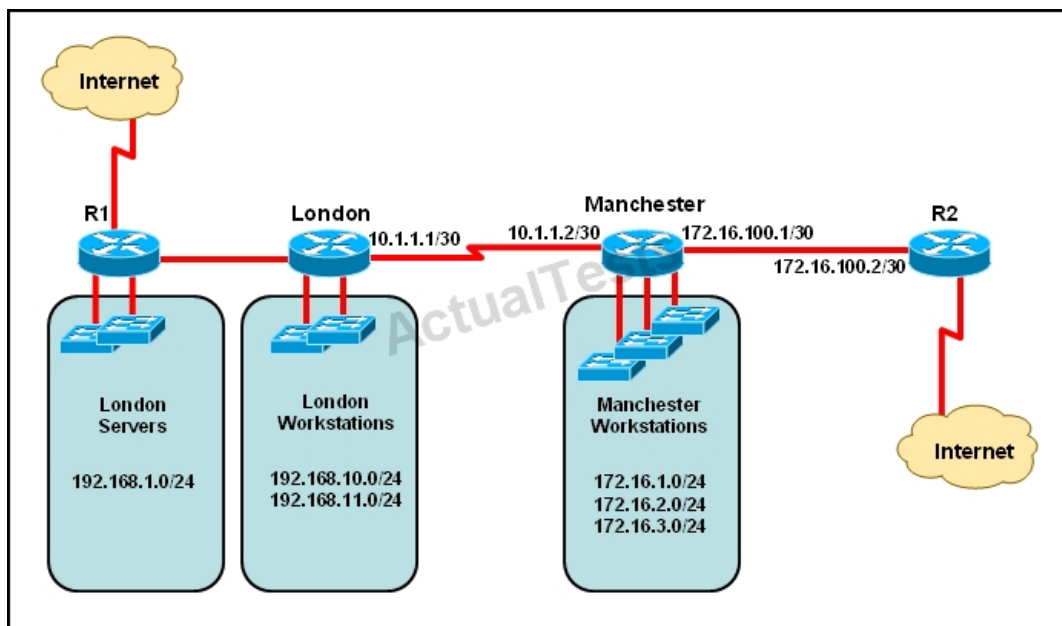
The network administrator must establish a route by which London workstations can forward traffic to the Manchester workstations. What is the simplest way to accomplish this?

A. Configure a dynamic routing protocol on London to advertise all routes to Manchester.
B. Configure a dynamic routing protocol on London to advertise summarized routes to Manchester.
C. Configure a dynamic routing protocol on Manchester to advertise a default route to the London router.
D. Configure a static default route on London with a next hop of 10.1.1.1.
E. Configure a static route on London to direct all traffic destined for 172.16.0.0/22 to 10.1.1.2.
F. Configure Manchester to advertise a static default route to London.

Answer: E

Explanation:

This static route will allow for communication to the Manchester workstations and it is better to use this more specific route than a default route as traffic destined to the Internet will then not go out the London Internet connection.

QUESTION NO: 132

Refer to the exhibit.
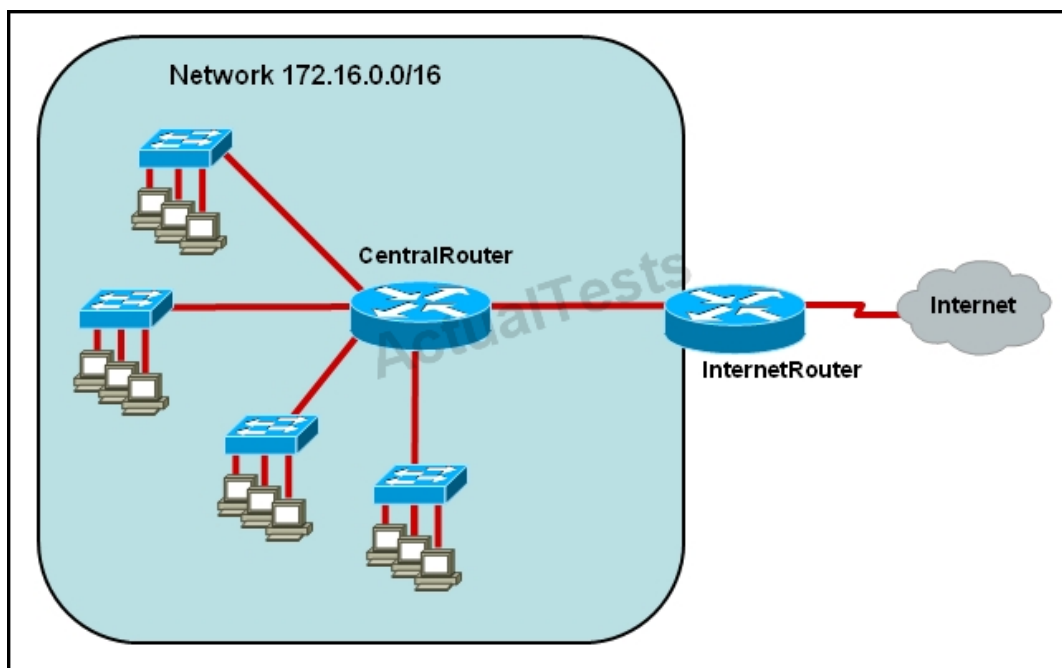
The network administrator requires easy configuration options and minimal routing protocol traffic. What two options provide adequate routing table information for traffic that passes between the two routers and satisfy the requests of the network administrator? (Choose two.)

A. a dynamic routing protocol on InternetRouter to advertise all routes to CentralRouter.

B. a dynamic routing protocol on InternetRouter to advertise summarized routes to CentralRouter.
C. a static route on InternetRouter to direct traffic that is destined for 172.16.0.0/16 to CentralRouter.
D. a dynamic routing protocol on CentralRouter to advertise all routes to InternetRouter.
E. a dynamic routing protocol on CentralRouter to advertise summarized routes to InternetRouter.
F. a static, default route on CentralRouter that directs traffic to InternetRouter.

Answer: C,F

Explanation:

The use of static routes will provide the necessary information for connectivity while producing no routing traffic overhead.

QUESTION NO: 133

What is the effect of using the service password-encryption command?

A. Only the enable password will be encrypted.
B. Only the enable secret password will be encrypted.
C. Only passwords configured after the command has been entered will be encrypted.
D. It will encrypt the secret password and remove the enable secret password from the configuration.
E. It will encrypt all current and future passwords.

Answer: E

Explanation:

Enable vty, console, AUX passwords are configured on the Cisco device. Use the show run command to show most passwords in clear text. If the service password-encryption is used, all the passwords are encrypted. As a result, the security of device access is improved.

QUESTION NO: 134

Refer to the exhibit.

```
line vty 0 4
 password 7 030752180500
 login
 transport input ssh
```

What is the effect of the configuration that is shown?

A. It configures SSH globally for all logins.
B. It tells the router or switch to try to establish an SSh connection first and if that fails to use Telnet.
C. It configures the virtual terminal lines with the password 030752180500.
D. It configures a Cisco network device to use the SSH protocol on incoming communications via the virtual terminal ports.
E. It allows seven failed login attempts before the VTY lines are temporarily shutdown.

Answer: D

Explanation:

Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. Communication between the client and server is encrypted in both SSH version 1 and SSH version 2. If you want to prevent non-SSH connections, add the "transport input ssh" command under the lines to limit the router to SSH connections only. Straight (non-SSH) Telnets are refused.

Reference: www.cisco.com/warp/public/707/ssh.shtml

QUESTION NO: 135

Refer to the exhibit.

```
Router# show interface s0/0/0
Serial 0/0/0 is administratively down, line protocol is down
```

What is the reason that the interface status is "administratively down, line protocol down"?

A. There is no encapsulation type configured.

B. There is a mismatch in encapsulation types.
C. The interface is not receiving any keepalives.
D. The interface has been configured with the shutdown command.
E. The interface needs to be configured as a DTE device.
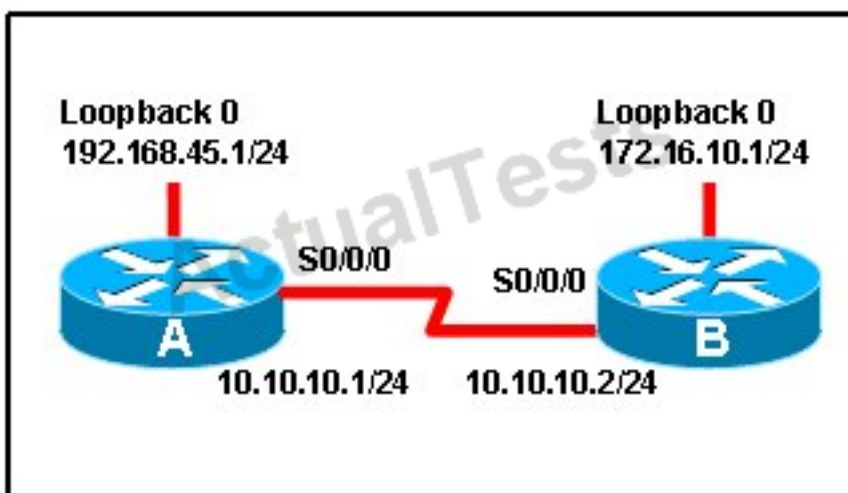**F.** The wrong type of cable is connected to the interface.

Answer: D
Explanation:

Interfaces can be enabled or disabled with shutdown/no shutdown command. If you interface is down, it will display administratively down status. You can bring up an interface having administratively down interface using no shutdown command.

QUESTION NO: 136

Refer to the exhibit.

When running OSPF, what would cause router A not to form an adjacency with router B?

A. The loopback addresses are on different subnets.
B. The values of the dead timers on the routers are different.
C. Route summarization is enabled on both routers.
D. The process identifier on router A is different than the process identifier on router B.

Answer: B
Explanation: Explanation
To form an adjacency (become neighbor), router A & B must have the same Hello interval, Dead interval and AREA numbers

QUESTION NO: 137

A router has learned three possible routes that could be used to reach a destination network. One route is from EIGRP and has a composite metric of 20514560. Another route is from OSPF with a metric of 782. The last is from RIPv2 and has a metric of 4. Which route or routes will the router install in the routing table?

A. the OSPF route
B. the EIGRP route
C. the RIPv2 route
D. all three routes
E. the OSPF and RIPv2 routes

Answer: B
Explanation: Explanation

When one route is advertised by more than one routing protocol, the router will choose to use the routing protocol which has lowest Administrative Distance. The Administrative Distances of popular routing protocols are listed below:

Route Source	Administrative Distance
Directly Connected	0
Static	1
EIGRP	90
EIGRP Summary route	5
OSPF	110
RIP	120

QUESTION NO: 138

Refer to the exhibit.
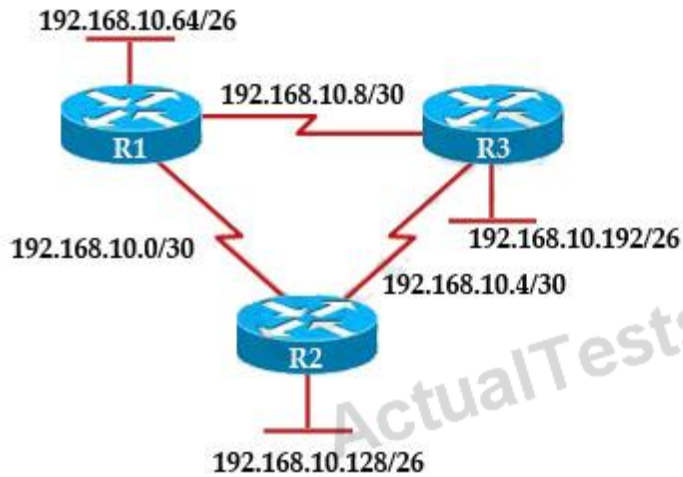
192.168.10.64/26

192.168.10.8/30

R1

R3

192.168.10.0/30

192.168.10.192/26

192.168.10.4/30

R2

192.168.10.128/26

```
R3# show ip route
Gateway of last resort is not set
192 168.10.0/24 is variably subnetted, 6 subnets, 2 masks
D 192.168. 10.64/26 [90/2195456] via 192.168.10.9, 00:03:31, Serial0/0
D 192.168.10.0/30 [90/2681856] via 192.168.10.9, 00:03:31, Serial0/0
C 192.168.10.4/30 is directly connected, Serial 0/1
C 192.168.10.8/30 is directly connected, Serial 0/0
C 192.168.10.192/26 is directly connected, FastEthernet0/0
D 192.168.10.128/26 [90/2195456] via 192.168.10.5,00:03 31, Serial 0/1
```

The company uses EIGRP as the routing protocol. What path will packets take from a host on the 192.168.10.192/26 network to a host on the LAN attached to router R1?

A. The path of the packets will be R3 to R2 to R1.
B. The path of the packets will be R3 to R1 to R2.
C. The path of the packets will be both R3 to R2 to R1 AND R3 to R1.
D. The path of the packets will be R3 to R1.

Answer: D

Explanation: Explanation

Host on the LAN attached to router R1 belongs to 192.168.10.64/26 subnet. From the output of the routing table of R3 we learn this network can be reach via 192.168.10.9, which is an IP address in 192.168.10.8/30 network (the network between R1 & R3) -> packets destined for 192.168.10.64 will be routed from R3 -> R1 -> LAN on R1.

QUESTION NO: 139

A network administrator is troubleshooting an EIGRP problem on a router and needs to confirm the IP addresses of the devices with which the router has established adjacency. The retransmit interval and the queue counts for the adjacent routers also need to be checked. What command

will display the required information?

A. Router# show ip eigrp adjacency
B. Router# show ip eigrp topology
C. Router# show ip eigrp interfaces
D. Router# show ip eigrp neighbors

Answer: D

Explanation: Explanation

Below is an example of the show ip eigrp neighbors command. The retransmit interval (Smooth Round Trip Timer – SRTT) and the queue counts (Q count, which shows the number of queued EIGRP packets) for the adjacent routers are listed:

```
Router1# show ip eigrp neighbors
Address       Interface  Holdtime  Uptime   Q      Seq   SRTT  RTO
                         (secs)    (h:m:s)  Count  Num   (ms)  (ms)
192.168.1.2   Se0        13        01:10:20 106    636   0     30
```

QUESTION NO: 140

Refer to the graphic.
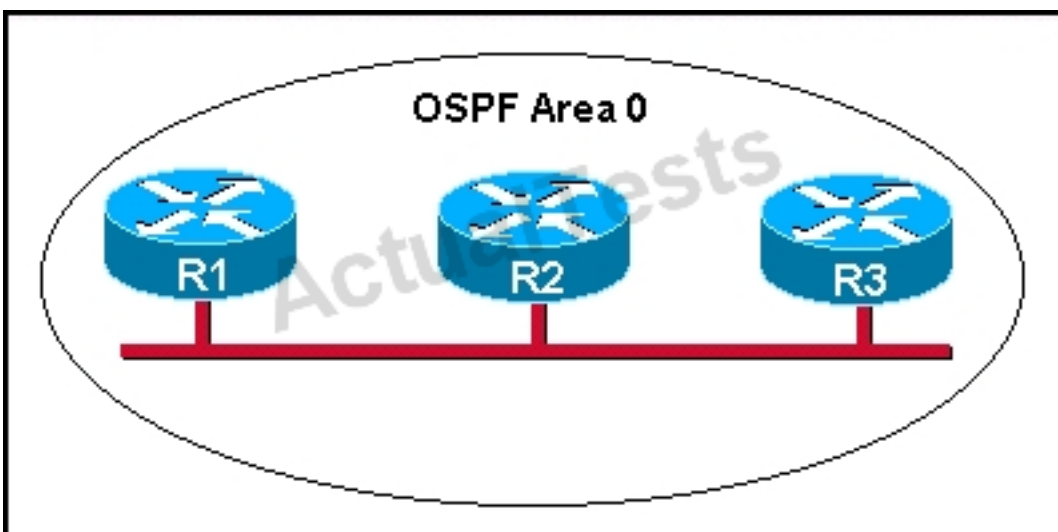
R1 is unable to establish an OSPF neighbor relationship with R3. What are possible reasons for this problem? (Choose two.)

A. All of the routers need to be configured for backbone Area 1.

B. R1 and R2 are the DR and BDR, so OSPF will not establish neighbor adjacency with R3.

C. A static route has been configured from R1 to R3 and prevents the neighbor adjacency from being established.

D. The hello and dead interval timers are not set to the same values on R1 and R3.

E. EIGRP is also configured on these routers with a lower administrative distance.

F. R1 and R3 are configured in different areas.

Answer: D,F

Explanation:

This question is to examine the conditions for OSPF to create neighborhood.

So as to make the two routers become neighbors, each router must be matched with the following items:

1. The area ID and its types;

2. Hello and failure time interval timer;

3. OSPF Password (Optional);

QUESTION NO: 141

What is a global command?

A. a command that is set once and affects the entire router

B. a command that is implemented in all foreign and domestic IOS versions

C. a command that is universal in application and supports all protocols

D. a command that is available in every release of IOS, regardless of the version or deployment status

E. a command that can be entered in any configuration mode

Answer: A

Explanation:

When you enter global configuration mode and enter a command, it is applied to the running configuration file that is currently running in ram. The configuration of a global command affects the entire router. An example of a global command is one used for the hostname of the router.

QUESTION NO: 142

Refer to the exhibit.
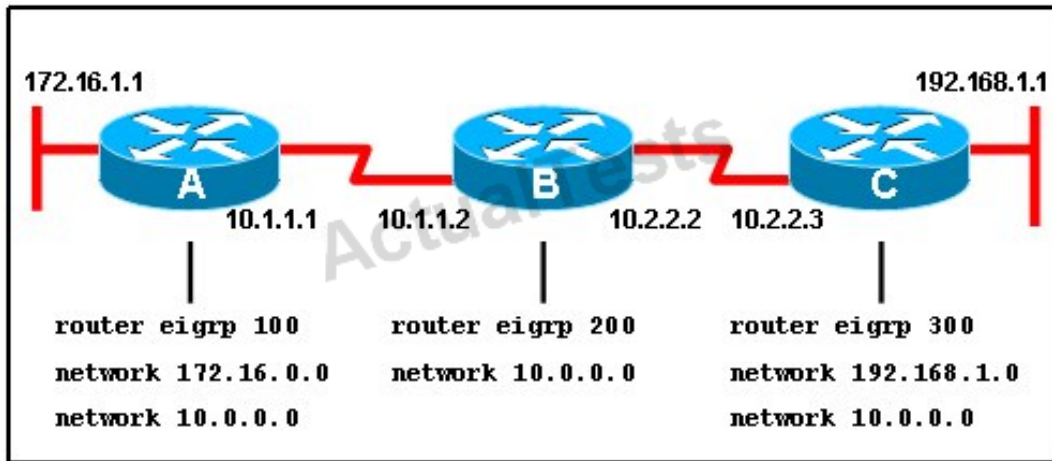
When running EIGRP, what is required for RouterA to exchange routing updates with RouterC?

A. AS numbers must be changed to match on all the routers
B. Loopback interfaces must be configured so a DR is elected
C. The no auto-summary command is needed on Router A and Router C
D. Router B needs to have two network statements, one for each connected network

Answer: A
Explanation:
This question is to examine the understanding of the interaction between EIGRP routers.
The following information must be matched so as to create neighborhood.
EIGRP routers to establish, must match the following information:
1. AS Number;
2. K value.

QUESTION NO: 143

A Cisco router is booting and has just completed the POST process. It is now ready to find and load an IOS image. What function does the router perform next?

A. It checks the configuration register.
B. It attempts to boot from a TFTP server.
C. It loads the first image file in flash memory.
D. It inspects the configuration file in NVRAM for boot instructions.

Answer: A
Explanation:
Default (normal) Boot Sequence Power on Router - Router does POST - Bootstrap starts IOS
load - Check configuration register to see what mode the router should boot up in (usually 0x2102

to read startup-config in NVRAM / or 0x2142 to start in "setup-mode") - check the startup-config file in NVRAM for boot-system commands - load IOS from Flash.

QUESTION NO: 144

Refer to the exhibit.

```
Router# show interfaces ethernet 0
Ethernet0 is up, line protocol is up
Hardware is QUICC Ethernet, address is 00c0.ab73.dead (bia 0010.7bcc.7321)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
<output omitted>
```

What is the meaning of the output MTU 1500 bytes?

A. The maximum number of bytes that can traverse this interface per second is 1500.
B. The minimum segment size that can traverse this interface is 1500 bytes.
C. The maximum segment size that can traverse this interface is 1500 bytes.
D. The minimum packet size that can traverse this interface is 1500 bytes.
E. The maximum packet size that can traverse this interface is 1500 bytes.
F. The maximum frame size that can traverse this interface is 1500 bytes.

Answer: E
Explanation: Explanation
The Maximum Transmission Unit (MTU) defines the maximum Layer 3 packet (in bytes) that the layer can pass onwards.

QUESTION NO: 145

On a corporate network, hosts on the same VLAN can communicate with each other, but they are unable to communicate with hosts on different VLANs. What is needed to allow communication between the VLANs?

A. a router with subinterfaces configured on the physical interface that is connected to the switch
B. a router with an IP address on the physical interface connected to the switch

C. a switch with an access link that is configured between the switches
D. a switch with a trunk link that is configured between the switches

Answer: A
Explanation:

Different VLANs can't communicate with each other , they can communicate with the help of Layer3 router. Hence , it is needed to connect a router to a switch , then make the sub-interface on the router to connect to the switch, establishing Trunking links to achieve communications of devices which belong to different VLANs.

When using VLANs in networks that have multiple interconnected switches, you need to use VLAN trunking between the switches. With VLAN trunking, the switches tag each frame sent between switches so that the receiving switch knows to what VLAN the frame belongs. End user devices connect to switch ports that provide simple connectivity to a single VLAN each. The attached devices are unaware of any VLAN structure.

By default, only hosts that are members of the same VLAN can communicate. To change this and allow inter-VLAN communication, you need a router or a layer 3 switch.

Here is the example of configuring the router for inter-vlan communication
RouterA(config)#int f0/0.1
RouterA(config-subif)#encapsulation ?
dot1Q IEEE 802.1Q Virtual LAN
RouterA(config-subif)#encapsulation dot1Q or isl VLAN ID
RouterA(config-subif)# ip address x.x.x.x y.y.y.y

QUESTION NO: 146

Which command displays CPU utilization?

A. show protocols
B. show process
C. show system
D. show version

Answer: B
Explanation: Explanation
The "show process" (in fact, the full command is "show processes") command gives us lots of information about each process but in fact it is not easy to read. Below shows the output of this command (some next pages are omitted)

```
Router#show process
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID QTy       PC Runtime (ms)   Invoked   uSecs    Stacks TTY Process
   1 Cwe 6048DB4C         0          1        0 5604/6000   0 Chunk Manager
   2 Csp 604BCD68         0         15        0 2632/3000   0 Load Meter
   3 M*         0        28         20 140010724/12000   0 Exec
   5 Mwe 61496B84         0          1        023460/24000   0 EDDRI_MAIN
   6 Lst 6049C5E4        88         10     8800 5632/6000   0 Check heaps
   7 Cwe 604A2754         0          1        0 5592/6000   0 Pool Manager
   8 Mst 603D219C         0          2        0 5580/6000   0 Timers
   9 Mwe 600245DC         0          2        0 5584/6000   0 Serial Backgroun
  10 Mwe 602D6BB4         0          2        0 5680/6000   0 IPC Dynamic Cach
  11 Mwe 602CEF94         0          1        0 5636/6000   0 IPC Zone Manager
  12 Mwe 602CECF4         0         75        0 5708/6000   0 IPC Periodic Tim
  13 Mwe 602CEC3C         4         77       51 5624/6000   0 IPC Deferred Por
  14 Mwe 602CEDA8         4          1     4000 5596/6000   0 IPC Seat Manager
  15 Mwe 603A4900         0          2        0 5576/6000   0 AAA high-capacit
  16 Mwe 60547C2C         0          1        011604/12000   0 OIR Handler
  17 Msi 60572C2C         0          4        0 5600/6000   0 Environmental mo
  19 Mwe 6057B190         4          5      800 5588/6000   0 ARP Input
  20 Mwe 6079D838         0         19        0 5660/6000   0 HC Counter Timer
  21 Mwe 6081D4A0         0          2        0 5576/6000   0 DDR Timers
  22 Lwe 60A9AE28         0          3        0 5532/6000   0 Entity MIB API
  23 Mwe 613B56A0         0          2        0 5584/6000   0 ATM Idle Timer
```

A more friendly way to check the CPU utilization is the command "show processes cpu history", in which the total CPU usage on the router over a period of time: one minute, one hour, and 72 hours are clearly shown:

+ The Y-axis of the graph is the CPU utilization.+ The X-axis of the graph is the increment within the period displayed in the graph

For example, from the last graph (last 72 hours) we learn that the highest CPU utilization within 72 hours is 37% about six hours ago.

QUESTION NO: 147

What two things will a router do when running a distance vector routing protocol? (Choose two.)

A. Send periodic updates regardless of topology changes.
B. Send entire routing table to all routers in the routing domain.
C. Use the shortest-path algorithm to the determine best path.
D. Update the routing table based on updates from their neighbors.
E. Maintain the topology of the entire network in its database.

Answer: A,D
Explanation:
Distance means how far and Vector means in which direction. Distance Vector routing protocols pass periodic copies of routing table to neighbor routers and accumulate distance vectors. In distance vector routing protocols, routers discover the best path to destination from each neighbor. The routing updates proceed step by step from router to router.

QUESTION NO: 148

Which command is used to display the collection of OSPF link states?

A. show ip ospf link-state
B. show ip ospf lsa database
C. show ip ospf neighbors
D. show ip ospf database

Answer: D
Explanation:
The "show ip ospf database" command displays the link states. Here is an example:
Here is the lsa database on R2.
R2#show ip ospf database

OSPF Router with ID (2.2.2.2) (Process ID 1)

Router Link States (Area 0)

Link ID ADV Router Age Seq# Checksum Link count2.2.2.2 2.2.2.2 793 0x80000003 0x004F85 210.4.4.4 10.4.4.4 776 0x80000004 0x005643 1111.111.111.111 111.111.111.111 755 0x80000005 0x0059CA 2133.133.133.133 133.133.133.133 775 0x80000005 0x00B5B1 2

Net Link States (Area 0)

Link ID ADV Router Age Seq# Checksum10.1.1.1 111.111.111.111 794 0x80000001 0x001E8B10.2.2.3 133.133.133.133 812 0x80000001 0x004BA910.4.4.1 111.111.111.111 755 0x80000001 0x007F1610.4.4.3 133.133.133.133 775 0x80000001 0x00C31F

QUESTION NO: 149

Refer to the exhibit.


```
System flash director
File Length Name/status
1 3802992 c827v-y6-mz.121-1.XB
[3803056 bytes used,4585552 available, 8388608 total]
8192K bytes of processor board System flash(Read/Write)
```

The technician wants to upload a new IOS in the router while keeping the existing IOS. What is the maximum size of an IOS file that could be loaded if the original IOS is also kept in flash?

A. 3 MB
B. 4 MB
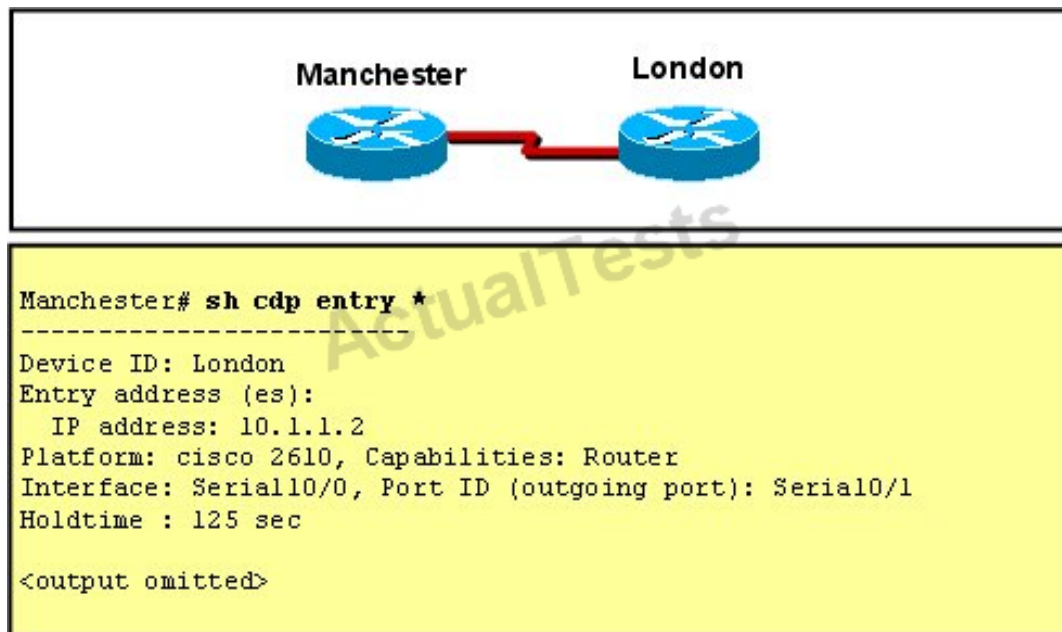**C.** 5 MB
D. 7 MB
E. 8 MB

Answer: B

Explanation:

In this example, there are a total of 8 MB, but 3.8 are being used already, so another file as large as 4MB can be loaded in addition to the original file.

QUESTION NO: 150

Refer to the exhibit.

```
Manchester# sh cdp entry *
-------------------------
Device ID: London
Entry address (es):
  IP address: 10.1.1.2
Platform: cisco 2610, Capabilities: Router
Interface: Serial10/0, Port ID (outgoing port): Serial0/1
Holdtime : 125 sec

<output omitted>
```

The two exhibited devices are the only Cisco devices on the network. The serial network between the two devices has a mask of 255.255.255.252. Given the output that is shown, what three statements are true of these devices? (Choose three.)

A. The Manchester serial address is 10.1.1.1.
B. The Manchester serial address is 10.1.1.2.
C. The London router is a Cisco 2610.
D. The Manchester router is a Cisco 2610.
E. The CDP information was received on port Serial0/0 of the Manchester router.
F. The CDP information was sent by port Serial0/0 of the London router.

Answer: A,C,E
Explanation:
From the output, we learn that the IP address of the neighbor router is 10.1.1.2 and the question stated that the subnet mask of the network between two router is 255.255.255.252. Therefore there are only 2 available hosts in this network (22 – 2 = 2). So we can deduce the ip address (of the serial interface) of Manchester router is 10.1.1.1 ->
The platform of the neighbor router is cisco 2610, as shown in the output ->
Maybe the most difficult choice of this question is the answer E or F. Please notice that "Interface" refers to the local port on the local router, in this case it is the port of Manchester router, and "Port ID (outgoing port)" refers to the port on the neighbor router.

QUESTION NO: 151

If IP routing is enabled, which two commands set the gateway of last resort to the default gateway? (Choose two.)

A. ip default-gateway 0.0.0.0
B. ip route 172.16.2.1 0.0.0.0 0.0.0.0
C. ip default-network 0.0.0.0
D. ip default-route 0.0.0.0 0.0.0.0 172.16.2.1
E. ip route 0.0.0.0 0.0.0.0 172.16.2.1

Answer: C,E

Explanation:

Both the "ip default-network" and "ip route 0.0.0.0 0.0.0.0 (next hop)" commands can be used to set the default gateway in a Cisco router.

QUESTION NO: 152

Which parameter would you tune to affect the selection of a static route as a backup, when a dynamic protocol is also being used?

A. hop count
B. administrative distance
C. link bandwidth
D. link delay
E. link cost

Answer: B

Explanation:

By default the administrative distance of a static route is 1, meaning it will be preferred over all dynamic routing protocols. If you want to have the dynamic routing protocol used and have the static route be used only as a backup, you need to increase the AD of the static route so that it is higher than the dynamic routing protocol.

QUESTION NO: 153

Refer to the exhibit.

```
City#show ip interface brief

Interface          IP-Address       OK?   Method   Status    Protocol
FastEthernet0/0    192.168.12.48    YES   manual    up        up
FastEthernet0/1    192.168.12.65    YES   manual    up        up
Serial0/0          192.168.12.121   YES   manual    up        up
Serial0/1          unassigned       YES   unset     up        up
Serial0/1.102      192.168.12.125   YES   manual    up        up
Serial0/1.103      192.168.12.129   YES   manual    up        up
Serial0/1.104      192.168.12.133   YES   manual    up        up
City#
```

A network associate has configured OSPF with the command:

City(config-router)# network 192.168.12.64 0.0.0.63 area 0

After completing the configuration, the associate discovers that not all the interfaces are participating in OSPF. Which three of the interfaces shown in the exhibit will participate in OSPF according to this configuration statement? (Choose three.)

A. FastEthernet0 /0
B. FastEthernet0 /1
C. Serial0/0
D. Serial0/1.102
E. Serial0/1.103
F. Serial0/1.104

Answer: B,C,D

Explanation: Explanation

The "network 192.168.12.64 0.0.0.63 equals to network 192.168.12.64/26. This network has:

+ Increment: 64 (/26= 1111 1111.1111 1111.1111 1111.1100 0000)

+ Network address: 192.168.12.64

+ Broadcast address: 192.168.12.127

Therefore all interface in the range of this network will join OSPF.

QUESTION NO: 154

Refer to the exhibit.
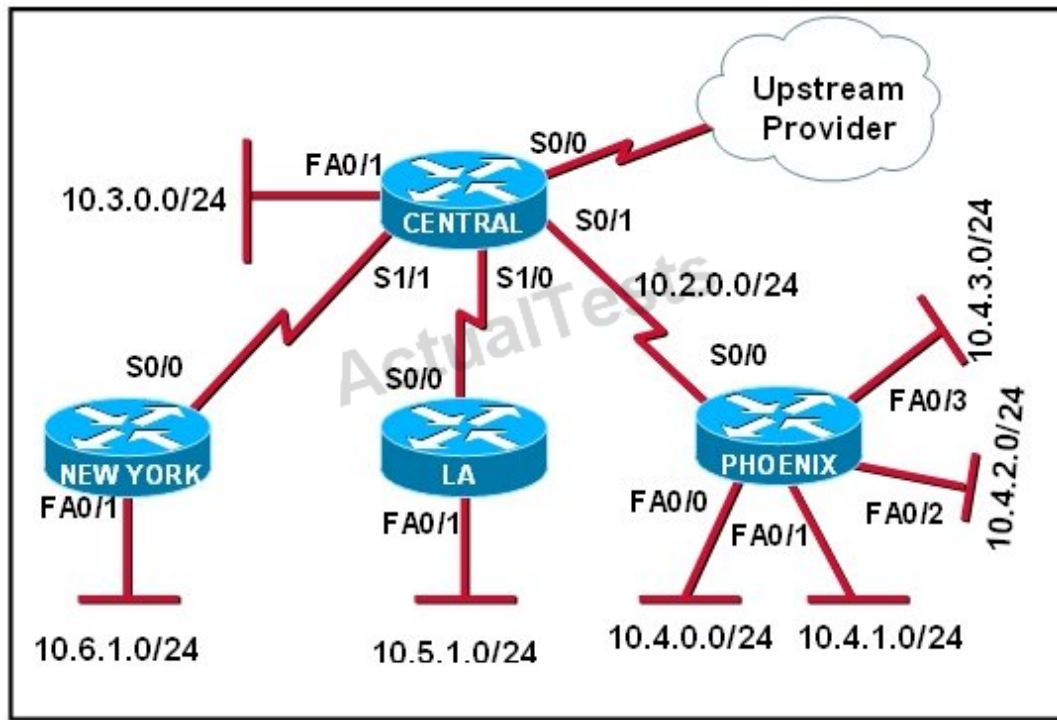
The Lakeside Company has the internetwork in the exhibit. The administrator would like to reduce the size of the routing table on the Central router. Which partial routing table entry in the Central router represents a route summary that represents the LANs in Phoenix but no additional subnets?

A. 10.0.0.0/22 is subnetted, 1 subnets
D 10.0.0.0 [90/20514560] via 10.2.0.2, 6w0d, Serial0/1
B. 10.0.0.0/28 is subnetted, 1 subnets
D 10.2.0.0 [90/20514560] via 10.2.0.2, 6w0d, Serial0/1
C. 10.0.0.0/30 is subnetted, 1 subnets
D 10.2.2.0 [90/20514560] via 10.2.0.2, 6w0d, Serial0/1
D. 10.0.0.0/22 is subnetted, 1 subnets
D 10.4.0.0 [90/20514560] via 10.2.0.2, 6w0d, Serial0/1
E. 10.0.0.0/28 is subnetted, 1 subnets
D 10.4.4.0 [90/20514560] via 10.2.0.2, 6w0d, Serial0/1
F. 10.0.0.0/30 is subnetted, 1 subnets
D 10.4.4.4 [90/20514560] via 10.2.0.2, 6w0d, Serial0/1

Answer: D
Explanation:
The 10.4.0.0/22 route includes 10.4.0.0/24, 10.4.1.0/24, 10.4.2.0/24 and 10.4.3.0/24 only.

QUESTION NO: 155

Refer to the graphic.
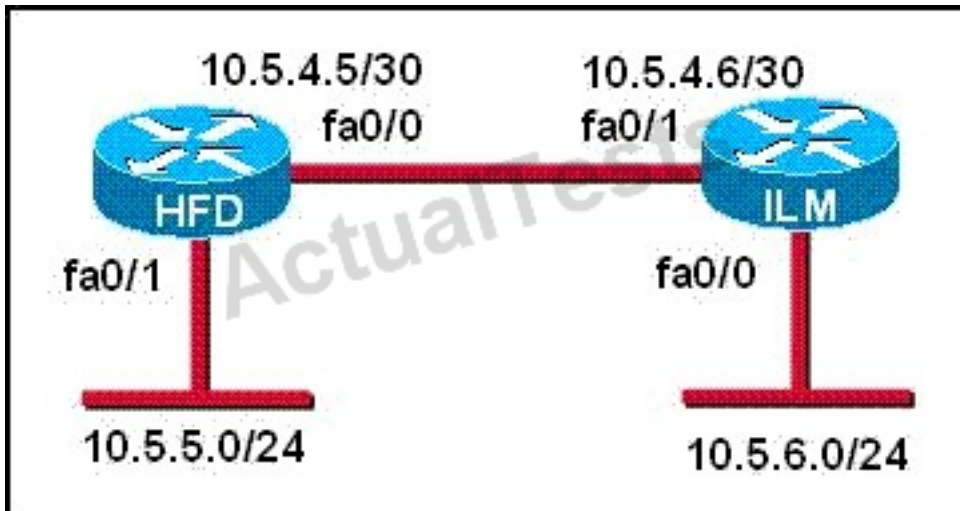
A static route to the 10.5.6.0/24 network is to be configured on the HFD router. Which commands will accomplish this? (Choose two.)

A. HFD(config)# ip route 10.5.6.0 0.0.0.255 fa0/0
B. HFD(config)# ip route 10.5.6.0 0.0.0.255 10.5.4.6
C. HFD(config)# ip route 10.5.6.0 255.255.255.0 fa0/0
D. HFD(config)# ip route 10.5.6.0 255.255.255.0 10.5.4.6
E. HFD(config)# ip route 10.5.4.6 0.0.0.255 10.5.6.0
F. HFD(config)# ip route 10.5.4.6 255.255.255.0 10.5.6.0

Answer: C,D
Explanation:
The simple syntax of static route:
ip route destination-network-address subnet-mask {next-hop-IP-address | exit-interface}
+ destination-network-address: destination network address of the remote network
+ subnet mask: subnet mask of the destination network
+ next-hop-IP-address: the IP address of the receiving interface on the next-hop router
+ exit-interface: the local interface of this router where the packets will go out
In the statement "ip route 10.5.6.0 255.255.255.0 fa0/0:
+ 10.5.6.0 255.255.255.0: the destination network
+fa0/0: the exit-interface

QUESTION NO: 156

Before installing a new, upgraded version of the IOS, what should be checked on the router, and

which command should be used to gather this information? (Choose two.)

A. the amount of available ROM
B. the amount of available flash and RAM memory
C. the version of the bootstrap software present on the router
D. show version
E. show processes
F. show running-config

Answer: B,D

Explanation: Explanation

When upgrading new version of the IOS we need to copy the IOS to the Flash so first we have to check if the Flash has enough memory or not. Also running the new IOS may require more RAM than the older one so we should check the available RAM too. We can check both with the "show version" command.

QUESTION NO: 157

Which command reveals the last method used to powercycle a router?

A. show reload
B. show boot
C. show running-config
D. show version

Answer: D

Explanation: Explanation

The "show version" command can be used to show the last method to powercycle (reset) a router

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-IK9S-M), Version 12.2(40a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by cisco Systems, Inc.
Compiled Sat 10-Mar-07 21:57 by pwade
Image text-base: 0x60008930, data-base: 0x612A2000

ROM: ROMMON Emulation Microcode
ROM: 3600 Software (C3640-IK9S-M), Version 12.2(40a), RELEASE SOFTWARE (fc1)

Router uptime is 3 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0
System image file is "tftp://255.255.255.255/unknown"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 3640 (R4700) processor (revision 0xFF) with 126976K/4096K bytes of memory.
Processor board ID 00000000
R4700 CPU at 100Mhz, Implementation 33, Rev 1.2
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
1 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
DRAM configuration is 64 bits wide with parity enabled.
125K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2142

Router>
```

QUESTION NO: 158

Which command would you use on a Cisco router to verify the Layer 3 path to a host?

A. tracert address
B. traceroute address
C. telnet address
D. ssh address

Answer: B

Explanation:

In computing, traceroute is a computer network diagnostic tool for displaying the route (path) and

measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point.

QUESTION NO: 159

What information does a router running a link-state protocol use to build and maintain its topological database? (Choose two.)

A. hello packets
B. SAP messages sent by other routers
C. LSAs from other routers
D. beacons received on point-to-point links
E. routing tables received from other link-state routers
F. TTL packets from designated routers

Answer: A,C
Explanation:
Neighbor discovery is the first step in getting a link state environment up and running. In keeping with the friendly neighbor terminology, a Hello protocol is used for this step. The protocol will define a Hello packet format and a procedure for exchanging the packets and processing the information the packets contain.
After the adjacencies are established, the routers may begin sending out LSAs. As the term flooding implies, the advertisements are sent to every neighbor. In turn, each received LSA is copied and forwarded to every neighbor except the one that sent the LSA.

QUESTION NO: 160

Which statements describe the routing protocol OSPF? (Choose three.)

A. It supports VLSM.
B. It is used to route between autonomous systems.
C. It confines network instability to one area of the network.
D. It increases routing overhead on the network.

E. It allows extensive control of routing updates.

F. It is simpler to configure than RIP v2.

Answer: A,C,E

Explanation:

The OSPF protocol is based on link-state technology, which is a departure from the Bellman-Ford vector based algorithms used in traditional Internet routing protocols such as RIP. OSPF has introduced new concepts such as authentication of routing updates, Variable Length Subnet Masks (VLSM), route summarization, and so forth.

OSPF uses flooding to exchange link-state updates between routers. Any change in routing information is flooded to all routers in the network. Areas are introduced to put a boundary on the explosion of link-state updates. Flooding and calculation of the Dijkstra algorithm on a router is limited to changes within an area.

QUESTION NO: 161

Refer to the exhibit.

```
— System Configuration Dialog —
Would you like to enter the initial configuration dialog? [yes/no]: % Please answer yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/ho]: n

Would you like to terminate autoinstall? [yes]:

Press RETURN to get started!
```

A network administrator configures a new router and enters the copy startup-config running-config command on the router. The network administrator powers down the router and sets it up at a remote location. When the router starts, it enters the system configuration dialog as shown. What is the cause of the problem?

A. The network administrator failed to save the configuration.

B. The configuration register is set to 0x2100.

C. The boot system flash command is missing from the configuration.

D. The configuration register is set to 0x2102.

E. The router is configured with the boot system startup command.

Answer: A

Explanation: Explanation

The "System Configuration Dialog" appears only when no startup configuration file is found. The network administrator has made a mistake because the command "copy startup-config running-config" will copy the startup config (which is empty) over the running config (which is configured by

the administrator). So everything configured was deleted.

Note: We can tell the router to ignore the start-up configuration on the next reload by setting the register to 0×2142. This will make the "System Configuration Dialog" appear at the next reload.

QUESTION NO: 162

What is the default administrative distance of OSPF?

A. 90
B. 100
C. 110
D. 120

Answer: C

Explanation:

Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

Default Distance Value Table

This table 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

QUESTION NO: 163

Which characteristics are representative of a link-state routing protocol? (Choose three.)

A. provides common view of entire topology
B. exchanges routing tables with neighbors
C. calculates shortest path
D. utilizes event-triggered updates
E. utilizes frequent periodic updates

Answer: A,C,D

Explanation: Explanation

Each of routers running link-state routing protocol learns paths to all the destinations in its "area" so we can say although it is a bit unclear.

Link-state routing protocols generate routing updates only (not the whole routing table) when a change occurs in the network topology so

Link-state routing protocol like OSPF uses Dijkstra algorithm to calculate the shortest path -> .

Unlike Distance vector routing protocol (which utilizes frequent periodic updates), link-state routing protocol utilizes event-triggered updates (only sends update when a change occurs) ->

QUESTION NO: 164

Refer to the exhibit.
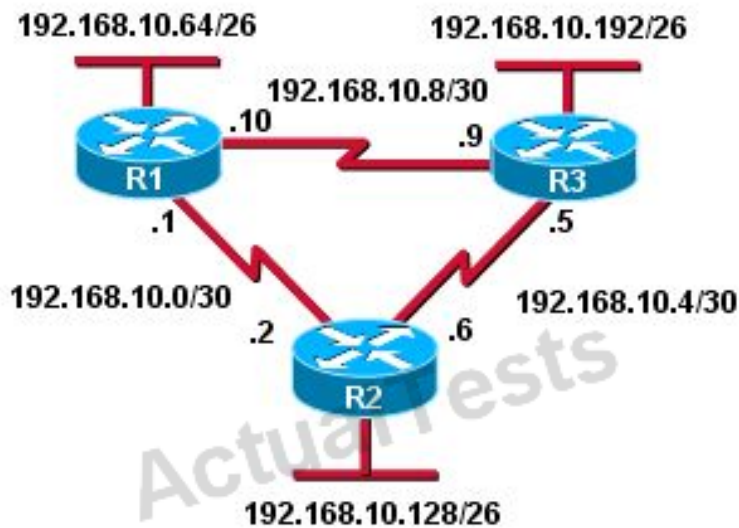
```
R3# show ip route
Gateway of last resort is not set
    192.168.10.0/24 is variably subnetted, 6 subnets, 2 masks
D      192.168.10.64/26 [90/2195456] via 192.168.10.9, 00:03:31, Serial0/0
D      192.168.10.0/30 [90/2681856] via 192.168.10.9, 00:03:31, Serial0/0
                       [90/2681856] via 192.168.10.5, 00:03:31, Serial0/1
C      192.168.10.4/30 is directly connected, Serial 0/1
C      192.168.10.8/30 is directly connected, Serial 0/0
C      192.168.10.192/26 is directly connected, FastEthernet0/0
D      192.168.10.128/26 [90/2195456] via 192.168.10.5, 00:03:31, Serial 0/1
```

Based on the exhibited routing table, how will packets from a host within the 192.168.10.192/26 LAN be forwarded to 192.168.10.1?

A. The router will forward packets from R3 to R2 to R1.
B. The router will forward packets from R3 to R1 to R2.
C. The router will forward packets from R3 to R2 to R1 AND from R3 to R1.
D. The router will forward packets from R3 to R1.

Answer: C

Explanation: Explanation

From the routing table we learn that network 192.168.10.0/30 is learned via 2 equal-cost paths (192.168.10.9 &192.168.10.5) -> traffic to this network will be load-balancing.

QUESTION NO: 165

Refer to the exhibit.
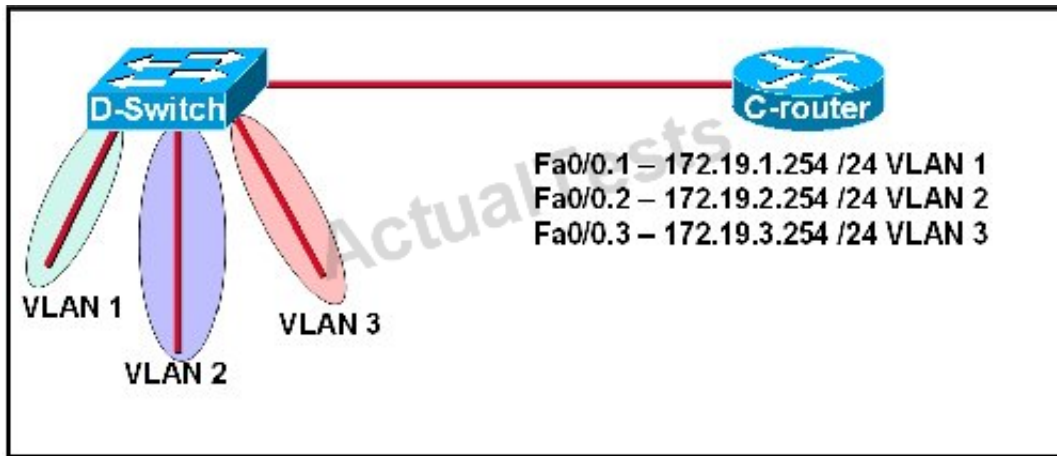
C-router is to be used as a "router-on-a-stick" to route between the VLANs. All the interfaces have been properly configured and IP routing is operational. The hosts in the VLANs have been configured with the appropriate default gateway. What is true about this configuration?

A. These commands need to be added to the configuration:
C-router(config)# router eigrp 123
C-router(config-router)# network 172.19.0.0
B. These commands need to be added to the configuration:
C-router(config)# router ospf 1
C-router(config-router)# network 172.19.0.0 0.0.3.255 area 0
C. These commands need to be added to the configuration:
C-router(config)# router rip
C-router(config-router)# network 172.19.0.0
D. No further routing configuration is required.

Answer: D
Explanation:
Since all the same router (C-router) is the default gateway for all three VLANs, all traffic destined to a different VLA will be sent to the C-router. The C-router will have knowledge of all three networks since they will appear as directly connected in the routing table. Since the C-router already knows how to get to all three networks, no routing protocols need to be configured.

QUESTION NO: 166

Refer to the exhibit.

```
Router# copy tftp flash
Address or name of remote host []? 192.168.2.167
Source filename []? c1600-k8sy-mz.123-16a.bin
Destination filename [c1600-k8sy-mz.123-16a.bin]?
Accessing tftp://192.168.2.167/ c1600-k8sy-mz.l23-16a.bin...
Erasing flash before copying? [confirm]
Erasing the flash filesystem will remove all files! continue? [confirm]
Erasing device
Eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
Eeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of flash: complete
Loading c1600-k8sy-mz.l23-16a.bin from 192.168.2.167 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6888962/13777920 bytes]

verifying checksum... OK (0x7BF3)
6888962 bytes copied in 209.920 secs (32961 bytes/sec)
Router#
```

Why is flash memory erased prior to upgrading the IOS image from the TFTP server?

A. The router cannot verify that the Cisco IOS image currently in flash is valid.
B. Flash memory on Cisco routers can contain only a single IOS image.
C. Erasing current flash content is requested during the copy dialog.
D. In order for the router to use the new image as the default, it must be the only IOS image in flash.

Answer: C

Explanation: Explanation

During the copy process, the router asked "Erasing flash before copying? [confirm]" and the administrator confirmed (by pressing Enter) so the flash was deleted.

Note: In this case, the flash has enough space to copy a new IOS without deleting the current one. The current IOS is deleted just because the administrator wants to do so. If the flash does not have enough space you will see an error message like this:

%Error copying tftp://192.168.2.167/ c1600-k8sy-mz.l23-16a.bin (Not enough space on device)

QUESTION NO: 167

Which command would you configure globally on a Cisco router that would allow you to view directly connected Cisco devices?

A. enable cdp
B. cdp enable

C. cdp run
D. run cdp

Answer: C

Explanation:

CDP is enabled on Cisco routers by default. If you prefer not to use the CDP capability, disable it with the no cdp run command. In order to reenable CDP, use the cdp run command in global configuration mode. The "cdp enable" command is an interface command, not global.

QUESTION NO: 168

Refer to the exhibit.

Network	Interface	Next-hop
10.1.1.0/24	e0	directly connected
10.1.2.0/24	e1	directly connected
10.1.3.0/25	s0	directly connected
10.1.4.0/24	s1	directly connected
10.1.5.0/24	e0	10.1.1.2
10.1.5.64/28	e1	10.1.2.2
10.1.5.64/29	s0	10.1.3.3
10.1.5.64/27	s1	10.1.4.4

According to the routing table, where will the router send a packet destined for 10.1.5.65?

A. 10.1.1.2
B. 10.1.2.2
C. 10.1.3.3
D. 10.1.4.4

Answer: C

Explanation: Explanation

The destination IP address 10.1.5.65 belongs to 10.1.5.64/28, 10.1.5.64/29 & 10.1.5.64/27 subnets but the "longest prefix match" algorithm will choose the most specific subnet mask -> the prefix "/29 will be chosen to route the packet. Therefore the next-hop should be 10.1.3.3 -> .

QUESTION NO: 169

Refer to the exhibit.

```
Gateway of last resort is not set

    192.168.25.0/30 is subnetted, 4 subnets
D      192.168.25.20 [90/2681856] via 192.168.15.5, 00:00:10, Serial0/1
D      192.168.25.16 [90/1823638] via 192.168.15.5, 00:00:50, Serial0/1
D      192.168.25.24 [90/3837233] via 192.168.15.5, 00:05:23, Serial0/1
D      192.168.25.28 [90/8127323] via 192.168.15.5, 00:06:45, Serial0/1
C   192.168.15.4/30 is directly connected, Serial0/1
C   192.168.2.0/24 is directly connected, FastEthernet0/0
```

Which address and mask combination represents a summary of the routes learned by EIGRP?

A. 192.168.25.0 255.255.255.240
B. 192.168.25.0 255.255.255.252
C. 192.168.25.16 255.255.255.240
D. 192.168.25.16 255.255.255.252
E. 192.168.25.28 255.255.255.240
F. 192.168.25.28 255.255.255.252

Answer: C
Explanation:
The binary version of 20 is 10100.
The binary version of 16 is 10000.
The binary version of 24 is 11000.
The binary version of 28 is 11100.
The subnet mask is /28. The mask is 255.255.255.240.

Note:
From the output above, EIGRP learned 4 routes and we need to find out the summary of them:
+ 192.168.25.16
+ 192.168.25.20
+ 192.168.25.24
+ 192.168.25.28
-> The increment should bE. 28 – 16 = 12 but 12 is not an exponentiation of 2 so we must choose 16 (24). Therefore the subnet mask is /28 (=1111 1111.1111 1111.1111 1111.11110000) = 255.255.255.240

So the best answer should be 192.168.25.16 255.255.255.240

QUESTION NO: 170

Refer to the exhibit.
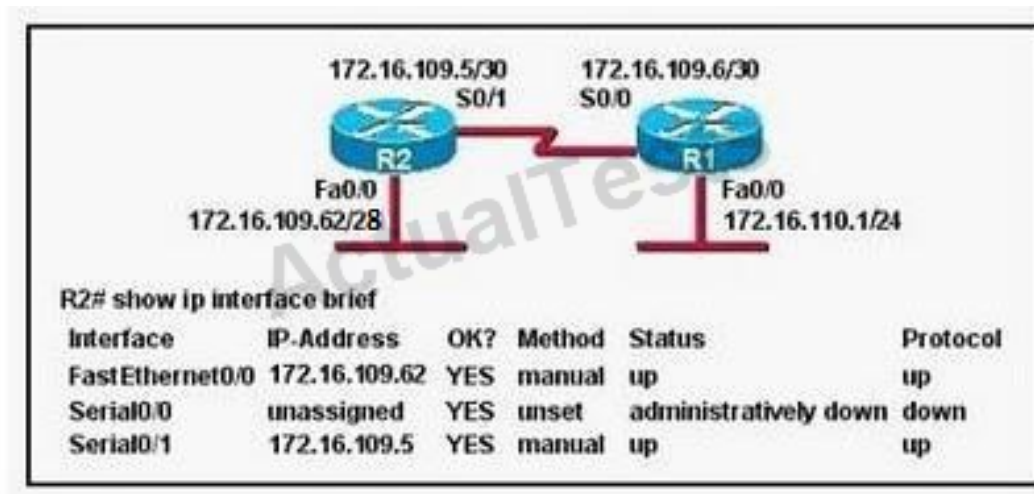
Assuming that the entire network topology is shown, what is the operational status of the interfaces of R2 as indicated by the command output shown?

A. One interface has a problem.
B. Two interfaces have problems.
C. The interfaces are functioning correctly.
D. The operational status of the interfaces cannot be determined from the output shown.

Answer: C
Explanation:
The output shown shows normal operational status of the router's interfaces. Serial0/0 is down because it has been disabled using the "shutdown" command.

QUESTION NO: 171

Which two locations can be configured as a source for the IOS image in the boot system command? (Choose two.)

A. RAM
B. NVRAM
C. flash memory
D. HTTP server
E. TFTP server
F. Telnet server

Answer: C,E

Explanation: Explanation

The following locations can be configured as a source for the IOS image:

1. + Flash (the default location)

2. + TFTP server

3. + ROM (used if no other source is found)

4. (Please read the explanation of Question 4 for more information)

QUESTION NO: 172

Refer to the exhibit.

```
RouterD# show ip interface brief
Interface        IP-Address     OK? Method Status Protocol
FastEthernet0/0  192.168.5.3    YES manual up     up
FastEthernet0/1  10.1.1.2       YES manual up     up
Loopback0        172.16.5.1     YES NVRAM  up     up
Loopback1        10.154.154.1   YES NVRAM  up     up
```

Given the output for this command, if the router ID has not been manually set, what router ID will OSPF use for this router?

A. 10.1.1.2
B. 10.154.154.1
C. 172.16.5.1
D. 192.168.5.3

Answer: C

Explanation: Explanation

The highest IP address of all loopback interfaces will be chosen -> Loopback 0 will be chosen as the router ID.

QUESTION NO: 173

Refer to the exhibit.
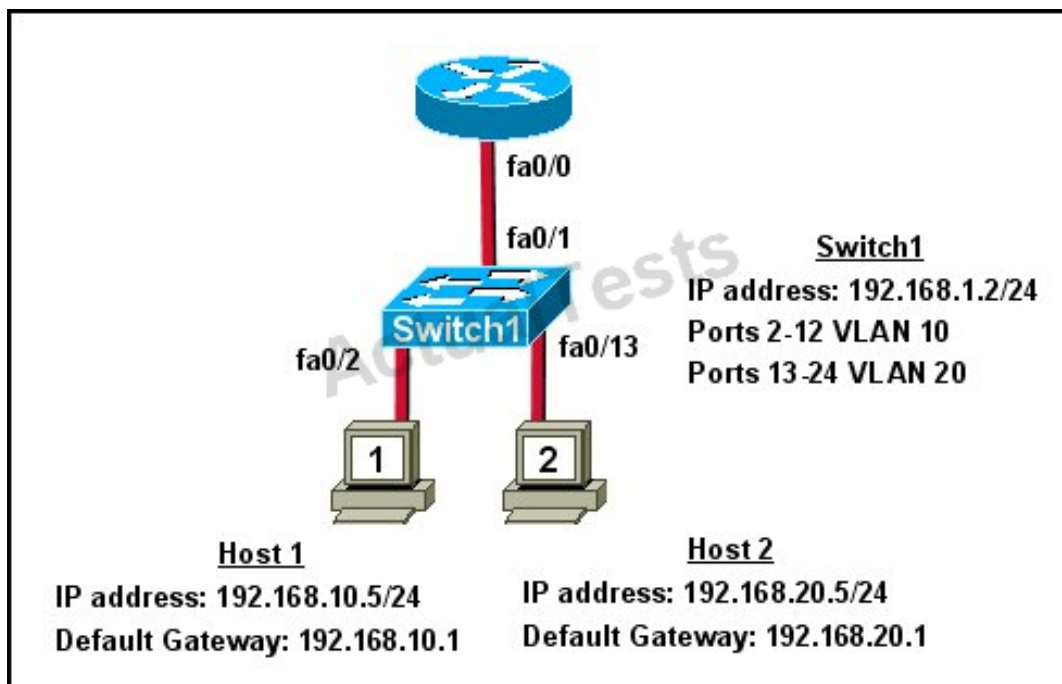
What commands must be configured on the 2950 switch and the router to allow communication between host 1 and host 2? (Choose two.)

A. Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shut down
B. Router(config)# interface fastethernet 0/0
Router(config-if)# no shut down
Router(config)# interface fastethernet 0/0.1
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config)# interface fastethernet 0/0.2
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
C. Router(config)# router eigrp 100

Router(config-router)# network 192.168.10.0
Router(config-router)# network 192.168.20.0
D. Switch1(config)# vlan database
Switch1(config-vlan)# vtp domain XYZ
Switch1(config-vlan)# vtp server
E. Switch1(config)# interface fastethernet 0/1
Switch1(config-if)# switchport mode trunk
F. Switch1(config)# interface vlan 1
Switch1(config-if)# ip default-gateway 192.168.1.1

Answer: B,E
Explanation:
The router will need to use subinterfaces, where each subinterface is assigned a VLAN and IP address for each VLAN. On the switch, the connection to the router need to be configured as a trunk using the switchport mode trunk command and it will need a default gateway for VLAN 1.

QUESTION NO: 174

Which two statements describe the process identifier that is used in the command to configure OSPF on a router? (Choose two.)

Router(config)# router ospf 1

A. All OSPF routers in an area must have the same process ID.
B. Only one process number can be used on the same router.
C. Different process identifiers can be used to run multiple OSPF processes
D. The process number can be any number from 1 to 65,535.
E. Hello packets are sent to each neighbor to determine the processor identifier.

Answer: C,D
Explanation: Multiple OSPF processes can be configured on a router using multiple process ID's.
The valid process ID's are shown below:
Edge-B(config)#router ospf ?
<1-65535> Process ID

QUESTION NO: 175

Refer to the exhibit.

```
Router1> show version
Cisco Internetwork Operating System Software
IOS ™ 7200 Software (C7200-J-M), Experimental Version 11.3tl997091S:1647S2)
[hampton-nitro-baseline 249]
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Wed 08-Oct-97 06:39 by hampton
Image text-base: 0×60008900, data-base: 0x60B98000

ROM: System Bootstrap, Version 11.1(11855) [beta 2], INTERIM SOFTWARE
BOOTPLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE (fcl)

Router1 uptime is 23 hours, 33 minutes
System restarted by abort at PC 0x6022322C at 10:50:SS PDT Tue Oct 21 1997
System image file is "tftp://112.16.1.129/hampton/nitro/c7200-j-mz"

cisco 7206 (NPE150) processor with 57344K/8192K bytes of memory.

Configuration register is 0×2102
```

For what two reasons has the router loaded its IOS image from the location that is shown? (Choose two.)

A. Router1 has specific boot system commands that instruct it to load IOS from a TFTP server.
B. Router1 is acting as a TFTP server for other routers.
C. Router1 cannot locate a valid IOS image in flash memory.
D. Router1 defaulted to ROMMON mode and loaded the IOS image from a TFTP server.
E. Cisco routers will first attempt to load an image from TFTP for management purposes.

Answer: A,C

Explanation:

The loading sequence of CISCO IOS is as follows:

Booting up the router and locating the Cisco IOS

1. POST (power on self test)

2. Bootstrap code executed

3. Check Configuration Register value (NVRAM) which can be modified using the config-register command

0 = ROM Monitor mode

1 = ROM IOS

2 - 15 = startup-config in NVRAM

4. Startup-config filE. Check for boot system commands (NVRAM)

If boot system commands in startup-config

a. Run boot system commands in order they appear in startup-config to locate the IOS

b. [If boot system commands fail, use default fallback sequence to locate the IOS (Flash, TFTP, ROM)?]

If no boot system commands in startup-config use the default fallback sequence in locating the IOS:

a. Flash (sequential)

b. TFTP server (netboot)

c. ROM (partial IOS) or keep retrying TFTP depending upon router model

5. If IOS is loaded, but there is no startup-config file, the router will use the default fallback

sequence for locating the IOS and then it will enter setup mode or the setup dialogue.

QUESTION NO: 176

Refer to the exhibit.

```
1 FastEthernet/IEEE 802.3 interface(s)
125K bytes of non-volatile configuration memory.

65536K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).

        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

What can be determined about the router from the console output?

A. No configuration file was found in NVRAM.
B. No configuration file was found in flash.
C. No configuration file was found in the PCMCIA card.
D. Configuration file is normal and will load in 15 seconds.

Answer: A

Explanation: Explanation

When no startup configuration file is found in NVRAM, the System Configuration Dialog will appear

to ask if we want to enter the initial configuration dialog or not.

QUESTION NO: 177

Which three elements must be used when you configure a router interface for VLAN trunking?
(Choose three.)

A. one physical interface for each subinterface

B. one IP network or subnetwork for each subinterface

C. a management domain for each subinterface

D. subinterface encapsulation identifiers that match VLAN tags

E. one subinterface per VLAN

F. subinterface numbering that matches VLAN tags

Answer: B,D,E

Explanation:

This scenario is commonly called a router on a stick. A short, well written article on this operation can be found here:

http://www.thebryantadvantage.com/RouterOnAStickCCNACertificationExamTutorial.htm

QUESTION NO: 178

Which commands are required to properly configure a router to run OSPF and to add network 192.168.16.0/24 to OSPF area 0? (Choose two.)

A. Router(config)# router ospf 0

B. Router(config)# router ospf 1

C. Router(config)# router ospf area 0

D. Router(config-router)# network 192.168.16.0 0.0.0.255 0

E. Router(config-router)# network 192.168.16.0 0.0.0.255 area 0

F. Router(config-router)# network 192.168.16.0 255.255.255.0 area 0

Answer: B,E

Explanation: Explanation

In the router ospf

command, the ranges from 1 to 65535 so o is an invalid number -> but

To configure OSPF, we need a wildcard in the "network" statement, not a subnet mask. We also need to assgin an area to this process -> .

QUESTION NO: 179

A router receives information about network 192.168.10.0/24 from multiple sources. What will the router consider the most reliable information about the path to that network?

A. a directly connected interface with an address of 192.168.10.254/24

B. a static route to network 192.168.10.0/24

C. a RIP update for network 192.168.10.0/24

D. an OSPF update for network 192.168.0.0/16

E. a default route with a next hop address of 192.168.10.1

F. a static route to network 192.168.10.0/24 with a local serial interface configured as the next hop

Answer: A

Explanation:

When there is more than one way to reach a destination, it will choose the best one based on a couple of things. First, it will choose the route that has the longest match; meaning the most specific route. So, in this case the /24 routes will be chosen over the /16 routes. Next, from all the /24 routes it will choose the one with the lowest administrative distance. Directly connected routes have an AD of 1 so this will be the route chosen.

QUESTION NO: 180

What is the default maximum number of equal-cost paths that can be placed into the routing table of a Cisco OSPF router?

A. 2

B. 8

C. 16

D. unlimited

Answer: B

Explanation:

maximum-paths (OSPF)

To control the maximum number of parallel routes that Open Shortest Path First (OSPF) can support, use the **maximum-paths** command.

Syntax Description

maximum

Maximum number of parallel routes that OSPF can install in a routing table. The range is from 1 to 16 routes.

Command Default

8 *paths*

QUESTION NO: 181

Which command shows your active Telnet connections?

A. show cdp neigbors
B. show session
C. show users
D. show vty logins

Answer: B

Explanation: Explanation

The "show users" shows telnet/ssh connections to your router while "show sessions" shows telnet/ssh connections from your router (to other devices). The question asks about "your active Telnet connections", meaning connections from your router so the answer should be A.

QUESTION NO: 182

Which type of EIGRP route entry describes a feasible successor?

A. a backup route, stored in the routing table
B. a primary route, stored in the routing table
C. a backup route, stored in the topology table
D. a primary route, stored in the topology table

Answer: C
Explanation:

EIGRP uses the Neighbor Table to list adjacent routers. The Topology Table list all the learned routers to destination whilst the Routing Table contains the best route to a destination, which is known as the Successor. The Feasible Successor is a backup route to a destination which is kept in the Topology Table.

QUESTION NO: 183

The network administrator cannot connect to Switch1 over a Telnet session, although the hosts attached to Switch1 can ping the interface Fa0/0 of the router. Given the information in the graphic and assuming that the router and Switch2 are configured properly, which of the following commands should be issued on Switch1 to correct this problem?

A. Switch1(config)# line con0

Switch1(config-line)# password cisco
Switch1(config-line)#login
B. Switch1(config)# interface fa0/1
Switch1(config-if)# ip address 192.168.24.3 255.255.255.0
C. Switch1(config)# ip default-gateway 192.168.24.1
D. Switch1(config)# interface fa0/1
Switch1(config-if)# duplex full
Switch1(config-if)# speed 100
E. Switch1(config)# interface fa0/1
Switch1(config-if)# switchport mode trunk

Answer: C
Explanation:
Since we know hosts can reach the router through the switch, we know that connectivity, duplex. Speed, etc. are good. However, for the switch itself to reach networks outside the local one, the ip default-gateway command must be used.

QUESTION NO: 184

Refer to the exhibit.

```
00:00:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:40: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:42: %SYS-5-CONFIG_I: Configured from memory by console
00:00:42: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh
00:00:44: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
00:00:44: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:00:44: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
00:00:44: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to up
00:00:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
00:00:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
00:00:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up
00:00:48: %LINK-3-UPDOWN: Interface FastEthernet0/12, changed state to up
00:00:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to up
```

Which of these statements correctly describes the state of the switch once the boot process has been completed?

A. As FastEthernet0/12 will be the last to come up, it will be blocked by STP.
B. Remote access management of this switch will not be possible without configuration change.
C. More VLANs will need to be created for this switch.

**D.** The switch will need a different IOS code in order to support VLANs and STP.

Answer: B
Explanation:
Notice the line, which says "Interface VLAN1, changed state to administratively down". This shows that VLAN1 is shut down. Hence remote management of this switch is not possible unless VLAN1 is brought back up. Since VLAN1 is the only interface shown in the output, you have to assume that no other VLAN interface has been configured with an IP Address.

QUESTION NO: 185

Two routers named Atlanta and Brevard are connected via their serial interfaces as illustrated, but they are unable to communicate. The Atlanta router is known to have the correct configuration.
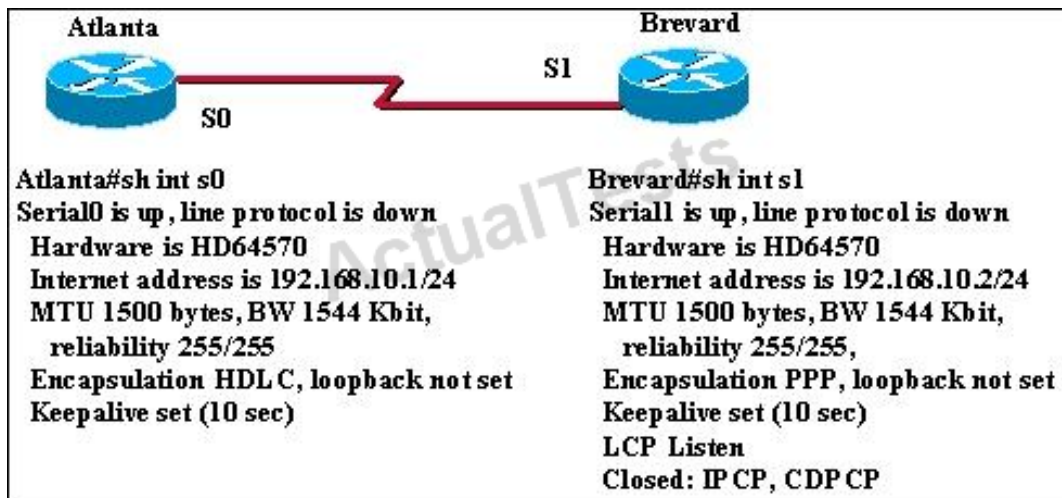
Given the partial configurations, identify the fault on the Brevard router that is causing the lack of connectivity.

A. incompatible IP address
B. insufficient bandwidth
C. incorrect subnet mask
D. incompatible encapsulation
E. link reliability too low
F. IPCP closed

Answer: D
Explanation:
Because Interface Serial 0 of Atlanta Router has 192.168.10.1 And Interface Serial 1 of Router Brevard has 192.168.11.2. These are from different network.

QUESTION NO: 186

Users on the 172.17.22.0 network cannot reach the server located on the 172.31.5.0 network. The network administrator connected to router Coffee via the console port, issued the show ip route command, and was able to ping the server.


```
Coffee#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - 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, L1 - IS-IS level-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 172.19.22.2 to network 0.0.0.0

C    172.17.22.0 is directly connected, FastEthernet0/0
C    172.18.22.0 is directly connected, Serial0/0
S*   0.0.0.0/0 [1/0] via 172.19.22.2
```

Based on the output of the show ip route command and the topology shown in the graphic, what is the cause of the failure?

A. The network has not fully converged.
B. IP routing is not enabled.
C. A static route is configured incorrectly.
D. The FastEthernet interface on Coffee is disabled.
E. The neighbor relationship table is not correctly updated.
F. The routing table on Coffee has not updated .

Answer: C
Explanation: The default route or the static route was configured with incorrect next-hop ip address 172.19.22.2 The correct ip address will be 172.18.22.2 to reach server located on 172.31.5.0 network. Ip route 0.0.0.0 0.0.0.0 172.18.22.2

QUESTION NO: 187

A network administrator is trying to add a new router into an established OSPF network. The networks attached to the new router do not appear in the routing tables of the other OSPF routers. Given the information in the partial configuration shown below, what configuration error is causing this problem?

Router(config)# router ospf 1

Router(config-router)# network 10.0.0.0 255.0.0.0 area 0

A. The process id is configured improperly.
B. The OSPF area is configured improperly.
C. The network wildcard mask is configured improperly.
D. The network number is configured improperly.
E. The AS is configured improperly.
F. The network subnet mask is configured improperly.

Answer: C
Explanation:
When configuring OSPF, the mask used for the network statement is a wildcard mask similar to an access list. In this specific example, the correct syntax would have been "network 10.0.0.0 0.0.0.255 area 0."

Topic 5, IP Services

QUESTION NO: 188

Which statement is correct regarding the operation of DHCP?

A. A DHCP client uses a ping to detect address conflicts.
B. A DHCP server uses a gratuitous ARP to detect DHCP clients.
C. A DHCP client uses a gratuitous ARP to detect a DHCP server.
D. If an address conflict is de0tected, the address is removed from the pool and an administrator must resolve the conflict.
E. If an address conflict is detected, the address is removed from the pool for an amount of time configurable by the administrator.
F. If an address conflict is detected, the address is removed from the pool and will not be reused until the server is rebooted.

Answer: D
Explanation:
An address conflict occurs when two hosts use the same IP address. During address assignment, DHCP checks for conflicts using ping and gratuitous ARP. If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

(Reference: http://www.cisco.com/en/US/docs/ios/12_1/iproute/configuration/guide/1cddhcp.html)

QUESTION NO: 189

Refer to the exhibit.
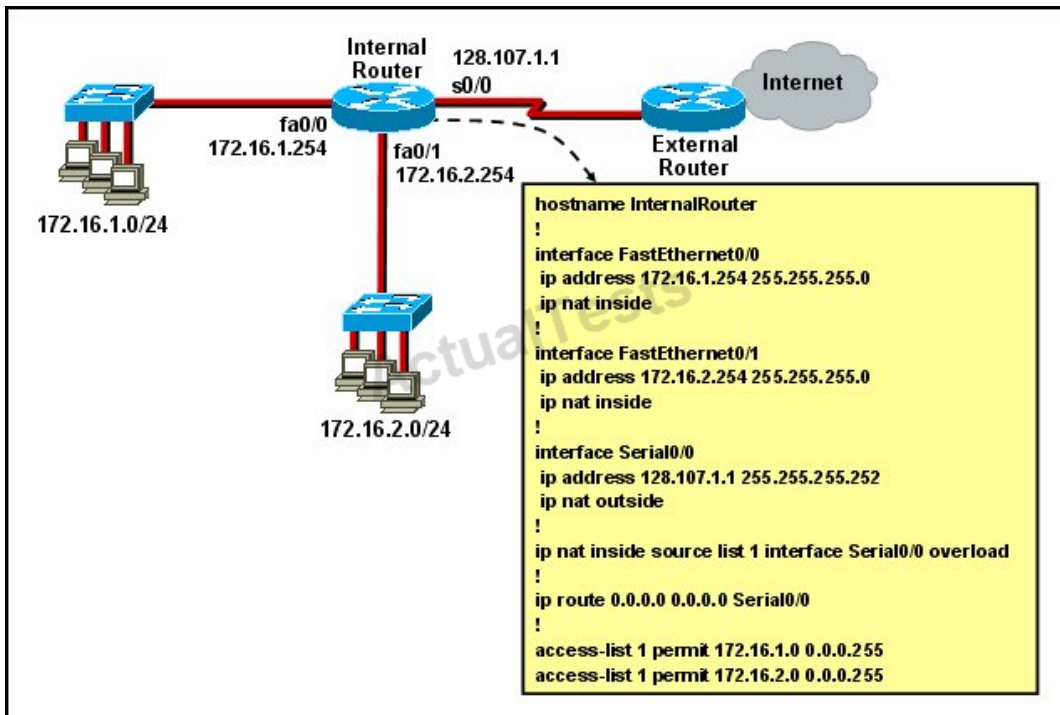
What statement is true of the configuration for this network?

A. The configuration that is shown provides inadequate outside address space for translation of the number of inside addresses that are supported.
B. Because of the addressing on interface FastEthernet0/1, the Serial0/0 interface address will not support the NAT configuration as shown.
C. The number 1 referred to in the ip nat inside source command references access-list number 1.
D. ExternalRouter must be configured with static routes to networks 172.16.1.0/24 and 172.16.2.0/24.

Answer: C

Explanation: Explanation
The "list 1 refers to the access-list number 1.

QUESTION NO: 190

Which statement describes the process of dynamically assigning IP addresses by the DHCP server?

A. Addresses are allocated after a negotiation between the server and the host to determine the length of the agreement.
B. Addresses are permanently assigned so that the hosts uses the same address at all times.
C. Addresses are assigned for a fixed period of time, at the end of the period, a new request for an address must be made.
D. Addresses are leased to hosts, which periodically contact the DHCP server to renew the lease.

Answer: D

Explanation: The DHCP lifecycle consists of the following:
Release: The client may decide at any time that it no longer wishes to use the IP address it was assigned, and may terminate the lease, *releasing* the IP address.

QUESTION NO: 191

What are two benefits of using NAT? (Choose two.)

A. NAT facilitates end-to-end communication when IPsec is enabled.
B. NAT eliminates the need to re-address all hosts that require external access.
C. NAT conserves addresses through host MAC-level multiplexing.
D. Dynamic NAT facilitates connections from the outside of the network.
E. NAT accelerates the routing process because no modifications are made on the packets.
F. NAT protects network security because private networks are not advertised.

Answer: B,F
Explanation:

By not revealing the internal Ip addresses, NAT adds some security to the inside network -> F is correct.

NAT has to modify the source IP addresses in the packets -> E is not correct.

Connection from the outside of the network through a "NAT" network is more difficult than a more network because IP addresses of inside hosts are hidden -> C is not correct.

In order for IPsec to work with NAT we need to allow additional protocols, including Internet Key Exchange (IKE), Encapsulating Security Payload (ESP) and Authentication Header (AH) -> more complex -> A is not correct.

By allocating specific public IP addresses to inside hosts, NAT eliminates the need to re-address the inside hosts -> B is correct.

NAT does conserve addresses but not through host MAC-level multiplexing. It conserves addresses by allowing many private IP addresses to use the same public IP address to go to the Internet -> C is not correct.

QUESTION NO: 192

On which options are standard access lists based?

A. destination address and wildcard mask
B. destination address and subnet mask
C. source address and subnet mask
D. source address and wildcard mask

Answer: D
Explanation:
Standard ACL's only examine the source IP address/mask to determine if a match is made.
Extended ACL's examine the source and destination address, as well as port information.

QUESTION NO: 193

A network engineer wants to allow a temporary entry for a remote user with a specific username and password so that the user can access the entire network over the Internet. Which ACL can be used?

A. standard
B. extended
C. dynamic
D. reflexive

Answer: C
Explanation: Explanation
We can use a dynamic access list to authenticate a remote user with a specific username and password. The authentication process is done by the router or a central access server such as a

TACACS+ or RADIUS server. The configuration of dynamic ACL can be read here:
http://www.cisco.com/en/US/tech/tk583/tk822/technologies_tech_note09186a0080094524.shtml

QUESTION NO: 194

How does a DHCP server dynamically assign IP addresses to hosts?

A. Addresses are permanently assigned so that the host uses the same address at all times.
B. Addresses are assigned for a fixed period of time. At the end of the period, a new request for an address must be made, and another address is then assigned.
C. Addresses are leased to hosts. A host will usually keep the same address by periodically contacting the DHCP server to renew the lease.
D. Addresses are allocated after a negotiation between the server and the host to determine the length of the agreement.

Answer: C
Explanation:
DHCP works in a client/server mode and operates like any other client/server relationship. When a PC connects to a DHCP server, the server assigns or leases an IP address to that PC. The PC connects to the network with that leased IP address until the lease expires. The host must contact the DHCP server periodically to extend the lease. This lease mechanism ensures that hosts that move or power off do not hold onto addresses that they do not need. The DHCP server returns these addresses to the address pool and reallocates them as necessary.

QUESTION NO: 195

Refer to the exhibit.

```
Router# show ip dhcp conflict
IP address          Detection method    Detection time
172.16.1.32         Ping                Feb 16 1998 12:28 PM
172.16.1.64         Gratuitous ARP      Feb 23 1998 08:12 AM
```

Which rule does the DHCP server use when there is an IP address conflict?

A. The address is removed from the pool until the conflict is resolved.
B. The address remains in the pool until the conflict is resolved.
C. Only the IP detected by Gratuitous ARP is removed from the pool.
D. Only the IP detected by Ping is removed from the pool.
**E.** The IP will be shown, even after the conflict is resolved.

Answer: A
Explanation:
An address conflict occurs when two hosts use the same IP address. During address assignment, DHCP checks for conflicts using ping and gratuitous ARP. If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.
(Reference: http://www.cisco.com/en/US/docs/ios/12_1/iproute/configuration/guide/1cddhcp.html)

QUESTION NO: 196

Refer to the exhibit.
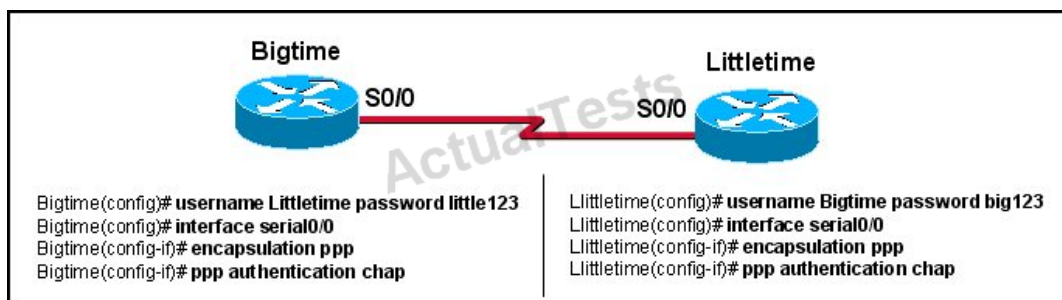
The Bigtime router is unable to authenticate to the Littletime router. What is the cause of the problem?

A. The usernames are incorrectly configured on the two routers.
B. The passwords do not match on the two routers.
C. CHAP authentication cannot be used on a serial interface.
D. The routers cannot be connected from interface S0/0 to interface S0/0.
E. With CHAP authentication, one router must authenticate to another router. The routers cannot be configured to authenticate to each other.

Answer: B
Explanation:
With CHAP authentication, the configured passwords must be identical on each router. Here, it is configured as little123 on one side and big123 on the other.

QUESTION NO: 197

Which two tasks does the Dynamic Host Configuration Protocol perform? (Choose two.)

A. Set the IP gateway to be used by the network.
B. Perform host discovery used DHCPDISCOVER message.
C. Configure IP address parameters from DHCP server to a host.
D. Provide an easy management of layer 3 devices.
E. Monitor IP performance using the DHCP server.
F. Assign and renew IP address from the default pool.

Answer: C,F

Explanation:

The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure devices that are connected to a network (known as hosts) so they can communicate on that network using the Internet Protocol (IP). It involves clients and a server operating in a client-server model. DHCP servers assigns IP addresses from a pool of addresses and also assigns other parameters such as DNS and default gateways to hosts.

QUESTION NO: 198

When a DHCP server is configured, which two IP addresses should never be assignable to hosts? (Choose two.)

A. network or subnetwork IP address
B. broadcast address on the network
C. IP address leased to the LAN
D. IP address used by the interfaces
E. manually assigned address to the clients
F. designated IP address to the DHCP server

Answer: A,B

Explanation: Explanation

Network or subnetwork IP address (for example 11.0.0.0/8 or 13.1.0.0/16) and broadcast address (for example 23.2.1.255/24) should never be assignable to hosts. When try to assign these addresses to hosts, you will receive an error message saying that they can't be assignable.

QUESTION NO: 199

Which two statements about static NAT translations are true? (Choose two.)

A. They allow connections to be initiated from the outside.
B. They require no inside or outside interface markings because addresses are statically defined.
C. They are always present in the NAT table.
D. They can be configured with access lists, to allow two or more connections to be initiated from the outside.

Answer: A,C

Explanation:

Static NAT is to map a single outside IP address to a single inside IP address. This is typically done to allow incoming connections from the outside (Internet) to the inside. Since these are static, they are always present in the NAT table even if they are not actively in use.

Topic 6, Network Device Security

QUESTION NO: 200

A network administrator needs to configure port security on a switch. Which two statements are true? (Choose two.)

A. The network administrator can apply port security to dynamic access ports.
B. The network administrator can apply port security to EtherChannels.
C. When dynamic MAC address learning is enabled on an interface, the switch can learn new addresses, up to the maximum defined.
D. The sticky learning feature allows the addition of dynamically learned addresses to the running configuration.
E. The network administrator can configure static secure or sticky secure MAC addresses in the voice VLAN.

Answer: C,D

Explanation:

Follow these guidelines when configuring port security:

+ Port security can only be configured on static access ports, trunk ports, or 802.1Q tunnel ports.

+ A secure port cannot be a dynamic access port.

+ A secure port cannot be a destination port for Switched Port Analyzer (SPAN).

+ A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.

+ You cannot configure static secure or sticky secure MAC addresses on a voice VLAN.

+ When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to at least two.

+ If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

+ When a voice VLAN is configured on a secure port that is also configured as a sticky secure port, all addresses seen on the voice VLAN are learned as dynamic secure addresses, and all addresses seen on the access VLAN (to which the port belongs) are learned as sticky secure addresses.

+ The switch does not support port security aging of sticky secure MAC addresses.

+ The protect and restrict options cannot be simultaneously enabled on an interface.

(Reference:
http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_19_ea1/config uration/guide/swtrafc.html)

QUESTION NO: 201 DRAG DROP

Drag the security features on the left to the specific security risks they help protect against on the right. (Not all options are used.)	
access-group	remote access to device console
console password	access to the console 0 line
enable secret	access to connected networks or resources
CHAP authentication	viewing of passwords
VTY password	access to privileged mode
service password-encryption	

Answer:

Drag the security features on the left to the specific security risks they help protect against on the right. (Not all options are used.)
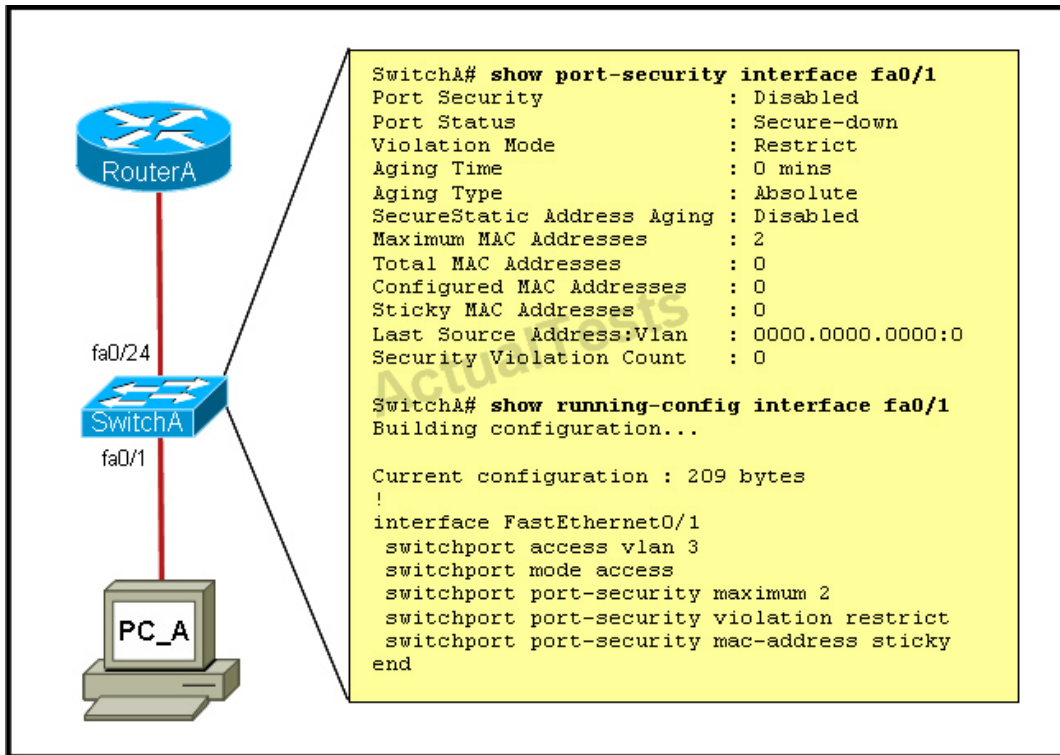
access-group	VTY password
console password	console password
enable secret	access-group
CHAP authentication	service password-encryption
VTY password	enable secret
service password-encryption	

Explanation:

VTY password
console password
access-group
service password-encryption
enable secret

QUESTION NO: 202

Refer to the exhibit.

```
SwitchA# show port-security interface fa0/1
Port Security                : Disabled
Port Status                  : Secure-down
Violation Mode               : Restrict
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 2
Total MAC Addresses          : 0
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0000.0000.0000:0
Security Violation Count     : 0

SwitchA# show running-config interface fa0/1
Building configuration...

Current configuration : 209 bytes
!
interface FastEthernet0/1
 switchport access vlan 3
 switchport mode access
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
end
```

A junior network administrator was given the task of configuring port security on SwitchA to allow only PC_A to access the switched network through port fa0/1. If any other device is detected, the port is to drop frames from this device. The administrator configured the interface and tested it with successful pings from PC_A to RouterA, and then observes the output from these two show commands.

Which two of these changes are necessary for SwitchA to meet the requirements? (Choose two.)

A. Port security needs to be globally enabled.
B. Port security needs to be enabled on the interface.
C. Port security needs to be configured to shut down the interface in the event of a violation.
D. Port security needs to be configured to allow only one learned MAC address.
E. Port security interface counters need to be cleared before using the show command.
F. The port security configuration needs to be saved to NVRAM before it can become active.

Answer: B,D
Explanation:
From the output we can see that port security is disabled so this needs to be enabled. Also, the maximum number of devices is set to 2 so this needs to be just one if we want the single host to have access and nothing else.

QUESTION NO: 203

Which set of commands is recommended to prevent the use of a hub in the access layer?

A. switch(config-if)#switchport mode trunk
switch(config-if)#switchport port-security maximum 1
B. switch(config-if)#switchport mode trunk
switch(config-if)#switchport port-security mac-address 1
C. switch(config-if)#switchport mode access
switch(config-if)#switchport port-security maximum 1
D. switch(config-if)#switchport mode access
switch(config-if)#switchport port-security mac-address 1

Answer: C

Explanation:

This question is to examine the layer 2 security configuration.

In order to satisfy the requirements of this question, you should perform the following
configurations in the interface mode:

First, configure the interface mode as the access mode

Second, enable the port security and set the maximum number of connections to 1.

QUESTION NO: 204

How does using the service password-encryption command on a router provide additional
security?

A. by encrypting all passwords passing through the router
B. by encrypting passwords in the plain text configuration file
C. by requiring entry of encrypted passwords for access to the device
D. by configuring an MD5 encrypted key to be used by routing protocols to validate routing
exchanges
E. by automatically suggesting encrypted passwords for use in configuring the router

Answer: B

Explanation: Explanation

By using this command, all the (current and future) passwords are encrypted. This command is
primarily useful for keeping unauthorized individuals from viewing your password in your
configuration file

QUESTION NO: 205

Refer to the exhibit.

```
ACL 10
Statements are written in this order:
A.  permit any
B.  deny   172.21.1.128 0.0.0.15
C.  permit 172.21.1.129 0.0.0.0
D.  permit 172.21.1.142 0.0.0.0
```

Statements A, B, C, and D of ACL 10 have been entered in the shown order and applied to interface E0 inbound, to prevent all hosts (except those whose addresses are the first and last IP of subnet 172.21.1.128/28) from accessing the network. But as is, the ACL does not restrict anyone from the network. How can the ACL statements be re-arranged so that the system works as intended?

A. ACDB
B. BADC
C. DBAC
D. CDBA

Answer: D
Explanation:
Routers go line by line through an access list until a match is found and then will not look any further, even if a more specific of better match is found later on in the access list. So, it it best to begin with the most specific entries first, in this cast the two hosts in line C and D. Then, include the subnet (B) and then finally the rest of the traffic (A).

QUESTION NO: 206

Refer to the exhibit.

```
ACL 102
access-list 102 deny tcp  172.21.1.1 0.0.0.255 any eq 80
access-list 102 deny ip any any

RouterA#sho ip int
FastEthernet0/0 is up , line protocol is up
  Internet address is 192.168.1.144/20
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is 102
  Inbound  access list is not set
  Proxy ARP is enabled
```

An attempt to deny web access to a subnet blocks all traffic from the subnet. Which interface command immediately removes the effect of ACL 102?

A. no ip access-class 102 in
B. no ip access-class 102 out
C. no ip access-group 102 in
D. no ip access-group 102 out
E. no ip access-list 102 in

Answer: D
Explanation:
The "ip access-group" is used to apply and ACL to an interface. From the output shown, we know that the ACL is applied to outbound traffic, so "no ip access-group 102 out" will remove the effect of this ACL.

QUESTION NO: 207

Which Cisco Catalyst feature automatically disables the port in an operational PortFast upon receipt of a BPDU?

A. BackboneFast
B. UplinkFast
C. Root Guard

D. BPDU Guard
E. BPDU Filter

Answer: D

Explanation: Explanation

We only enable PortFast feature on access ports (ports connected to end stations). But if someone does not know he can accidentally plug that port to another switch and a loop may occur when BPDUs are being transmitted and received on these ports.

With BPDU Guard, when a PortFast receives a BPDU, it will be shut down to prevent a loop.

QUESTION NO: 208

When you are troubleshooting an ACL issue on a router, which command would you use to verify which interfaces are affected by the ACL?

A. show ip access-lists
B. show access-lists
C. show interface
D. show ip interface
E. list ip interface

Answer: D

Explanation:

Incorrect answer:

show ip access-lists does not show interfaces affected by an ACL.

QUESTION NO: 209 CORRECT TEXT

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.
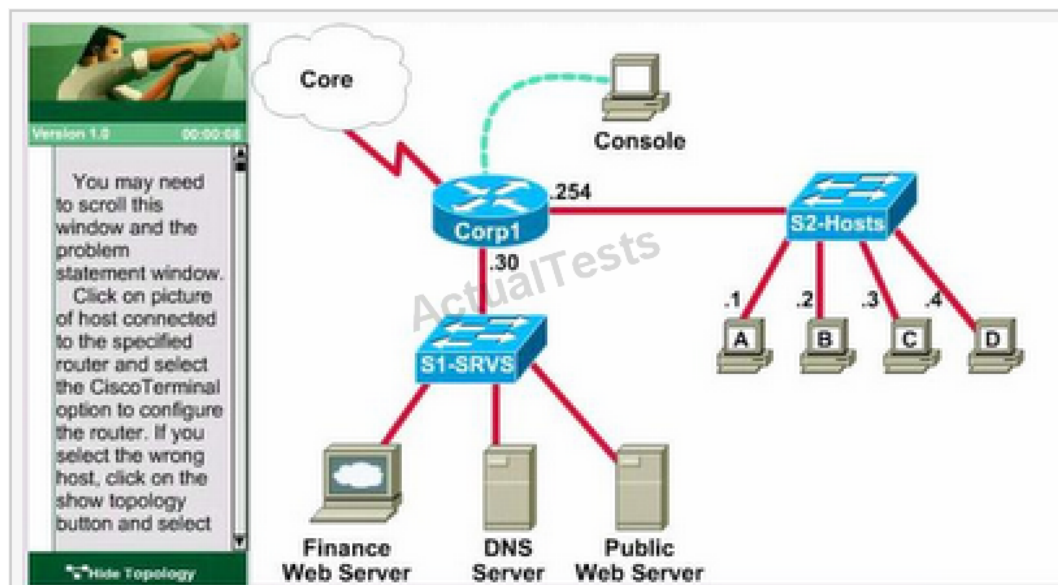
All passwords have been temporarily set to "cisco".

The Core connection uses an IP address of 198.18.196.65

The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254

Host A 192.168.33.1

Host B 192.168.33.2

Host C 192.168.33.3

Host D 192.168.33.4

The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30

The Finance Web Server is assigned an IP address of 172.22.242.23.

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".
The Core connection uses an IP address of 198.18.196.65
The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254.
   o   host A 192.168.33.1
   o   host B 192.168.33.2
   o   host C 192.168.33.3
   o   host D 192.168.33.4
The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30
The Finance Web Server is assigned an IP address of 172.22.242.23

Answer: Select the console on Corp1 router

Configuring ACL

Corp1>enable

Corp1#configure terminal

comment: To permit only Host C (192.168.33.3){source addr} to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)

Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80

comment: To deny any source to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)

Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80

comment: To permit ip protocol from any source to access any destination because of the implicit deny any any statement at the end of ACL.

Corp1(config)#access-list 100 permit ip any any

Applying the ACL on the Interface

comment: Check show ip interface brief command to identify the interface type and number by checking the IP address configured.

Corp1(config)#interface fa 0/1

If the ip address configured already is incorrect as well as the subnet mask. this should be corrected in order ACL to work

type this commands at interface mode :

no ip address 192.x.x.x 255.x.x.x (removes incorrect configured ipaddress and subnet mask)

Configure Correct IP Address and subnet mask :

ip address 172.22.242.30 255.255.255.240 (range of address specified going to server is given as 172.22.242.17 - 172.22.242.30)

Comment: Place the ACL to check for packets going outside the interface towards the finance web server.

Corp1(config-if)#ip access-group 100 out

Corp1(config-if)#end

Important: To save your running config to startup before exit.

Corp1#copy running-config startup-config

Verifying the Configuration:

Step1: show ip interface brief command identifies the interface on which to apply access list.

Step2: Click on each host A, B, C, & D. Host opens a web browser page, Select address box of the web browser and type the ip address of finance web server (172.22.242.23) to test whether it permits /deny access to the finance web Server.

Step 3: Only Host C (192.168.33.3) has access to the server. If the other host can also access then maybe something went wrong in your configuration. Check whether you configured correctly and in order.

Step 4: If only Host C (192.168.33.3) can access the Finance Web Server you can click on NEXT button to successfully submit the ACL SIM.

QUESTION NO: 210

Refer to exhibit.

```
Router#show running-config
Building configuration...

Current configuration : 659 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!

enable secret 5 $1$mERr$hx5rvt7rPNoS4wqbXKX7m0
!

interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 in
 duplex auto
 speed auto
!
access-list 101 deny tcp any any eq 22
access-list 101 permit ip any any
!
line con 0
 password 7 0822455D0A16
 login
line vty 0 4
 login
line vty 5 14
 login|
!
end
```

A network administrator cannot establish a Telnet session with the indicated router. What is the cause of this failure?

A. A Level 5 password is not set.
B. An ACL is blocking Telnet access.
C. The vty password is missing.
D. The console password is missing.

Answer: C

Explanation:

The login keyword has been set, but not password. This will result in the "password required, but none set" message to users trying to telnet to this router.

QUESTION NO: 211

Which statement about access lists that are applied to an interface is true?

A. You can place as many access lists as you want on any interface.
B. You can apply only one access list on any interface.
C. You can configure one access list, per direction, per Layer 3 protocol.
D. You can apply multiple access lists with the same protocol or in different directions.

Answer: C

Explanation:

We can have only 1 access list per protocol, per direction and per interface. It means:

+ We can not have 2 inbound access lists on an interface

+ We can have 1 inbound and 1 outbound access list on an interface

QUESTION NO: 212

Which item represents the standard IP ACL?

A. access-list 110 permit ip any any
B. access-list 50 deny 192.168.1.1 0.0.0.255
C. access list 101 deny tcp any host 192.168.1.1
D. access-list 2500 deny tcp any host 192.168.1.1 eq 22

Answer: B

Explanation: Explanation

The standard access lists are ranged from 1 to 99 and from 1300 to 1999 so only access list 50 is a standard access list.

QUESTION NO: 213

A network administrator is configuring ACLs on a Cisco router, to allow traffic from hosts on networks 192.168.146.0, 192.168.147.0, 192.168.148.0, and 192.168.149.0 only. Which two ACL statements, when combined, would you use to accomplish this task? (Choose two.)

A. access-list 10 permit ip 192.168.146.0 0.0.1.255
B. access-list 10 permit ip 192.168.147.0 0.0.255.255
C. access-list 10 permit ip 192.168.148.0 0.0.1.255
D. access-list 10 permit ip 192.168.149.0 0.0.255.255
E. access-list 10 permit ip 192.168.146.0 0.0.0.255
F. access-list 10 permit ip 192.168.146.0 255.255.255.0

Answer: A,C

Explanation:

"access-list 10 permit ip 192.168.146.0 0.0.1.255" would allow only the 192.168.146.0 and 192.168.147.0 networks, and "access-list 10 permit ip 192.168.148.0 0.0.1.255" would allow only the 192.168.148.0 and 192.168.149.0 networks.

QUESTION NO: 214

What can be done to secure the virtual terminal interfaces on a router? (Choose two.)

A. Administratively shut down the interface.
B. Physically secure the interface.
C. Create an access list and apply it to the virtual terminal interfaces with the access-group command.
D. Configure a virtual terminal password and login process.
E. Enter an access list and apply it to the virtual terminal interfaces using the access-class command.

Answer: D,E

Explanation: Explanation

It is a waste to administratively shut down the interface. Moreover, someone can still access the virtual terminal interfaces via other interfaces ->

We can not physically secure a virtual interface because it is "virtual" ->

To apply an access list to a virtual terminal interface we must use the "access-class" command. The "access-group" command is only used to apply an access list to a physical interface -> C is not correct.

The most simple way to secure the virtual terminal interface is to configure a username & password to prevent unauthorized login.

QUESTION NO: 215
Which two commands correctly verify whether port security has been configured on port

FastEthernet 0/12 on a switch? (Choose two.)

A. SW1#show port-secure interface FastEthernet 0/12
B. SW1#show switchport port-secure interface FastEthernet 0/12
C. SW1#show running-config
D. SW1#show port-security interface FastEthernet 0/12
E. SW1#show switchport port-security interface FastEthernet 0/12

Answer: C,D

Explanation: Explanation

We can verify whether port security has been configured by using the "show running-config" or "show port-security interface " for more detail. An example of the output of "show port-security interface " command is shown below:

```
Switch# show port-security interface fa0/12
Port Security               : Enabled
Port Status                 : Secure-down
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 2
```

QUESTION NO: 216

Refer to the exhibit.
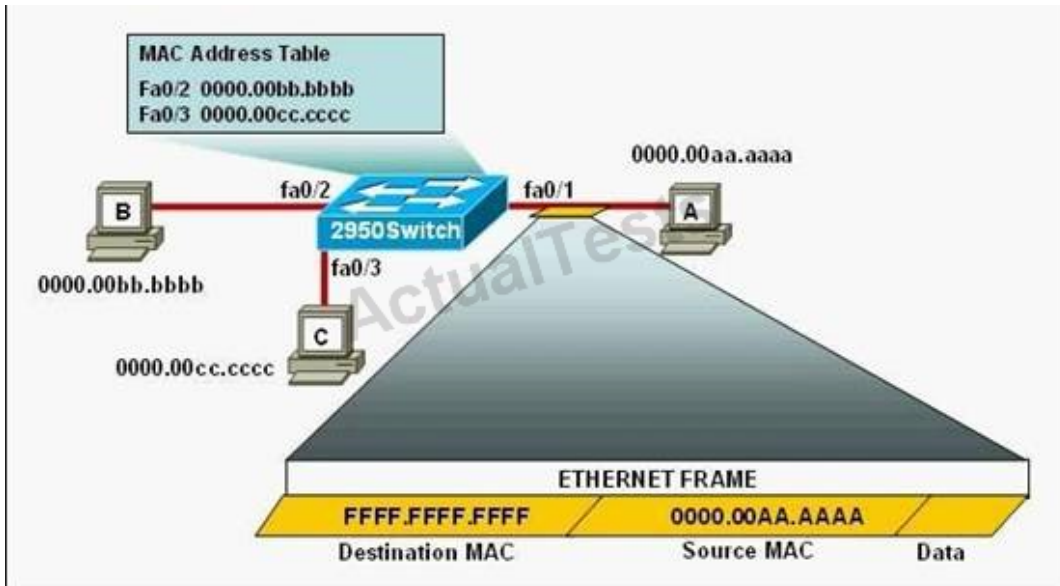
The following commands are executed on interface fa0/1 of 2950Switch.

2950Switch(config-if)# switchport port-security

2950Switch(config-if)# switchport port-security mac-address sticky

2950Switch(config-if)# switchport port-security maximum 1

The Ethernet frame that is shown arrives on interface fa0/1. What two functions will occur when this frame is received by 2950Switch? (Choose two.)

A. The MAC address table will now have an additional entry of fa0/1 FFFF.FFFF.FFFF.
B. Only host A will be allowed to transmit frames on fa0/1.
C. This frame will be discarded when it is received by 2950Switch.
D. All frames arriving on 2950Switch with a destination of 0000.00aa.aaaa will be forwarded out fa0/1.
E. Hosts B and C may forward frames out fa0/1 but frames arriving from other switches will not be forwarded out fa0/1.
F. Only frames from source 0000.00bb.bbbb, the first learned MAC address of 2950Switch, will be forwarded out fa0/1.

Answer: B,D
Explanation:
The configuration shown here is an example of port security, specifically port security using sticky addresses. You can use port security with dynamically learned and static MAC addresses to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. When you assign secure MAC addresses to a secure port, the port does not forward

ingress traffic that has source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the device attached to that port has the full bandwidth of the port.

Port security with sticky MAC addresses provides many of the same benefits as port security with static MAC addresses, but sticky MAC addresses can be learned dynamically. Port security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down condition.

QUESTION NO: 217

What will be the result if the following configuration commands are implemented on a Cisco switch?

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security mac-address sticky

A. A dynamically learned MAC address is saved in the startup-configuration file.
B. A dynamically learned MAC address is saved in the running-configuration file.
C. A dynamically learned MAC address is saved in the VLAN database.
D. Statically configured MAC addresses are saved in the startup-configuration file if frames from that address are received.
E. Statically configured MAC addresses are saved in the running-configuration file if frames from that address are received.

Answer: B
Explanation:
In the interface configuration mode, the command switchport port-security mac-address sticky enables sticky learning. When entering this command, the interface converts all the dynamic secure MAC addresses to sticky secure MAC addresses.

Topic 7, Troubleshooting

QUESTION NO: 218 DRAG DROP

Drag each category on the left to its corresponding router output line on the right. Each router output line is the result of a **show ip interface** command. Not all categories are used.

Layer 1 problem	Serial0/1 is up, line protocol is up
Layer 2 problem	Serial0/1 is up, line protocol is down
Layer 3 problem	Serial0/1 is down, line protocol is down
port operational	Serial0/1 is administratively down, line protocol is down
port disabled	

Answer:

Drag each category on the left to its corresponding router output line on the right. Each router output line is the result of a **show ip interface** command. Not all categories are used.

Layer 1 problem	port operational
Layer 2 problem	Layer 2 problem
Layer 3 problem	Layer 1 problem
port operational	port disabled
port disabled	

Explanation:

port operational
Layer 2 problem
Layer 1 problem
port disabled

A simple way to find out which layer is having problem is to remember this rule: "the first statement is for Layer 1, the last statement is for Layer 2 and if Layer 1 is down then surely Layer 2 will be down too", so you have to check Layer 1 before checking Layer 2. For example, from the output "Serial0/1 is up, line protocol is down" we know that it is a layer 2 problem because the first statement (Serial0/1 is up) is good while the last statement (line protocol is down) is bad. For the statement "Serial0/1 is down, line protocol is down", both layers are down so the problem belongs to Layer 1.

There is only one special case with the statement "…. is administrator down, line protocol is down". In this case, we know that the port is currently disabled and shut down by the administrators.

QUESTION NO: 219 DRAG DROP

A user is unable to connect to the Internet. Based on the layered approach to troubleshooting and beginning with the lowest layer, drag each procedure on the left to its proper category on the right.	
verify URL	Step 1
verify NIC operation	Step 2
verify IP configuration	Step 3
verify Ethernet cable connection	Step 4

Answer:

A user is unable to connect to the Internet. Based on the layered approach to troubleshooting and beginning with the lowest layer, drag each procedure on the left to its proper category on the right.	
verify URL	verify Ethernet cable connection
verify NIC operation	verify NIC operation
verify IP configuration	verify IP configuration
verify Ethernet cable connection	verify URL

Explanation:

verify Ethernet cable connection
verify NIC operation
verify IP configuration
verify URL

The question asks us to "begin with the lowest layer" so we have to begin with Layer 1: verify physical connection; in this case an Ethernet cable connection. For your information, "verify Ethernet cable connection" means that we check if the type of connection (crossover, straight-through, rollover…) is correct, the RJ45 headers are plugged in, the signal on the cable is acceptable…

Next we "verify NIC operation". We do this by simply making a ping to the loopback interface 127.0.0.1. If it works then the NIC card (layer 1, 2) and TCP/IP stack (layer 3) are working properly.

Verify IP configuration belongs to layer 3. For example, checking if the IP can be assignable for host, the PC's IP is in the same network with the gateway…

Verifying the URL by typing in your browser some popular websites like google.com, microsoft.com to assure that the far end server is not down (it sometimes make we think we can't access to the Internet). We are using a URL so this step belongs to layer 7 of the OSI model.

QUESTION NO: 220

Refer to the exhibit.
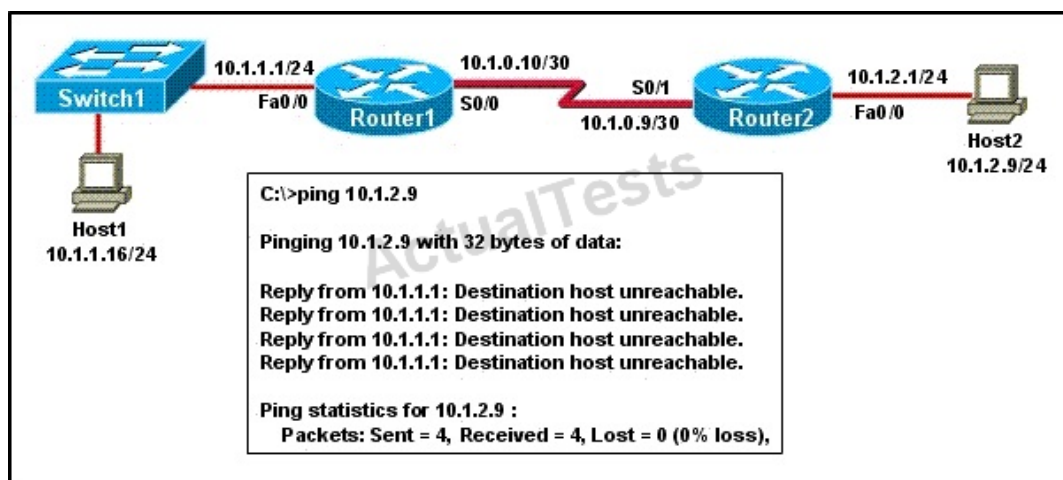
A network administrator attempts to ping Host2 from Host1 and receives the results that are shown. What is the problem?

A. The link between Host1 and Switch1 is down.
B. TCP/IP is not functioning on Host1
C. The link between Router1 and Router2 is down.
D. The default gateway on Host1 is incorrect.
E. Interface Fa0/0 on Router1 is shutdown.
F. The link between Switch1 and Router1 is down.

Answer: C
Explanation:
Host1 tries to communicate with Host2. The message destination host unreachable from Router1 indicates that the problem occurs when the data is forwarded from Host1 to Host2. According to the topology, we can infer that the link between Router1 and Router2 is down.

QUESTION NO: 221

Refer to the exhibit.


```
RouterA# show ip interface brief
Interface        IP-Address    OK?  Method Status               Protocol
FastEthernet0/0  192.168.2.1   YES  manual up                   up
Serial0/0        192.168.1.5   YES  manual up                   down
Serial0/1        unassigned    YES  manual administratively down down
```
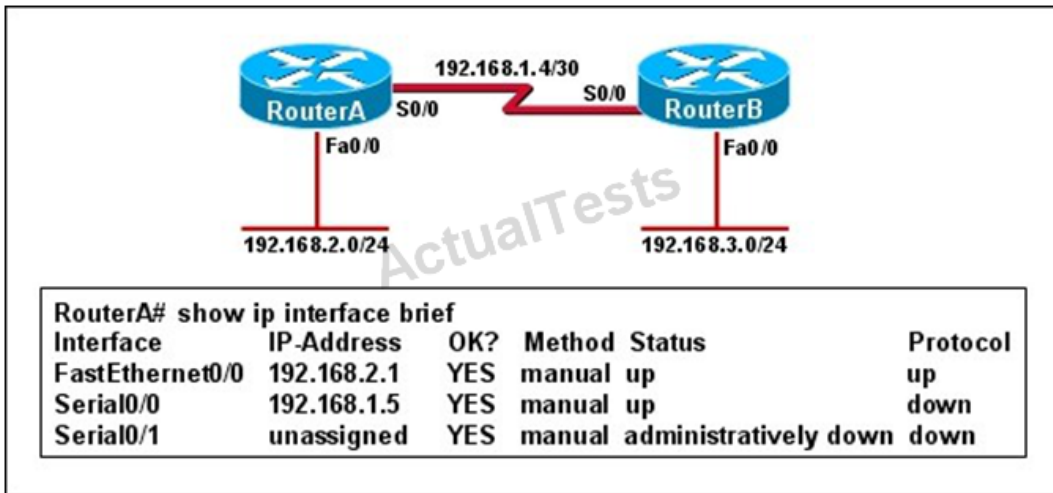
Hosts in network 192.168.2.0 are unable to reach hosts in network 192.168.3.0. Based on the output from RouterA, what are two possible reasons for the failure? (Choose two.)

A. The cable that is connected to S0/0 on RouterA is faulty.
B. Interface S0/0 on RouterB is administratively down.
C. Interface S0/0 on RouterA is configured with an incorrect subnet mask.
D. The IP address that is configured on S0/0 of RouterB is not in the correct subnet.
E. Interface S0/0 on RouterA is not receiving a clock signal from the CSU/DSU.
F. The encapsulation that is configured on S0/0 of RouterB does not match the encapsulation that is configured on S0/0 of RouterA.

Answer: E,F
Explanation:
From the output we can see that there is a problem with the Serial 0/0 interface. It is enabled, but the line protocol is down. The could be a result of mismatched encapsulation or the interface not receiving a clock signal from the CSU/DSU.

QUESTION NO: 222

Refer to the exhibit.

```
C:\> ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.10.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

An administrator pings the default gateway at 10.10.10.1 and sees the output as shown. At which OSI layer is the problem?

A. data link layer
B. application layer
C. access layer
D. session layer
E. network layer

Answer: E

Explanation:

The command ping uses ICMP protocol, which is a network layer protocol used to propagate control message between host and router. The command ping is often used to verify the network connectivity, so it works at the network layer.

QUESTION NO: 223

Refer to the exhibit.
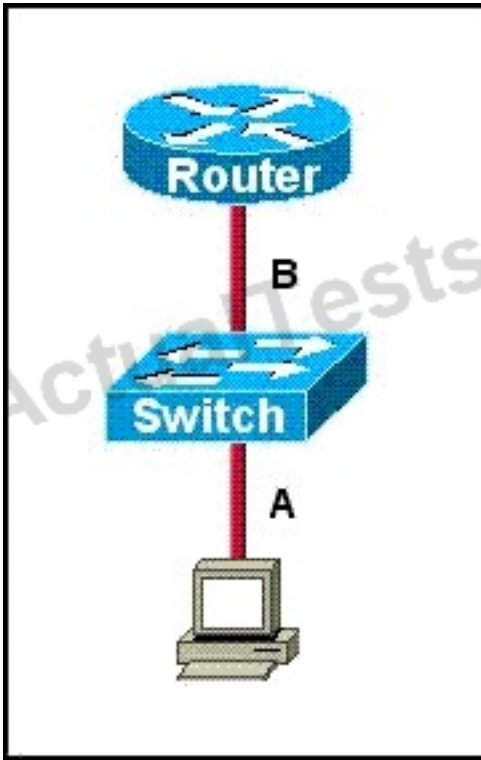
The two connected ports on the switch are not turning orange or green. What would be the most effective steps to troubleshoot this physical layer problem? (Choose three.)

A. Ensure that the Ethernet encapsulations match on the interconnected router and switch ports.
B. Ensure that cables A and B are straight-through cables.
C. Ensure cable A is plugged into a trunk port.
D. Ensure the switch has power.
E. Reboot all of the devices.
F. Reseat all cables.

Answer: B,D,F

Explanation: Explanation
The ports on the switch are not up indicating it is a layer 1 (physical) problem so we should check cable type, power and how they are plugged in.

QUESTION NO: 224

Refer to the exhibit.
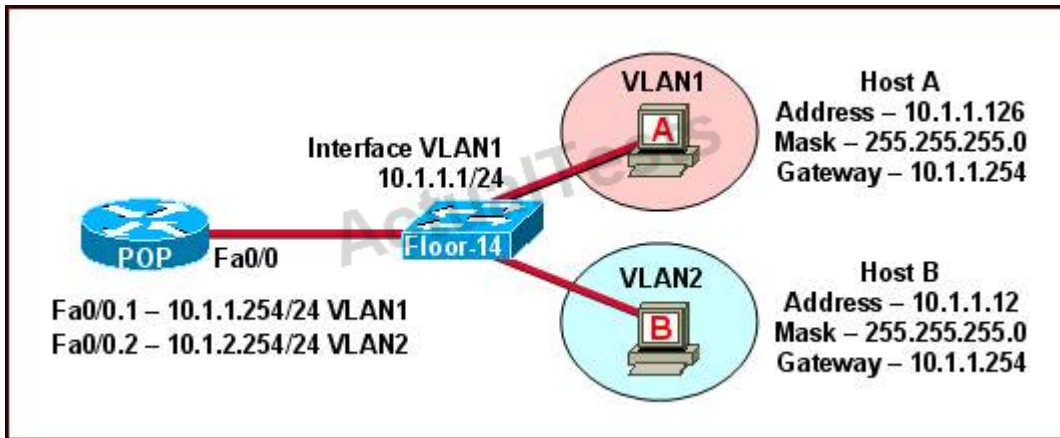
The network shown in the diagram is experiencing connectivity problems. Which of the following will correct the problems? (Choose two.)

A. Configure the gateway on Host A as 10.1.1.1.
B. Configure the gateway on Host B as 10.1.2.254.
C. Configure the IP address of Host A as 10.1.2.2.
D. Configure the IP address of Host B as 10.1.2.2.
E. Configure the masks on both hosts to be 255.255.255.224.
F. Configure the masks on both hosts to be 255.255.255.240.

Answer: B,D

Explanation:

The switch 1 is configured with two VLANs: VLAN1 and VLAN2.

The IP information of member Host A in VLAN1 is as follows:

Address : 10.1.1.126

Mask : 255.255.255.0

Gateway : 10.1.1.254

The IP information of member Host B in VLAN2 is as follows:

Address : 10.1.1.12

Mask : 255.255.255.0

Gateway : 10.1.1.254

The configuration of sub-interface on router 2 is as follows:

Fa0/0.1 -- 10.1.1.254/24 VLAN1

Fa0/0.2 -- 10.1.2.254/24 VLAN2

It is obvious that the configurations of the gateways of members in VLAN2 and the associated network segments are wrong. The layer3 addressing information of Host B should be modified as follows:

Address : 10.1.2.X

Mask : 255.255.255.0

QUESTION NO: 225

Refer to the exhibit.
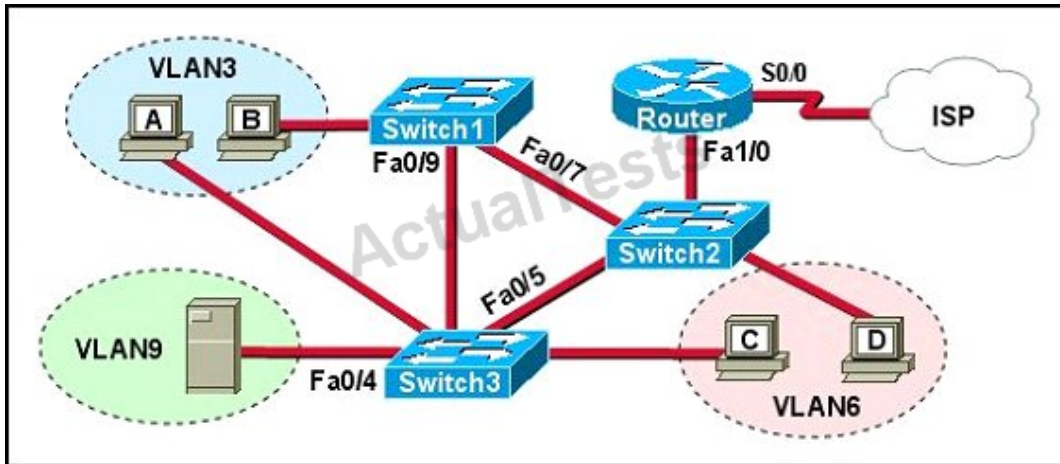
A problem with network connectivity has been observed. It is suspected that the cable connected to switch port Fa0/9 on Switch1 is disconnected. What would be an effect of this cable being disconnected?

A. Host B would not be able to access the server in VLAN9 until the cable is reconnected.
B. Communication between VLAN3 and the other VLANs would be disabled.
C. The transfer of files from Host B to the server in VLAN9 would be significantly slower.
D. For less than a minute, Host B would not be able to access the server in VLAN9. Then normal network function would resume.

Answer: D
Explanation:
Spanning-Tree Protocol (STP) is a Layer 2 protocol that utilizes a special-purpose algorithm to discover physical loops in a network and effect a logical loop-free topology. STP creates a loop-free tree structure consisting of leaves and branches that span the entire Layer 2 network. The actual mechanics of how bridges communicate and how the STP algorithm works will be discussed at length in the following topics. Note that the terms bridge and switch are used interchangeably when discussing STP. In addition, unless otherwise indicated, connections between switches are assumed to be trunks.

QUESTION NO: 226

Refer to the exhibit.
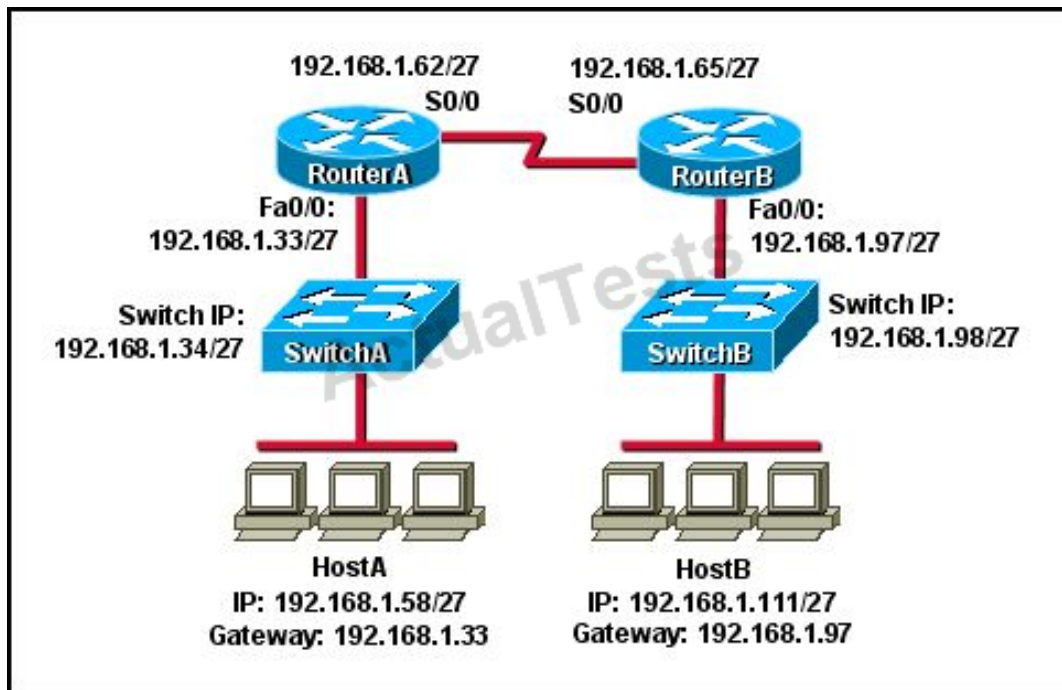
HostA cannot ping HostB. Assuming routing is properly configured, what is the cause of this problem?

A. HostA is not on the same subnet as its default gateway.
B. The address of SwitchA is a subnet address.
C. The Fa0/0 interface on RouterA is on a subnet that can't be used.
D. The serial interfaces of the routers are not on the same subnet.
E. The Fa0/0 interface on RouterB is using a broadcast address.

Answer: D

Explanation: Explanation

Now let's find out the range of the networks on serial link:

For the network 192.168.1.62/27:

Increment: 32

Network address: 192.168.1.32

Broadcast address: 192.168.1.63

For the network 192.168.1.65/27:

Increment: 32

Network address: 192.168.1.64

Broadcast address: 192.168.1.95

-> These two IP addresses don't belong to the same network and they can't see each other

QUESTION NO: 227

Which router IOS commands can be used to troubleshoot LAN connectivity problems? (Choose three.)

A. ping
B. tracert
C. ipconfig
D. show ip route
E. winipcfg
F. show interfaces

Answer: A,D,F

Explanation:

Ping, show ip route, and show interfaces are all valid troubleshooting IOS commands. Tracert, ipconfig, and winipcfg are PC commands, not IOS.

QUESTION NO: 228

A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common Ethernet link.

```
R1:    Ethernet0 is up, line protocol is up
       Internet address 192.168.1.2/24, Area 0
       Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 10
       Transmit Delay is 1 sec, State DR, Priority 1
       Designated Router (ID) 192.168.31.33, Interface address 192.168.1.2
       No backup designated router on this network
       Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5

R2:    Ethernet0 is up, line protocol is up
       Internet address 192.168.1.1/24, Area 0
       Process ID 2, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 10
       Transmit Delay is 1 sec, State DR, Priority 1
       Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
       No backup designated router on this network
       Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

The graphic shows the output of the show ip ospf interface e0 command for routers R1 and R2. Based on the information in the graphic, what is the cause of this problem?

A. The OSPF area is not configured properly.
B. The priority on R1 should be set higher.
C. The cost on R1 should be set higher.

D. The hello and dead timers are not configured properly.

E. A backup designated router needs to be added to the network.

F. The OSPF process ID numbers must match.

Answer: D

Explanation:

In OSPF, the hello and dead intervals must match and here we can see the hello interval is set to 5 on R1 and 10 on R2. The dead interval is also set to 20 on R1 but it is 40 on R2.

QUESTION NO: 229

In which circumstance are multiple copies of the same unicast frame likely to be transmitted in a switched LAN?

A. during high traffic periods

B. after broken links are re-established

C. when upper-layer protocols require high reliability

D. in an improperly implemented redundant topology

E. when a dual ring topology is in use

Answer: D

Explanation: Explanation

If we connect two switches via 2 or more links and do not enable STP on these switches then a loop (which creates multiple copies of the same unicast frame) will occur. It is an example of an improperly implemented redundant topology.

QUESTION NO: 230

Instructions

An administrator is trying to ping and telnet from SwitchC to RouterC with the results shown below.

SwitchC>
SwitchC> ping 10.4.4.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.3, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
SwitchC>
SwitchC> telnet 10.4.4.3
Trying 10.4.4.3 ...
% Destination unreachable; gateway or host down
SwitchC>

Click the console connected to RouterC and issue the appropriate commands to answer the questions.

Topology

```
RouterC
```

```
Press RETURN to get started!
RouterC>
```

```
<output omitted>

interface Loopback1
 ip address 172.16.4.1.255.255.255.0
!
interface Loopback2
 ip address 10.145.145.1  255.255.255.0
 ipv6 address 2001:410:2:3::/64 eui-64
!
interface FastEthernet0/0
 ip address 10.4.4.3.255.255.255.0
 ip access-group 106 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
speed auto
!
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 ip ospf authentication
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.3.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serail0/0/1
 bandwidth 64
 ip address 10.45.45.1 255.255.255.0
 ip access-group 102 in
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
```

```
router eigrp 100
  network 10.0.0.0
  network 172.16.0.0
  network 192.168.2.0
  not auto-summary
!
router ospf 100
  log-adjacency-changes
  network 10.4.4.3 0.0.0.0 area 0
  network 10.45.45.1 0.0.0.0 area 0
  network 10.140.3.2 0.0.0.0 area 0
  network 192.168.2.62 0.0.0.0 area 0
!
router rip
  version 2
  network 10.0.0.0
  network 172.16.0.0
!
ip default-gateway 10.1.1.2
!
!
ip http server
no ip http secure-server
!
```

```
access-list 102 permit tcp any any eq ftp
access-list 102 permit tcp any any eq ftp-data
access-list 102 deny tcp any any eq telnet
access-list 102 deny icmp any any echo-reply
access-list 102 permit ip any any


access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 deny icmp any any echo-reply
access-list 104 permit ip any any


access-list 106 permit tcp any any eq ftp
access-list 106 permit tcp any any ftp-data
access-list 106 deny tcp any any eq telnet
access-list 106 permit icmp any any echo-reply
access-list 110 permit udp any any eq domain
access-list 110 permit udp any eq domain any
access-list 110 permit tcp any any eq domain
access-list 110 permit tcp any eq domain any
access-list 110 permit tcp any any


access-list 114 permit ip 10.4.4.0.0.0.0.255 any


access-list 115 permit ip 0.0.0.0 255.255.255.0 any


access-list 122 deny tcp any any
access-list 122 deny imp any any echo-reply
access-list 122 permit ip any any
!
<output omitted>
```

Which will fix the issue and allow ONLY ping to work while keeping telnet disabled?

A. Correctly assign an IP address to interface fa0/1.
B. Change the ip access-group command on fa0/0 from "in* to "out.

C. Remove access-group 106 in from interface fa0/0 and add access-group 115 in.

D. Remove access-group 102 out from interface s0/0/0 and add access-group 114 in

E. Remove access-group 106 in from interface fa0/0 and add access-group 104 in.

Answer: E

Explanation:

Let's have a look at the access list 104:

```
access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telent
access-list 104 permit icmp any any echo
access-list 104 permit icmp any any echo-reply
access-list 104 permit ip any any
```

The question does not ask about ftp traffic so we don't care about the two first lines. The 3rd line denies all telnet traffic and the 4th line allows icmp traffic to be sent (ping). Remember that the access list 104 is applied on the inbound direction so the 5th line "access-list 104 deny icmp any any echo-reply" will not affect our icmp traffic because the "echo-reply" message will be sent over the outbound direction.

QUESTION NO: 231

Instructions

An administrator is trying to ping and telnet from SwitchC to RouterC with the results shown below.

```
SwitchC>
SwitchC> ping 10.4.4.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.3, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
SwitchC>
SwitchC> telnet 10.4.4.3
Trying 10.4.4.3 ...
% Destination unreachable; gateway or host down
SwitchC>
```

Click the console connected to RouterC and issue the appropriate commands to answer the questions.

Topology

RouterC

```
Press RETURN to get started!
RouterC>
```

```
<output omitted>

interface Loopback1
 ip address 172.16.4.1.255.255.255.0
!
interface Loopback2
 ip address 10.145.145.1  255.255.255.0
 ipv6 address 2001:410:2:3::/64 eui-64
!
interface FastEthernet0/0
 ip address 10.4.4.3.255.255.255.0
 ip access-group 106 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
speed auto
!
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 ip ospf authentication
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.3.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serail0/0/1
 bandwidth 64
 ip address 10.45.45.1 255.255.255.0
 ip access-group 102 in
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
```

```
router eigrp 100
  network 10.0.0.0
  network 172.16.0.0
  network 192.168.2.0
  not auto-summary
!
router ospf 100
  log-adjacency-changes
  network 10.4.4.3 0.0.0.0 area 0
  network 10.45.45.1 0.0.0.0 area 0
  network 10.140.3.2 0.0.0.0 area 0
  network 192.168.2.62 0.0.0.0 area 0
!
router rip
  version 2
  network 10.0.0.0
  network 172.16.0.0
!
ip default-gateway 10.1.1.2
!
!
ip http server
no ip http secure-server
!
```

```
access-list 102 permit tcp any any eq ftp
access-list 102 permit tcp any any eq ftp-data
access-list 102 deny tcp any any eq telnet
access-list 102 deny icmp any any echo-reply
access-list 102 permit ip any any


access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 deny icmp any any echo-reply
access-list 104 permit ip any any


access-list 106 permit tcp any any eq ftp
access-list 106 permit tcp any any ftp-data
access-list 106 deny tcp any any eq telnet
access-list 106 permit icmp any any echo-reply
access-list 110 permit udp any any eq domain
access-list 110 permit udp any eq domain any
access-list 110 permit tcp any any eq domain
access-list 110 permit tcp any eq domain any
access-list 110 permit tcp any any


access-list 114 permit ip 10.4.4.0.0.0.0.255 any


access-list 115 permit ip 0.0.0.0 255.255.255.0 any


access-list 122 deny tcp any any
access-list 122 deny imp any any echo-reply
access-list 122 permit ip any any
!
<output omitted>
```

What would be the effect of issuing the command ip access-group 114 in to the fa0/0 interface?

A. Attempts to telnet to the router would fail.

B. It would allow all traffic from the 10.4.4.0 network.

C. IP traffic would be passed through the interface but TCP and UDP traffic would not.

D. Routing protocol updates for the 10.4.4.0 network would not be accepted from the fa0/0 interface.

Answer: B

Explanation:

From the output of access-list 114: access-list 114 permit ip 10.4.4.0 0.0.0.255 any we can easily understand that this access list allows all traffic (ip) from 10.4.4.0/24 network

QUESTION NO: 232

Instructions

An administrator is trying to ping and telnet from SwitchC to RouterC with the results shown below.

SwitchC>
SwitchC> ping 10.4.4.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.3, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
SwitchC>
SwitchC> telnet 10.4.4.3
Trying 10.4.4.3 ...
% Destination unreachable; gateway or host down
SwitchC>

Click the console connected to RouterC and issue the appropriate commands to answer the questions.

Topology

```
RouterC

Press RETURN to get started!
RouterC>
```

```
<output omitted>

interface Loopback1
  ip address 172.16.4.1.255.255.255.0
!
interface Loopback2
  ip address 10.145.145.1  255.255.255.0
  ipv6 address 2001:410:2:3::/64 eui-64
!
interface FastEthernet0/0
  ip address 10.4.4.3.255.255.255.0
  ip access-group 106 in
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
 speed auto
!
interface Serial0/0/0
  bandwidth 64
  no ip address
  ip access-group 102 out
  encapsulation frame-relay
  ip ospf authentication
  ip ospf authentication
  ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
  ip address 10.140.3.2 255.255.255.0
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 icndchain
  frame-relay interface-dlci 120
!
interface Serail0/0/1
  bandwidth 64
  ip address 10.45.45.1 255.255.255.0
  ip access-group 102 in
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 icndchain
```

```
router eigrp 100
  network 10.0.0.0
  network 172.16.0.0
  network 192.168.2.0
  not auto-summary
!
router ospf 100
  log-adjacency-changes
  network 10.4.4.3 0.0.0.0 area 0
  network 10.45.45.1 0.0.0.0 area 0
  network 10.140.3.2 0.0.0.0 area 0
  network 192.168.2.62 0.0.0.0 area 0
!
router rip
  version 2
  network 10.0.0.0
  network 172.16.0.0
!
ip default-gateway 10.1.1.2
!
!
ip http server
no ip http secure-server
!
```

```
access-list 102 permit tcp any any eq ftp
access-list 102 permit tcp any any eq ftp-data
access-list 102 deny tcp any any eq telnet
access-list 102 deny icmp any any echo-reply
access-list 102 permit ip any any


access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 deny icmp any any echo-reply
access-list 104 permit ip any any


access-list 106 permit tcp any any eq ftp
access-list 106 permit tcp any any ftp-data
access-list 106 deny tcp any any eq telnet
access-list 106 permit icmp any any echo-reply

access-list 110 permit udp any any eq domain
access-list 110 permit udp any eq domain any
access-list 110 permit tcp any any eq domain
access-list 110 permit tcp any eq domain any
access-list 110 permit tcp any any


access-list 114 permit ip 10.4.4.0.0.0.0.255 any


access-list 115 permit ip 0.0.0.0 255.255.255.0 any


access-list 122 deny tcp any any
access-list 122 deny imp any any echo-reply
access-list 122 permit ip any any
!
<output omitted>
```

What would be the effect of Issuing the command ip access-group 115 in on the s0/0/1 interface?

- No host could connect to RouterC through s0/0/1.

A. Telnet and ping would work but routing updates would fail.

B. FTP, FTP-DATA, echo, and www would work but telnet would fail.

C. Only traffic from the 10.4.4.0 network would pass through the interface.

Answer: A

Explanation:

First let's see what was configured on interface S0/0/1:

```
interface Serial0/0/1
  bandwidth 64
  ip address 10.45.45.1 255.255.255.0
  ip access-group 102 in
```

QUESTION NO: 233 CORRECT TEXT

CCNA.com has a small network that is using EIGRP as its IGP. All routers should be running an EIGRP AS number of 12. Router MGT is also running static routing to the ISP.

CCNA.com has recently adding the ENG router. Currently, the ENG router does not have connectivity to the ISP router. All other interconnectivity and Internet access for the existing locations of the company are working properly.

The task is to identify the fault(s) and correct the router configuration(s) to provide full connectivity between the routers.

Access to the router CLI can be gained by clicking on the appropriate host.
All passwords on all routers are **cisco**.
IP addresses are listed in the chart below.
MGT
Fa0/0 - 192.168.77.33
S1/0 - 198.0.18.6
S0/0 - 192.168.27.9
S0/1 - 192.168.50.21

ENG
Fa0/0 - 192.168.77.34
Fa1/0 - 192.168.12.17
Fa0/1 - 192.168.12.1
Parts1
Fa0/0 - 192.168.12.33
Fa0/1 - 192.168.12.49
S0/0 - 192.168.27.10

Parts2
Fa0/0 - 192.168.12.65
Fa0/1 - 192.168.12.81
S0/1 - 192.168.50.22

• You may need to scroll this window and the problem statement window.
• Click on picture of host connected to the specified router and select the CiscoTerminal option to configure the router. If you select the wrong host, click on the show topology

Hide Topology
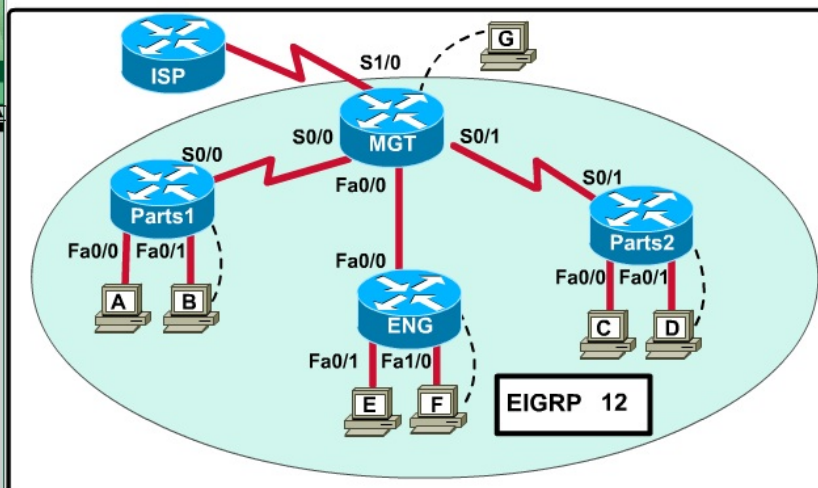
Answer: On the MGT Router:
Config t
Router eigrp 12
Network 192.168.77.0

QUESTION NO: 234 CORRECT TEXT

The following have already been configured on the router:
- The basic router configuration
- The appropriate interfaces have been configured for NAT inside and NAT outside.
- The appropriate static routes have also been configured (since the company will be a stub network, no routing protocol will be required)
- All passwords have been temporarily set to "cisco".

The task is to complete the NAT configuration using all IP addresses assigned by the ISP to provide Internet access for the hosts in the Weaver LAN. Functionality can be tested by clicking on the host provided for testing.

Configuration information
router name - Weaver
inside global addresses-198.18.184.105 198.18.184.110/29
inside local addresses - 192.168.100.17 - 192.168.100.30/28
number of inside hosts - 14
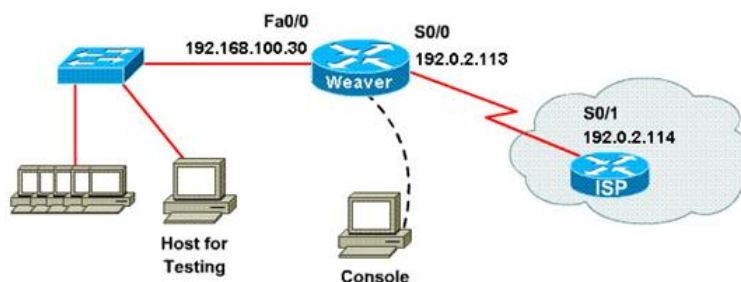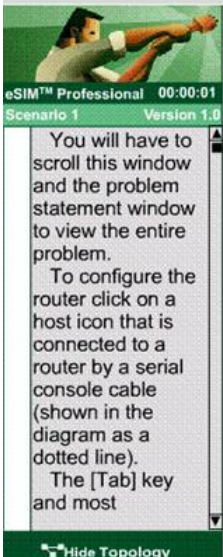
A network associate is configuring a router for the weaver company to provide internet access. The ISP has provided the company six public IP addresses of 198.18.184.105 198.18.184.110. The company has 14 hosts that need to access the internet simultaneously. The hosts in the company LAN have been assigned private space addresses in the range of 192.168.100.17 – 192.168.100.30.

Answer: The company has 14 hosts that need to access the internet simultaneously but

we just have 6 public IP addresses from 198.18.184.105 to 198.18.184.110/29.

Therefore we have to use NAT overload (or PAT)

Double click on the Weaver router to open it

Router>enable

Router#configure terminal

First you should change the router's name to Weaver

Router(config)#hostname Weaver

Create a NAT pool of global addresses to be allocated with their netmask.

Weaver(config)#ip nat pool mypool 198.18.184.105 198.18.184.110 netmask

255.255.255.248

Create a standard access control list that permits the addresses that are to be

translated

Weaver(config)#access-list 1 permit 192.168.100.16 0.0.0.15

Establish dynamic source translation, specifying the access list that was defined
in the prior step

Weaver(config)#ip nat inside source list 1 pool mypool overload

This command translates all source addresses that pass access list 1, which
means a source address from 192.168.100.17 to 192.168.100.30, into an
address from the pool named mypool (the pool contains addresses from
198.18.184.105 to 198.18.184.110)

Overload keyword allows to map multiple IP addresses to a single registered IP
address (many-to-one) by using different ports

The question said that appropriate interfaces have been configured for NAT
inside and NAT outside statements.

This is how to configure the NAT inside and NAT outside, just for your
understanding:

Weaver(config)#interface fa0/0

Weaver(config-if)#ip nat inside

Weaver(config-if)#exit

Weaver(config)#interface s0/0

Weaver(config-if)#ip nat outside

Weaver(config-if)#end

Finally, we should save all your work with the following command:

Weaver#copy running-config startup-config

Check your configuration by going to "Host for testing" and type:

C :\>ping 192.0.2.114

The ping should work well and you will be replied from 192.0.2.114

QUESTION NO: 235 CORRECT TEXT

Central Florida Widgets recently installed a new router in their office. Complete the network
installation by performing the initial router configurations and configuring R1PV2 routing using the
router command line interface (CLI) on the RC.

Configure the router per the following requirements:

Name of the router is R2

Enable. secret password is cisco

The password to access user EXEC mode using the console is cisco2

The password to allow telnet access to the router is cisco3

IPV4 addresses mast be configured as follows:

Ethernet network 209.165.201.0/27 - router has fourth assignable host address in subnet

Serial network is 192.0.2.176/28 - router has last assignable host address in the subnet.

Interfaces should be enabled.

Router protocol is RIPV2

Attention:

In practical examinations, please note the following, the actual information will prevail.

1. Name or the router is xxx

2. EnablE. secret password is xxx

3. Password In access user EXEC mode using the console is xxx

4. The password to allow telnet access to the router is xxx

5. IP information

Answer: Router>enable
Router#config terminal
Router(config)#hostname R2
R2(config)#enable secret Cisco 1
R2(config)#line console 0
R2(config-line)#password Cisco 2
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password Cisco 3
R2(config-line)#login
R2(config-line)#exit
R2(config)#interface faO/0
R2(config-if)#ip address 209.165.201.1 255.255.255.224
R2(config)#interface s0/0/0
R2(config-if)#ip address 192.0.2.176 255.255.255.240

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 209.165.201.0

R2(config-router)#network 192.0.2.176

R2(config-router)#end

R2#copy run start

QUESTION NO: 236 CORRECT TEXT

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".
The Core connection uses an IP address of 198.18.196.65
The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254.
  o   host A 192.168.33.1
  o   host B 192.168.33.2
  o   host C 192.168.33.3
  o   host D 192.168.33.4
The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30
The Finance Web Server is assigned an IP address of 172.22.242.23

Answer: Select the console on Corp1 router

Configuring ACL

Corp1>enable

Corp1#configure terminal

comment: To permit only Host C (192.168.33.3){source addr} to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)

Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80

comment: To deny any source to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)

Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80

comment: To permit ip protocol from any source to access any destination because of the implicit deny any any statement at the end of ACL.

Corp1(config)#access-list 100 permit ip any any

Applying the ACL on the Interface

comment: Check show ip interface brief command to identify the interface type and number by checking the IP address configured.

Corp1(config)#interface fa 0/1

If the ip address configured already is incorrect as well as the subnet mask. this should be corrected in order ACL to work

type this commands at interface mode :

no ip address 192.x.x.x 255.x.x.x (removes incorrect configured ipaddress and subnet mask)

Configure Correct IP Address and subnet mask :

ip address 172.22.242.30 255.255.255.240 (range of address specified going to server is given as 172.22.242.17 - 172.22.242.30)

comment: Place the ACL to check for packets going outside the interface towards the finance web server.

Corp1(config-if)#ip access-group 100 out

Corp1(config-if)#end

Important: To save your running config to startup before exit.

Corp1#copy running-config startup-config

Verifying the Configuration :

Step1: show ip interface brief command identifies the interface on which to apply access list.

Step2: Click on each host A,B,C & D . Host opens a web browser page , Select address box of the web browser and type the ip address of finance web server(172.22.242.23) to test whether it permits /deny access to the finance web Server .

Step 3: Only Host C (192.168.33.3) has access to the server . If the other host can also access then maybe something went wrong in your configuration . check whether you configured correctly and in order.
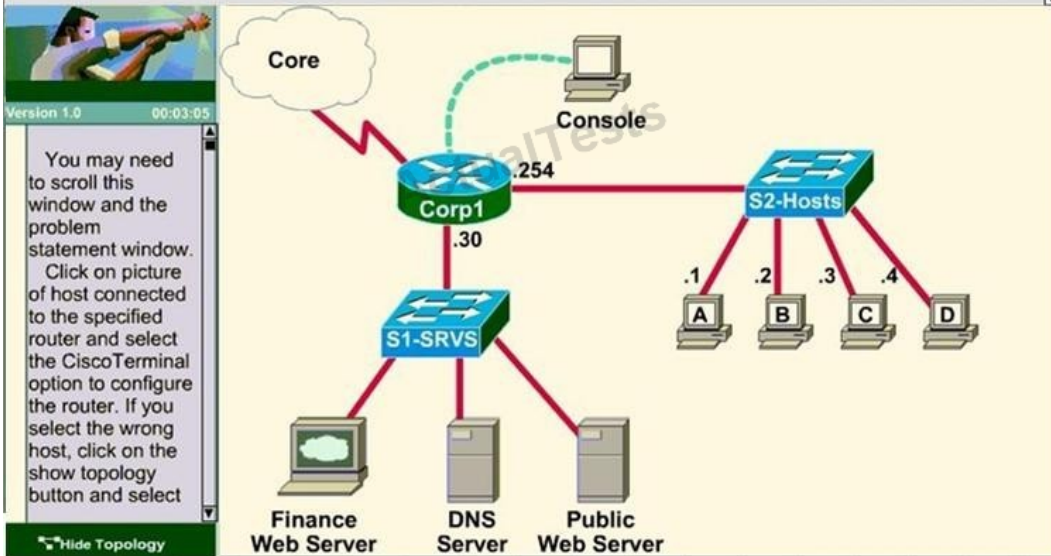
Step 4: If only Host C (192.168.33.3) can access the Finance Web Server you can click on NEXT button to successfully submit the ACL SIM.

QUESTION NO: 237 CORRECT TEXT

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".
The Core connection uses an IP address of 198.18.247.65
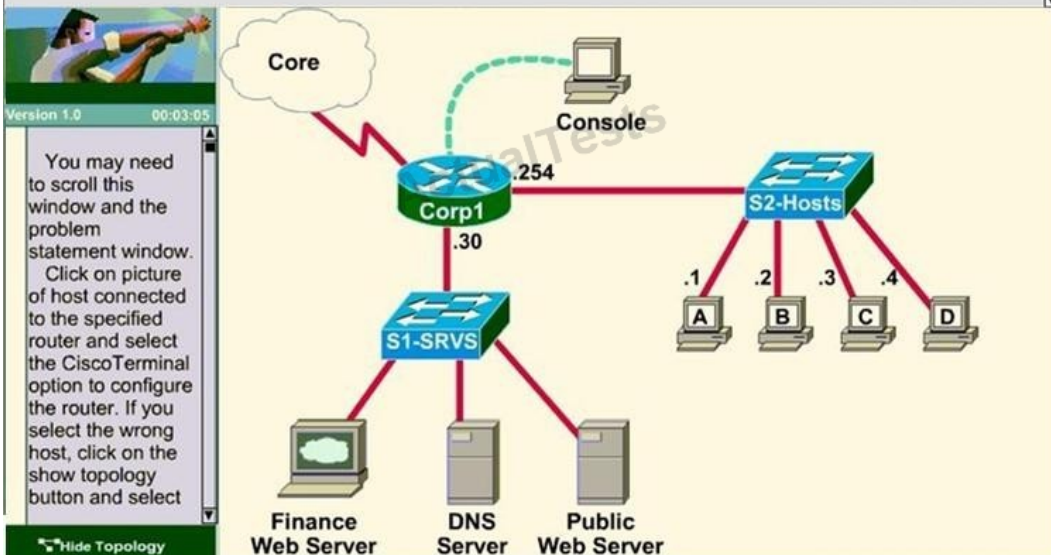The computers in the Hosts LAN have been assigned addresses of 192.168.240.1 - 192.168.240.254.
  o   host A 192.168.240.1
  o   host B 192.168.240.2
  o   host C 192.168.240.3

Answer: Corp1#conf t

Corp1(config)# access-list 128 permit tcp host 192.168.240.1 host 172.22.141.26 eq www

Corp1(config)# access-list 128 deny tcp any host 172.22.141.26 eq www

Corp1(config)# access-list 128 permit ip any any

Corp1(config)#int fa0/1

Corp1(config-if)#ip access-group 128 out

Corp1(config-if)#end

Corp1#copy run startup-config

QUESTION NO: 238 CORRECT TEXT

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.
Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".
The Core connection uses an IP address of 198.18.196.65
The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254.
    o   host A 192.168.33.1
    o   host B 192.168.33.2
    o   host C 192.168.33.3
    o   host D 192.168.33.4
The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30
The Finance Web Server is assigned an IP address of 172.22.242.23

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Answer: Corp1>enable

Corp1#configure terminal

Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80

Corp1(config)#access-list 100 deny tcp 192.168.33.0 0.0.0.255 host 172.22.242.23 eq 80

Corp1(config)#access-list 100 permit ip any any

Corp1(config)#interface fa 0/1 sh ip int brief

Corp1(config-if)#ip access-group 100 out

Corp1(config-if)#end

Corp1#copy running-config startup-config

Explanation:

Select the console on Corp1 router

Configuring ACL Corp1 >enable Corp1#configure terminal

comment: To permit only Host C (192.168. 33. 3){source addr} to access finance server address (172. 22. 242. 23)

{destination addr} on port number 80 (web)

Corp1(config)#access-list 100 permit tcp host 192. 168. 33. 3 host 172. 22. 242. 23 eq 80

comment: To deny any source to access finance server address (172. 22. 242. 23) {destination addr} on port number 80 (web)

Corp1(config)#access-list 100 deny tcp any host 172. 22. 242. 23 eq 80

comment: To permit ip protocol from any source to access any destination because of the implicit deny any any statement at the end of ACL.

Corp1(config)#access-list 100 permit ip any any

Applying the ACL on the Interface

comment: Check show ip interface brief command to identify the interface type and number by checking the IP address configured.

Corp1(config)#interface fa 0/1

If the ip address configured already is incorrect as well as the subnet mask, this should be corrected in order

ACL to work

type this commands at interface mode :

no ip address 192. x. x. x 255. x. x. x (removes incorrect configured ip address and subnet mask)

Configure Correct IP Address and subnet mask:

ip address 172. 22. 242. 30 255. 255. 255. 240 (range of address specified going to server is given as 172. 22. 242. 17-172. 22. 242. 30)

comment: Place the ACL to check for packets going outside the interface towards the finance web server.

Corp1(config-if)#ip access-group 100 out

Corp1(config-if)#end

Important: To save your running config to startup before exit. Corp1#copy running-config startup-config Verifying the Configuration :

Step1: show ip interface brief command identifies the interface on which to apply access list.

Step2: Click on each host A,B,C & D. Host opens a web browser page, Select address box of the web browser and type the ip address of finance web server(172. 22. 242. 23) to test whether it permits /deny access to the finance web Server.

Step 3: Only Host C (192.168. 33. 3) has access to the server. If the other host can also access then maybe something went wrong in your configuration check whether you configured correctly and in order.

Step 4: If only Host C (192.168. 33. 3) can access the Finance Web Server you can click on NEXT button to successfully submit the ACL SIM.

Topic 8, WAN Technologies

QUESTION NO: 239

The output of the show frame-relay pvc command shows "PVC STATUS = INACTIVE". What does this mean?

A. The PVC is configured correctly and is operating normally, but no data packets have been detected for more than five minutes.
B. The PVC is configured correctly, is operating normally, and is no longer actively seeking the address of the remote router.
C. The PVC is configured correctly, is operating normally, and is waiting for interesting traffic to trigger a call to the remote router.
D. The PVC is configured correctly on the local switch, but there is a problem on the remote end of the PVC.
E. The PVC is not configured on the local switch.

Answer: D

Explanation: Explanation

The PVC STATUS displays the status of the PVC. The DCE device creates and sends the report to the DTE devices. There are 4 statuses:

+ ACTIVE: the PVC is operational and can transmit data

+ INACTIVE: the connection from the local router to the switch is working, but the connection to the remote router is not available

+ DELETED: the PVC is not present and no LMI information is being received from the Frame Relay switch

+ STATIC: the Local Management Interface (LMI) mechanism on the interface is disabled (by using the "no keepalive" command). This status is rarely seen so it is ignored in some books.

QUESTION NO: 240 DRAG DROP

Drag the Frame Relay acronym on the left to match its definition on the right. (Not all acronyms are used.)

CIR		a router is this type of device
DCE		the most common type of virtual circuit
DTE		provides status messages between DTE and DCE devices
LMI		identifies the virtual connection between the DTE and the switch
PVC		
SVC		
DLCI		

Answer:

Drag the Frame Relay acronym on the left to match its definition on the right. (Not all acronyms are used.)

CIR		DTE
DCE		PVC
DTE		LMI
LMI		DLCI
PVC		
SVC		
DLCI		

Explanation:

| DTE |
| PVC |
| LMI |
| DLCI |

QUESTION NO: 241

Refer to the exhibit.
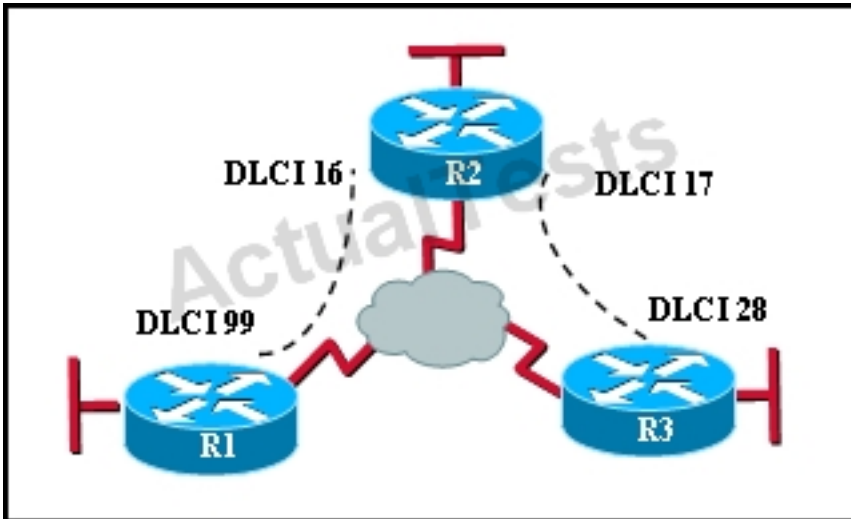
In the Frame Relay network, which IP addresses would be assigned to the interfaces with point-to-point PVCs?

A. DLCI 16: 192.168.10.1 /24
DLCI 17: 192.168.10.1 /24
DLCI 99: 192.168.10.2 /24
DLCI 28: 192.168.10.3 /24
B. DLCI 16: 192.168.10.1 /24
DLCI 17: 192.168.11.1 /24
DLCI 99: 192.168.12.1 /24
DLCI 28: 192.168.13.1 /24
C. DLCI 16: 192.168.10.1 /24
DLCI 17: 192.168.11.1 /24
DLCI 99: 192.168.10.2 /24
DLCI 28: 192.168.11.2 /24
D. DLCI 16: 192.168.10.1 /24
DLCI 17: 192.168.10.2 /24
DLCI 99: 192.168.10.3 /24
DLCI 28: 192.168.10.4 /24

Answer: C
Explanation:
With point to point PVC, each connection needs to be in a separate subnet. The R2-R1 connection (DLCI 16 to 99) would have each router within the same subnet. Similarly, the R3-R1 connection would also be in the same subnet, but it must be in a different one than the R2-R1 connection.

QUESTION NO: 242

Which command is used to enable CHAP authentication, with PAP as the fallback method, on a serial interface?

A. Router(config-if)# ppp authentication chap fallback ppp
B. Router(config-if)# ppp authentication chap pap
C. Router(config-if)# authentication ppp chap fallback ppp
D. Router(config-if)# authentication ppp chap pap

Answer: B
Explanation:
This command tells the router to first use CHAP and then go to PAP if CHAP isn't available.

QUESTION NO: 243

Which protocol is an open standard protocol framework that is commonly used in VPNs, to provide secure end-to-end communications?

A. RSA
B. L2TP
C. IPsec
D. PPTP

Answer: C
Explanation:
IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers at the IP layer. IPSec can be used to protect one or more data flows between IPSec peers.

QUESTION NO: 244

At which layer of the OSI model does PPP perform?

A. Layer 2
B. Layer 3
C. Layer 4
D. Layer 5

Answer: A

Explanation:

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP was originally emerged as an encapsulation protocol for transporting IP traffic between two peers. It is a data link layer protocol (layer 2 in the OSI model)

QUESTION NO: 245

The command frame-relay map ip 10.121.16.8 102 broadcast was entered on the router. Which of the following statements is true concerning this command?

A. This command should be executed from the global configuration mode.
B. The IP address 10.121.16.8 is the local router port used to forward data.
C. 102 is the remote DLCI that will receive the information.
D. This command is required for all Frame Relay configurations.
E. The broadcast option allows packets, such as RIP updates, to be forwarded across the PVC.

Answer: E
Explanation:

Broadcast is added to the configurations of the frame relay, so the PVC supports broadcast, allowing the routing protocol updates that use the broadcast update mechanism to be forwarded across itself.

QUESTION NO: 246

Which two options are valid WAN connectivity methods? (Choose two.)

A. PPP
B. WAP
C. DSL
D. L2TPv3
E. Ethernet

Answer: A,C
Explanation:

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP was originally emerged as an encapsulation protocol for transporting IP traffic between two peers. It is a data link layer protocol used for WAN connections.

DSL is also considered a WAN connection, as it can be used to connect networks, typically when used with VPN technology.

QUESTION NO: 247

Which Layer 2 protocol encapsulation type supports synchronous and asynchronous circuits and has built-in security mechanisms?

A. HDLC
B. PPP
C. X.25
D. Frame Relay

Answer: B

Explanation:

PPP: Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP was designed to work with several network layer protocols, including IP. PPP also has built-in security mechanisms, such as Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

QUESTION NO: 248

Which encapsulation type is a Frame Relay encapsulation type that is supported by Cisco routers?

A. IETF
B. ANSI Annex D
C. Q9333-A Annex A
D. HDLC

Answer: A

Explanation: Explanation

Cisco supports two Frame Relay encapsulation types: the **Cisco encapsulation** and the **IETF Frame Relay encapsulation**, which is in conformance with RFC 1490 and RFC 2427. The former is often used to connect two Cisco routers while the latter is used to connect a Cisco router to a non-Cisco router. You can test with your Cisco router when typing the command Router(config-if)# **encapsulation frame-relay ?** on a WAN link. Below is the output of this command (notice Cisco is

the default encapsulation so it is not listed here, just press Enter to use it).

Note: Three LMI options are supported by Cisco routers are ansi, Cisco, and Q933a. They represent the ANSI Annex D, Cisco, and ITU Q933-A (Annex A) LMI types, respectively. HDLC is a WAN protocol same as Frame-Relay and PPP so it is not a Frame Relay encapsulation type.

QUESTION NO: 249

RouterA is unable to reach RouterB. Both routers are running IOS version 12.0.
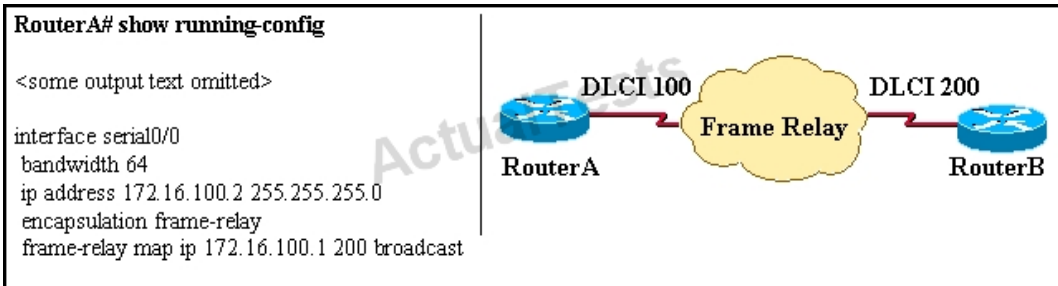
After reviewing the command output and graphic, what is the most likely cause of the problem?

A. incorrect bandwidth configuration
B. incorrect LMI configuration
C. incorrect map statement
D. incorrect IP address

Answer: C
Explanation: Explanation
With this topology and the DLCI, we can only think of "incorrect map statement". From the topology we can deduce traffic with a DLCI of 75 will be sent to 192.168.2.1 but the text below wrongly shows "DLCI 50 for the next router 192.168.2.1 -> .

QUESTION NO: 250

Refer to the exhibit.

```
R1# show frame-relay map
Serial0/0 (up): ip 172.16.3.1 dlci 100 (0x64, 0x1840), dynamic
              broadcast,, status defined, active
```

What is the meaning of the term dynamic as displayed in the output of the show frame-relay map command shown?

A. The Serial0/0 interface is passing traffic.
B. The DLCI 100 was dynamically allocated by the router.
C. The Serial0/0 interface acquired the IP address of 172.16.3.1 from a DHCP server.
D. The DLCI 100 will be dynamically changed as required to adapt to changes in the Frame Relay cloud.
E. The mapping between DLCI 100 and the end station IP address 172.16.3.1 was learned through Inverse ARP.

Answer: E
Explanation:
Inverse Address Resolution Protocol (Inverse ARP) was developed to provide a mechanism for dynamic DLCI to Layer 3 address maps. Inverse ARP works much the same way Address Resolution Protocol (ARP) works on a LAN. However, with ARP, the device knows the Layer 3 IP address and needs to know the remote data link MAC address. With Inverse ARP, the router knows the Layer 2 address which is the DLCI, but needs to know the remote Layer 3 IP address. When using dynamic address mapping, Inverse ARP requests a next-hop protocol address for each active PVC. Once the requesting router receives an Inverse ARP response, it updates its DLCI-to-Layer 3 address mapping table. Dynamic address mapping is enabled by default for all protocols enabled on a physical interface. If the Frame Relay environment supports LMI autosensing and Inverse ARP, dynamic address mapping takes place automatically. Therefore, no static address mapping is required.

QUESTION NO: 251

A network administrator needs to configure a serial link between the main office and a remote location. The router at the remote office is a non-Cisco router. How should the network administrator configure the serial interface of the main office router to make the connection?

A. Main(config)# interface serial 0/0
Main(config-if)# ip address 172.16.1.1 255.255.255.252
Main(config-if)# no shut
B. Main(config)# interface serial 0/0
Main(config-if)# ip address 172.16.1.1 255.255.255.252
Main(config-if)# encapsulation ppp
Main(config-if)# no shut
C. Main(config)# interface serial 0/0
Main(config-if)# ip address 172.16.1.1 255.255.255.252
Main(config-if)# encapsulation frame-relay
Main(config-if)# authentication chap
Main(config-if)# no shut
D. Main(config)# interface serial 0/0
Main(config-if)#ip address 172.16.1.1 255.255.255.252
Main(config-if)#encapsulation ietf
Main(config-if)# no shut

Answer: B
Explanation:
With serial point to point links there are two options for the encapsulation. The default, HDLC, is Cisco proprietary and works only with other Cisco routers. The other option is PPP which is standards based and supported by all vendors.

QUESTION NO: 252

What are three reasons that an organization with multiple branch offices and roaming users might implement a Cisco VPN solution instead of point-to-point WAN links? (Choose three.)

A. reduced cost
B. better throughput
C. broadband incompatibility
D. increased security
E. scalability
F. reduced latency

Answer: A,D,E
Explanation:
IPsec offer a number of advantages over point to point WAN links, particularly when multiple locations are involved. These include reduced cost, increased security since all traffic is encrypted, and increased scalability as s single WAN link can be used to connect to all locations in a VPN, where as a point to point link would need to be provisioned to each location.

QUESTION NO: 253

Which two statistics appear in show frame-relay map output? (Choose two.)

A. the number of BECN packets that are received by the router
B. the value of the local DLCI
C. the number of FECN packets that are received by the router
D. the status of the PVC that is configured on the router
E. the IP address of the local router

Answer: B,D

Explanation:

Sample "show frame-relay map" output:

R1#sh frame mapSerial0/0 (up): ip 10.4.4.1 **dlci 401**(0x191,0x6410), dynamic,broadcast,, **status defined, active**Serial0/0 (up): ip 10.4.4.3 **dlci 403**(0x193,0x6430), dynamic,broadcast,, **status defined, active**Serial0/0 (up): ip 10.4.4.4 **dlci 401**(0x191,0x6410), static,CISCO, **status defined, active**

QUESTION NO: 254

Users have been complaining that their Frame Relay connection to the corporate site is very slow. The network administrator suspects that the link is overloaded.

```
PVC Statistics for interface Serial0 (Frame Relay DTE)

          Active    Inactive    Deleted    Static
Local       1          0           0          0
Switched    0          0           0          0
Unused      0          0           0          0

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0

  input pkts 1300        output pkts 1270       in bytes 22121000
  out bytes 21802000       dropped pkts 4        in FECN pkts 147
  in BECN pkts 192       out FECN pkts 259      out BECN pkts 214
  in DE pkts 0          out DE pkts 0
  out bcast pkts 107      out bcast bytes 19722
  pvc create time 00:25:50, last time pvc status changed 00:25:40
```

Based on the partial output of the Router# show frame relay pvc command shown in the graphic, which output value indicates to the local router that traffic sent to the corporate site is experiencing congestion?

A. DLCI = 100
B. last time PVC status changed 00:25:40
C. in BECN packets 192
D. in FECN packets 147
E. in DE packets 0

Answer: C

Explanation:

If device A is sending data to device B across a Frame Relay infrastructure and one of the intermediate Frame Relay switches encounters congestion, congestion being full buffers, over-subscribed port, overloaded resources, etc, it will set the BECN bit on packets being returned to the sending device and the FECN bit on the packets being sent to the receiving device.

QUESTION NO: 255

Which command allows you to verify the encapsulation type (CISCO or IETF) for a Frame Relay link?

A. show frame-relay lmi
B. show frame-relay map
C. show frame-relay pvc
D. show interfaces serial

Answer: B

Explanation:

When connecting Cisco devices with non-Cisco devices, you must use IETF4 encapsulation on both devices. Check the encapsulation type on the Cisco device with the **show frame-relay map** exec command.

QUESTION NO: 256

It has become necessary to configure an existing serial interface to accept a second Frame Relay virtual circuit. Which of the following procedures are required to accomplish this task? (Choose three.)

A. Remove the IP address from the physical interface.
B. Encapsulate the physical interface with multipoint PPP.
C. Create the virtual interfaces with the interface command.
D. Configure each subinterface with its own IP address.
E. Disable split horizon to prevent routing loops between the subinterface networks.
F. Configure static Frame Relay map entries for each subinterface network.

Answer: A,C,D

Explanation:

For multiple PVC's on a single interface, you must use subinterfaces, with each subinterface configured for each PVC. Each subinterface will then have its own IP address, and no IP address will be assigned to the main interface.

QUESTION NO: 257

What occurs on a Frame Relay network when the CIR is exceeded?

A. All TCP traffic is marked discard eligible.
B. All UDP traffic is marked discard eligible and a BECN is sent.
C. All TCP traffic is marked discard eligible and a BECN is sent.
D. All traffic exceeding the CIR is marked discard eligible.

Answer: D

Explanation: Explanation

Committed information rate (CIR): The minimum guaranteed data transfer rate agreed to by the Frame Relay switch. Frames that are sent in excess of the CIR are marked as discard eligible (DE) which means they can be dropped if the congestion occurs within the Frame Relay network. Note: In the Frame Relay frame format, there is a bit called Discard eligible (DE) bit that is used to identify frames that are first to be dropped when the CIR is exceeded.

QUESTION NO: 258

Which two statements about using the CHAP authentication mechanism in a PPP link are true? (Choose two.)

A. CHAP uses a two-way handshake.
B. CHAP uses a three-way handshake.
C. CHAP authentication periodically occurs after link establishment.

D. CHAP authentication passwords are sent in plaintext.

E. CHAP authentication is performed only upon link establishment.

**F.** CHAP has no protection from playback attacks.

Answer: B,C

Explanation:

CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).

QUESTION NO: 259

Refer to the exhibit.
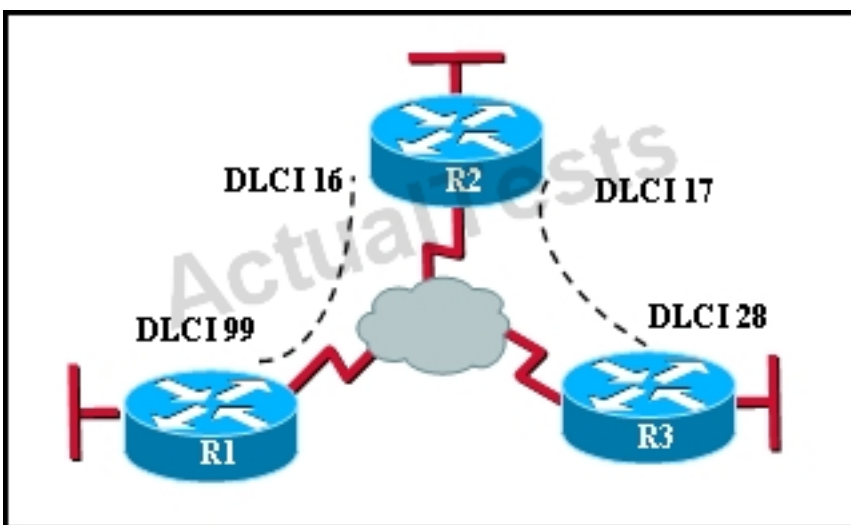
Which statement describes DLCI 17?

A. DLCI 17 describes the ISDN circuit between R2 and R3.

B. DLCI 17 describes a PVC on R2. It cannot be used on R3 or R1.

C. DLCI 17 is the Layer 2 address used by R2 to describe a PVC to R3.

D. DLCI 17 describes the dial-up circuit from R2 and R3 to the service provider.

Answer: C

Explanation:

DLCI-Data Link Connection Identifier Bits: The DLCI serves to identify the virtual connection so that the receiving end knows which information connection a frame belongs to. Note that this DLCI

has only local significance. Frame Relay is strictly a Layer 2 protocol suite.

QUESTION NO: 260

What is the result of issuing the frame-relay map ip 192.168.1.2 202 broadcast command?

A. defines the destination IP address that is used in all broadcast packets on DCLI 202
B. defines the source IP address that is used in all broadcast packets on DCLI 202
C. defines the DLCI on which packets from the 192.168.1.2 IP address are received
D. defines the DLCI that is used for all packets that are sent to the 192.168.1.2 IP address

Answer: D
Explanation:
This command identifies the DLCI that should be used for all packets destined to the 192.168.1.2
address. In this case, DLCI 202 should be used.

QUESTION NO: 261

Which PPP subprotocol negotiates authentication options?

A. NCP
B. ISDN
C. SLIP
D. LCP
E. DLCI

Answer: D
Explanation:
The PPP Link Control Protocol (LCP) is documented in RFC 1661. LPC negotiates link and PPP
parameters to dynamically configure the data link layer of a PPP connection. Common LCP
options include the PPP MRU, the authentication protocol, compression of PPP header fields,
callback, and multilink options.

QUESTION NO: 262

What are two characteristics of Frame Relay point-to-point subinterfaces? (Choose two.)

A. They create split-horizon issues.
B. They require a unique subnet within a routing domain.
C. They emulate leased lines.
D. They are ideal for full-mesh topologies.
E. They require the use of NBMA options when using OSPF.

Answer: B,C

Explanation:

Subinterfaces are used for point to point frame relay connections, emulating virtual point to point leased lines. Each subinterface requires a unique IP address/subnet. Remember, you can not assign multiple interfaces in a router that belong to the same IP subnet.

QUESTION NO: 263

What command is used to verify the DLCI destination address in a Frame Relay static configuration?

A. show frame-relay pvc
B. show frame-relay lmi
C. show frame-relay map
D. show frame relay end-to-end

Answer: C

Explanation:

Sample "show frame-relay map" output:

R1#sh frame mapSerial0/0 (up): ip 10.4.4.1 **dlci 401**(0x191,0x6410), dynamic,broadcast,, status defined, activeSerial0/0 (up): ip 10.4.4.3 **dlci 403**(0x193,0x6430), dynamic,broadcast,, status defined, activeSerial0/0 (up): ip 10.4.4.4 **dlci 401**(0x191,0x6410), static,CISCO, status defined, active

QUESTION NO: 264

What is the purpose of Inverse ARP?

A. to map a known IP address to a MAC address

B. to map a known DLCI to a MAC address

C. to map a known MAC address to an IP address

D. to map a known DLCI to an IP address

E. to map a known IP address to a SPID

F. to map a known SPID to a MAC address

Answer: D

Explanation:

Dynamic address mapping relies on the Frame Relay Inverse Address Resolution Protocol (Inverse ARP), defined by RFC 1293, to resolve a next hop network protocol (IP) address to a local DLCI value. The Frame Relay router sends out Inverse ARP requests on its Frame Relay PVC to discover the protocol address of the remote device connected to the Frame Relay network. The responses to the Inverse ARP requests are used to populate an address-to-DLCI mapping table on the Frame Relay router or access server. The router builds and maintains this address-to-DLCI mapping table, which contains all resolved Inverse ARP requests, including both dynamic and static mapping entries.

Topic 9, Mix Questions Set

QUESTION NO: 265

What is a valid HSRP virtual MAC address?

A. 0000.5E00.01A3

B. 0007.B400.AE01

C. 0000.0C07.AC15

D. 0007.5E00.B301

Answer: C

Explanation:

QUESTION NO: 266

In GLBP, which router will respond to client ARP requests?

A. The active virtual gateway will reply with one of four possible virtual MAC addresses.

B. All GLBP member routers will reply in round-robin fashion.

C. The active virtual gateway will reply with its own hardware MAC address.

D. The GLBP member routers will reply with one of four possible burned in hardware addresses.

Answer: A

Explanation:

QUESTION NO: 267

Which statement describes VRRP object tracking?

A. It monitors traffic flow and link utilization.
B. It ensures the best VRRP router is the virtual router master for the group.
C. It causes traffic to dynamically move to higher bandwidth links.
D. It thwarts man-in-the-middle attacks.

Answer: B

Explanation:

QUESTION NO: 268

What are three benefits of GLBP? (Choose three.)

A. GLBP supports up to eight virtual forwarders per GLBP group.
B. GLBP supports clear text and MD5 password authentication between GLBP group members.
C. GLBP is an open source standardized protocol that can be used with multiple vendors.
D. GLBP supports up to 1024 virtual routers.
E. GLBP can load share traffic across a maximum of four routers.
F. GLBP elects two AVGs and two standby AVGs for redundancy.

Answer: B,D,E

Explanation:

QUESTION NO: 269

Which three statements about HSRP operation are true? (Choose three.)

A. The virtual IP address and virtual MA+K44C address are active on the HSRP Master router.
B. The HSRP default timers are a 3 second hello interval and a 10 second dead interval.
C. HSRP supports only clear-text authentication.
D. The HSRP virtual IP address must be on a different subnet than the routers' interfaces on the same LAN.

E. The HSRP virtual IP address must be the same as one of the router's interface addresses on the LAN.
F. HSRP supports up to 255 groups per interface, enabling an administrative form of load balancing.

Answer: A,B,F
Explanation:

QUESTION NO: 270

Which three statements about Syslog utilization are true? (Choose three.)

A. Utilizing Syslog improves network performance.
B. The Syslog server automatically notifies the network administrator of network problems.
C. A Syslog server provides the storage space necessary to store log files without using router disk space.
D. There are more Syslog messages available within Cisco IOS than there are comparable SNMP trap messages.
E. Enabling Syslog on a router automatically enables NTP for accurate time stamping.
F. A Syslog server helps in aggregation of logs and alerts.

Answer: C,D,F
Explanation:

QUESTION NO: 271

A network administrator enters the following command on a router: logging trap 3. What are three message types that will be sent to the Syslog server? (Choose three.)

A. informational
B. emergency
C. warning
D. critical
E. debug
F. error

Answer: B,D,F
Explanation:

QUESTION NO: 272

What is the default Syslog facility level?

A. local4
B. local5
C. local6
D. local7

Answer: D
Explanation:

QUESTION NO: 273

What command instructs the device to timestamp Syslog debug messages in milliseconds?

A. service timestamps log datetime localtime
B. service timestamps debug datetime msec
C. service timestamps debug datetime localtime
D. service timestamps log datetime msec

Answer: B
Explanation:

QUESTION NO: 274

Refer to the exhibit.

```
*Mar 01, 00:37:57.3737: %SYS-5-CONFIG_I: Configured from console by console
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.11.2 (FastEthernet0/1) is down: interface down
```

What is the cause of the Syslog output messages?

A. The EIGRP neighbor on Fa0/1 went down due to a failed link.
B. The EIGRP neighbor connected to Fa0/1 is participating in a different EIGRP process, causing the adjacency to go down.
C. A shut command was executed on interface Fa0/1, causing the EIGRP adjacency to go down.

D. Interface Fa0/1 has become error disabled, causing the EIGRP adjacency to go down.

Answer: C
Explanation:

QUESTION NO: 275

What are three components that comprise the SNMP framework? (Choose three.)

A. MIB
B. agent
C. set
D. AES
E. supervisor
F. manager

Answer: A,B,F
Explanation:

QUESTION NO: 276

What are three components that comprise the SNMP framework? (Choose three.)

A. MIB
B. agent
C. set
D. AES
E. supervisor
F. manager

Answer: A,B,F
Explanation:

QUESTION NO: 277

What SNMP message alerts the manager to a condition on the network?

A. response

B. get
C. trap
D. capture

Answer: C
Explanation:

QUESTION NO: 278

What authentication type is used by SNMPv2?

A. HMAC-MD5
B. HMAC-SHA
C. CBC-DES
D. community strings

Answer: D
Explanation:

QUESTION NO: 279

Which three statements about the features of SNMPv2 and SNMPv3 are true? (Choose three.)

A. SNMPv3 enhanced SNMPv2 security features.
B. SNMPv3 added the Inform protocol message to SNMP.
C. SNMPv2 added the Inform protocol message to SNMP.
D. SNMPv3 added the GetBulk protocol messages to SNMP.
E. SNMPv2 added the GetBulk protocol message to SNMP.
F. SNMPv2 added the GetNext protocol message to SNMP.

Answer: A,C,E
Explanation:

QUESTION NO: 280

What are three reasons to collect Netflow data on a company network? (Choose three.)

A. To identify applications causing congestion.

B. To authorize user network access.

C. To report and alert link up / down instances.

D. To diagnose slow network performance, bandwidth hogs, and bandwidth utilization.

E. To detect suboptimal routing in the network.

F. To confirm the appropriate amount of bandwidth that has been allocated to each Class of Service.

Answer: A,D,F

Explanation:

QUESTION NO: 281

What Netflow component can be applied to an interface to track IPv4 traffic?

A. flow monitor

B. flow record

C. flow sampler

D. flow exporter

Answer: A

Explanation:

QUESTION NO: 282

What Cisco IOS feature can be enabled to pinpoint an application that is causing slow network performance?

A. SNMP

B. Netflow

C. WCCP

D. IP SLA

Answer: B

Explanation:

QUESTION NO: 283

What command visualizes the general NetFlow data on the command line?

A. show ip flow export
B. show ip flow top-talkers
C. show ip cache flow
D. show mls sampling
E. show mls netflow ip

Answer: C
Explanation:

QUESTION NO: 284

What are three values that must be the same within a sequence of packets for Netflow to consider them a network flow? (Choose three.)

A. source IP address
B. source MAC address
C. egress interface
D. ingress interface
E. destination IP address
F. IP next-hop

Answer: A,D,E
Explanation:

QUESTION NO: 285

What are three factors a network administrator must consider before implementing Netflow in the network? (Choose three.)

A. CPU utilization
B. where Netflow data will be sent
C. number of devices exporting Netflow data
D. port availability
E. SNMP version
F. WAN encapsulation

Answer: A,B,C
Explanation:

QUESTION NO: 286

Refer to the exhibit.
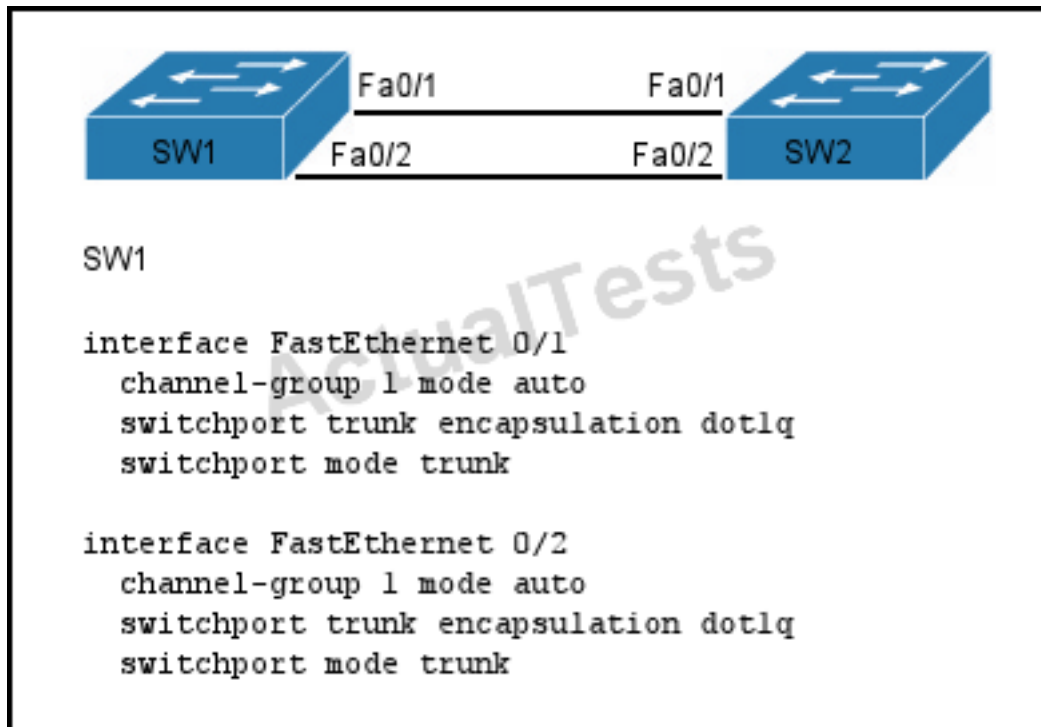
A network administrator is configuring an EtherChannel between SW1 and SW2. The SW1 configuration is shown. What is the correct configuration for SW2?

A. interface FastEthernet 0/1
channel-group 1 mode active
switchport trunk encapsulation dot1q
switchport mode trunk
interface FastEthernet 0/2
channel-group 1 mode active
switchport trunk encapsulation dot1q
switchport mode trunk
B. interface FastEthernet 0/1
channel-group 2 mode auto
switchport trunk encapsulation dot1q
switchport mode trunk
interface FastEthernet 0/2
channel-group 2 mode auto
switchport trunk encapsulation dot1q
switchport mode trunk
C. interface FastEthernet 0/1
channel-group 1 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk

interface FastEthernet 0/2
channel-group 1 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk
D. interface FastEthernet 0/1
channel-group 1 mode passive
switchport trunk encapsulation dot1q
switchport mode trunk
interface FastEthernet 0/2
channel-group 1 mode passive
switchport trunk encapsulation dot1q
switchport mode trunk

Answer: C

Explanation:

QUESTION NO: 287

Which two statements about the OSPF Router ID are true? (Choose two.)

A. It identifies the source of a Type 1 LSA.
B. It should be the same on all routers in an OSPF routing instance.
C. By default, the lowest IP address on the router becomes the OSPF Router ID.
D. The router automatically chooses the IP address of a loopback as the OSPF Router ID.
E. It is created using the MAC Address of the loopback interface.

Answer: A,D

Explanation:

QUESTION NO: 288

What parameter can be different on ports within an EtherChannel?

A. speed
B. DTP negotiation settings
C. trunk encapsulation
D. duplex

Answer: B

Explanation:

QUESTION NO: 289

What are two benefits of using a single OSPF area network design? (Choose two.)

A. It is less CPU intensive for routers in the single area.
B. It reduces the types of LSAs that are generated.
C. It removes the need for virtual links.
D. It increases LSA response times.
E. It reduces the number of required OSPF neighbor adjacencies.

Answer: B,C
Explanation:

QUESTION NO: 290

Refer to the exhibit.

```
FastEthernet0/3:
Port state     = 1
Channel group = 2        Mode = Passive        Gcchange = -
Port-channel  = Po2      GC   =  -             Pseudo port-channel = Po2
Port index    = 0        Load = 0x00           Protocol =   LACP
```

What set of commands was configured on interface Fa0/3 to produce the given output?

A. interface FastEthernet 0/3
channel-group 1 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk
B. interface FastEthernet 0/3
channel-group 2 mode passive
switchport trunk encapsulation dot1q
switchport mode trunk
C. interface FastEthernet 0/3
channel-group 2 mode active
switchport trunk encapsulation dot1q
switchport mode trunk
D. interface FastEthernet 0/3
channel-group 2 mode on
switchport trunk encapsulation dot1q

switchport mode trunk

Answer: B

Explanation:

QUESTION NO: 291

What are two enhancements that OSPFv3 supports over OSPFv2? (Choose two.)
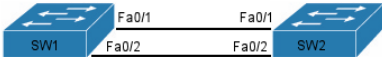
A. It requires the use of ARP.
B. It can support multiple IPv6 subnets on a single link.
C. It supports up to 2 instances of OSPFv3 over a common link.
D. It routes over links rather than over networks.

Answer: B,D

Explanation:

QUESTION NO: 292

Refer to the exhibit.

If the devices produced the given output, what is the cause of the EtherChannel problem?

A. SW1's Fa0/1 interface is administratively shut down.

B. There is an encapsulation mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.

C. There is an MTU mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.

D. There is a speed mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.

Answer: D

Explanation:

QUESTION NO: 293

When a router undergoes the exchange protocol within OSPF, in what order does it pass through each state?

A. exstart state > loading state > exchange state > full state

B. exstart state > exchange state > loading state > full state

C. exstart state > full state > loading state > exchange state

D. loading state > exchange state > full state > exstart state

Answer: B

Explanation:

QUESTION NO: 294

A network administrator creates a layer 3 EtherChannel, bundling four interfaces into channel group 1. On what interface is the IP address configured?

A. the port-channel 1 interface

B. the highest number member interface

C. all member interfaces

D. the lowest number member interface

Answer: A

Explanation:

QUESTION NO: 295

What command sequence will configure a router to run OSPF and add network 10.1.1.0 /24 to area 0?

A. router ospf area 0
network 10.1.1.0 255.255.255.0 area 0
B. router ospf
network 10.1.1.0 0.0.0.255
C. router ospf 1
network 10.1.1.0 0.0.0.255 area 0
D. router ospf area 0
network 10.1.1.0 0.0.0.255 area 0
E. router ospf
network 10.1.1.0 255.255.255.0 area 0
F. router ospf 1
network 10.1.1.0 0.0.0.255

Answer: C

Explanation:

QUESTION NO: 296

Refer to the exhibit.

```
Cisco#show ip interface brief
Interface          IP-Address     OK? Method Status              Protocol

FastEthernet0/0    192.168.1.1    YES manual up                  up

FastEthernet0/1    172.16.1.1     YES manual up                  up

Loopback0          1.1.1.1        YES manual up                  up

Loopback1          2.2.2.2        YES manual up                  up

Vlan1              unassigned     YES unset  administratively down down
```

If the router Cisco returns the given output and has not had its router ID set manually, what value will OSPF use as its router ID?

A. 192.168.1.1
B. 172.16.1.1
C. 1.1.1.1
D. 2.2.2.2

Answer: D

Explanation:

QUESTION NO: 297

What OSPF command, when configured, will include all interfaces into area 0?

A. network 0.0.0.0 255.255.255.255 area 0
B. network 0.0.0.0 0.0.0.0 area 0
C. network 255.255.255.255 0.0.0.0 area 0
D. network all-interfaces area 0

Answer: A
Explanation:

QUESTION NO: 298

Which statement describes the process ID that is used to run OSPF on a router?

A. It is globally significant and is used to represent the AS number.
B. It is locally significant and is used to identify an instance of the OSPF database.
C. It is globally significant and is used to identify OSPF stub areas.
D. It is locally significant and must be the same throughout an area.

Answer: B
Explanation:

QUESTION NO: 299

Which three are the components of SNMP? (Choose three)

A. MIB
B. SNMP Manager
C. SysLog Server
D. SNMP Agent
E. Set

Answer: A,B,D
Explanation:

QUESTION NO: 300

What are the Popular destinations for syslog messages to be saved?

A. Flash
B. The logging buffer .RAM
C. The console terminal
D. Other terminals
E. Syslog server

Answer: B,C,E
Explanation:

QUESTION NO: 301

Syslog was configured with a level 3 trap. Which 3 types of logs would be generated (choose three)

A. Emergencies
B. Alerts
C. Critical
D. Errors
E. Warnings

Answer: A,B,C
Explanation:

QUESTION NO: 302

What are the benefit of using Netflow? (Choose three.)

A. Network, Application & User Monitoring
B. Network Planning
C. Security Analysis
D. Accounting/Billing

Answer: A,C,D
Explanation:

QUESTION NO: 303

Which protocol can cause overload on a CPU of a managed device?

A. Netflow
B. WCCP
C. IP SLA
D. SNMP

Answer: D

Explanation:

QUESTION NO: 304

What are the three things that the Netflow uses to consider the traffic to be in a same flow?

A. IP address
B. Interface name
C. Port numbers
D. L3 protocol type
E. MAC address

Answer: A,C,D

Explanation:

QUESTION NO: 305

What is the alert message generated by SNMP agents called ?

A. TRAP
B. INFORM
C. GET
D. SET

Answer: A,B

Explanation:

QUESTION NO: 306

Which three features are added in SNMPv3 over SNMPv2?

A. Message Integrity
B. Compression
C. Authentication

D. Encryption
E. Error Detection

Answer: A,C,D
Explanation:

QUESTION NO: 307

In a GLBP network, who is responsible for the arp request?

A. AVF
B. AVG
C. Active Router
D. Standby Router

Answer: B