Cisco 640-802

640-802 Cisco Certified Network Associate (CCNA)

Practice Test

Version 4.2

QUESTION NO: 1

What functions do routers perform in a network? (Choose two.)

A. path selection
B. packet switching
C. VLAN membership assignment
D. microsegmentation of broadcast domains

Answer: A,B

Explanation:
The primary functions of a router are: Packet Switching and Path Selection. It is the routers job to determine the best method for delivering the data, and switching that data as quickly as possible.

(1)Intercept datagrams sent to remote network segments between networks, playing a translated role.

(2)Select the most reasonable route to guide communications. In order to achieve this function, the router will check the routing table based on certain routing communication protocol, and the routing table lists all the nodes contained in the entire internet , the path conditions between nodes and transmission costs associated with them. If a specific node has more than one path, then select the optimal path based on pre-determined specifications. Because a variety of network segments and their mutual connection situations may change, the routing information needs to be updated in time, which is completed by timing update or updating according to changes determined by the routing information protocol used. Each router in the network dynamically updates its routing table according to this rule to maintain effective routing information.

(3)When forwarding datagrams, in order to facilitate transferring datagrams between networks, routers will divide large data packets into appropriate sized data packets according to pre-determined specifications, and those appropriate sized data packets will be turned into their original form when reaching the destination.

(4)Multi-protocol routers can connect and use network segments of different communication protocols , they can be used as communication connecting platforms of network segments of different communication protocols.

(5)The main task of router is to guide the communications to the destination network, and then reach the addresses of the specific node station. Another function is completed through the decomposition of internet address. For example, assign parts of the network address to specific network, subnet and a group of regional nodes , while the rest can be used to specify the particular station of subnet. Hierarchical addressing allows routers to store addressing information of networks with many node stations.

QUESTION NO: 2

Which of the following is true regarding the use of switches and hubs for network connectivity?

A. Using hubs can increase the amount of bandwidth available to hosts.
B. Hubs can filter frames.
C. Switches increase the number of collision domains in the network.
D. Switches do not forward broadcasts.
E. Switches take less time to process frames than hubs take.

Answer: C

Explanation:
A hub is a broadcast domain and a collision domain, while a switch is a broadcast domain, each interface is a collision domain. The switch is a device of data link layer, forwards and floods data frames based on the MAC address. The hub adopts the shared bandwidth working mode, while the switch adopts dedicated bandwidth.

Switches increases the number of collisions domains in the network. Switches that are configured with VLANs will reduce the size of the collision domains by increasing the number of collision domains in a network, but making them smaller than that of one big, flat network.
Incorrect Answers:
A: Switches and hubs can be equally efficient in processing frames, in theory. In practice, switches are generally more efficient as they usually have more CPU and memory allocated to them, and are generally much more expensive than a simple hub.
B: Switches are capable of VLAN configurations, but hubs are not.
E: Switches forward broadcasts and multicasts, by default, to all ports within the same VLAN. Only routers block all broadcast traffic by default.

QUESTION NO: 3

When comparing and contrasting the similarities and differences between bridges and switches, which of the following are valid statements? (Choose two)

A. Bridges and switches learn MAC addresses by examining the source MAC address of each frame received.
B. A switch is a multiport bridge
C. Bridges and switches increase the size of a collision domain.
D. Bridges are faster than switches because they have fewer ports.

Answer: A,B

Explanation:
Bridge is a Layer2 device, which is designed to create two or more LAN segments. Each segment is an independent collision domain. Bridge is also created to provide more available bandwidth, Its purpose is to filter the LAN traffic, making local traffic be in the local area, and those directed to other parts of the LAN (sub) be forwarded there. Each NIC on each device has a unique MAC address. Bridge will record the MAC address of each port and then make forwarding decisions based on this MAC address table.
Switch is a device of the data link layer, it combines multiple physical LAN segments into a large network.. Similar to bridge, the switch will transfer and flood the communication frames based on the MAC address. Because the switching process is performed in hardware, the switching speed of the switch is faster than that of a bridge performed by software. Regarding each switching port as a mini-bridge, then each switching port will work as an independent bridge to provide full medium??s bandwidth to each host.
The number of ports of bridges and switches are the same as that of collision domains. All ports are in the same broadcast domain.

Both bridges and switches build the bridge table by listening to incoming frames and examining the source MAC address in the frame.
Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.
Incorrect Answers:
D: Switches are generally faster than bridges. Bridges also do not necessarily have fewer ports than switches.

QUESTION NO: 4

As a network administrator, you will need to decide on the appropriate network devices to use. Which of the following correctly describes the roles of devices in a WAN? (Choose three)

A. A modem terminates a digital local loop.
B. A CSU/DSU 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.

Answer: B,D,E

Explanation:
Layer 2 switching is considered hardware-based bridging because it uses specialized hardware called an application-specific integrated circuit (ASIC). ASICs can run up to gigabit speeds with very low latency rates.

A router is commonly considered to be a DTE device, while a CSU/DSU is considered the DCE device.
Switches usually have higher port number then bridge. Generally bridges have two ports. Both operates on Data link layer.

QUESTION NO: 5

Which of the following statements are true regarding bridges and switches? (Choose 3.)

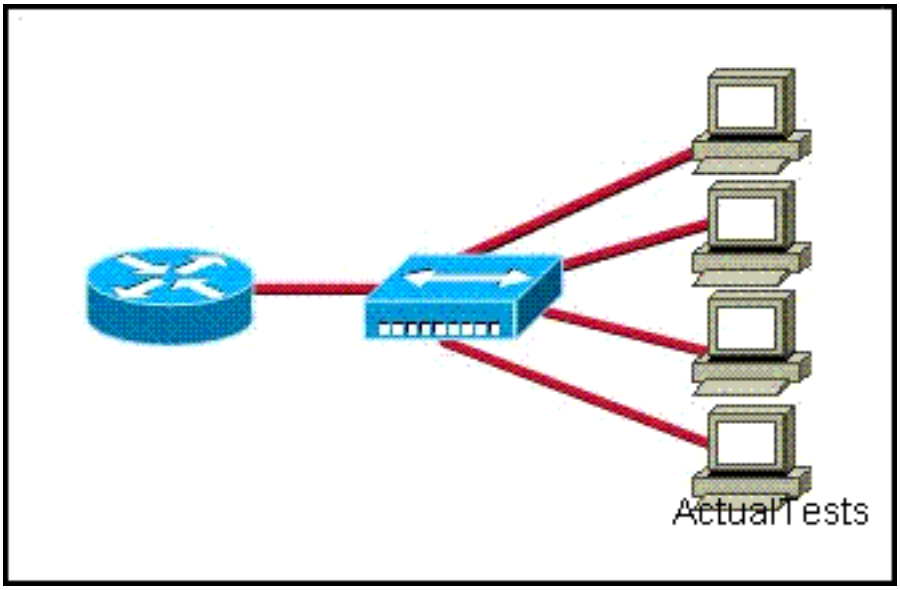
A. Both bridges and switches make forwarding decisions based on Layer 2 addresses.
B. Switches have a higher number of ports than most bridges.
C. Switches are primarily software based while bridges are hardware based.
D. Both bridges and switches forward Layer 2 broadcasts.
E. Bridges define broadcast domains while switches define collision domains.
F. Bridges are frequently faster than switches.
G. Both bridges and switches make forwarding decisions based on Layer 2 addresses.

Answer: A,B,D

Explanation:
Both bridges and switches operate at the second layer of the OSI model, processing and forwarding frames from the data-link layer.
Bridges are software based and switches are hardware based.
Switches have more ports than bridges.
Both bridges and switches forward frames based on MAC addresses.

QUESTION NO: 6

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

Answer: A,B

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.

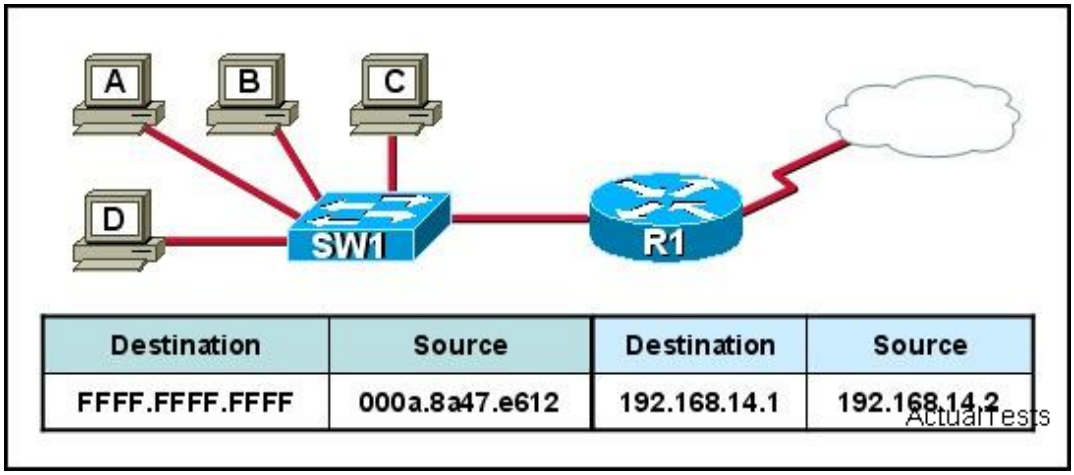
How to count them?

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: 7

Refer to the exhibit. The switch in the graphic has a default configuration and the MAC table is fully populated. In addition, this network is operating properly. The graphic represents selected header information in a frame leaving host A. What can be concluded from this information?

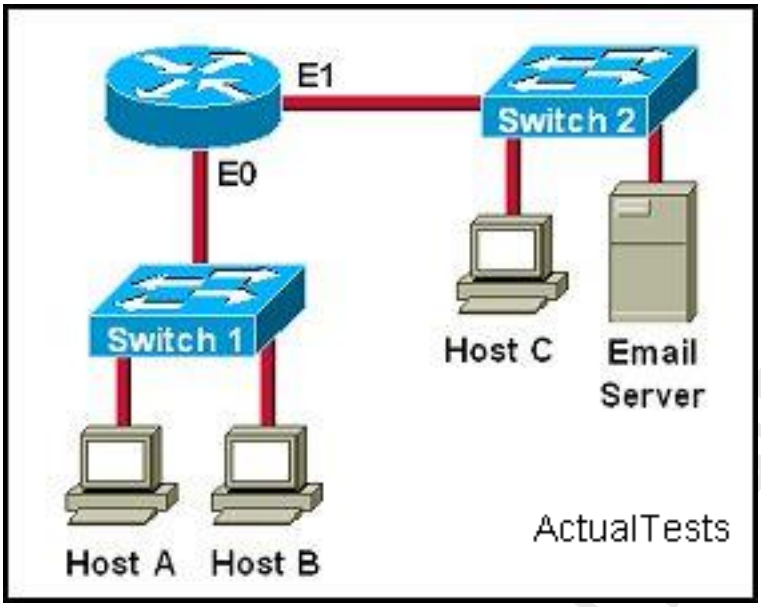


A. The MAC address of host A is FFFF.FFFF.FFFF.
B. The router will forward the packet in this frame to the Internet.
C. The switch will only forward this frame to the attached router interface.
D. All devices in this LAN except host A will pass the packet to Layer 3.

Answer: D

QUESTION NO: 8

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

QUESTION NO: 9

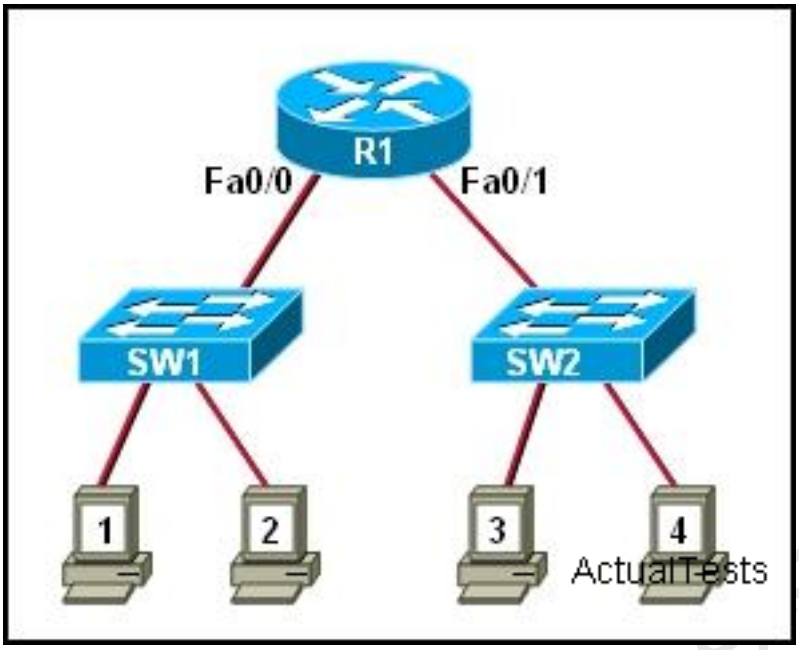
Which two of the following are advantages of Layer 2 Ethernet switches over hubs? (Choose two.)

A. increasing the size of broadcast domains
B. filtering frames based on MAC addresses
C. allowing simultaneous frame transmissions
D. increasing the maximum length of UTP cabling between devices

Answer: B,C

QUESTION NO: 10

Refer to the exhibit. SW1 and SW2 have default configurations. What will happen if host 1 sends a broadcast?



A. Hosts 2, 3, and 4 will receive the broadcast.
B. Hosts 1, 2, 3, and 4 will receive the broadcast.
C. Host 2 and the Fa0/0 interface of R1 will receive the broadcast.
D. Hosts 1, 2 and the Fa0/0 interface of R1 will receive the broadcast.
E. Hosts 1, 2, 3, 4 and interface Fa0/0 of R1 will receive the broadcast.
F. Hosts 2, 3, 4, and interfaces Fa0/0 and Fa0/1 of R1 will receive the broadcast.

Answer: C

QUESTION NO: 11

As a frame leaves a Layer 3 device, the Layer 2 encapsulation information is changed from what it was when it entered the device. For what two reasons can this happen? (Choose two.)

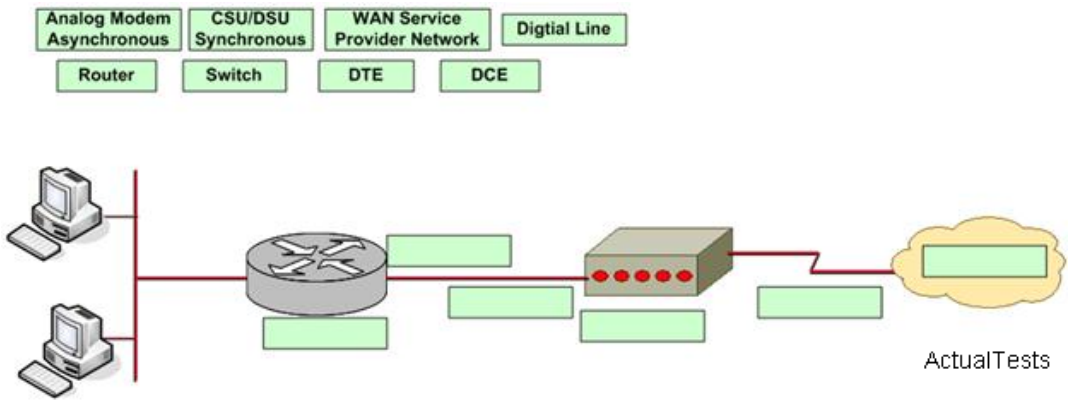
A. The data is moving from 10BASE-TX to 100BASE-TX.
B. The WAN encapsulation type has changed.
C. The data format has changed from analog to digital.
D. The source and destination hosts are in the same subnet.
E. The source and destination MAC addresses have changed.

Answer: B,E

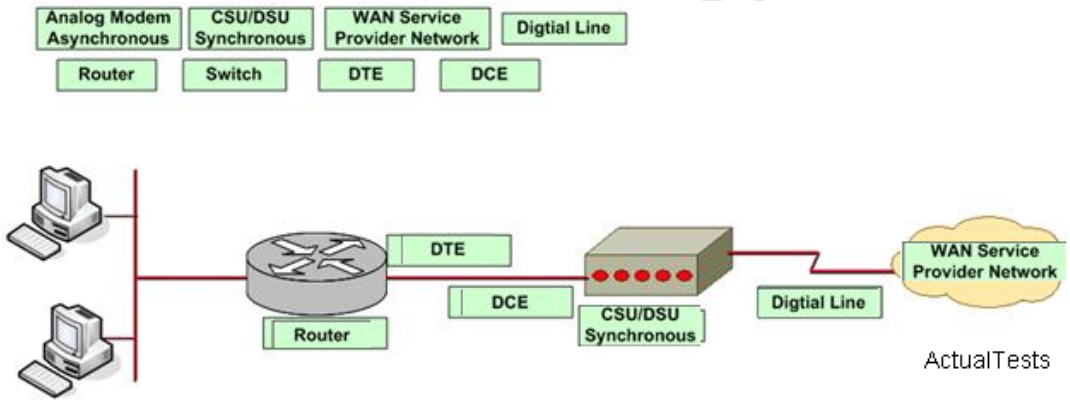
Explanation:
Section 2: Select the components required to meet a network specification (3 questions)

QUESTION NO: 12 DRAG DROP

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



Answer:



QUESTION NO: 13

What are two reasons a network administrator would use CDP? (Choose two.)

A. to obtain VLAN information from directly connected switches
B. to determine the status of network services on a remote device
C. to determine the status of the routing protocols between directly connected routers
D. to verify the type of cable interconnecting two devices
E. to verify Layer 2 connectivity between two devices when Layer 3 fails
F. to obtain the IP address of a connected device in order to telnet to the device

Answer: E,F

Explanation:
Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is an independent media protocol and runs on all Cisco-manufactured devices including routers, bridges, access servers, and switches. It should be noted that CDP is a protocol which works on the layer2. By default, multicast advertise is sent every 60 seconds to 01-00-0 c-cc-cc-cc as the destination address . When reaching the holdtime of 180 seconds , if not receiving the advertise from neighboring devices yet, the information of neighboring devices will be cleared.

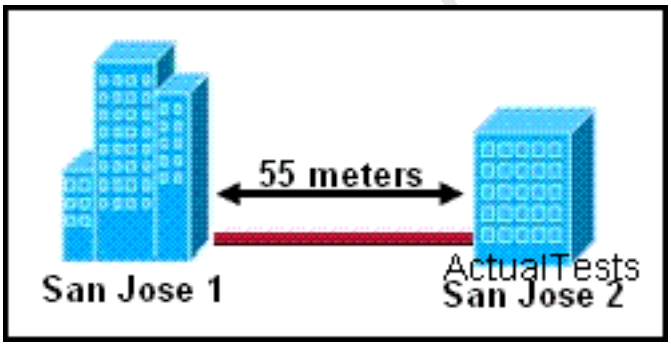
Cisco Discovery Protocol (CDP) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices. By using CDP, you can gather hardware and protocol information about neighbor devices, which is useful info for troubleshooting and documenting the network.

You can use:

Show cdp neighbor
Show cdp neighbor details
Commands to gather the information of connected neighbors.

QUESTION NO: 14

Refer to the exhibit. Two buildings on the San Jose campus of a small company must be connected to use Ethernet with a bandwidth of at least 100 Mbps. The company is concerned about possible problems from voltage potential differences between the two buildings. Which media type should be used for the connection?



A. coaxial cable
B. STP cable
C. UTP cable
D. fiber optic cable

Answer: D

Explanation:
Current Ethernet technology typically comes via either copper UTP or fiber cables. In this scenario the distance between the buildings is only 55 meters so either copper or fiber could be used, as the distance limitation for 100M UTP Ethernet is 100 meters . However, fiber would be a better fit as it is not prone to errors that could occur due to the voltage potential differences. Because fiber is a dielectric material, it's not susceptible to electrical interference. FO-product vendors also claim that fiber systems make secure communications easier. Interference immunity and lack of emissions are givens in FO systems and in the fiber medium itself.
Section 3: Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network (9 questions)

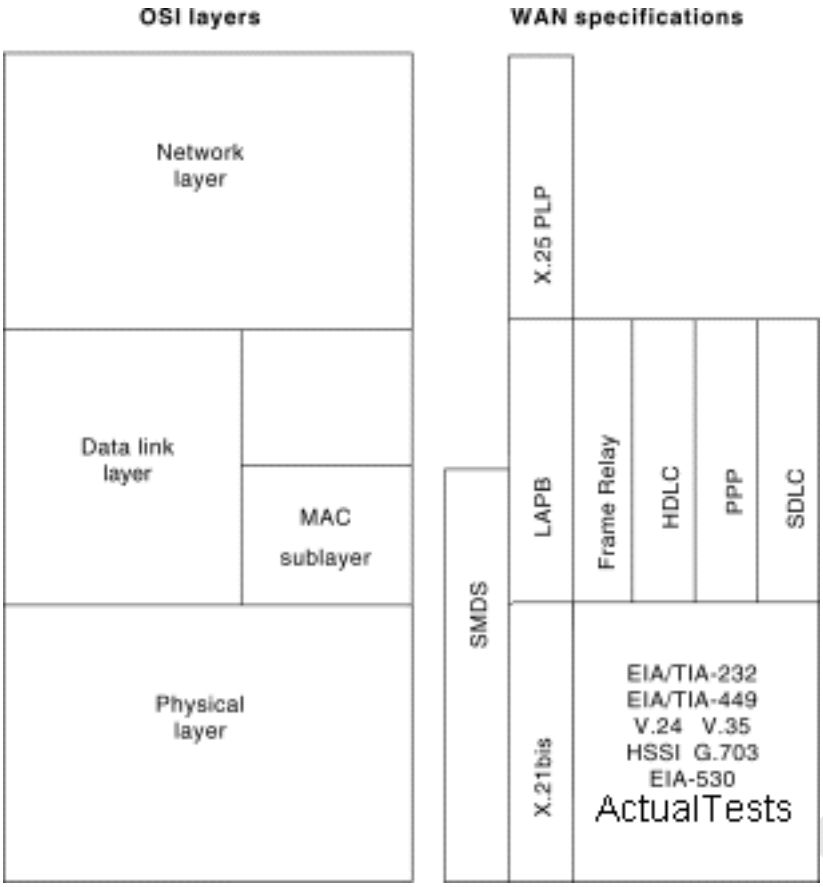
QUESTION NO: 15

It is known that the OSI model has seven layers. Can you tell me at which layers of the OSI model WANs operate? (Choose two.)

A. session layer
B. datalink layer
C. transport layer
D. physical layer

Answer: B,D

Explanation:
A WAN is a data communications network that covers a relatively broad geographic area and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower two layers of the OSI reference model: the physical layer and the data link layer as shown below.



Note: Occasionally WAN's would also be considered to operate at layer 3, but since this question asked for only 2 choices layers 1 and 2 are better choices.

QUESTION NO: 16

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

A. The data link layer adds physical source and destination addresses and an FCS to the segment.
B. The transport layer divides a data stream into segments and adds reliability and flow control information.
C. The presentation layer translates bits into voltages for transmission across the physical link.
D. Packets are created when the network layer adds Layer 3 addresses and control information to a segment.

Answer: B,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.

The Physical Layer (Layer 1) deals with the physical characteristics of the transmission medium. Connectors, pins, use of pins, electrical currents, encoding, and light modulation are all part of different physical layer specifications. Examples includes: EIA/TIA-232, V.35, EIA/TIA-449, V.24, RJ-45, Ethernet, 802.3, 802.5, FDDI, NRZI, NRZ, and B8ZS.

The Transport Layer :

You can think of the transport layer of the OSI model as a boundary between the upper and lower protocols. The transport layer provides a data transport service that shields the upper layers from transport implementation issues such as the reliability of a connection. The transport layer provides mechanisms for:

Segmenting upper layer applications The establishment, maintenance, and orderly termination of virtual circuits Information flow control and reliability via TCP. Transport fault detection and recovery

The Network Layer :

Layer three of the OSI model is the network layer.

The network layer creates and sends packets from source network to destination network.

It provides consistent end-to-end packet delivery services and control information.
It creates and uses layer 3 addresses for use in path determination and to forward packets.

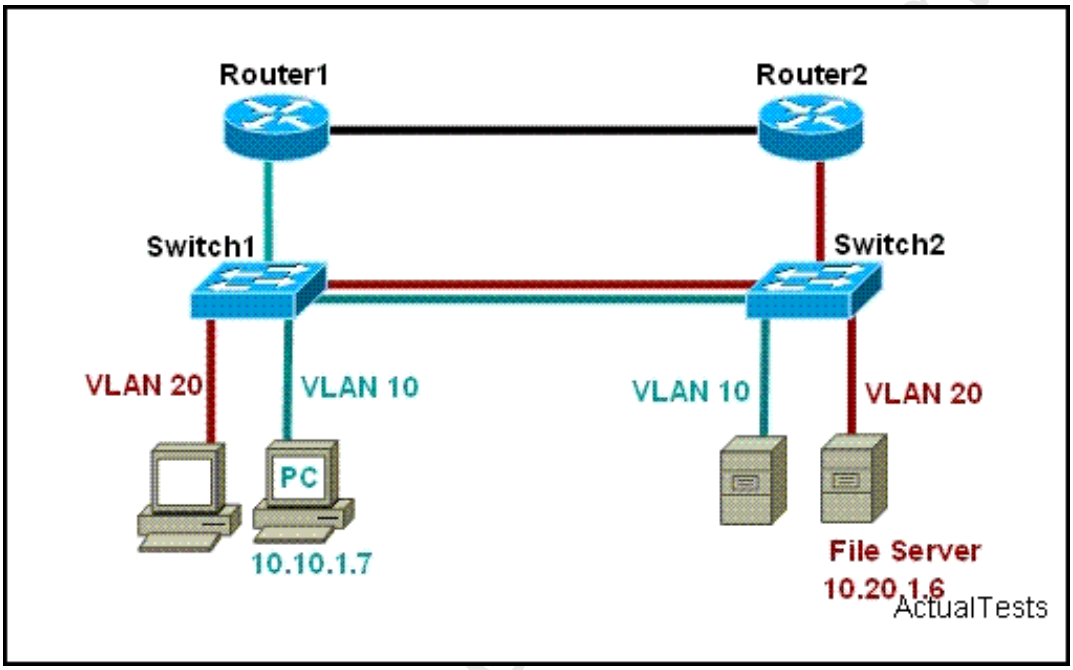
Incorrect Answers:

A: Although the data link layer adds physical (MAC) source and destination addresses, it adds it to a frame, not a segment.

C: This correctly describes the physical layer, not the presentation layer.

QUESTION NO: 17

Refer to the exhibit. The network manager is evaluating the efficiency of the current network design. RIPv2 is enabled on all Layer 3 devices in the network. What network devices participate in passing traffic from the PC at 10.10.1.7 to File Server at 10.20.1.6 in the order that they will forward traffic from source to destination?



A. Switch1, Switch2
B. Switch 1, Router1, Switch1, Switch2
C. Switch1, Router1, Router2, Switch2
D. Switch1, Switch2, Router2, Switch2

Answer: C

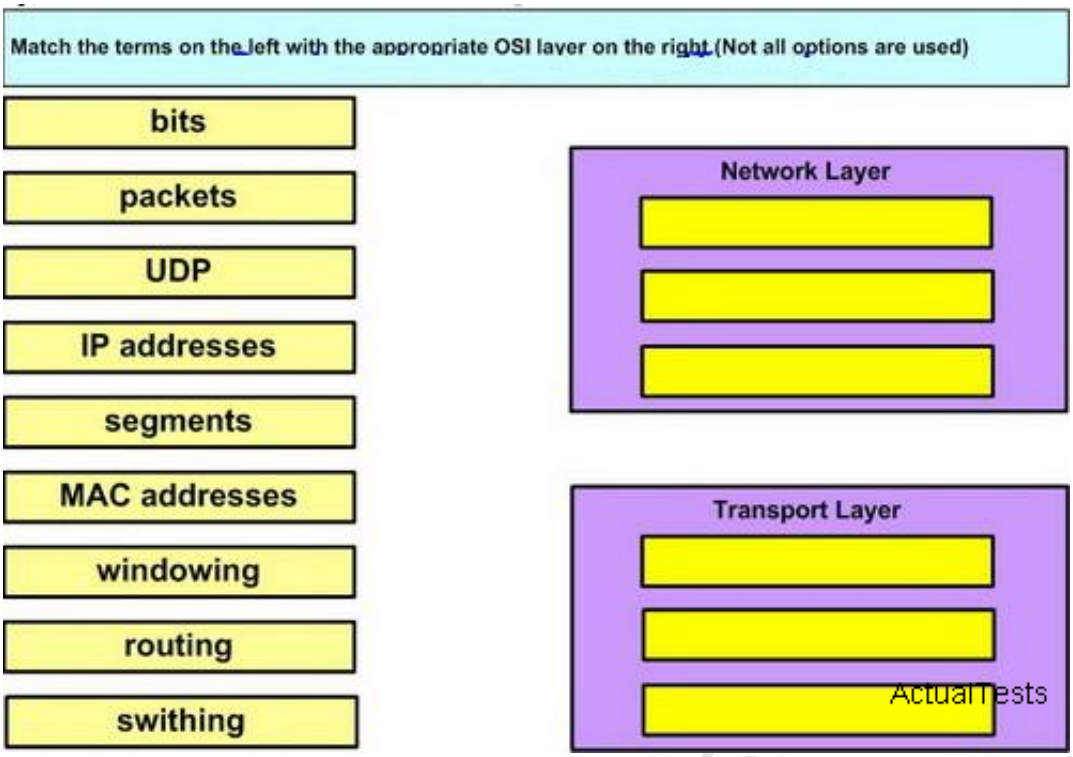
Explanation:

When data traffic is sent from the PC having the 10.10.1.7 IP address to the PC with 10.20.1.6 it goes through Switc1h, Router1, Router1, Switch2. Since the PC and server reside on different IP subnets traffic will need to go through a router.

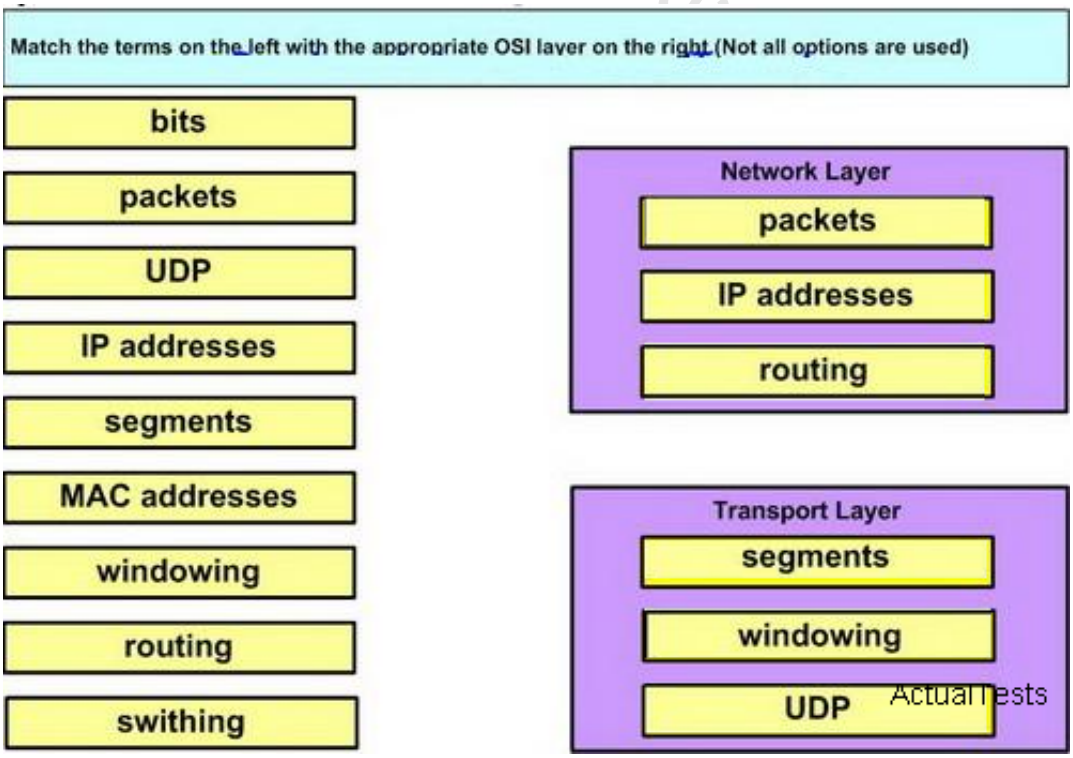
The gateway IP address of PC 10.10.1.7 is the router Switch1's Ethernet IP. So when sending the data it goes to gateway through switch1. When packet reached to router1 it forwards to the router2

based on the routing table. Finally, router2 forwards the packets to the switch2.

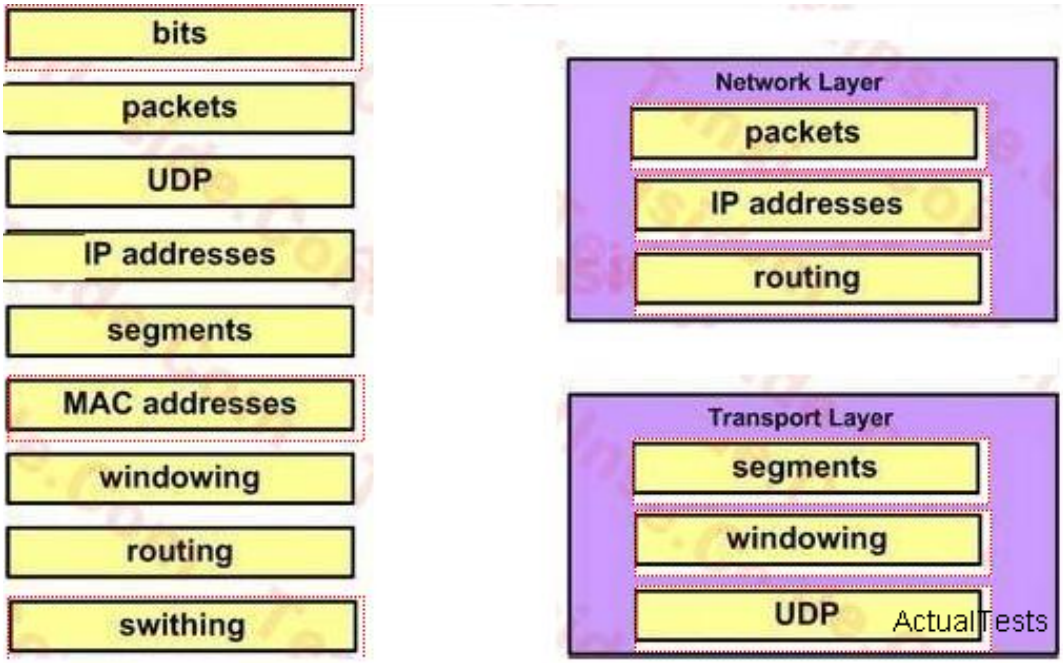
QUESTION NO: 18 DRAG DROP



Answer:



Explanation:



Network layer: Packets, IP addresses, routing
Transport Layer: UDP, segments, windowing

Physical layer: Bit, physical device, cable, NIC
Data link layer: MAC, NIC, Frame

QUESTION NO: 19

At which OSI layer is a logical path created between two host systems?

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

Answer: B

Explanation:
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.

QUESTION NO: 20

As a CCNA candidate, you need to know OSI model very well, a packet is the protocol data unit for which layer of the OSI model?

A. network
B. presentation
C. session
D. data link

Answer: A

Explanation:
PDU, Protocol Data Unit, is a kind of communication data unit, bit for Data layer, frame for data link layer, PDU for network layer, and message for transport layer.

QUESTION NO: 21

As data passes downward through the layers of the OSI model, it is encapsulated into various formats.

Which of the following is the correct order of encapsulation?

A. Bit, frame, packet, segment
B. Segment, packet, frame, bit
C. Segment, frame, packet, bit
D. Bit, packet, frame, segment

Answer: B

Explanation:
The OSI is the Open System Interconnection reference model for communications. As illustrated in Figure 1.1, the OSI reference model consists of seven layers, each of which can have several sublayers. The upper layers of the OSI reference model define functions focused on the application, while the lower three layers define functions focused on end-to-end delivery of the data.

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Interhost communication
	Segment/Datagram	4. Transport	End-to-end connections and reliability
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing (MAC & LLC)
	Bit	1. Physical	Media, signal and binary transmission

QUESTION NO: 22

While troubleshooting a network connectivity problem, a technician observes steady link lights on both the workstation NIC and the switch port to which the workstation is connected. However, when the ping command is issued from the workstation, the output message "Request timed out." is displayed. At which layer of the OSI model does the problem most likely exist?

A. the access layer
B. the application layer
C. the network layer
D. the session layer
E. the data link layer
F. the protocol layer

Answer: C

Explanation:
The ICMP protocol operates at the network layer.

QUESTION NO: 23

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

Answer: C

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.
Section 4: Describe common networked applications including web applications (4 questions)

QUESTION NO: 24

Which of the following services use UDP? (Choose three.)

A. Telnet
B. TFTP
C. SNMP
D. DNS

Answer: B,C,D

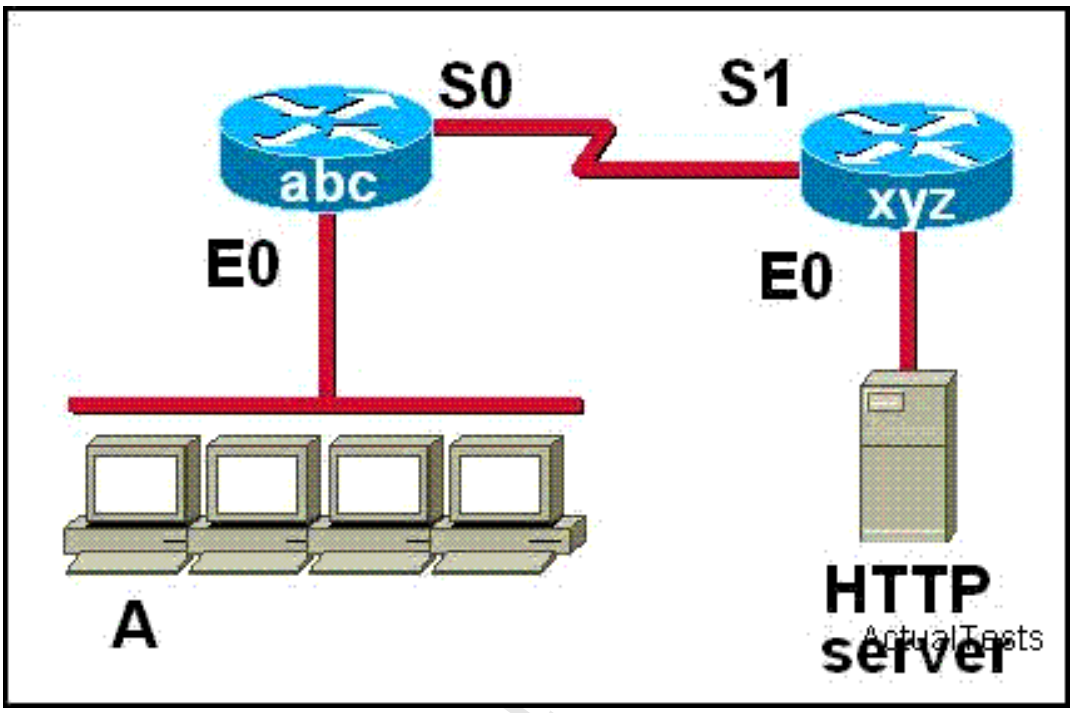
Explanation:
Common TCP/UDP ports:
TCP ports:
20 FTP data
21 FTP control
23 Telnet
25 SMTP
53 DNS
80 WWW
100 POP3
UDP ports:
53 DNS

69 TFTP
161 SNMP
Note: DNS use TCP for regional transmission, and use UDP for name inquiry.

QUESTION NO: 25

Refer to the graphic. Host A has established a connection with the HTTP server attached to interface E0 of the xyz router. Which of the following statements describe the information contained in protocol data units sent from host A to this server? (Choose three.)

Exhibit:



A. The destination IP address of a packet will be the IP address of the network interface of the HTTP server.
B. The destination address of a frame will be the MAC address of the E0 interface of the abc router.
C. The destination address of a frame will be the MAC address of the HTTP server interface.
D. The destination port number in a segment header will have a value of 80.
E. The destination port number in a segment header will have a unique value greater than or equal to 1023.
F. The destination IP address of a packet will be the IP address of the E0 interface of the abc router.

Answer: A,B,D

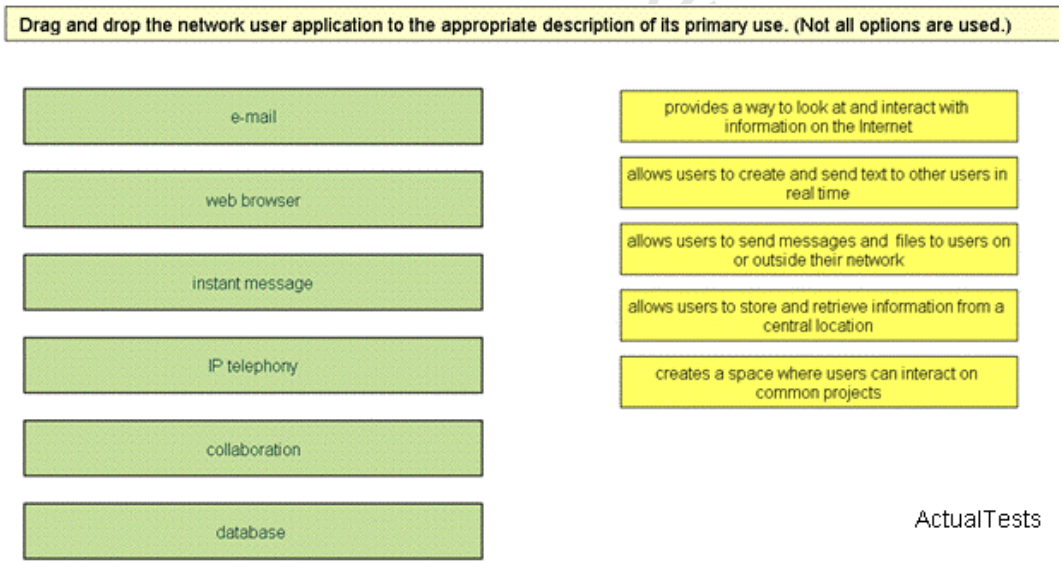
Explanation:

HTTP uses TCP port 80. The source port will be chosen randomly, but not the destination TCP port. The destination IP address will be left unchanged, and since HTTP server is on a remote network, the destination MAC address will be the MAC address of the default gateway (E0 on abc).

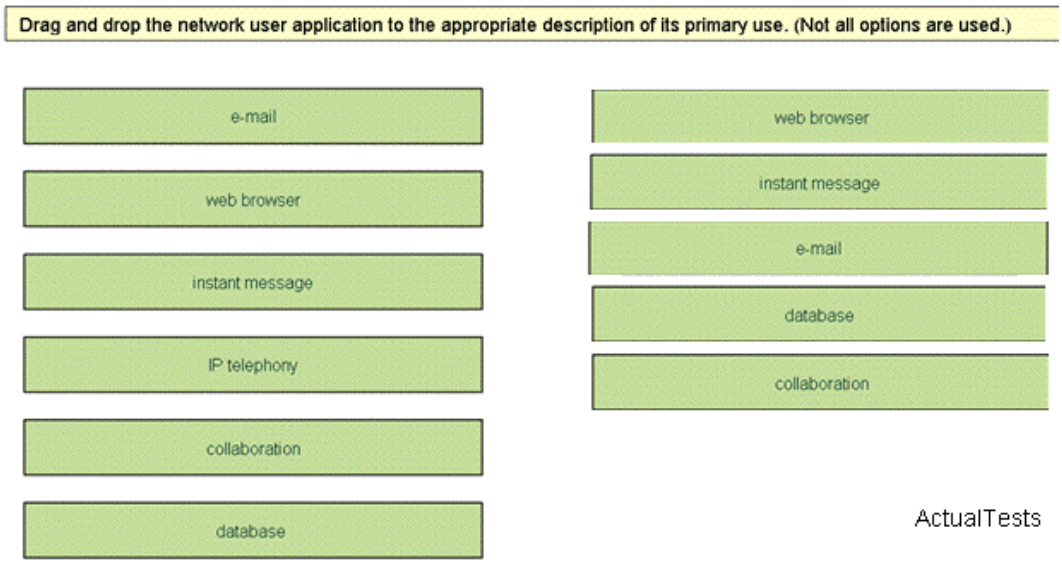
The exhibit shows the communications between the Host ABC and the HTTP Server. The port number of the HTTP server is 80, HTTP Server is connected to the E0 interface of the Router Xyz , so, the IP address is the IP address of E0 interface .
Before sending data packets to the HTTP server, the Host ABC will first send ARP request, the E0 interface of Abc will receive this broadcast ARP information, but it will not forward this broadcast information, so ARP request is still unreachable. Meanwhile, Abc knows the IP address of the HTTP Server which is its destination, so it will use its E0 interface to reply, that is the proxy ARP reply, at this time ,the MAC address is the MAC address of E0 interface of Abc .

Proxy ARP: Proxy ARP is evolved from ARP . If a computer without configuring the default gateway wants to communicate with computers of other networks, when receiving ARP request from the source computer , the gateway will use its own MAC address and the IP address of the destination computer to reply to the source computer.

QUESTION NO: 26 DRAG DROP



Answer:



QUESTION NO: 27

Which of the following are associated with the application layer of the OSI model? (Choose two.)

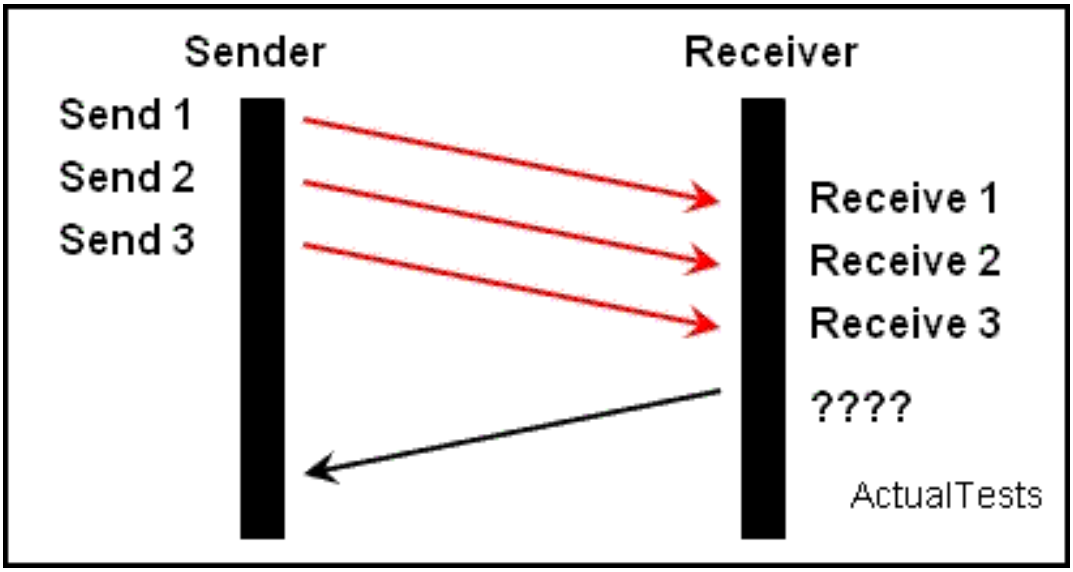
A. IP
B. Telnet
C. TCP
D. FTP
E. ping

Answer: B,D

Explanation:
Ping operates at the network layer; TCP operates at the transportation layer; and IP operates at the network layer.
Section 5: Describe the purpose and basic operation of the protocols in the OSI and TCP models (7 questions)

QUESTION NO: 28

A TCP/IP transfer is diagrammed in the exhibit.

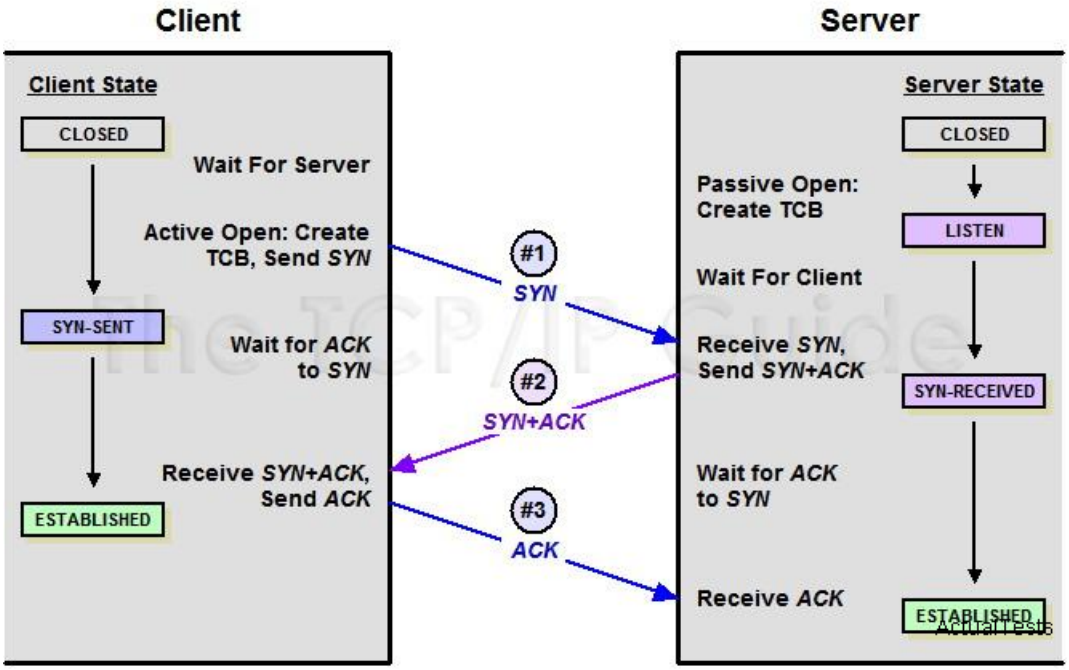


A window size of three has been negotiated for this transfer. Which message will be returned from the receiver to the sender as part of this TCP/IP transfer?

A. send ACK 3
B. send ACK 1-3
C. send ACK 4
D. send ACK 4-6

Answer: C

Explanation:



TCP is knows as a reliable service. Reliable data delivery ensures the integrity of a stream of data sent from one machine to the other through a fully functional data link. It guarantees that the data won't be duplicated or lost. This is achieved through something called positive acknowledgment with retransmission a technique that requires a receiving machine to communicate with the transmitting source by sending an acknowledgment message back to the sender when it receives

data.

The sender documents each segment it sends and waits for this acknowledgment before sending the next segment. When it sends a segment, the transmitting machine starts a timer and retransmits if it expires before an acknowledgment is returned from the receiving end. In this case, 3 segments were received, so the receiver sends back an ACK value of 4 as it is expecting the 4 th segment next.

QUESTION NO: 29

As a CCNA candidate, you will be expected to know the OSI model very well. Acknowledgements, sequencing, and flow control are characteristics of which OSI layer?

A. Layer 3
B. Layer 5
C. Layer 4
D. Layer 2
E. Layer 7
F. Layer 6

Answer: C

Explanation:
Layer 2 data link layer: This layer implements data sub-frame and deals with flow control. The layer also designates topology and provides hardware addressing;
Layer 3 network layer: This layer creates links between two nodes by addressing, including the routing and data trunking through interconnected network;
Layer 4 transport layer: routine data transmission, connected or non-connected, Includes full-duplex or half-duplex, flow control and error recovery services;
Layer 5 Session Layer: create links in-between two nodes. This service includes the establishment connection in manners of half-duplex or full-duplex, although full-duplex can be dealt with in layer 4.

QUESTION NO: 30

As a teacher in Cisco academe, you need to describe the various types of flow control to your students. Which of the following are types of flow control that can be used in a network? (Choose three)

A. congestion avoidance
B. buffering

C. windowing
D. load balancing

Answer: A,B,C

Explanation:
Buffering, including receive buffer and send buffer, is a temporary data storage area. Windowing is used for flow control, to prevent the flooding of data from sending end to receiving end, and thus avoid over flow of receiving end buffer. The size of window use packet byte as a unit, not packet amount. Windowing belongs to TCP flow control. Supported by monitoring network communications loading, congestion avoiding mechanism is able to predict and avoid congestion of common network bottlenecks point. With the use of complex algorithms (rather than simply discarding Tail Drop) to discard the packet, switches can avoid congestion.

QUESTION NO: 31

As a CCNA candidate, you will be expected to know the OSI model very well.

Why does the data communication industry use the layered OSI reference model? (Choose two.)

A. It provides a means by which changes in functionality in one layer require changes in other layers.
B. It encourages industry standardization by defining what functions occur at each layer of the model.
C. It supports the evolution of multiple competing standards, and thus provides business opportunities for equipment manufacturers.
D. It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.

Answer: B,D

Explanation:
The Open Systems Interconnection Basic Reference Model (OSI Reference Model or OSI Model) is an abstract description for layered communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative. In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the OSI Seven Layer Model.
A layer is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path.

The OSI (Open System Interconnection) reference model was created as a reference point for communications devices. A layered approach is used to segment the entire telecommunications process into a series of smaller steps.
A is correct because it encourages a level of standardization by encouraging that functions be compared to known layers. D is also correct because it allows engineers to focus on the development, refining, and perfection of simpler components.

QUESTION NO: 32

Which of the following protocols uses both TCP and UDP ports?

A. FTP
B. Telnet
C. SMTP
D. DNS

Answer: D

Explanation:
For further information please check RFC1035, reference link http://www.ietf.org/rfc/rfc1035.txt

The following port numbers for the protocols listed above are as follows:

FTP: TCP Port 20 and 21
SMTP: TCP Port 25
Telnet: TCP Port 23
DNS: both TCP and UDP Port 53

QUESTION NO: 33

Which of the following services use TCP? (Choose three.)

A. SNMP
B. SMTP
C. FTP
D. HTTP

Answer: B,C,D

Explanation:
TCP (Transmission Control Protocol) is a transport layer protocol which is connection-oriented, reliable, and based on byte-stream, usually stated by IETF RFC 793.
SMTP (Simple Mail Transfer Protocol): SMTP is a protocol that offers reliable and valid e-mail

transmission.
FTP (File Transfer Protocol): it is used for two-way transmission of control document On the Internet. It is also an application. Users are able to connect their PC to all servers operating FTP protocol all over the world, access a large number of programs and information.
HTTP (HyperText Transfer Protocol) is used to send the WWW data. For further information, please refer to RFC2616. HTTP protocol uses the request/response model. Client send a request to server, which contains request methods, URI, protocol version, and message structure, similar to MIME, which contains request modifier, customer information and content. Server use state as a response, relevant content includes message protocol agreement, success or error code, server information, entity meta-information and entity content if possible.

TCP (Transmission Control Protocol) is a reliable mechanism for data delivery. SMTP, FTP and HTTP services use TCP via ports 25, 20/21, and 80, respectively.

QUESTION NO: 34

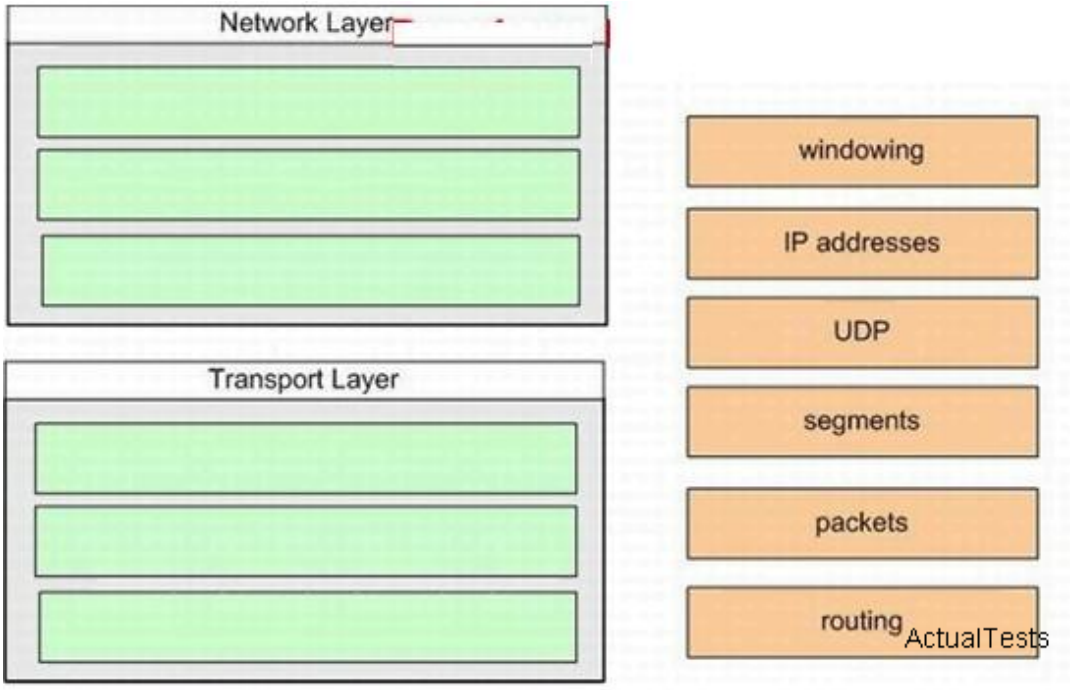
What is the purpose of an ARP request message?

A. It encapsulates the Layer 3 address and then passes the packet to Layer 2.
B. It binds the IP address of a host to the network that it is on.
C. It builds a correlation between an IP address and a MAC address.
D. It creates a session by passing a header with the destination Layer 2 address to the transport layer.
E. It provides connectivity and path selection between hosts on a network.

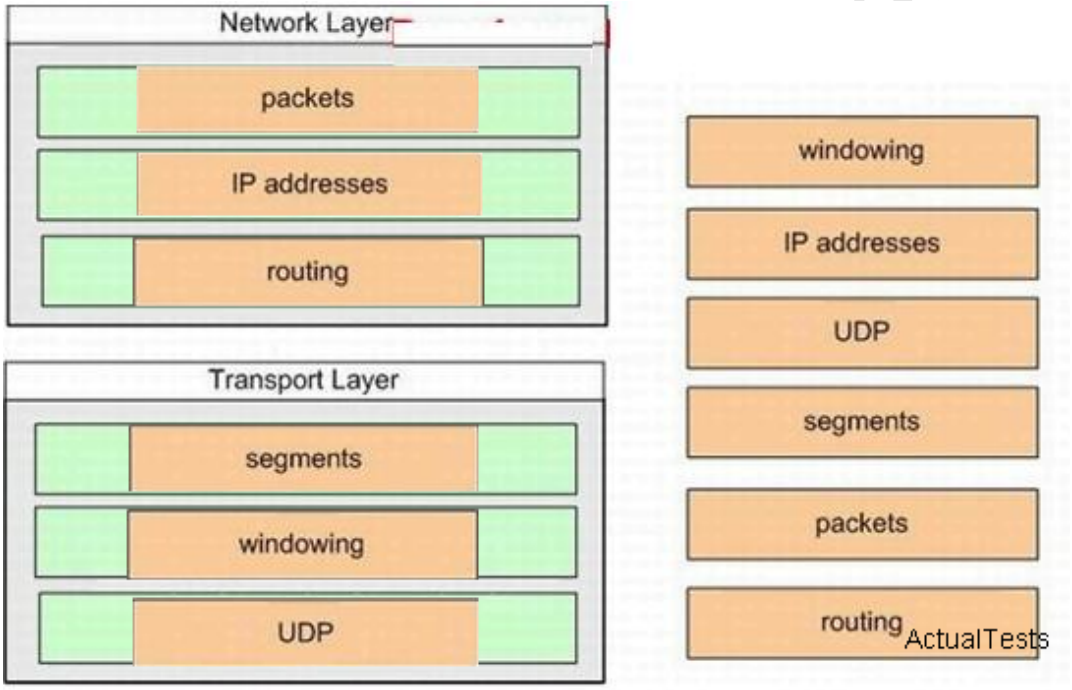
Answer: C

QUESTION NO: 35 DRAG DROP

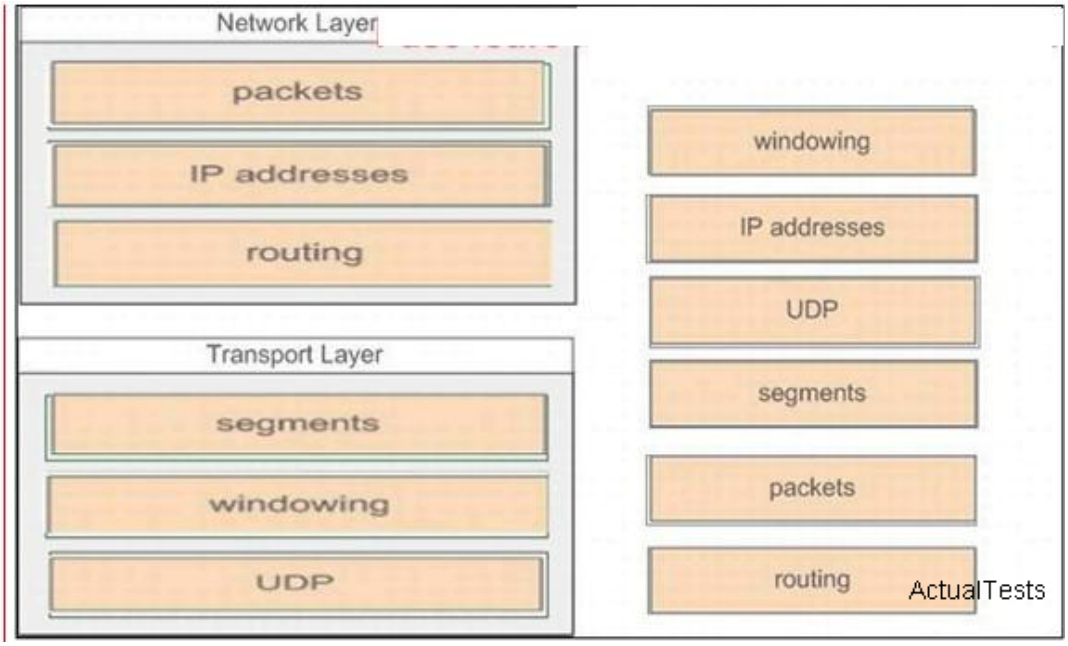
The left describes OSI layers, while the right provides some terms. Drag the items on the right to the proper locations.



Answer:



Explanation:



Section 6: Describe the impact of applications (Voice Over IP and Video Over IP) on a network (1 question)

QUESTION NO: 36

A company is installing IP phones. The phones and office computers connect to the same device. To ensure maximum throughput for the phone data, the company needs to make sure that the phone traffic is on a different network from that of the office computer data traffic. What is the best network device to which to directly connect the phones and computers, and what technology should be implemented on this device? (Choose two.)

A. VLAN
B. hub
C. STP
D. subinterfaces
E. router
F. switch

Answer: A,F

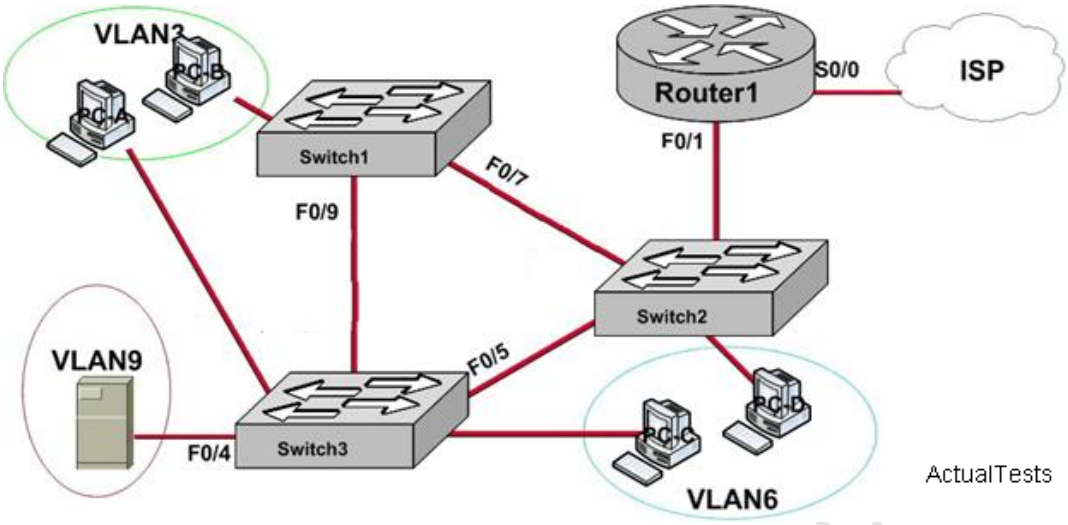
Explanation:
You can configure VLANs on the switch to distinguish two types of data traffic.
Section 7: Interpret network diagrams (3 questions)

QUESTION NO: 37

Refer to the exhibit. A technician is investigating a problem with the network that is shown. The router is a 2800 model and all switches are 2950 models. These symptoms have been observed:

- All of the user hosts can access the Internet.
- None of the user hosts can access the server located in VLAN 9.
- All of the hosts can ping each other.

What could cause these symptoms?



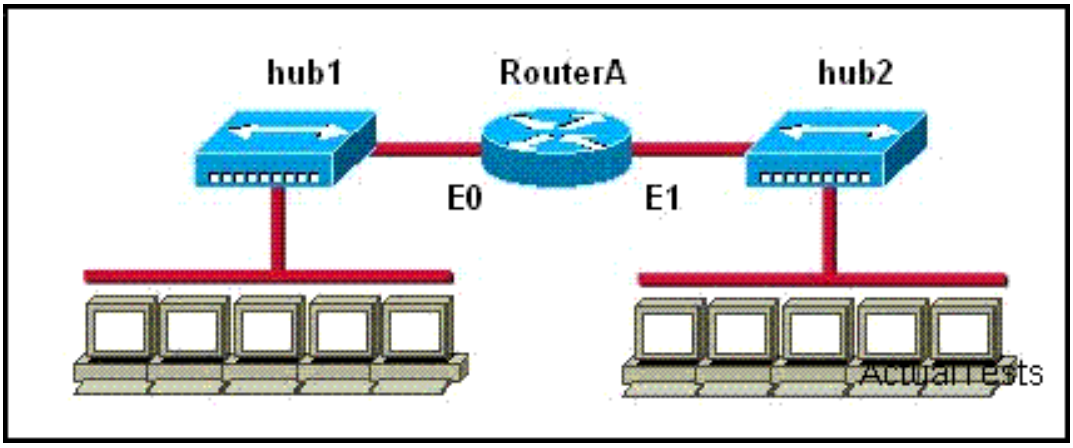
A. Interface Fa1/0 on the Router1 is down.
B. Interface S0/0 on the Router1 is down.
C. Trunking is not enabled on the link between Switch3 and Switch1.
D. Interface Fa0/4 on Switch1 is down.

Answer: D

Explanation:
A Router is used for communication between different VLANs and it is stated that none of the hosts can access the server in VLAN 9 it means that there is no connection of the network with router so FA1/0 is down. In this example, connectivity problems only occur with inter-VLAN communication, which means the problem is with the routing element.
Incorrect Answers:
A: This choice is wrong because Host C can ping Host D so FA0/5 cannot be down.
B: This may indeed be true, but until the LAN interface problems of the router are resolved, it is not an issue. If this was the only problem, then there would be no problems with Host A trying to reach Host C or D.

QUESTION NO: 38

Refer to the graphic. How many collision domains are shown?



A. four
B. one
C. six
D. fourteen
E. three
F. two

Answer: F

Explanation:
The hub cannot segment the network into collision domains. Each part connected to RouerA is considered as a collision domain.

The multi-segment configuration guidelines apply only to a single Ethernet "collision domain." A collision domain is formally defined as a single CSMA/CD network in which there will be a collision if two computers attached to the system transmit at the same time. An Ethernet system composed of a single segment or multiple segments linked with repeaters is a network that functions as a single collision domain.

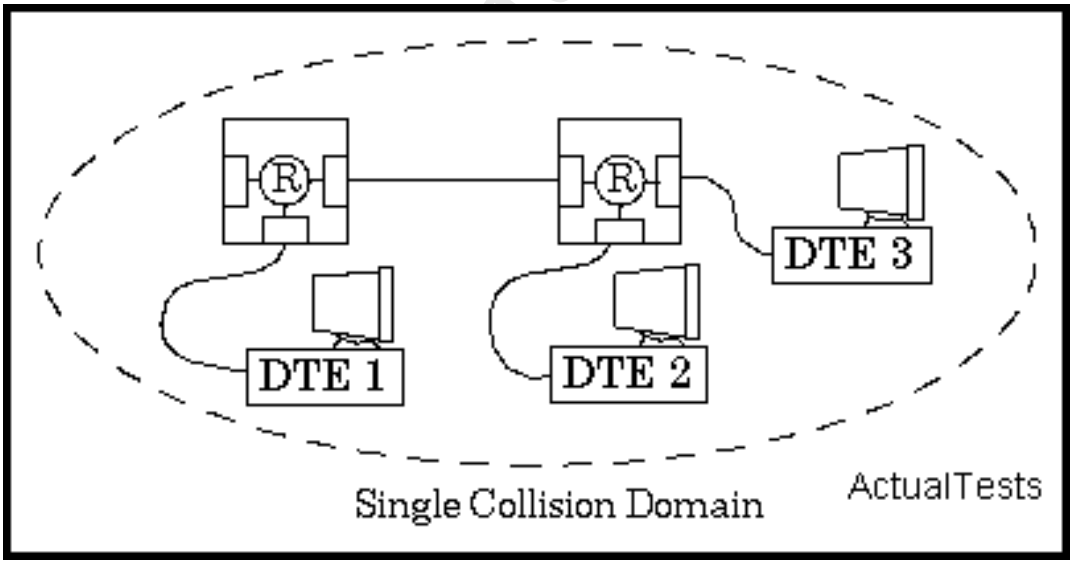


FIGURE 1 Repeater hubs create a single collision domain

The figure shows two repeater hubs connecting three computers. Since only repeater connections

are used between segments in this network, all of the segments and computers are in the same collision domain.

In the next figure, the repeaters and DTEs are instead separated by a router (packet switch) and are therefore in separate collision domains, since routers do not forward collision signals from one segment to another. Routers contain multiple Ethernet interfaces and are designed to receive a packet on one Ethernet port and transmit the data onto another Ethernet port in a new packet.

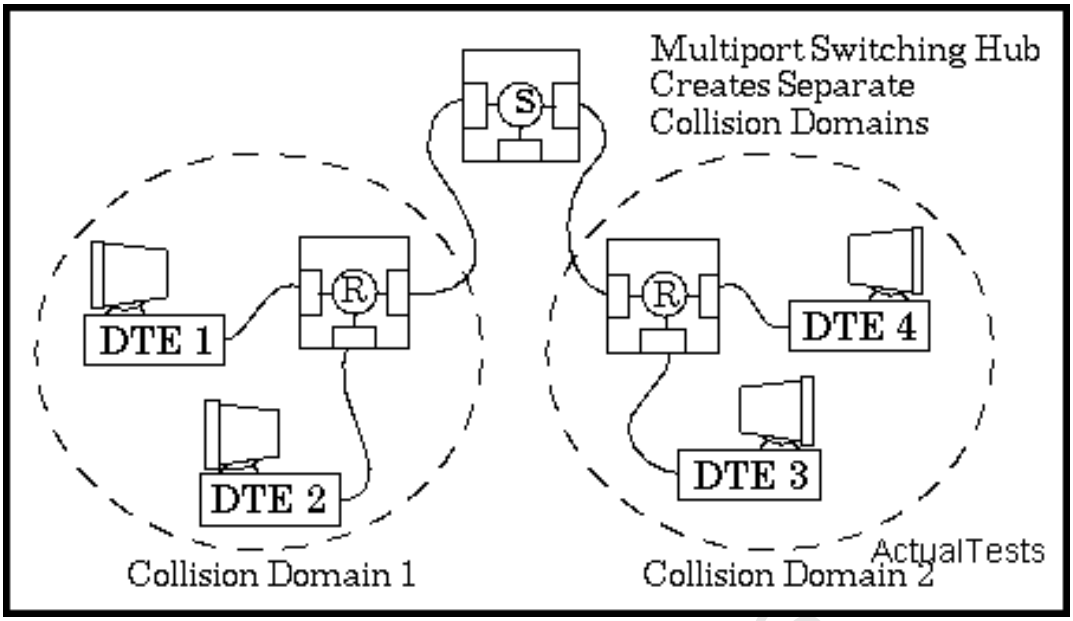
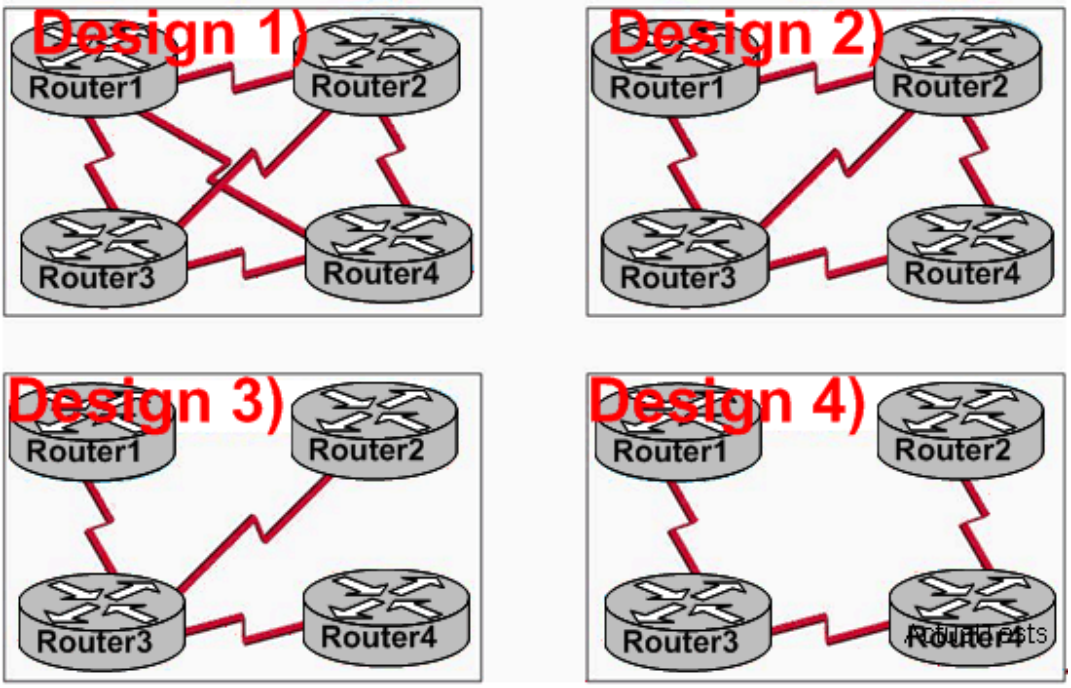


FIGURE 2 Routers creates separate collision domains

Instead of propagating collision signals between Ethernet segments, routers interrupt the collision domain and allow the Ethernets they link to operate independently. Therefore, you can use packet switching hubs to build larger network systems by interconnecting individual Ethernet systems.

QUESTION NO: 39

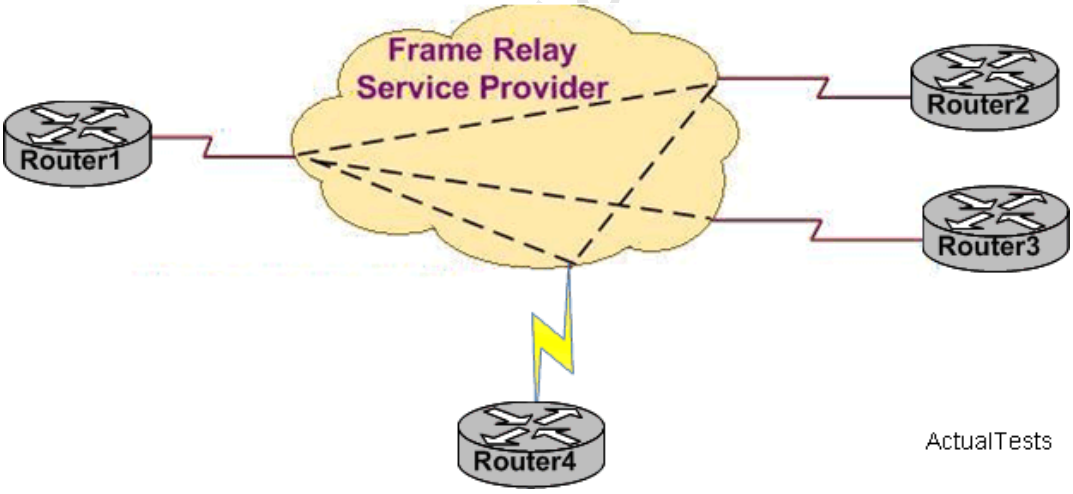
A network administrator is designing a new corporate internetwork. The corporation is concerned about downtime due to link failure and also about link costs. Which topology will provide some redundancy to increase reliability for all sites but will cost less than a fully redundant topology?



A. Design4
B. Design1
C. Design2
D. Design3

Answer: C

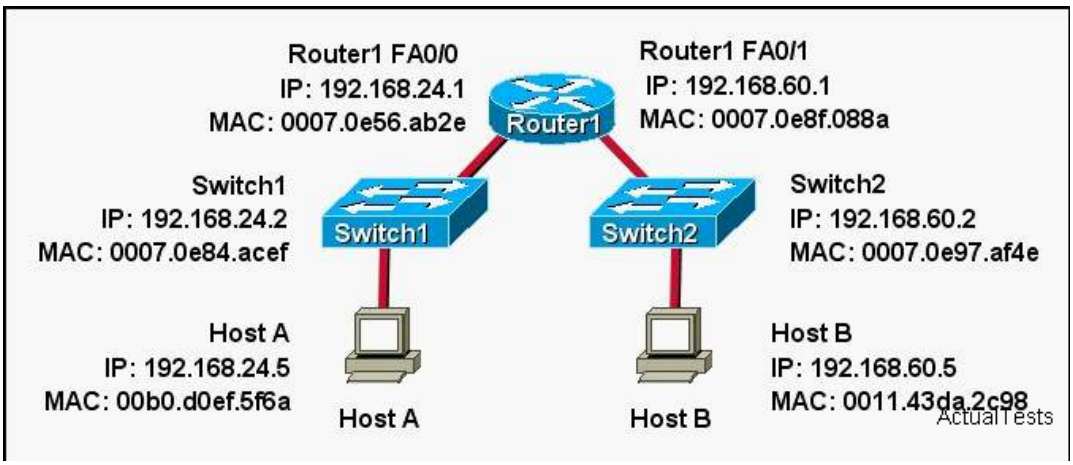
Explanation:
Partial-mesh network topology in Frame Relay network should be considered (not all nodes have the entire physical connection to other nodes), to reduce costs.
Take the following topology as an example:



Section 8: Determine the path between two hosts across a network (7 questions)

QUESTION NO: 40

Refer to the exhibit. What is the correct addressing for a frame and packet received by Host B from Host A?



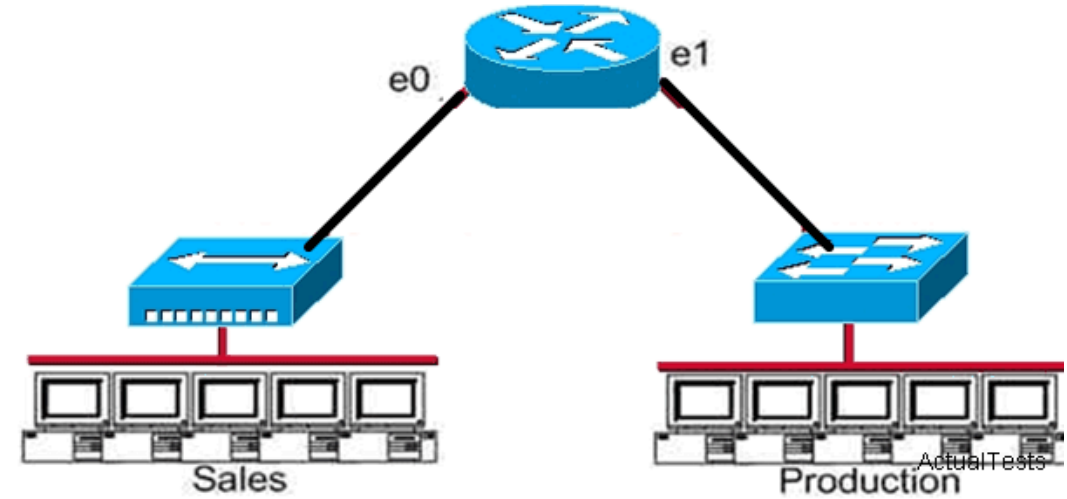
A. Destination MAC: 0011.43da.2c98
Source MAC: 0070.0e8f.088a
Destination IP: 192.168.60.5
Source IP: 192.168.24.5
B. Destination MAC: 0011.43da.2c98
Source MAC: 00b0.d0ef.5f6a
Destination IP: 192.168.60.5
Source IP: 192.168.24.5
C. Destination MAC: 0011.43da.2c98
Source MAC: 0070.0e8f.088a
Destination IP: 192.168.60.5
Source IP: 192.168.60.1
D. Destination MAC: 0011.43da.2c98
Source MAC: 0070.0e97.af4e
Destination IP: 192.168.60.5
Source IP: 192.168.60.2

Answer: A

Explanation:
When packets leave from the host, the packets contains the source MAC and IP of the host address. The source and destination IP address will not change. Because the host knows that the destination is on another subnet, it will forward the packet to the default gateway device, so the destination MAC address will be of the default gateway, which is the FA0/0 interface of router1.

QUESTION NO: 41

Refer to the graphic. Workstation A in the Sales location is communicating with the server in the Production location. What will be the source MAC address of the frames received by workstation A from the server?



-

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

Answer: D

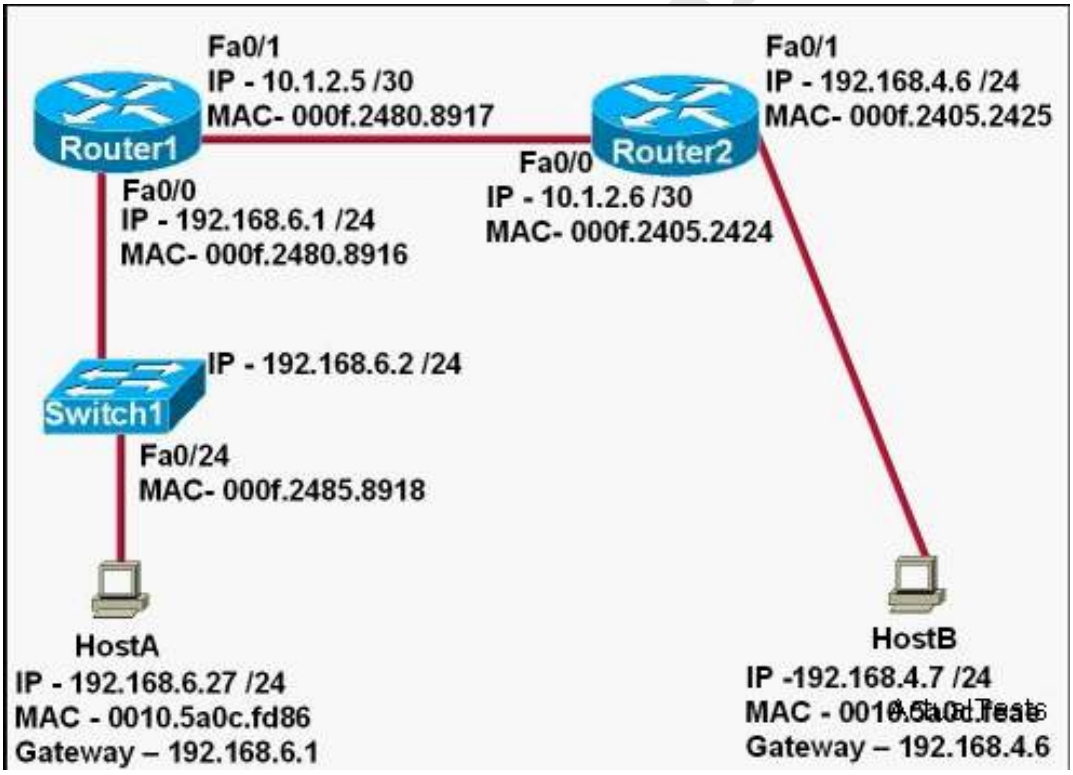
Explanation:
Whereas switches can only examine and forward packets based on the contents of the MAC header, routers can look further into the packet to discover the network for which a packet is destined. Routers make forwarding decisions based on the packet's network-layer header (such as an IPX header 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.
Figure 5 shows the contents of a packet before and after it has been forwarded by a router. Figure 5 also shows the contents of the router's routing tables.

The network of the sales department and the production department is separated by the router. From a technical point of view, regardless of data transmitted from the sales department to the production department, or the contrary, these data will be encapsulated and de-encapsulated several times. In this process, the layer3 address ???????¡ì???C the IP address included in the data will not have any change. Because of cross network segment addressing, IP addresses can be used to locate for devices. But the layer2 MAC address will be replaced by a new in certain network segment. In this subject, when receiving data from the host called server of the production department to the host named workstation A of the sales department, the router will re-encapsulate layer2 address to replace the MAC address whose MAC address is the address of its E0 interface .

QUESTION NO: 42

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

Answer: D

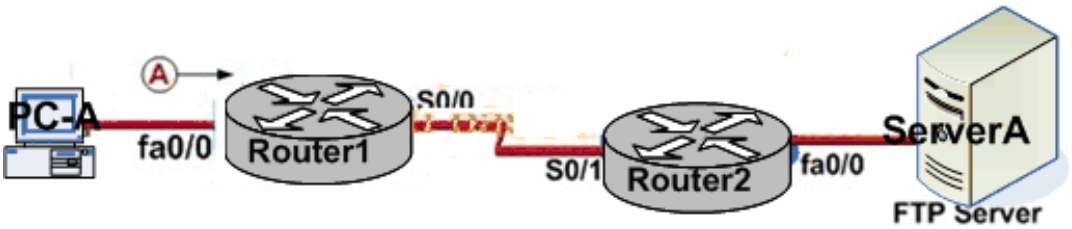
Explanation:
Configuring HostA with a default gateway to Router1, HostA knows that the destination host-HostB is in another network segment, so , Host A will not send ARP request directly to 192.168.4.7, instead , it will achieve its purpose with the help of its gateway 192.168.6.1. Therefore, HostA will send an ARP request to Router1, the gateway will advertise back its MAC address of interface Fa0/0. HostA will store this MAC address into its ARP cache.

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 (Router2).

QUESTION NO: 43

In the network below, host PC-A is transferring a file to the FTP server. Point A represents the frame as it goes toward router1. What will the Layer 2 destination address be at this point?



	IP Address	MAC Address
PC-A	192.168.1.5	abcd.1123.0045
fa0/0 (Router1)	192.168.1.1	abcd.2246.0035
fa0/0 (Router2)	192.168.7.1	aabb.7777.3333
FTP Server	192.168.7.17	aabb.5555.2222

ActualTests

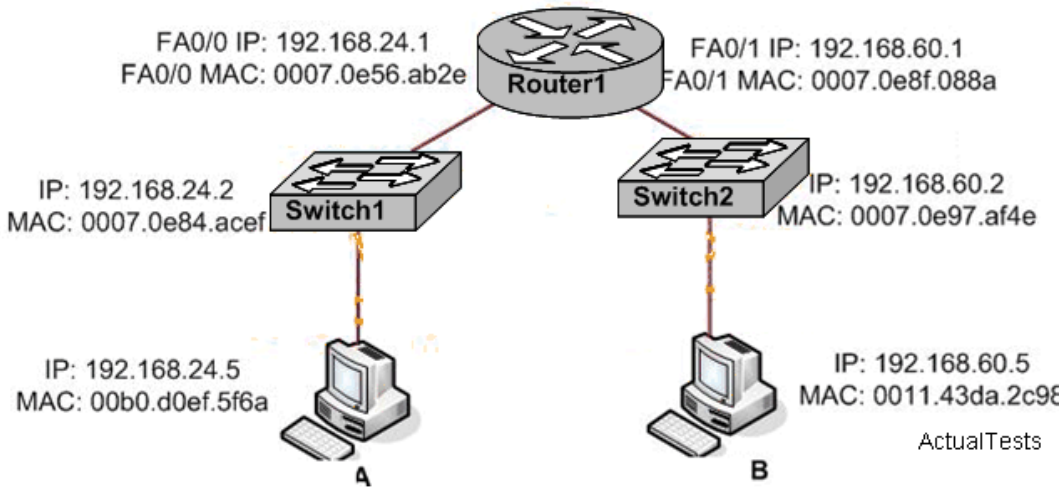
A. abcd.2246.0035
B. 192.168.1.1
C. 192.168.7.17
D. abcd.1123.0045

Answer: A

Explanation:
For packets destined to a host on another IP network, the destination MAC address will be the LAN interface of the router. Since the FTP server lies on a different network, the host will know to send the frame to it's default gateway, which is Router1.

QUESTION NO: 44

Refer to the exhibit. Host A needs to send data to Host B. Which Layer 2 and Layer 3 destination addresses will be used to send the data from Host A to Host B?



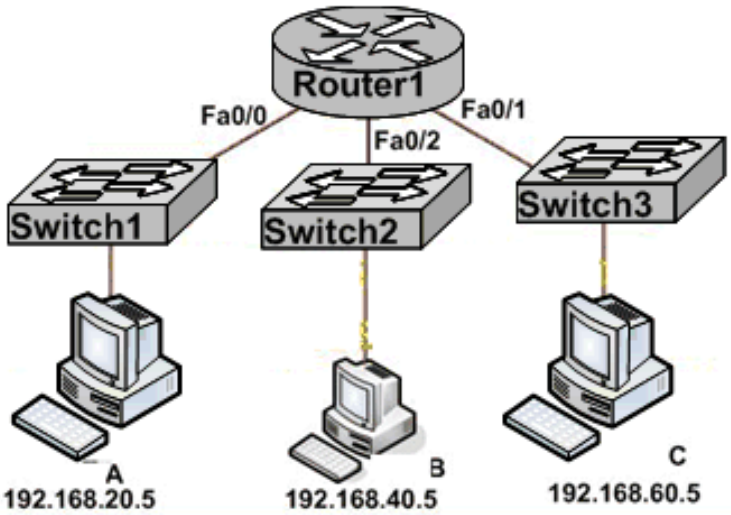
A. 192.168.24.2 and 0007.0e84.acef
B. 192.168.60.5 and 0007.0e56.ab2e
C. 192.168.60.5 and 0011.43da.2c98
D. 192.168.24.1 and 0007.0e56.ab2e

Answer: B

Explanation:
When packets leave from the host, the packets contains the source MAC and IP of the host address. The source and destination IP address will not change. Because the host knows that the destination is on another subnet, it will forward the packet to the default gateway device, so the destination MAC address will be of the default gateway, which is the FA0/0 interface of router Switch2.

QUESTION NO: 45

Refer to the exhibit. Host A is to send data to Host B. How will ROUTER1 handle the data frame received from Host A? (Choose three.)



Router1# show ip arp

Protocol	Address	Age(min)	Hardware Addr	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	-	0000.0c07.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	-	0000.0c63.6965	ARPA	FastEthernet0/2

A. ROUTER1 will strip off the destination MAC address and replace it with the MAC address of Host B
B. ROUTER1 will strip off the source IP address and replace it with the IP address on the forwarding FastEthernet interface.
C. ROUTER1 will forward the data frame out interface FastEthernet0/2.
D. ROUTER1 will strip off the source MAC address and replace it with the MAC address on the forwarding FastEthernet interface.

Answer: A,C,D

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

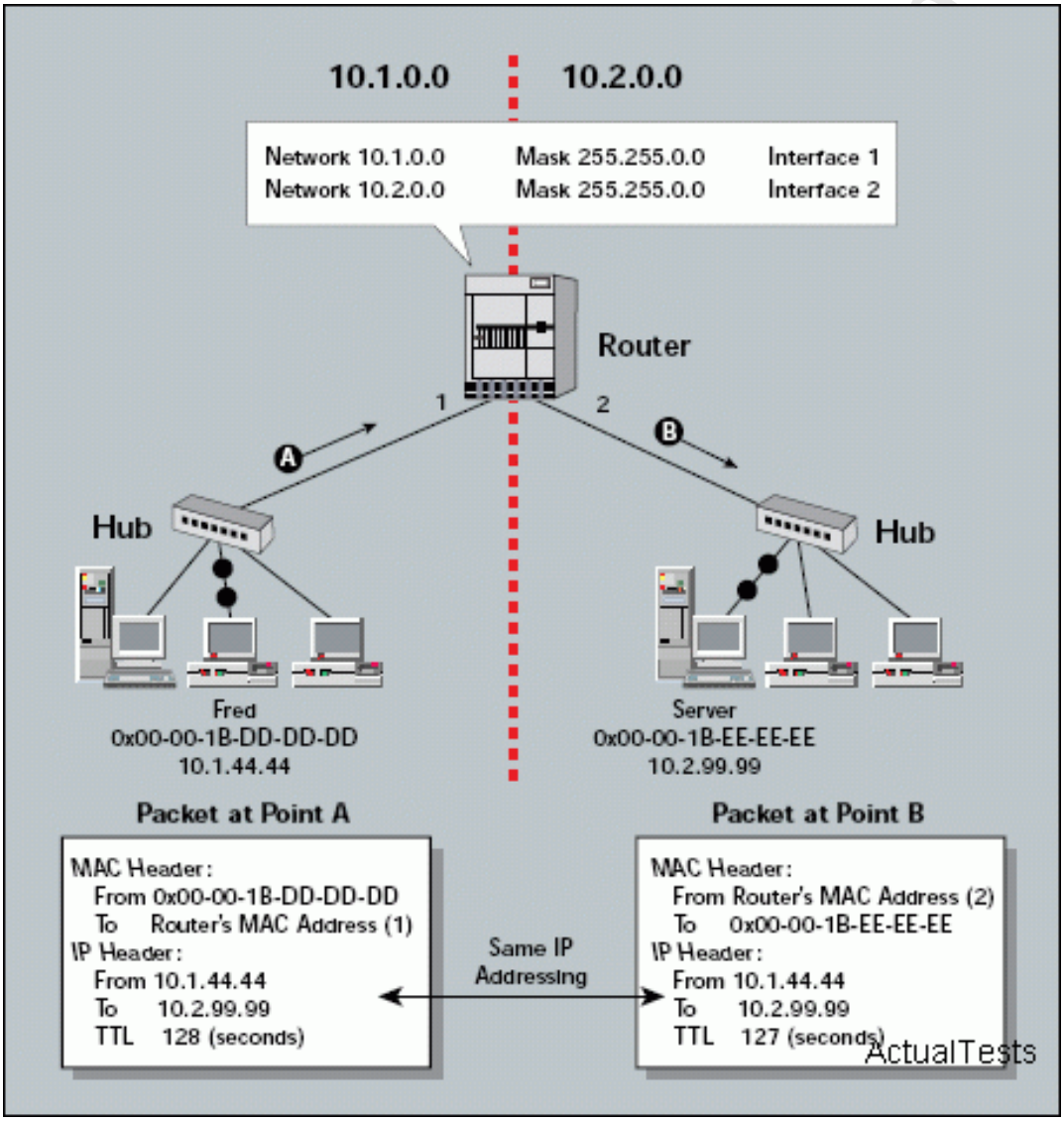
packet is forwarded through each router, the IP TTL value decrements as the IP packet is forwarded through each router. If an IP packet has a TTL value of 1, the router discards the packet. A router cannot decrement the TTL value to 1 and then forward the packet.

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.

Figure 5 shows the contents of a packet before and after it has been forwarded by a router. Figure 5 also shows the contents of the router's routing tables.

Figure 5: Routers forward packets based on the network address.



QUESTION NO: 46

Refer to the exhibit. The partial frame shown in the exhibit displays select header information as it arrives at the destination host. Which graphic represents the correct header information in the responding frame returned to the remote host?

Destination	Source	Destination	Source	Destination	Source	SYN	ACK
000d.56ad.a313	000a.8a47.e612	192.168.14.1	192.168.14.2	23	42335	1	0

A.

Destination	Source	Destination	Source	Destination	Source	SYN	ACK
000a.8a47.e612	000d.56ad.a313	192.168.14.2	192.168.14.1	23	42335	0	1

B.

Destination	Source	Destination	Source	Destination	Source	SYN	ACK
000a.8a47.e612	000d.56ad.a313	192.168.14.2	192.168.14.1	23	42336	1	1

C.

Destination	Source	Destination	Source	Destination	Source	SYN	ACK
000d.56ad.a313	000a.8a47.e612	192.168.14.1	192.168.14.2	42335	23	0	1

D.

Destination	Source	Destination	Source	Destination	Source	SYN	ACK
000a.8a47.e612	000d.56ad.a313	192.168.14.2	192.168.14.1	42335	23	1	1

E.

Destination	Source	Destination	Source	Destination	Source	SYN	ACK
000d.56ad.a313	000a.8a47.e612	192.168.14.2	192.168.14.1	42336	23	0	0

A. A
B. B
C. C
D. D
E. E

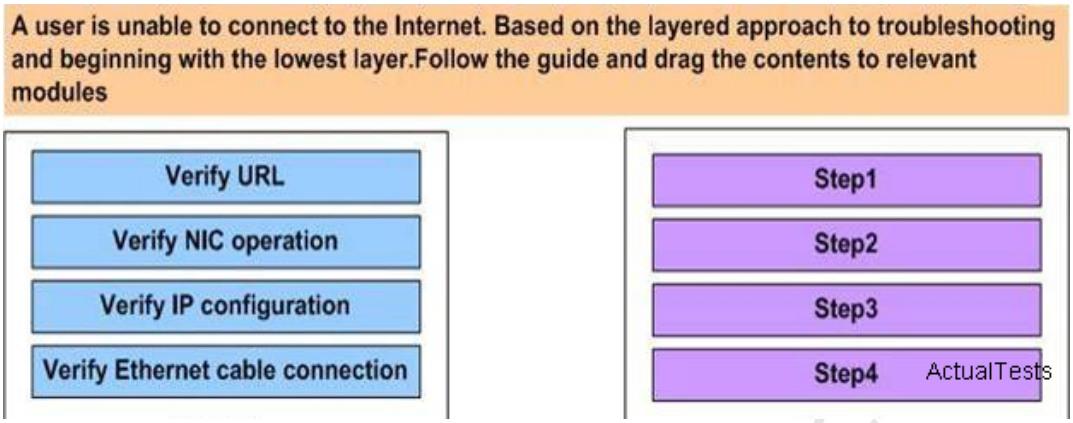
Answer: D

Explanation:
On the basis of the layer3 information of the datagram header provided in the subject, remote devices and destination devices are in the same network segment. So , when remote devices reply to this data, the source and the destination address of layer2 information will transfer order, so do the layer3 and layer4 information.
Section 9: Describe the components required for network and Internet communications (0

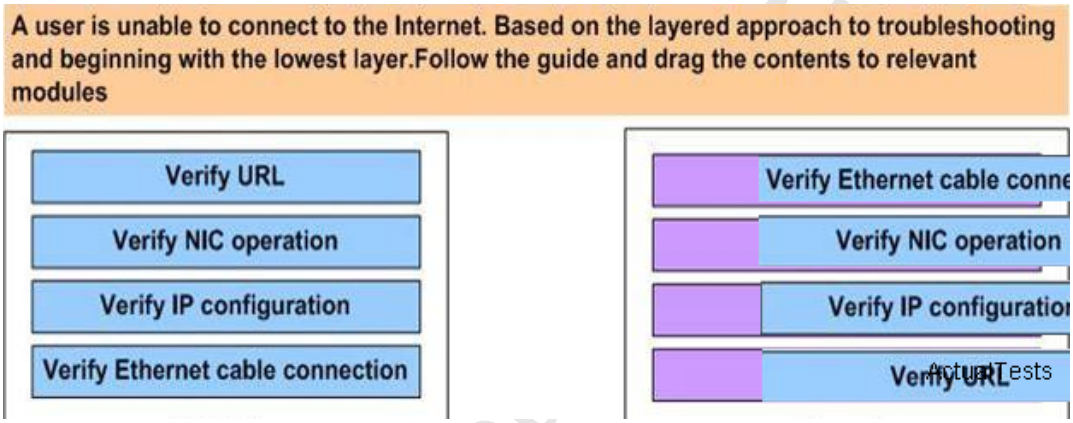
questions) Section 10: Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach (4 questions)

QUESTION NO: 47 DRAG DROP

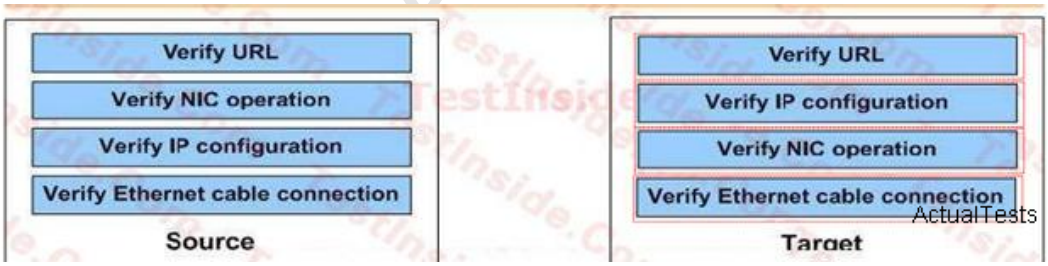
Answer image was added from the Engine.What kind of information can you deduce from an IOS image file name?

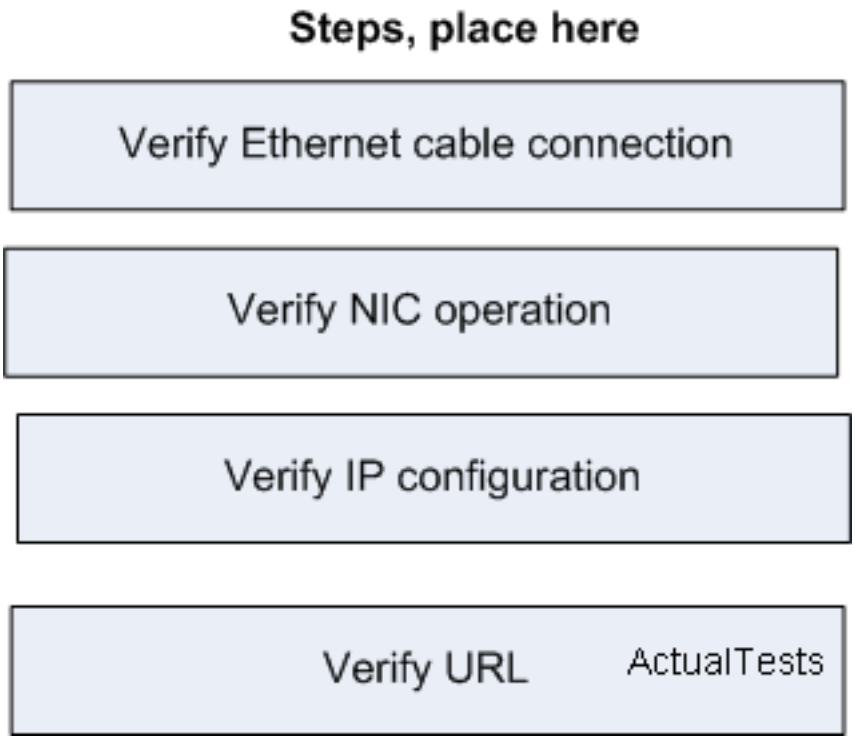


Answer:



Explanation:

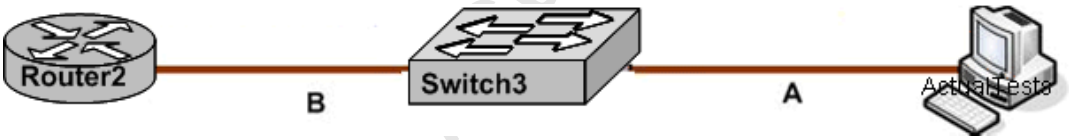




Step 1 ---- Check cable (Layer 0)
Step 2 ---- Check NIC (Layer 1, 2)
Step 3 ---- Check IP address (Network layer)
Step 4 ---- Check URL (Application layer)

QUESTION NO: 48

Refer to the exhibit. The two connected ports on the Switch3 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 Router2 and Switch3 ports.
B. Reseat all cables.
C. Ensure that cables A and B are straight-through cables.
D. Ensure the Switch3 has power.

Answer: B,C,D

Explanation:
Straight-through cables are used to connect hosts to a switch (or hub) and routers to a switch (or hub). See the table below:

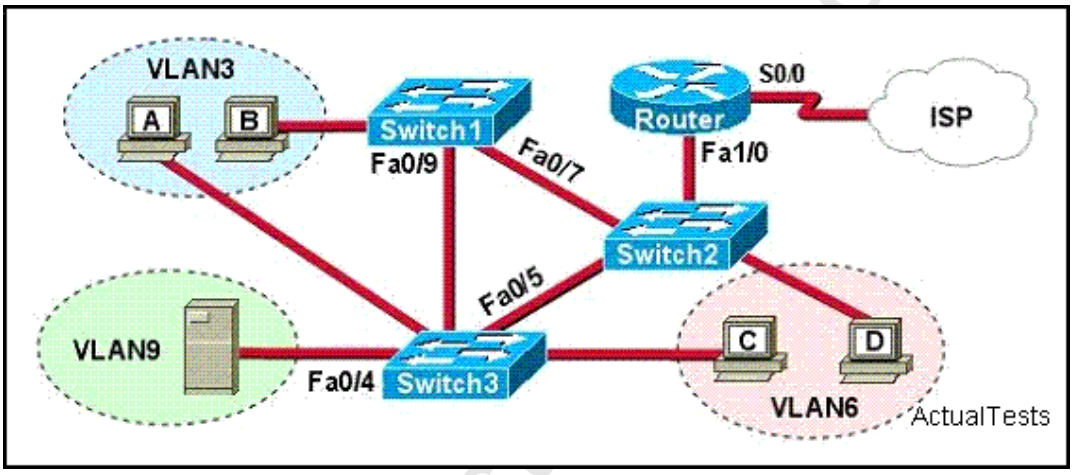
	Hub	Switch	Router	Workstation
Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
Workstation	Straight	Straight	Crossover	Crossover

Incorrect Answers:

A: This would mean that there was a layer 2 issue, not layer 1. If the problem was related to the encapsulation, the lights on the switch would indicate layer 1 activity.

QUESTION NO: 49

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. The transfer of files from Host B to the server in VLAN9 would be significantly slower.
C. For less than a minute, Host B would not be able to access the server in VLAN9. Then normal network function would resume.
D. Communication between VLAN3 and the other VLANs would be disabled.

Answer: C

Explanation:

After Fa0/9 is down, the topology is changed. The protocol builds a new topology. When the new topology is being built, the devices that communicate with other devices through Fa0/9 experience communication problems. Then normal network function would resume.

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.

STP keeps the port either in block or in forward states, when forward port disconnect then within the less then a minute blocked port comes into forward state so packets starts to go through new forward port.

The Spanning Tree Protocol (STP) would identify the best path as well as alternate path to reach in proper destination. In a redundant link, if the primary link fails then the secondary links will automatically start after few minutes. If port Fa0/9 became disconnected, then the packets would be re-routed automatically using the A-Switch2-Switch3 path.

QUESTION NO: 50

Which line from the output of the show ip interface command indicates a layer 1 problem?

A. Serial0/1 is up, line protocol is down
B. Serial0/1 is down, line protocol is down
C. Serial0/1 is up, line protocol is up
D. Serial0/1 is administratively down, line protocol is down

Answer: B

Explanation:
Section 11: Differentiate between LAN/WAN operation and features (2 questions)

QUESTION NO: 51

Which statement is true about full-duplex Ethernet in comparison to half-duplex Ethernet?

A. Full-duplex Ethernet uses a loopback circuit to detect collisions. Half-duplex Ethernet uses a jam signal.
B. Full-duplex Ethernet can provide higher throughput than can half-duplex Ethernet of the same bandwidth.
C. Full-duplex Ethernet consists of a shared cable segment. Half-duplex Ethernet provides a point-to-point link.
D. Full-duplex Ethernet uses two wires to send and receive. Half-duplex Ethernet uses one wire to send and receive.

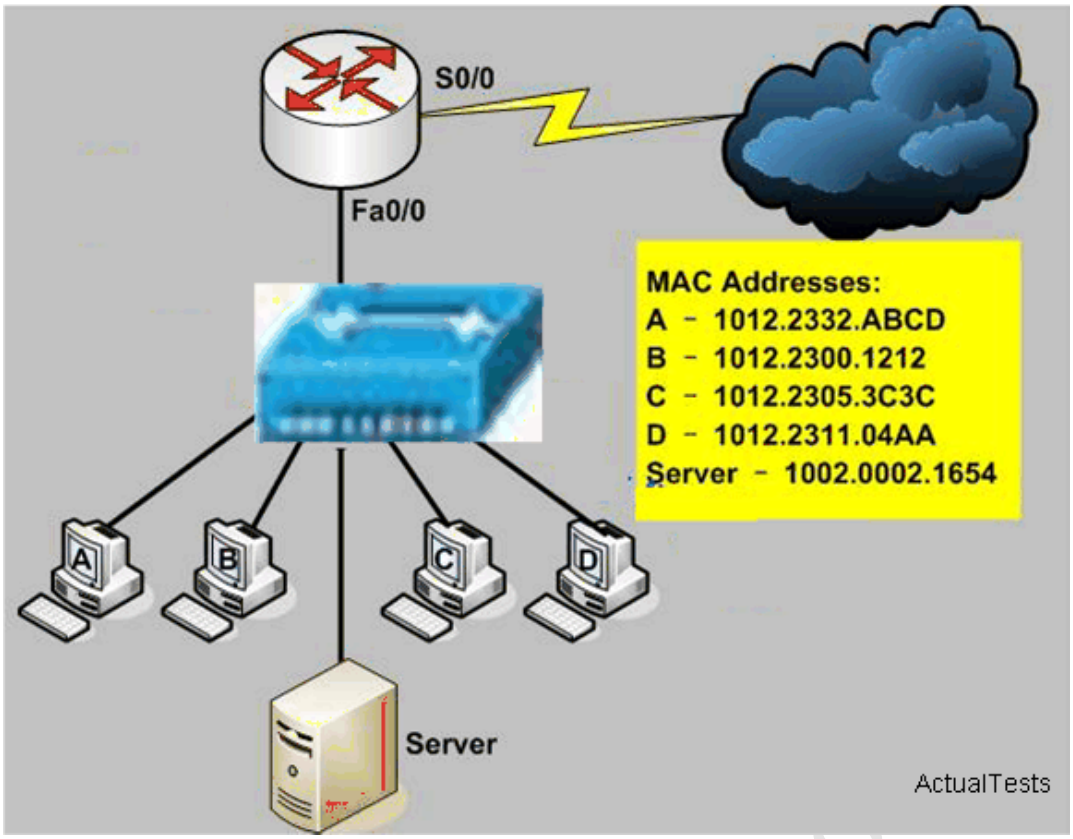
Answer: B

Explanation:
Full-duplex Ethernet uses two pairs of wires instead of one wire pair like half duplex. And full duplex uses a point-to-point connection between the transmitter of the transmitting device and the receiver of the receiving device. This means that with full-duplex data transfer, you get a faster data transfer compared to half duplex.

Full-duplex mode: when data sending and receiving split stream, and transmit through two different transmission lines, both communication sides are able to send and receive at the same time, this kind of transmission is called full-duplex;
Half duplex manner: If a single transmission line is used both for sending and receiving, although the data can be transmitted in two directions, but the two sides can not simultaneously send and receive data, such transmission is half-duplex.
CSMA/CD is used to detect whether conflict protocol exists in half-duplex Ethernet. It is a half-duplex Ethernet work mode.
Full-duplex mode will use two links to distinguish between send and receive action, and thus avoid conflict domain.
To use full-duplex, the following requirements are required:
1. P2P Link, or point-to-point connection;
2. Both nodes support full-duplex;
3. Close conflict detection (CSMA/CD).

QUESTION NO: 52

You work as a network engineer, study the exhibit carefully. Host B is actively communicating through Ethernet with the server. Host A has frames to send to the Internet. How will host A proceed?



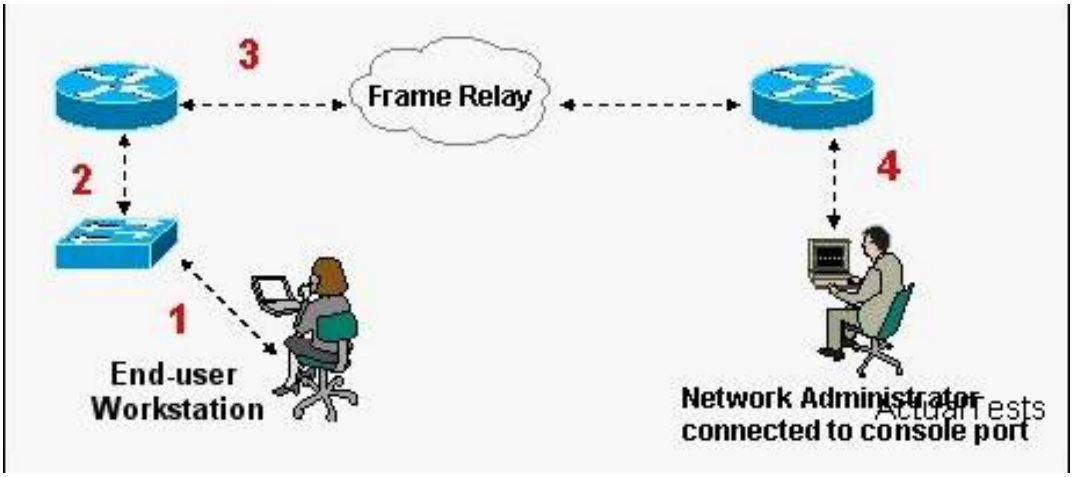
A. Host A will listen and transmit when there is no traffic on the segment.
B. Host A can send its frames at any time because it will be sending them through the router.
C. Host A will immediately begin transmitting because the destination is different.
D. Host A must wait for the server to reply to host B before transmitting.

Answer: A

Explanation:
The objective of this subject is to examine the examinee's understanding of CSMA/CD:
Ethernet is a type of LAN medium which works at the data link layer. Ethernet sends information by use of CSMA/CD(Carrier Sense Multiple Access/Collision Detection) in the shared environment. In the traditional or the hub-based Ethernet environment, only one NIC can successfully send frames at a certain moment. However, all NICs can listen before transmitting at the same time. Before transmitting frames, NIC will check to see whether the cable is busy, if there are no data frames being transmitted on cable, NIC will send its own frames ,otherwise it will not transmit frames until the completion of the previous transmission.
In this example, PC and server are connected to one hub. Therefore, PCA will listen first before sending data frames.

QUESTION NO: 53

Refer to the exhibit. What kind of cable should be used to make each connection that is identified by the numbers shown?



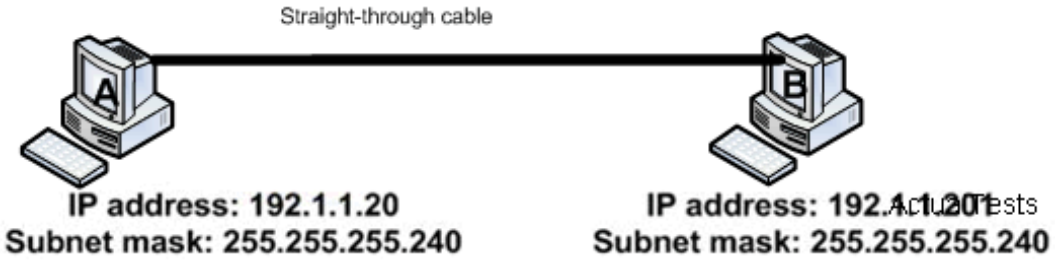
A. 1 - Ethernet straight-through cable
2 - Ethernet crossover cable
3 - serial cable
4 - Ethernet straight-through cable
B. 1 - Ethernet rollover cable
2 - Ethernet crossover cable
3 - serial cable
4 - null modem cable
C. 1 - Ethernet straight-through cable
2 - Ethernet crossover cable
3 - serial cable
4 - rollover cable
D. 1 - Ethernet crossover cable
2 - Ethernet straight-through cable
3 - fiber optic cable
4 - rollover cable
E. 1 - Ethernet straight-through cable
2 - Ethernet straight-through cable
3 - serial cable
4 - rollover cable

Answer: E

Explanation:
When connecting other devices to a switch, such as a router or workstations, a straight through cable is used. The only exception to this rule is when you are connecting another switch to a switch, in which case a cross over cable should be used.
For a serial connection to another router or to a WAN, a serial cable should be used. Finally, when connecting directly to the console port of a Cisco device, a rollover cable should be used. This cable is also commonly referred to as a console cable.

QUESTION NO: 54

The network administrator is connecting PC hosts A and B directly through their Ethernet interfaces as shown in the graphic. Ping attempts between the hosts are unsuccessful. What can be done to provide connectivity between the hosts? (Choose two.)



A. The hosts must be reconfigured to use private IP addresses for direct connections of this type.
B. A default gateway needs to be set on each host.
C. The subnet masks should be set to 255.255.255.0.
D. A crossover cable should be used in place of the straight-through cable.

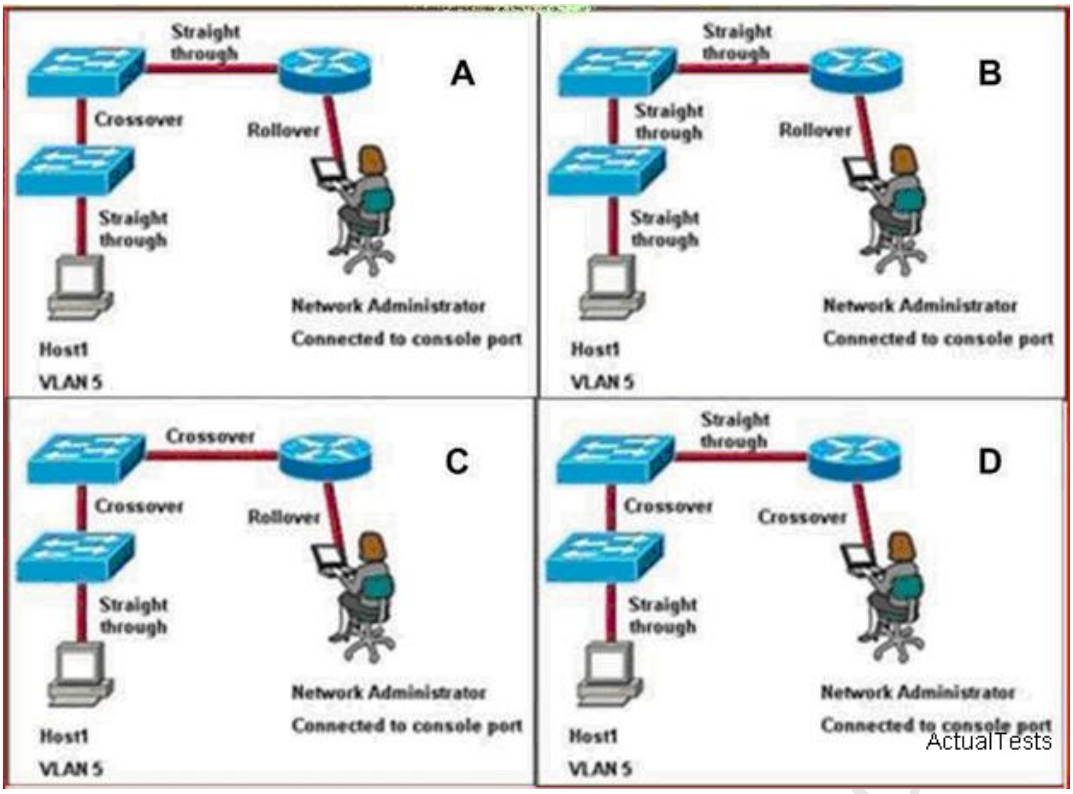
Answer: C,D

Explanation:
This problem is due to the misconfiguration of subnet mask as well as the fact that a straight-through cable is used to connect the two devices. To ensure connectivity, the correct subnet mask needs to be used so that the two devices are in the same subnet and when connecting two PC's back to back a crossover cable should be used.

First, from the IP address mask we can see that although both the two hosts are in 28 bit network, this subnet 192.1.1.0 can only include 15 hosts, because the two hosts do not belong to the same subnet. You may change the mask to make the two hosts belong to the same network segment. Second, the connection between hosts and hosts should use cross-line rather than straight line. Straight line is used to connect network devices.

QUESTION NO: 55

Refer to the exhibit. Assuming none of the switches autoconfigure, which of the topologies are properly cabled to allow the administrator to ping Host1 from the router?



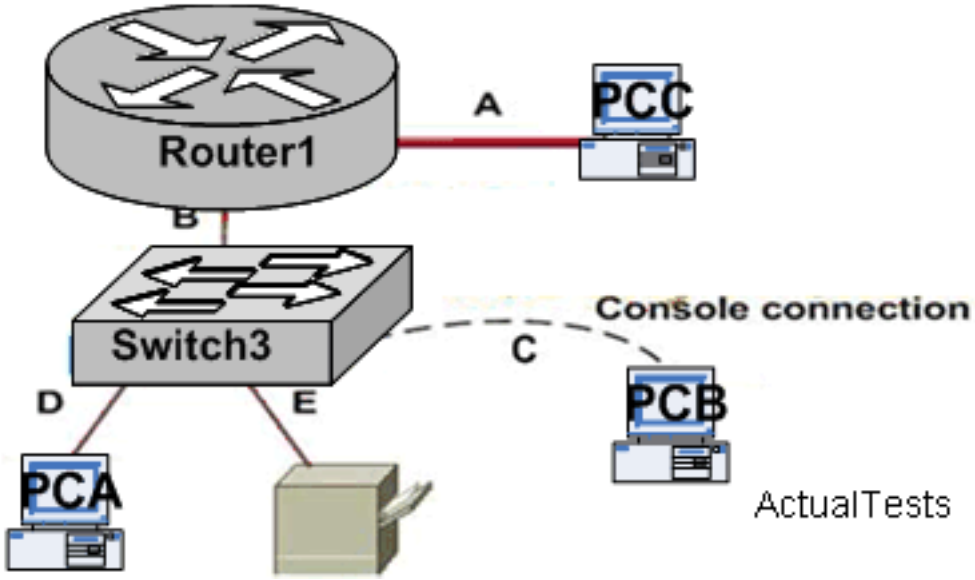
A. A
B. B
C. C
D. D

Answer: A

Explanation:
When connecting other devices to a switch, such as a router or workstations, a straight through cable is used. The only exception to this rule is when you are connecting another switch to a switch, in which case a cross over cable should be used. For a serial connection to another router or to a WAN, a serial cable should be used. Finally, when connecting directly to the console port of a Cisco device, a rollover cable should be used. This cable is also commonly referred to as a console cable.

QUESTION NO: 56

You work as a network technician. Please study the exhibit carefully. What types of cables are recommended to make the connections that are shown?



A. A-straight-through
B-crossover
C-rollover
D-straight-through
E-straight-through
B. A-rollover
B-straight-through
C-straight-through
D-rollover
E-crossover
C. A-straight-through
B-straight-through
C-rollover
D-straight-through
E-straight-through
D. A-crossover
B-straight-through
C-rollover
D-straight-through
E-straight-through

Answer: D

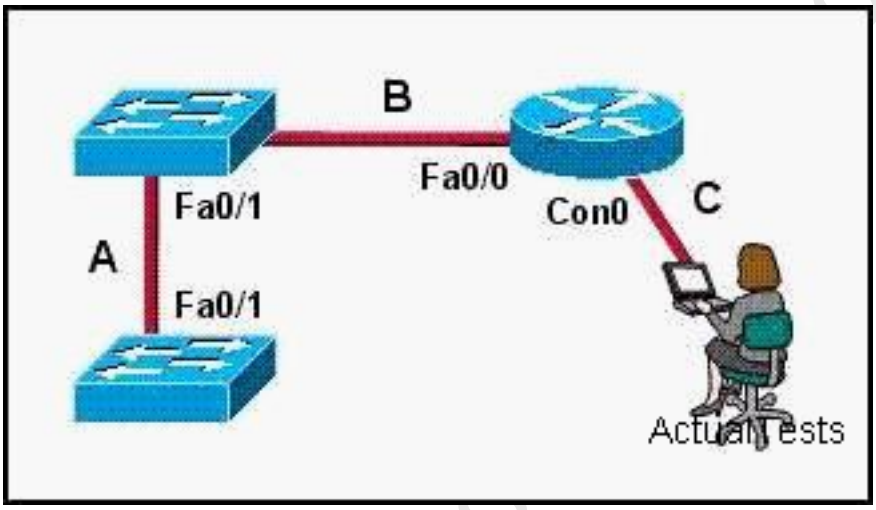
Explanation:
Crossover is used to connect two hosts; straight-through is to connect network devices and hosts, or network devices and network devices; rollover is mainly used to connect workstations and COM interface of network devices.

Crossover Cables are Used to Connect :
Host to Host (Peer to Peer) Networking

Switch to Switch
Hub to Hub
Computer to Router's Ethernet Port
Straight through Cable:
Host to Switch
Host to Hub
Switch to Router
Serial Cable:
Router's Serial Port to Serial Port
Rollover Cable :
To connect Router/Switch Console port.

QUESTION NO: 57

Which set of terms correctly identifies the cable types shown in the exhibit? Assume that none of the switches autoconfigure.



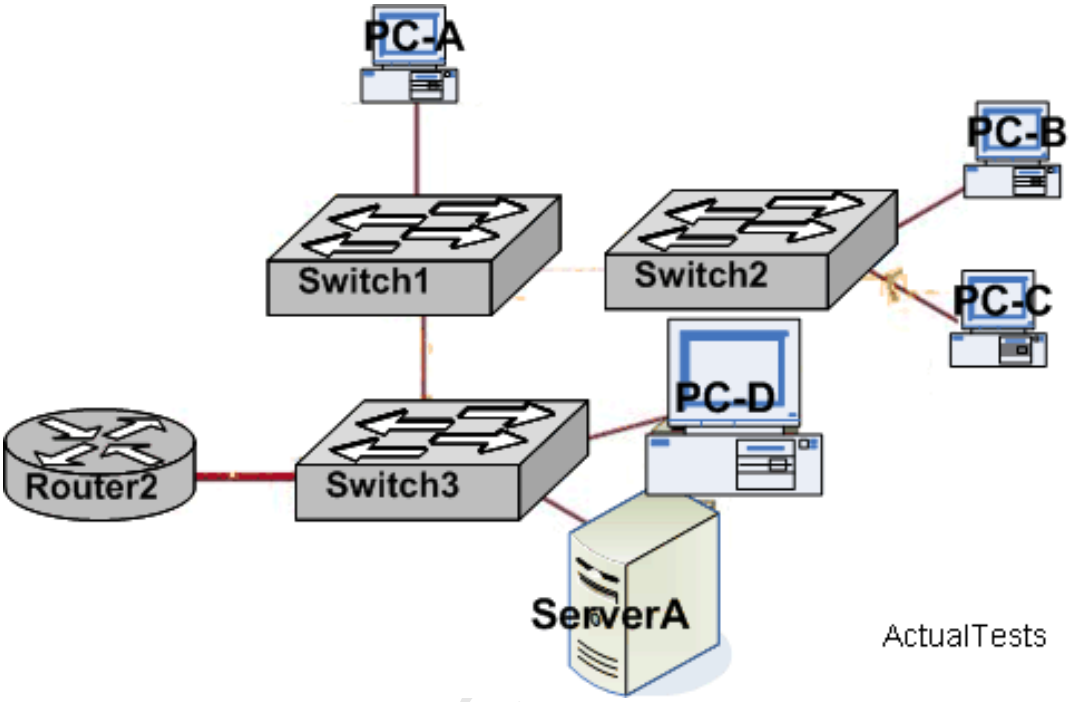
A. A: crossover
B. crossover
C. rollover
D. A: crossover
E. straight-through
F. rollover
G. A: straight-through
H. straight-through
I. rollover
J. A: crossover
K. straight-through
L. straight-through

Answer: B

Explanation:
For Ethernet, use crossover cable for connection between DTE devices or connection from DCE to DCE devices; use straight-through cable for connection from DTE to DCE. DCE device is a hub or switch. Rollover cable is not used to connect Ethernet, which is used to connect host and port com of the router. The cable to connect console port is known as console cable.

QUESTION NO: 58

You work as a network technician. Please study the exhibit carefully. Host PC-A has been added to the network. Which type of cable should be used between Switc2h and host PC-A?



A. straight-through cable
B. console cable
C. rollover cable
D. crossover cable

Answer: A

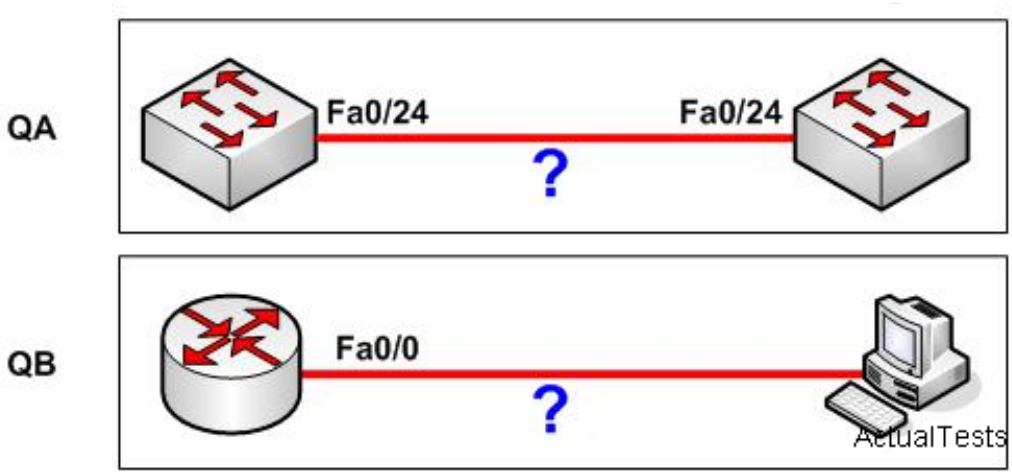
Explanation:
The same layer devices use crossover cable to connect, which is to connect two computers; different layer devices use straight-through cable to connect, which is to connect network devices and computers or network devices and network devices; rollover cable is used to connect host and the com interface of router.

Straight-through cables are used to connect hosts to a switch (or hub) and routers to a switch (or hub). See the table below:

	Hub	Switch	Router	Workstation
Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
Workstation	Straight	Straight	Crossover	Crossover

QUESTION NO: 59

Choose suitable connecting cables for the following two network equipment connection graphs (Choose two.)



A. QA --- straight-through
QB --- straight-through
B. QA --- Crossover
QB --- Crossover
C. QA --- straight-through
QB --- Crossover
D. QA --- Crossover
QB --- straight-through

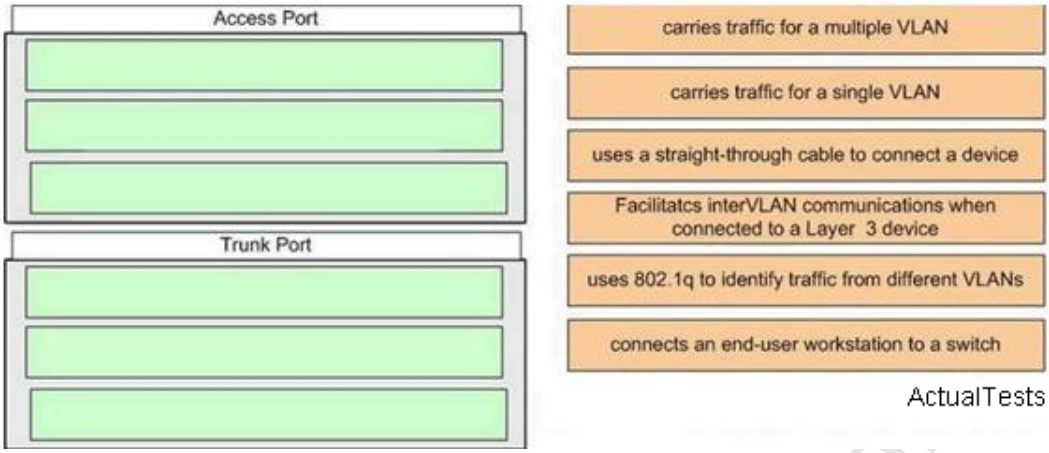
Answer: B

Explanation:
Devices of the same layer are connected by crossover cable, while devices of different layers are connected by straight-through cable.
Router ------ Crossover ------- Router
Router ------ Crossover ------- PC
Router ------ straight-through ------- Switch
Switch ------ straight-through ------- PC
Switch ------ Crossover ------- Switch

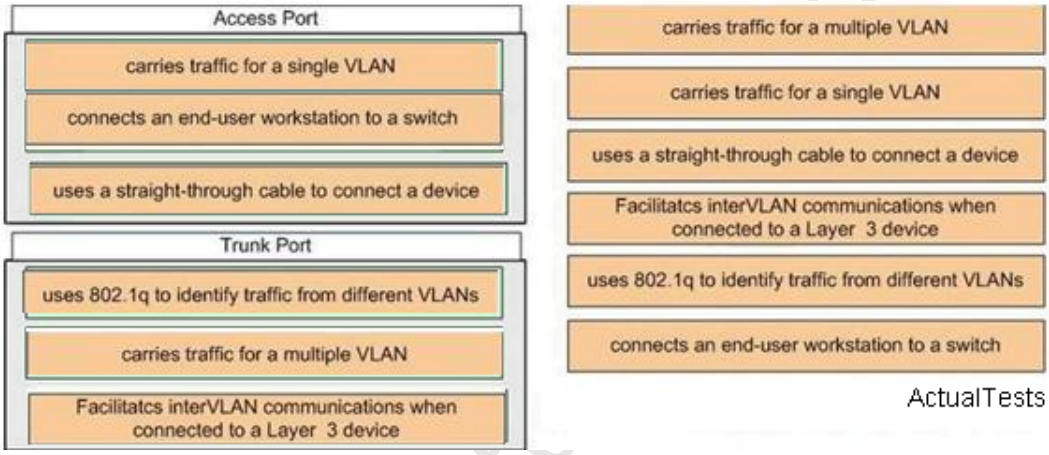
In addition, types of cables for special interfaces are used depending on the actual situations.

QUESTION NO: 60 DRAG DROP

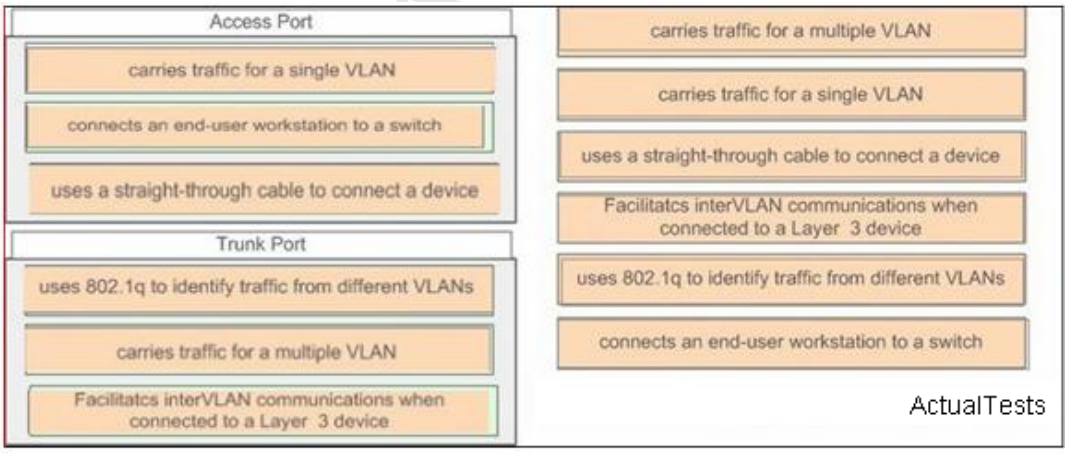
Drag the options on the right to the proper locations.



Answer:



Explanation:



Section 2: Explain the technology and media access control method for Ethernet networks (4 questions)

QUESTION NO: 61

Which one of the following statements is the media access method that Gigabit Ethernet uses?

A. CSMA/CA
B. CSMA/CD
C. point-to-point
D. token passing

Answer: B

Explanation:
Carrier Sense Multiple Access/Collision Detect (CSMA/CD) is the protocol for carrier transmission access in 10/100/1000 Ethernet networks. On Ethernet, any device can try to send a frame at any time. Each device senses whether the line is idle and therefore available to be used. If it is, the device begins to transmit its first frame. If another device has tried to send at the same time, a collision is said to occur and the frames are discarded. Each device then waits a random amount of time and retries until successful in getting its transmission sent. CSMA/CD is specified in the IEEE 802.3 standard.
Reference: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213869,00.html

QUESTION NO: 62

A network administrator wants to control which user hosts can access the network based on their MAC address. What will prevent workstations with unauthorized MAC addresses from connecting to the network through a switch?

A. port security
B. RSTP
C. STP
D. BPDU

Answer: A

Explanation:
Understanding How Port Security Works :
You can use port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses specified for that port. Alternatively, you can use port security to filter traffic destined to or received from a specific host based on the host MAC address.
When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device attached to the port differs from the list of secure addresses, the port either shuts down permanently (default mode), shuts down for the time you have

specified, or drops incoming packets from the insecure host. The port's behavior depends on how you configure it to respond to a security violation.
If a security violation occurs, the Link LED for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager. An SNMP trap is not sent if you configure the port for restrictive violation mode. A trap is sent only if you configure the port to shut down during a security violation.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_configuration_guide_chapter09186a008007fa13.html#xtocid256011

QUESTION NO: 63

When you consider half-duplex and full-duplex Ethernet, what are unique for half-duplex Ethernet? (Choose two.)

A. Half-duplex Ethernet operates in an exclusive broadcast domain.
B. Half-duplex Ethernet has efficient throughput.
C. Half-duplex Ethernet operates in a shared collision domain
D. Half-duplex Ethernet has lower effective throughput.

Answer: C,D

Explanation:
A single device could not be sending a frame and receiving a frame at the same time because it would mean that a collision was occurring. So, devices simply chose not to send a frame while receiving a frame. That logic is called half-duplex logic.
Ethernet switches allow multiple frames to be sent over different ports at the same time. Additionally, if only one device is connected to a switch port, there is never a possibility that a collision could occur. So, LAN switches with only one device cabled to each port of the switch allow the use of full-duplex operation. Full duplex means that an Ethernet card can send and receive concurrently.
Incorrect Answers:
A: Full duplex effectively doubles the throughput of half-duplex operation, because data can be both sent and received at the full 10/100 speed.
B: In half duplex operation, the network is shared between all devices in the collision domain.Reference: CCNA Self-Study CCNA INTRO exam certification Guide (Cisco Press, ISBN 1-58720-094-5) Page 62-63.

QUESTION NO: 64

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

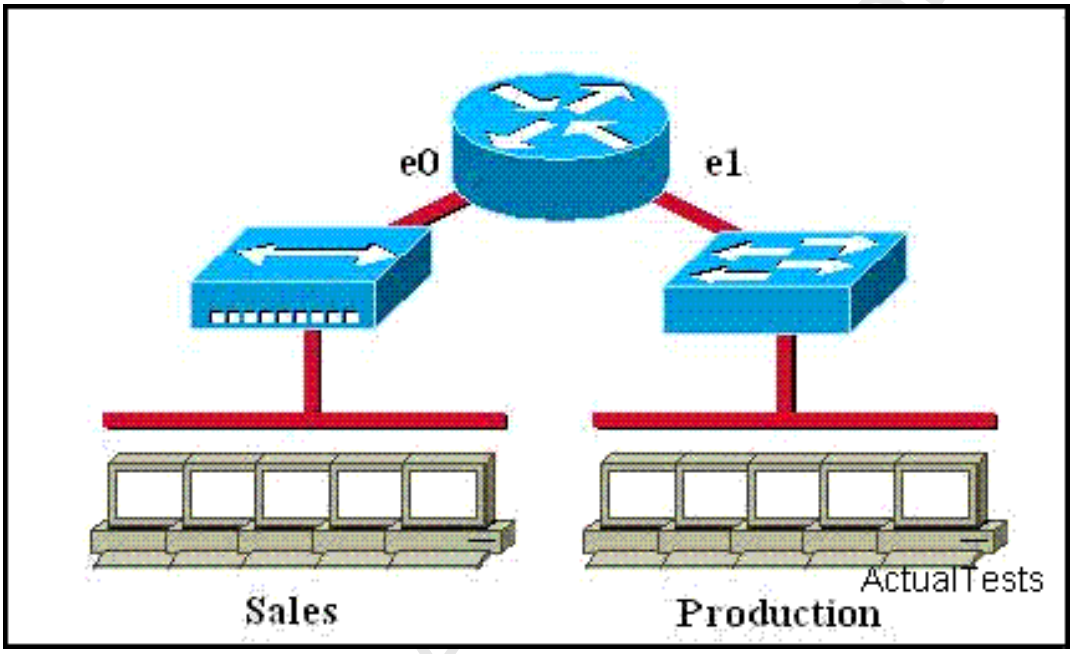
A. to uniquely identify devices at Layer 2
B. to allow communication with devices on a different network
C. to differentiate a Layer 2 frame from a Layer 3 packet
D. to establish a priority system to determine which device gets to transmit first
E. to allow communication between different devices on the same network
F. to allow detection of a remote device when its physical address is unknown

Answer: A,E

Explanation:
Section 3: Explain network segmentation and basic traffic management concepts (6 questions)

QUESTION NO: 65

Which of the following statements describe the network shown in the graphic? (Choose two.)



A. There are four broadcast domains in the network.
B. There are five collision domains in the network.
C. There are four collision domains in the network.
D. There are two broadcast domains in the network.
E. There are six broadcast domains in the network.
F. There are seven collision domains in the network.

Answer: D,F

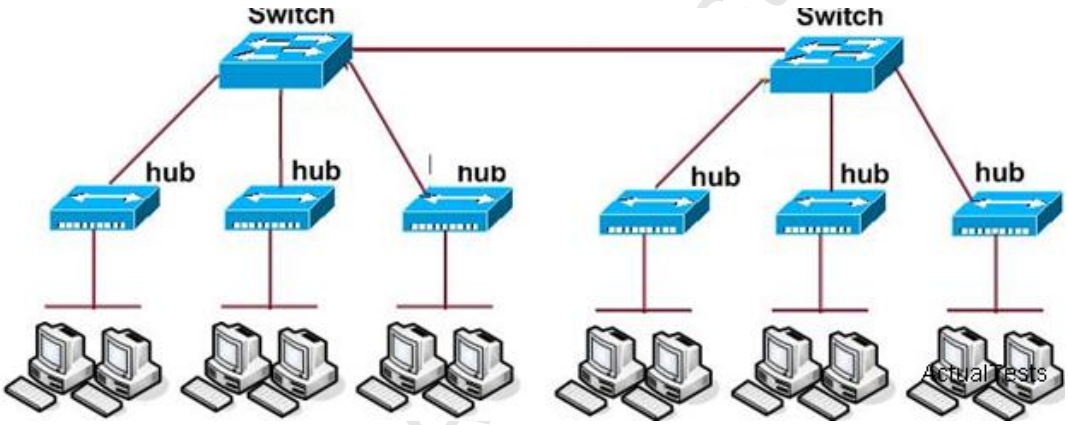
Explanation:
A hub is both a broadcast domain and a collision domain.
A switch is a broadcast domain and each interface of a switch is a collision domain.
Each interface of a router is a broadcast domain.

E0 and E1 are interfaces of the router; therefore, E0 and E1 are broadcast domains. There are two broadcast domains in the network.
The hub connected to the E0 interface of the router is a collision domain.
The switch connected to the E1 interface of the router is a collision domain.
The five PCs connected to the switch are five collision domains.
Therefore, there are seven collision domains in the network.

In this network we have a hub being used in the Sales department, and a switch being used in the Production department. Based on this, we have two broadcast domains: one for each network being separated by a router. For the collision domains, we have 5 computers and one port for E1 so we have 6 collision domains total because we use a switch in the Production Department so 5 are created there, plus one collision domain for the entire Sales department because a hub is being used.

QUESTION NO: 66

Both Switches and Hubs are used in the network, please study the exhibit carefully, how many broadcast domains are shown in the graphic assuming only the default VLAN is configured on the switches?



A. one
B. twelve
C. six
D. two

Answer: A

Explanation:
VLAN (Virtual Local Area Network) technology is to solve the problem that switches can't limit broadcast within the LAN interconnection. This technology can divide a LAN into more logical LAN- VLAN, each VLAN is a broadcast domain, the communication between the hosts within a VLAN is like that of the hosts in a LAN, while the communication can't be achieved between VLANs directly. Thus the broadcast datagram is limited within a LAN. Based on the network

structure shown in the above figure, there is only one default VLAN for two switches, so they are in the same broadcast domain and can communicate with each other.

A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer.
In terms of current popular technologies: Any computer connected to the same Ethernet repeater or switch is a member of the same broadcast domain. Further, any computer connected to the same set of inter-connected switches/repeaters is a member of the same broadcast domain. Routers and other higher-layer devices form boundaries between broadcast domains.
This is as compared to a collision domain, which would be all nodes on the same set of inter-connected repeaters, divided by switches and learning bridges. Collision domains are generally smaller than, and contained within, broadcast domains. In this case, since all devices belong to the default VLAN (VLAN 1) they all belong to the same broadcast domain.

QUESTION NO: 67

What are some of the advantages of using a router to segment the network? (Choose two.)

A. Filtering can occur based on Layer 3 information.
B. Broadcasts are eliminated.
C. Routers generally cost less than switches.
D. Adding a router to the network decreases latency.
E. Broadcasts are not forwarded across the router.

Answer: A,E

Explanation:
By using a router to segment the network, we can
1. Control the traffic across Layer 3 and filter data based on Layer 3 information.
2. Reduce broadcasts to save on network resources and improve efficiency.

When the router's interface receives the broadcast, it discard the broadcast without forwarding it on to other networks. Even though routers are known for breaking up broadcast domains by default, it's important to remember that they break up collision domains as well.
There are two advantages of using routers in your network:
* They don't forward broadcasts by default.
* They can filter the network based on layer 3 (Network layer) information (e.g., IP address) by using IOS based firewall ie. ACL
Four router functions in your network can be listed as follows:
* Packet switching
* Packet filtering
* Internetwork communication

* Path selection

QUESTION NO: 68

How does replacing a hub with a switch affect CSMA/CD behavior in an Ethernet network?

A. In increases the size of the collision domain by allowing more devices to be connected at once.
B. It effectively eliminates collisions.
C. It reduces the total amount of bandwidth available to each device.
D. It decreases the amount of time that a jam signal must be sent to reach all network devices.

Answer: B

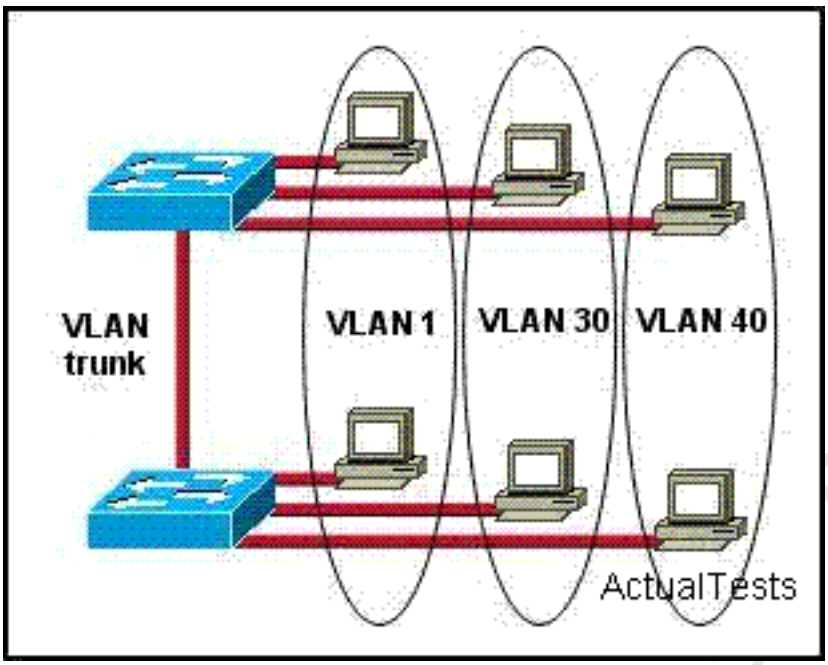
Explanation:
If all network segments in the Ethernet connect with repeaters, because they can not avoid conflict, they remain in the same conflict domain. Switches can be used effectively prevent conflict, but not HUB. Because switch can choose route using physical address, each of its port is a conflict domain. But HUB has no such ability, it will only send out the received data through broadcast, which will easily cause broadcasting storm. All of its ports are in a single conflict domain.

Ethernet hubs use a process with the name carrier sense multiple access collision detect (CSMA/CD) to communicate across the network. Under CSMA/CD, a node does not send out a packet unless the network is clear of traffic. If two nodes send out packets at the same time, a collision occurs and the packets are lost. Then, both nodes wait for a random amount of time and retransmit the packets. Any part of the network where packets from two or more nodes can interfere with each other is a collision domain. A network with a large number of nodes on the same segment often has a lot of collisions and, therefore, a large collision domain.
Switching on the other hand allows a network to maintain full-duplex Ethernet. Before switching existed, Ethernet was half duplex. Half duplex means that only one device on the network can transmit at any given time. In a fully switched network, nodes only communicate with the switch and never directly with each other. In the road analogy, half duplex is similar to the problem of a single lane, when road construction closes one lane of a two-lane road. Traffic attempts to use the same lane in both directions. Traffic that comes one way must wait until traffic from the other direction stops in order to avoid collision.
Fully switched networks employ either twisted pair or fiber-optic cable setups. Both twisted pair and fiber-optic cable systems use separate conductors to send and receive data. In this type of environment, Ethernet nodes can forgo the collision detection process and transmit at will; these nodes are the only devices with the potential to access the medium. In other words, the network dedicates a separate lane to traffic that flows in each direction. This dedication allows nodes to transmit to the switch at the same time that the switch transmits to the nodes. Thus, the environment is collision-free.

Reference: How LAN Switches Work
http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a00800a7af3.shtml

QUESTION NO: 69

Refer to the exhibit. How many broadcast domains exist in the exhibited topology?



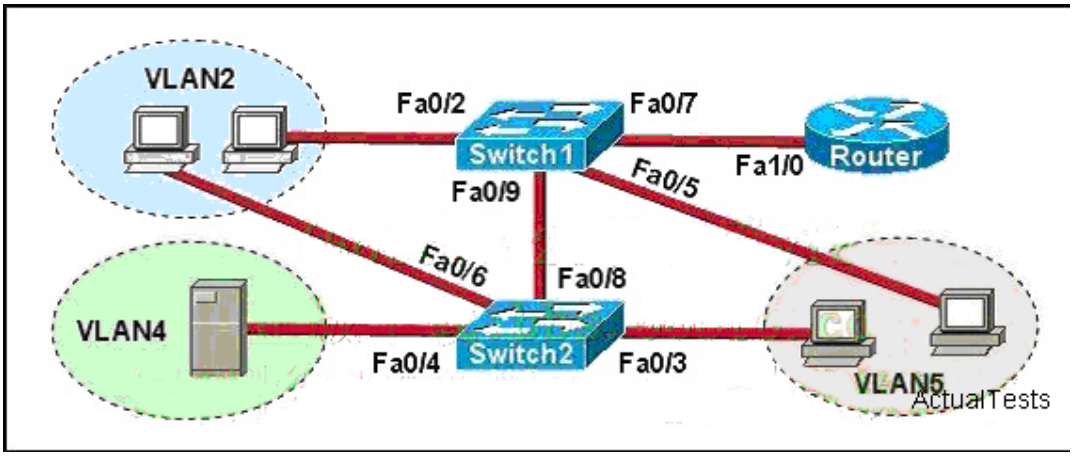
A. three
B. four
C. two
D. six
E. five
F. one

Answer: A

Explanation:
From the features of the VLAN, we know that a VLAN is a broadcast domain. There are three VLANs in the exhibit, so three broadcast domains exist in the exhibited topology.

QUESTION NO: 70

A network associate is trying to understand the operation of the FLD Corporation by studying the network in the exhibit. The associate knows that the server in VLAN 4 provides the necessary resources to support the user hosts in the other VLANs. The associate needs to determine which interfaces are access ports. Which interfaces are access ports? (Choose three.)



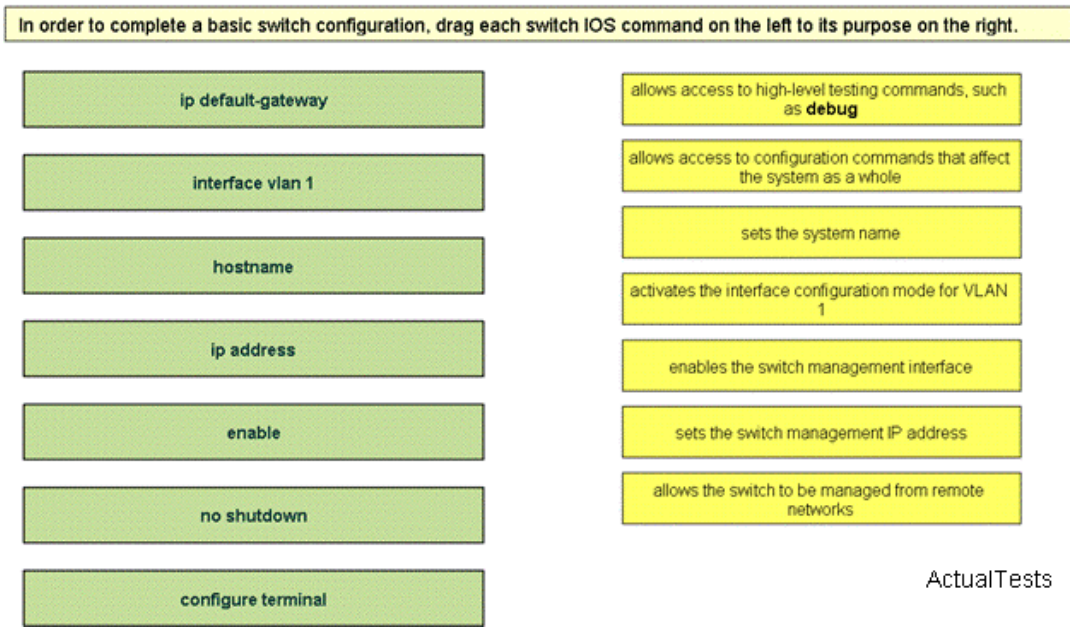
A. Switch1 - Fa 0/2
B. Switch1 - Fa 0/9
C. Switch2 - Fa 0/3
D. Switch2 - Fa 0/4
E. Switch2- Fa 0/8
F. Router - Fa 1/0

Answer: A,C,D

Explanation:
Section 4: Explain basic switching concepts and the operation of Cisco switches (16 questions)

QUESTION NO: 71 DRAG DROP

Drag and drop question. Drag the items to the proper locations.



Answer:

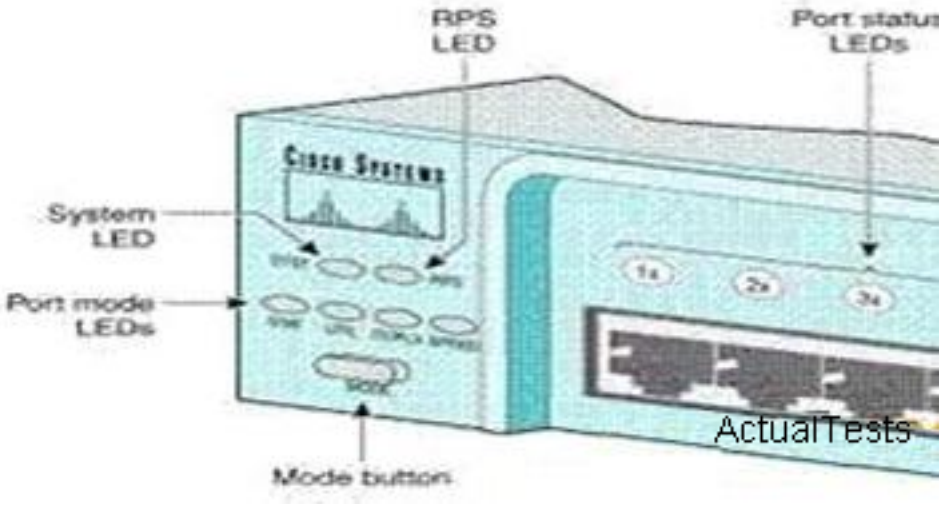
In order to complete a basic switch configuration, drag each switch IOS command on the left to its purpose on the right.

allows the switch to be managed from remote networks	allows access to high-level testing commands, such as **debug**
activates the interface configuration mode for VLAN 1	allows access to configuration commands that affect the system as a whole
sets the system name	sets the system name
sets the switch management IP address	activates the interface configuration mode for VLAN 1
allows access to high-level testing commands, such as **debug**	enables the switch management interface
enables the switch management interface	sets the switch management IP address
allows access to configuration commands that affect the system as a whole	allows the switch to be managed from remote networks

ActualTests

QUESTION NO: 72

Refer to the exhibit. After the power-on self test (POST), the system LED of a Cisco 2950 switch turns amber. What is the status of the switch?



A. The switch has a problem with the internal power supply and needs an external power supply to be attached.
B. The switch has experienced an internal problem but data can still be forwarded at a slower rate.
C. The POST was successful.
D. POST failed and there is a problem that prevents the operating system of the switch from being loaded.

Answer: D

Explanation:
When switch is connected to power and conduct Self Test, LED lights turn to Amber, this tells us of POST failure. POST failure is a fatal error; it means the switch does not work.

QUESTION NO: 73

In which circumstance are multiple copies of the same unicast frame likely to be transmitted in a switched LAN?

A. when a dual ring topology is in use
B. in an improperly implemented redundant topology
C. after broken links are re-established
D. when upper-layer protocols require high reliability
E. during high traffic periods

Answer: B

Explanation:
A redundant topology eliminates single points of failure, but it also causes broadcast storms, multiple frame copies, and MAC address table instability problems. Multiple Frame Copies--when a new switch is added, the other switches may not have learned its correct MAC address. The host may send a unicast frame to the new switch. The frame is sent through several paths at the same time. The new switch will receive several copies of the frame. This causes MAC database instability. MAC database instability results when multiple copies of a frame arrive on different ports of a switch. Layer 2 has no mechanism to stop the loop. This is the main reason for the Spanning Tree Protocol(STP) IEEE 802.1d which was developed to prevent routing loops.
If multiple connections between switches are created for redundancy purposes, network loops can occur in an improperly designed topology. Spanning Tree Protocol (STP) is used to stop network loops while still permitting redundancy.

QUESTION NO: 74

Why will a switch never learn a broadcast address?

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

Answer: C

Explanation:
Switches build the MAC address table by listening to incoming frames and examining the source MAC address in the frame. Broadcast addresses are not source addresses in the broadcasts.

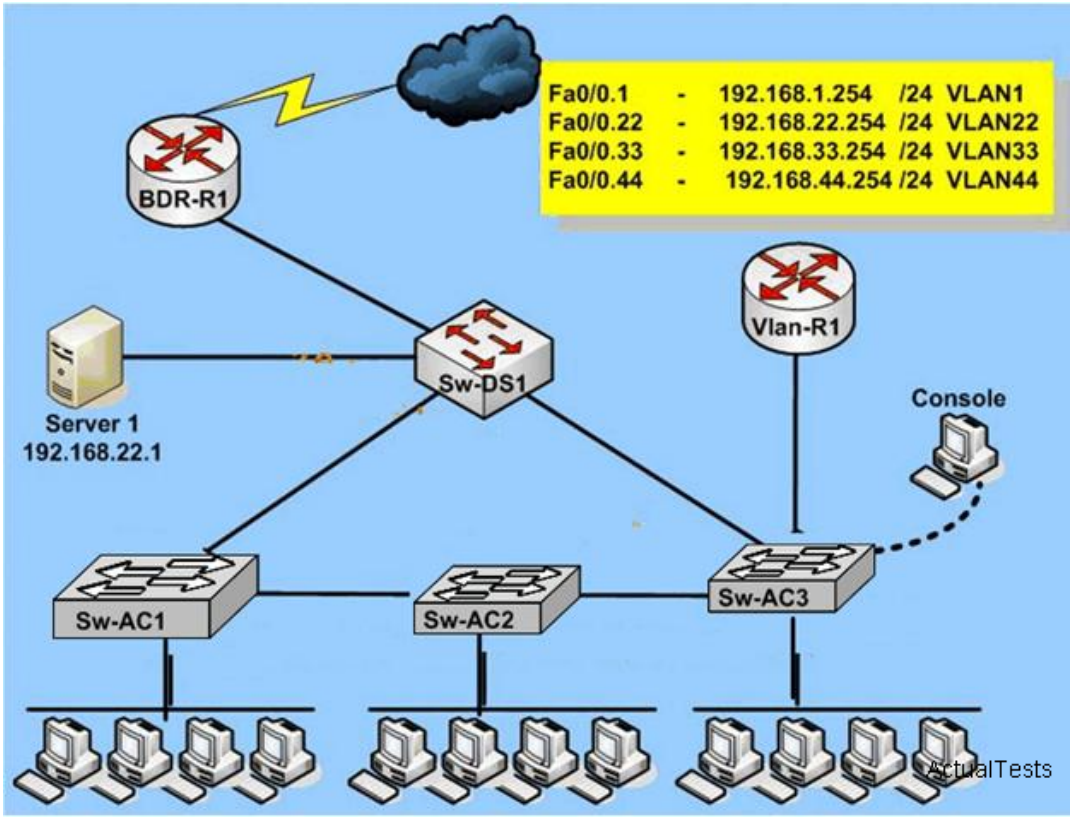
There are three different address types:

* Unicast : One source to One destination
* Broadcast: One source to multiple destination
* Multicast: One source to multiple destination joined to group

On unicast or broadcast or multicast communication, the source address is always the unicast address but the destination address can be unicast, broadcast or multicast.

QUESTION NO: 75

Out of which ports on Sw-AC3 will a frame be forwarded that has Source MAC address 0010.5a0c.fd86 and destination MAC address 000a.8a47.e612?(Choose three)



Sw-AC3#show mac-address-table

```
Sw-Ac3#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.2485.8900    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0009.e8b2.c28c    DYNAMIC     Fa0/12
   1    000a.b7e9.8360    DYNAMIC     Fa0/3
   1    000f.2485.8b49    DYNAMIC     Fa0/9
  22    0009.e8b2.c28c    DYNAMIC     Fa0/12
  22    000a.b7e9.8360    DYNAMIC     Fa0/3
  22    0010.5a0c.ffba    DYNAMIC     Fa0/12
  33    0009.e8b2.c28c    DYNAMIC     Fa0/12
  33    000a.b7e9.8360    DYNAMIC     Fa0/3
  33    000c.ce8d.8860    DYNAMIC     Fa0/12
  33    0010.5a0c.fd86    DYNAMIC     Fa0/6
  33    0010.5a0c.feae    DYNAMIC     Fa0/12
  33    0010.5a0c.ff9f    DYNAMIC     Fa0/1
  44    0009.e8b2.c28c    DYNAMIC     Fa0/12
--More--
```


Sw-AC3#show vlan

```
Sw-Ac3#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16
22   Servers                          active
33   Management                       active    Fa0/1, Fa0/2, Fa0/5, Fa0/6, Fa0/7
44   Production                       active    Fa0/4, Fa0/8, Fa0/10, Fa0/11
99   no-where                         active    Fa0/13, Fa0/14, Fa0/15, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                F0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
```


Sw-AC3#show int trunk

```
Sw-Ac3#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1
Fa0/9       desirable    802.1q         trunking      1
Fa0/12      desirable    802.1q         trunking      1
```


A. Fa0/1

B. Fa0/3

C. Fa0/12

D. Fa0/8

E. Fa0/4

F. Fa0/6

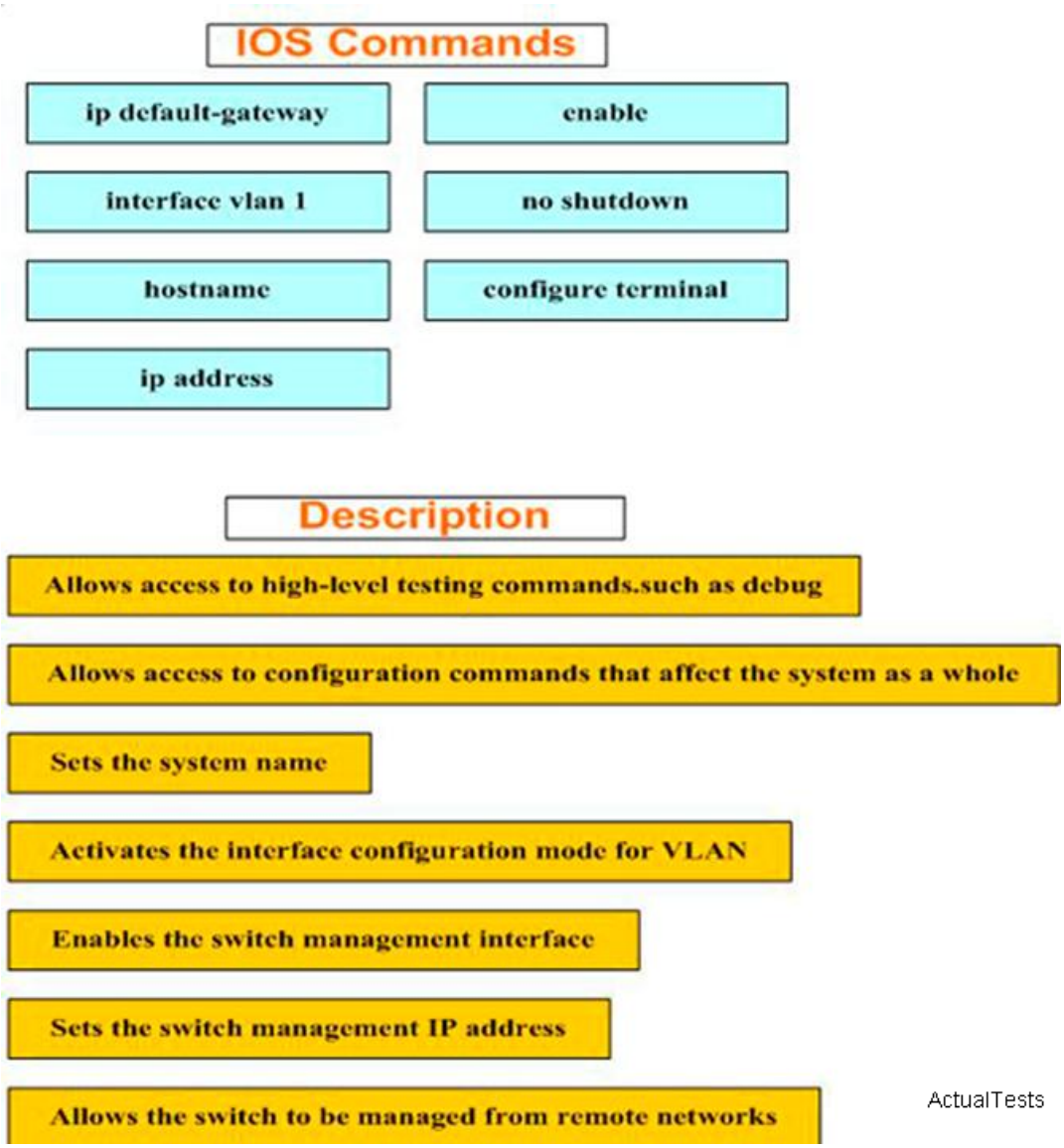
G. Fa0/7

Answer: A,B,C

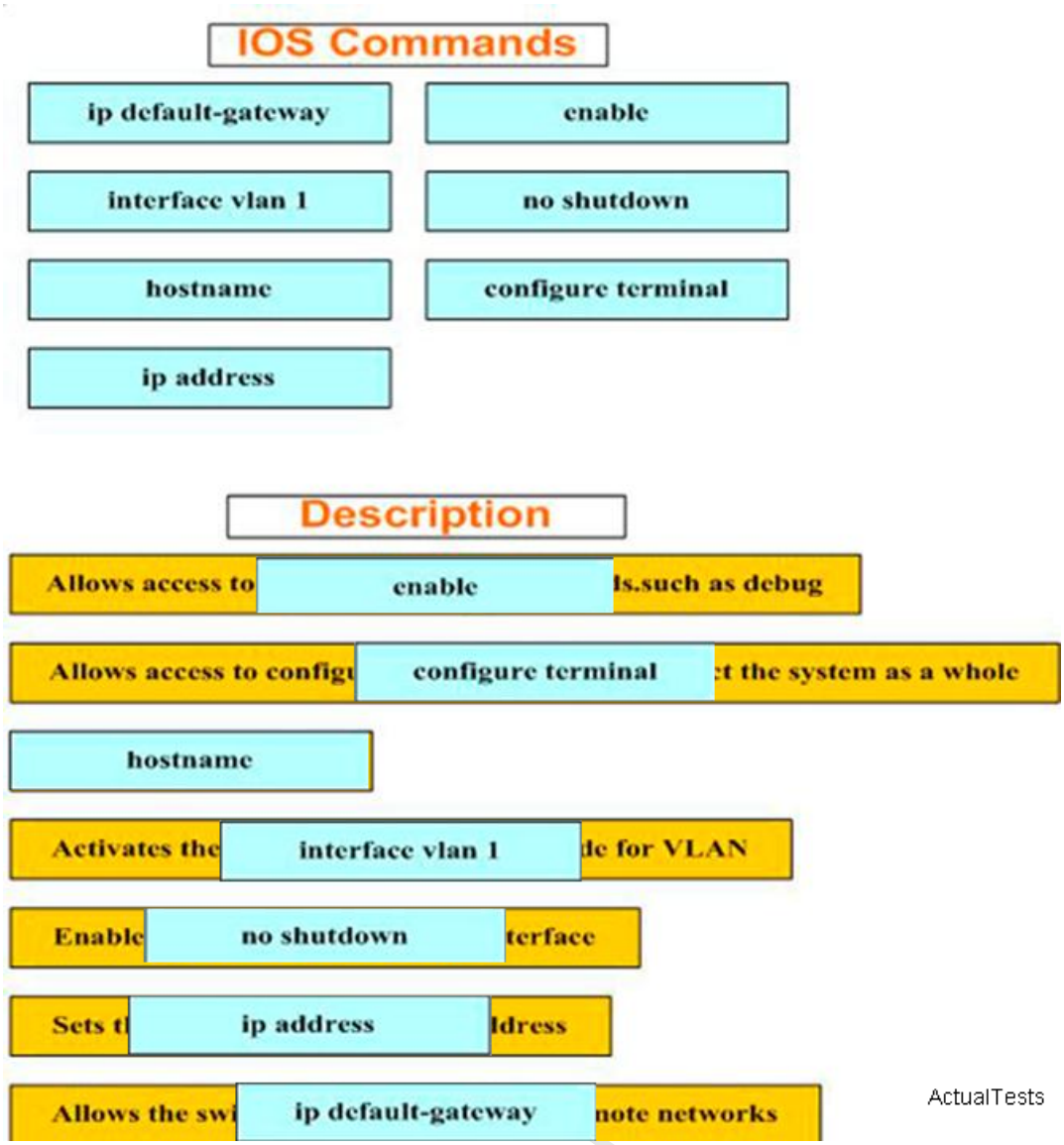
Explanation:
The source MAC address of the frame to be transmitted is 0010.5a0c.fd86
The destination MAC address is 000a.8a47.e612
Compared with the MAC address table of Sw-Ac3, we know that the destination address does not exist, so Sw-Ac3 will transmit this frame using all other ports (except the frame receiving port-Fa0/6), that is to say, flooding this frame from ports Fa0/1, Fa0/3, Fa0/9, Fa0/12.

QUESTION NO: 76 DRAG DROP

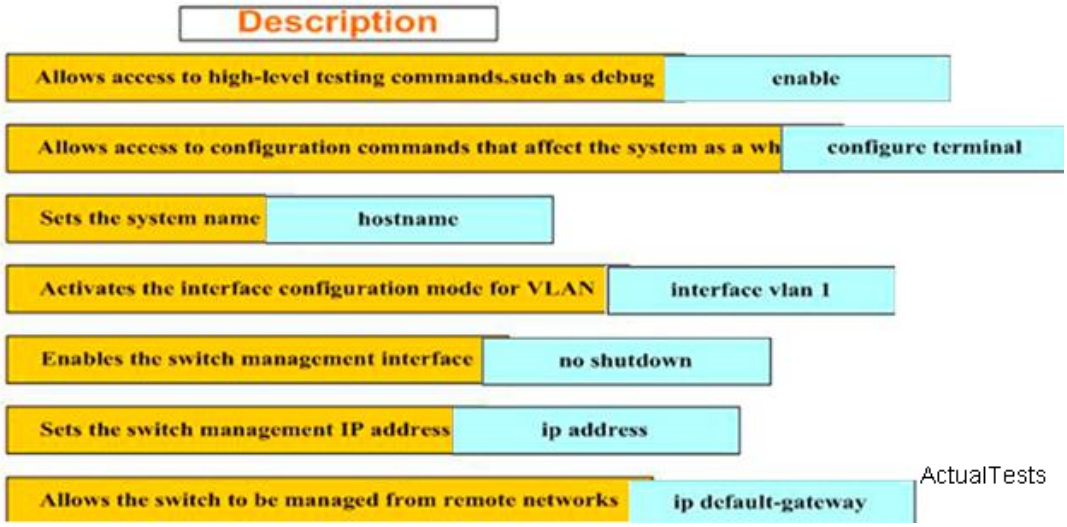
Drag the items to the proper locations.



Answer:



Explanation:



1. The high level testing commands such as debug that allow access should be conducted under enable mode
2. Access to configuration commands under configure terminal
3. The command to set the system name is hostname

4. Configure vlan, interface vlan 1 may be used to configure details in vlan
5. Input no shutdown under interface configure mode to activate interface
6. Use command ip address to configure IP address, and sets the switch management
7. Use command ip default-gateway to configure default gateway

QUESTION NO: 77

The system LED is amber on a Cisco Catalyst 2950 series switch. What does this indicate?

A. The system is powered up and operational.
B. The system is forwarding traffic.
C. The system is malfunctioning.
D. The system is not powered up.

Answer: C

Explanation:
While the switch powers on, it begins POST, a series of tests. POST runs automatically to verify that the switch functions properly. When the switch begins POST, the system LED is off. If POST completes successfully, the LED turns green. If POST fails, the LED turns amber.
Note : POST failures are usually fatal. Call Cisco Systems if your switch does not pass POST.

QUESTION NO: 78

A Catalyst 2950 needs to be reconfigured. What steps will ensure that the old configuration is erased?

A. Erase the running configuration.
B. Restart the switch.
C. Modify the configuration register.
D. Delete the VLAN database.

Answer: B,D

Explanation:
For switches such as the 2950, the process is much the same as a router, but you should delete the VLAN.DAT file before reloading the router. This file contains VLAN information and is kept in flash, so it will still be present after a reload.

switch1#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
switch1#reload

Make sure to hit for the two questions regarding the deletion - if you answer "y" instead, the switch thinks you're trying to erase a file named "y"!
After the reload is complete, you'll be prompted to enter setup mode. As you did with the router, enter "N" and begin to configure the router from user exec mode.

***

QUESTION NO: 79

Which two values are used by Spanning Tree Protocol to elect a root bridge? (Choose two.)

A. bridge priority
B. IP address
C. MAC address
D. IOS version
E. amount of RAM
F. speed of the links

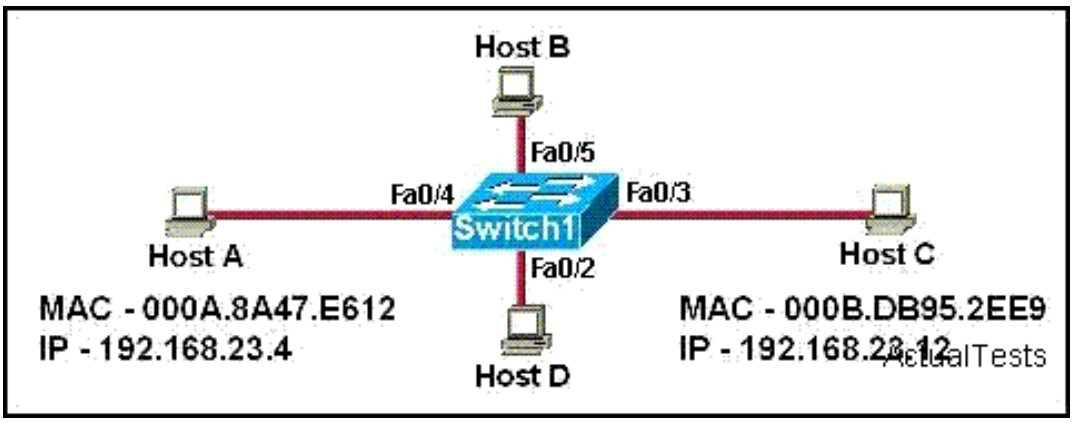
Answer: A,C

Explanation:
Two values are compared to elect a root bridge in STP: bridge priority and MAC address.

Switch having lowest bridge ID will become the root bridge. The bridge ID is how STP keeps track of all the switches in the network. It is determined by a combination of the bridge priority (32,768 by default on all Cisco switches) and the base MAC address. The bridge with the lowest bridge ID becomes the root bridge in the network.

QUESTION NO: 80

Refer to the exhibit. Switch1 has just been restarted and has passed the POST routine. Host A sends its initial frame to Host C. What is the first thing the switch will do as regards populating the switching table?



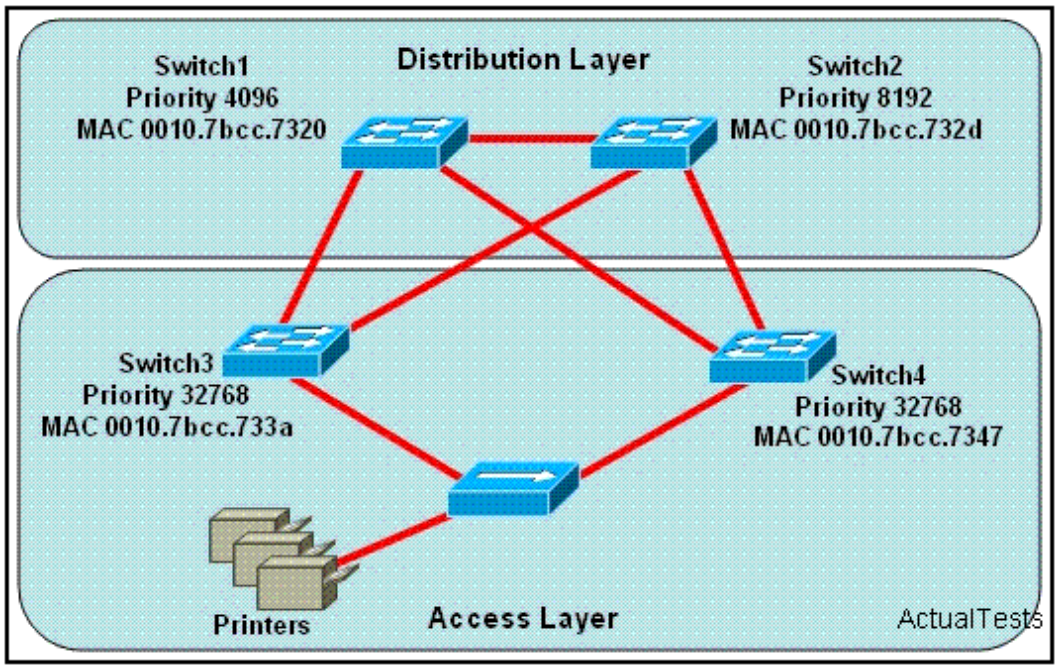
A. Switch1 will add 192.168.23.12 to the switching table.
B. Switch1 will add 000B.DB95.2EE9 to the switching table.
C. Switch1 will add 192.168.23.4 to the switching table.
D. Switch1 will add 000A.8A47.E612 to the switching table.

Answer: D

Explanation:
That Switch1 has just been restarted and has passed the POST routine indicates that the MAC address table of Switch1 is empty. When Host A sends its initial frame to Host C, Switch1 records the MAC address of Host A and the mapping port number in its MAC address table. Note that a switch records the source MAC address rather than the destination MAC address.

QUESTION NO: 81

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



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

Answer: A

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.

Designated port A designated port is one that has been determined as having the best (lowest) cost. A designated port will be marked as a forwarding port.

QUESTION NO: 82

What will an Ethernet switch do if it receives a unicast frame with a destination MAC that is listed in the switch table?

A. The switch will forward the frame to a specific port.
B. The switch will forward the frame to all ports except the port on which it was received.
C. The switch will return a copy of the frame out the source port.
D. The switch will remove the destination MAC from the switch table.
E. The switch will not forward unicast frames.

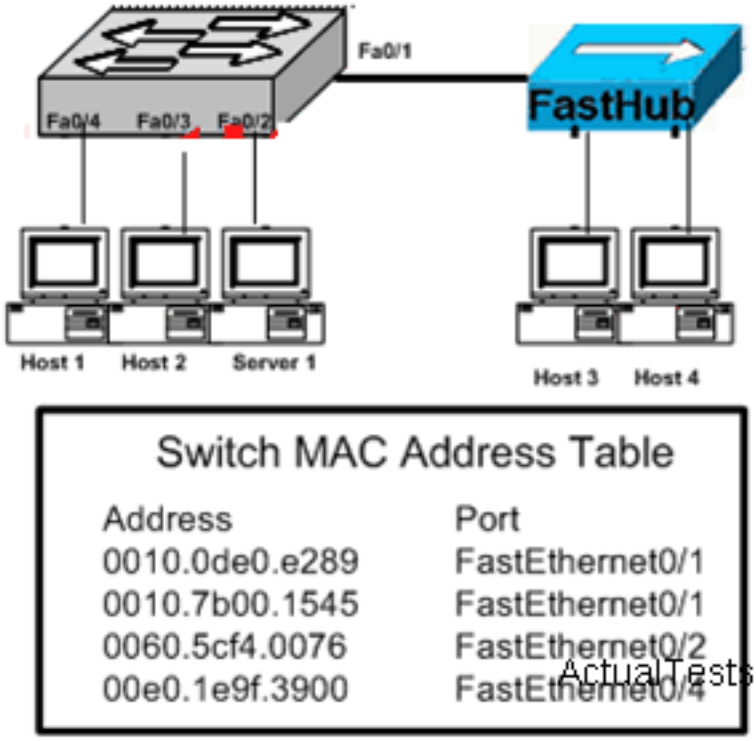
Answer: A

Explanation:
When an Ethernet switch receives a unicast frame with a destination MAC that is listed in the switch table, the switch will search its own MAC address table for the specific port mapping the MAC address. The switch won't forward the frame to all the ports. Thus, resources are saved and efficiency is improved.

How Does the Switch Find Host MACs?
Let's use the diagram below to help us understand how address learning process takes place.

QUESTION NO: 83

Refer to the exhibit. Why does the switch have two MAC addresses assigned to the FastEthernet 0/1 port in the switch address table?



A. Either Host3 or Host4 has just had the NIC replaced.
B. Data from Host3 and Host4 has been received by switch port FastEthernet 0/1.
C. Host3 and Host4 are on two different VLANs.
D. Data from two of the devices connected to the switch has been sent to Host3.

Answer: B

Explanation:
The reason that switches are able to send data packets directly to destination node, rather than send data packets to all nodes like hub using broadcasting, is that Switch is able to identify network card MAC address that connected to network nodes, andplace them to MAC address table. The MAC address table is stored in switch cache, when sending data to destination address, switch will search for the node location of this MAC address in the MAC address table, and then send directly to the node in this location.

Switches learn the MAC addresses of PCs or workstations that are connected to their switch ports by examining the source address of frames that are received on that port. When more than one device is attached to a switch port, such as via the use of a hub as shown in this example, the switch will retain the MAC address of each of the known devices on that port.

QUESTION NO: 84

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

A. source switch port

B. destination IP address
C. destination port address
D. destination MAC address

Answer: D

Explanation:
Switches use port address table to find locations of the receiving station. When a port receives a frame, switch will first study and then forward. Switches will check destination MAC addresses on the frame head, and search for the corresponding entries in port address table. If matching entry is found, switch will forward the frame from the designated port. If the port is the same port that receives this frame (sending and receiving stations are connected to the same port), switch will discard the frame. If no entry is found, or destination MAC address is broadcast address or multi-cast address, switch will flood out the frame from all the rest ports.

QUESTION NO: 85

A Catalyst 2950 needs to be reconfigured. What steps will ensure that the old configuration is erased? (Choose three.)

A. Erase flash.
B. Restart the switch.
C. Delete the VLAN database.
D. Erase the running configuration.
E. Erase the startup configuration.
F. Modify the configuration register.

Answer: B,C,E

Explanation:
For switches such as the 2950, the process is much the same as a router, but you should delete the VLAN.DAT file before reloading the router. This file contains VLAN information and is kept in flash, so it will still be present after a reload.

switch1#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
switch1#reload
Make sure to hit for the two questions regarding the deletion - if you answer "y" instead, the switch thinks you're trying to erase a file named "y"!
After the reload is complete, you'll be prompted to enter setup mode. As you did with the router, enter "N" and begin to configure the router from user exec mode.

QUESTION NO: 86

The network administrator has discovered that the power supply has failed on a switch in the company LAN and that the switch has stopped functioning. It has been replaced with a Cisco Catalyst 2950 series switch. What must be done to ensure that this new switch becomes the root bridge on the network?

A. Lower the bridge priority number.
B. Change the MAC address of the switch.
C. Increase the VTP revision number for the domain.
D. Lower the root path cost on the switch ports.
E. Assign the switch an IP address with the lowest value.

Answer: A

Explanation:
Section 5: Perform and verify initial switch configuration tasks including remote access management (10 questions)

QUESTION NO: 87

What is the purpose of assigning an IP address to a switch?

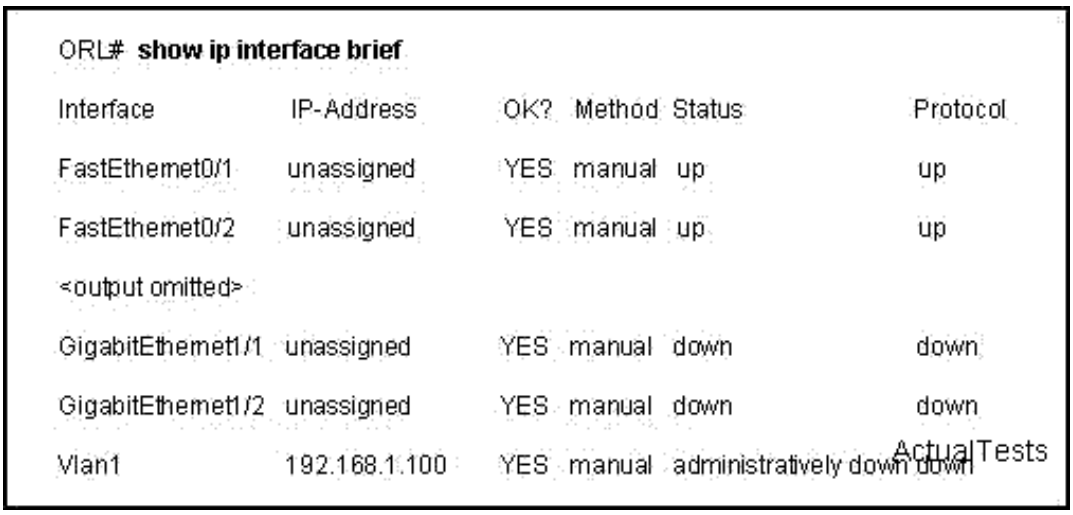
A. To ensure that hosts on the same LAN can communicate with each other.
B. To provide local hosts with a default gateway address
C. To allow the switch to respond to ARP requests between two hosts
D. To allow remote management of the switch.

Answer: D

Explanation:
Switch is a layer 2 device and doesn't use network layer for packet forwarding. The IP address may be used only for administrative purposes such as Telnet access or for network management purposes.

QUESTION NO: 88

Refer to the exhibit. A network administrator is unable to connect remotely to a device and initiates a console session. The administrator executes the show ip interface brief command. Why did the remote connection fail?



A. The Gigabit Ethernet interfaces are not up
B. The switch does not have a management IP address assigned.
C. The switch needs to have a clock rate entered on one of its interfaces.
D. VLAN1 is shut down.

Answer: D

Explanation:
The virtual LAN Interface 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. Since the only IP configured on the switch belongs to VLAN 1, it needs to be enabled for you to remotely access the device.

QUESTION NO: 89

As a trainee you are required to set the default gateway on a Cisco switch to the IP address of 192.168.1.115. Which IOS command should you use?

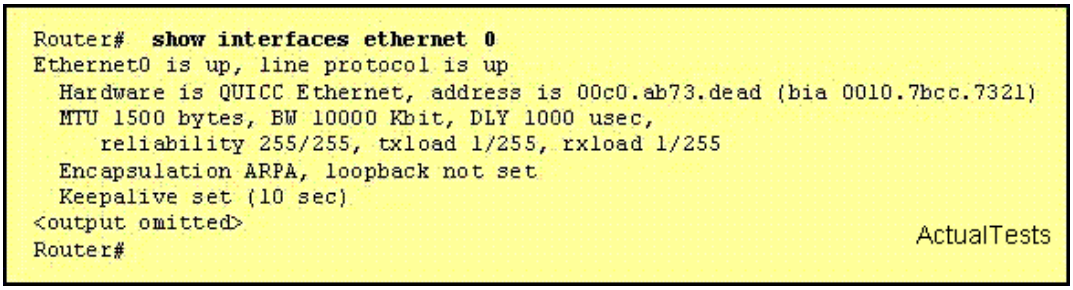
A. switch(config)# ip default-network 192.168.1.115
B. switch(config)# ip default-gateway 192.168.1.115
C. switch(config)# ip route-default 192.168.1.115
D. switch(config)# ip route 192.168.1.115 0.0.0.0

Answer: B

Explanation:
Use the "ip default-gateway" command to enter the IP address of the next-hop router interface that is directly connected to the switch where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch.
Once the default gateway is configured, the switch has connectivity to the remote networks with which a host needs to communicate.

QUESTION NO: 90

Refer to the exhibit. What is the meaning of the output MTU 1500 bytes?



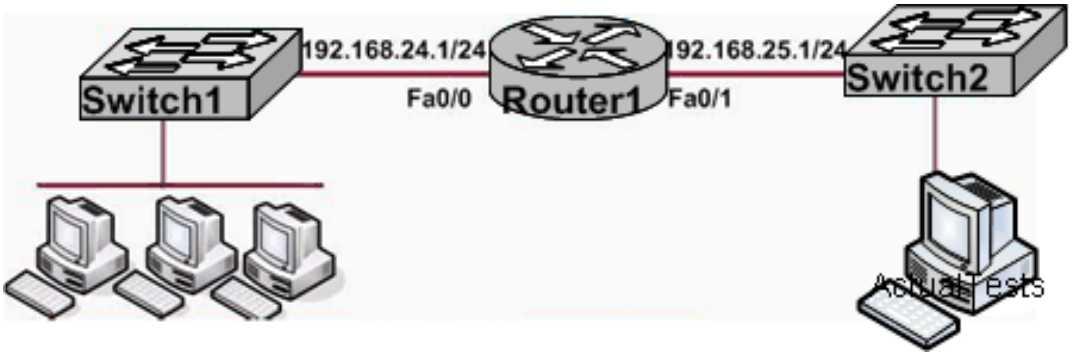
A. The maximum number of bytes that can traverse this interface per second is 1500.
B. The maximum frame size that can traverse this interface is 1500 bytes.
C. The maximum packet size that can traverse this interface is 1500 bytes.
D. The minimum packet size that can traverse this interface is 1500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

Answer: C

Explanation:
MTU is short for Maximum Transmission Unit , which refers to the largest data packet transmitted on the network. The unit of MTU is byte. The MTU of most network devices is 1500 byte. If the MTU of the router is larger than that of the gateway, large packets will be split in order to transmit, this causes the production of many data packet fragments, increasing the packet loss rate and lowering the network speed. If the MTU of one device matches that of another, the packet loss rate will be reduced.

QUESTION NO: 91

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?




```
Switch1 # show running-config
!
hostname Switch1
!
enable secret 5$1$8V43$Wm12DE8KlwUjf8EcZnFT7/
enable password guess
!
<outout omitted>
!
interface Vlan1
 ip address 192.168.24.2 255.255.255.0
 no ip route-cache
!
ip http server
!
line con 0
line vty 0 4
 password cisco
 login
!                                    ActualTests
end
```

A. SWITCH1(config)# interface fa0/1
SWITCH1(config-if)# ip address 192.168.24.3 255.255.255.0

B. SWITCH1(config)# ip default-gateway 192.168.24.1

C. SWITCH1(config)# interface fa0/1
SWITCH1(config-if)# duplex full
SWITCH1(config-if)# speed 100
D. SWITCH1(config)# line con0
SWITCH1(config-line)# password cisco
SWITCH1(config-line)#login

Answer: B

Explanation:
To route traffic to other vlans, we need to enter the IP address of the next-hop router interface that is directly connected to the switch where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch.
Once the default gateway is configured, the switch will have connectivity to the remote networks with which a host needs to communicate.

QUESTION NO: 92

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

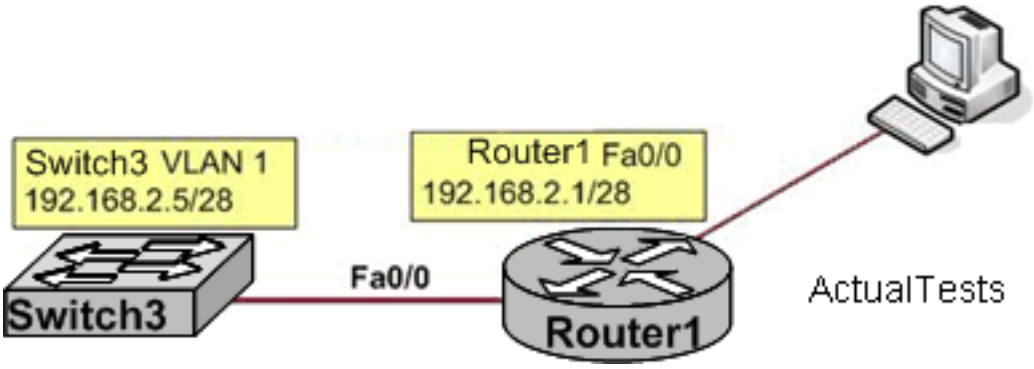
A. Auto
B. Desirable
C. On
D. Transparent

Answer: A,B,C

Explanation:
Here, the trunk link is identified by its physical location as the switch module number and port number. The trunking mode can be set to any of the following:
on -This setting places the port in permanent trunking mode. The corresponding switch port at the other end of the trunk should be similarly configured because negotiation is not allowed. The encapsulation or identification mode should also be manually configured.
off -Th
is setting places the port in permanent non-trunking mode. The port will attempt to convert the link to non-trunking mode.
desirable -Selecting this port will actively attempt to convert the link into trunking mode. If the far end switch port is configured to on , desirable , or auto mode, trunking will be successfully negotiated.
auto -The port will be willing to convert the link into trunking mode. If the far end switch port is configured to on or desirable , trunking will be negotiated. By default, all Fast Ethernet and Gigabit Ethernet links that are capable of negotiating using DTP are configured to this mode. Because of the passive negotiation behavior, the link will never become a trunk, if both ends of the link are left to the auto default.
nonegotiate -The port is placed in permanent trunking mode, but no DTP frames are generated for negotiation. The far end switch port must be manually configured for trunking mode.

QUESTION NO: 93

Refer to the exhibit. The host PC must be able to telnet to switch3 through router1 for management purposes. What must be configured for this connection to be successful?



A. cross-over cable connecting switch3 and Router1
B. VLAN 1 on router1
C. default gateway on switch3
D. IP routing on switch3

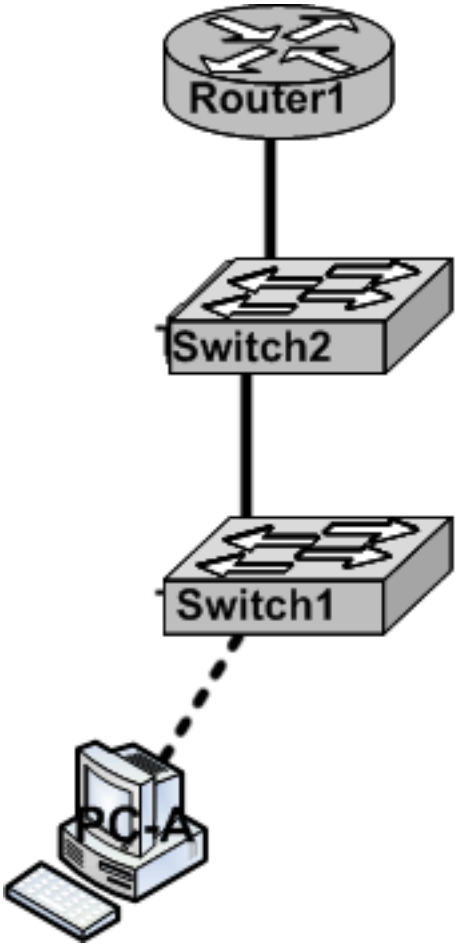
Answer: C

Explanation:
Default gateway refers to router default gateway, which is used to realize access between vlans. When a router receives a destination unknown address packet, it will be sent to the default gateway (such as a router's interface) if default gateway exists, otherwise the packet will be discarded.

In order for a switch to send traffic to a destination that is not located directly, as is the case in our example, a default gateway must be configured on the switch. This will enable it to send the traffic to router Router1 where it can be routed to the host.
Incorrect Answers:
A: A cross over cable is used to connect two switches or two routers together back to back, but a straight through cable should be used when connecting a switch to a routers.
B: This is the default VLAN used and does not need to be configured.
D: IP routing does not need to be enabled, just the default gateway.

QUESTION NO: 94

Refer to the graphic. Computer 1 is consoled into SWITCH1. Telnet connections and pings run from the command prompt on SWITCH1 fail. Which of the following could cause this problem?




```
Switch1# show run
hostname Switch1
<<output omitted>>
!interface FastEthernet0/1
switchport mode trunk
no ip address
!
<<output omitted>>
interface Vlan1
 no ip address
 no ip route-cache
!
<<output omitted>>
```

ActualTests

A. SWITCH1 is not directly connected to Router1.
B. Port 1 on SWITCH1 should be an access port rather than a trunk port.
C. SWITCH1 does not have a default gateway assigned.
D. SWITCH1 does not have an IP address.

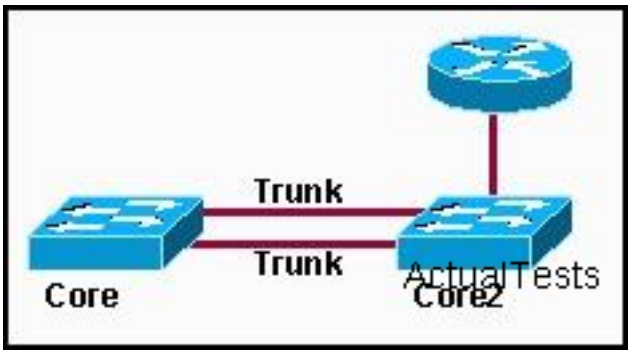
Answer: D

Explanation:
For ping and Telnet the switch should be configured with the IP address and the default gateway. IP is used for administrative purposes, and is needed so the end device will know which IP address to direct the ICMP and telnet reply traffic to.
Incorrect Answers:
A: This is not required, since switch LANs can span multiple VLANs and switches and hubs can be connected directly together.
B: The port type in this case will not cause any kind of connectivity problems, since Trunk ports pass information from all VLANs by default.
C: CDP is not required in order for ping and telnet traffic to work.

QUESTION NO: 95

The switches shown in the diagram, Core and Core2, are both Catalyst 2950s. The addressing scheme for each company site is as follows:

Router Ethernet port 1st usable address Core 2nd usable address Core2 3rd usable address For this network, which of the following commands must be configured on Core2 to allow it to be managed remotely from any subnet on the network? (Choose three.)



A. Core2(config)# interface f0/0 Core2(config-if)# ip address 192.168.1.10 255.255.255.248
B. Core2(config)# interface vlan 1 Core2(config-if)# ip address 192.168.1.11 255.255.255.248
C. Core2(config)# line con 0 Core2(config-line)# password cisco
D. Core2(config)# line vty 0 4 Core2(config-line)# password cisco
E. Core2(config)# ip default gateway 192.168.1.9
F. Core2(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.8

Answer: B,D,E

QUESTION NO: 96

An administrator would like to configure a switch over a virtual terminal connection from locations outside of the local LAN. Which of the following are required in order for the switch to be configured from a remote location? (Choose two.)

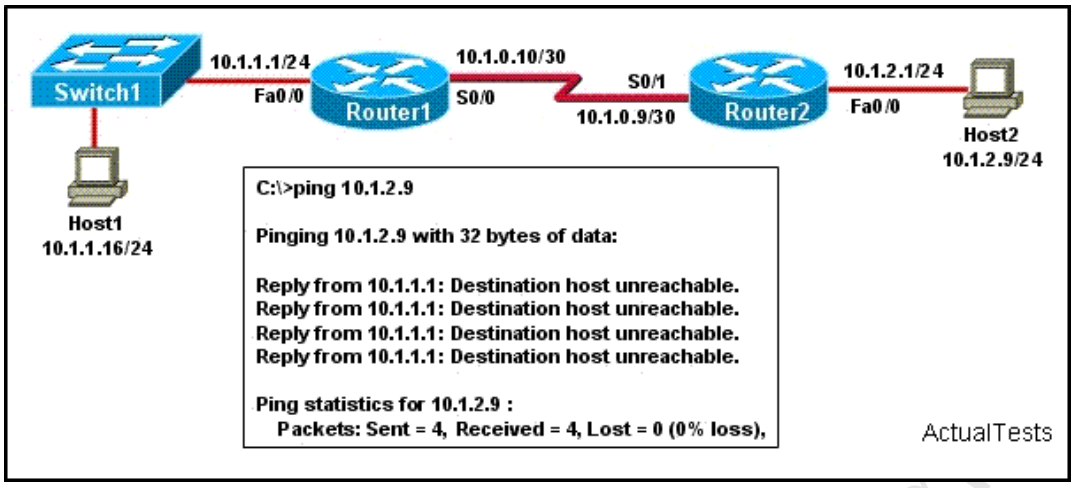
A. The switch must be configured with an IP address, subnet mask, and default gateway.
B. The switch must be connected to a router over a VLAN trunk.
C. The switch must be reachable through a port connected to its management VLAN.
D. The switch console port must be connected to the Ethernet LAN.
E. The switch management VLAN must be created and have a membership of at least one switch port.
F. The switch must be fully configured as an SNMP agent.

Answer: A,C

Explanation:
Section 6: Verify network status and switch operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands (12 questions)

QUESTION NO: 97

Refer to the exhibit. A network administrator attempts to ping Host2 from Host1 and receives the results that are shown. What is a possible problem?



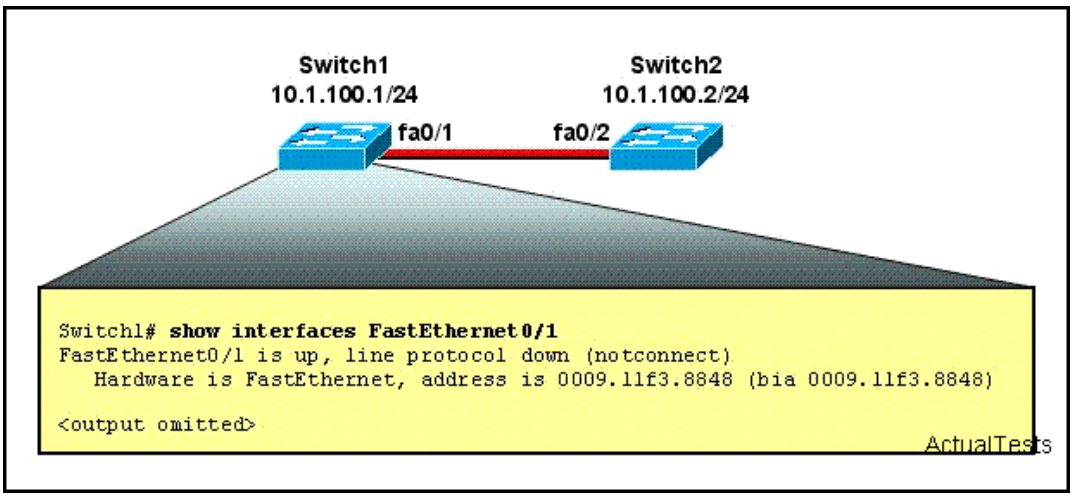
A. The default gateway on Host1 is incorrect.
B. Interface Fa0/0 on Router1 is shutdown.
C. The link between Router1 and Router2 is down.
D. TCP/IP is not functioning on Host1
E. The link between Host1 and Switch1 is down.
F. The link between Switch1 and Router1 is down.

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: 98

Refer to the exhibit. The network administrator has verified that a functioning cable connects Switch1 and Switch2. From the output that is shown, what two pieces of information can the administrator validly conclude? (Choose two.)



A. Interface fa0/1 on Switch1 is in a shutdown state.
B. Using a source MAC address of 0009.11f3.8848, Switch2 is sending frames to Switch1.
C. There is likely to be an IP address issue on Switch1 fa0/1.
D. The interface is functional at OSI Layer 1.
E. The status of fa0/2 should be checked on Switch2.

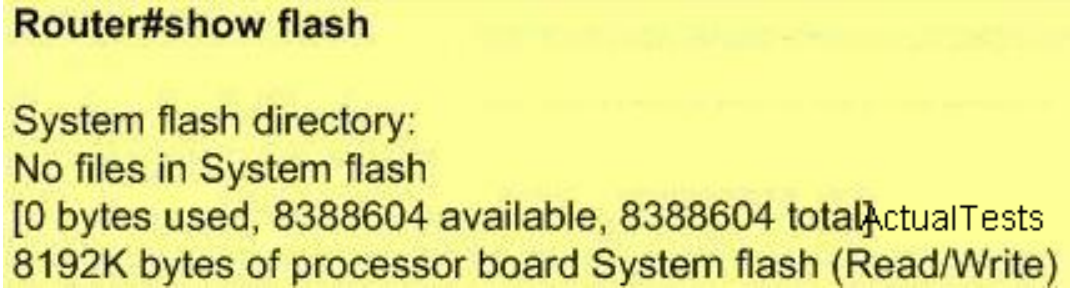
Answer: D,E

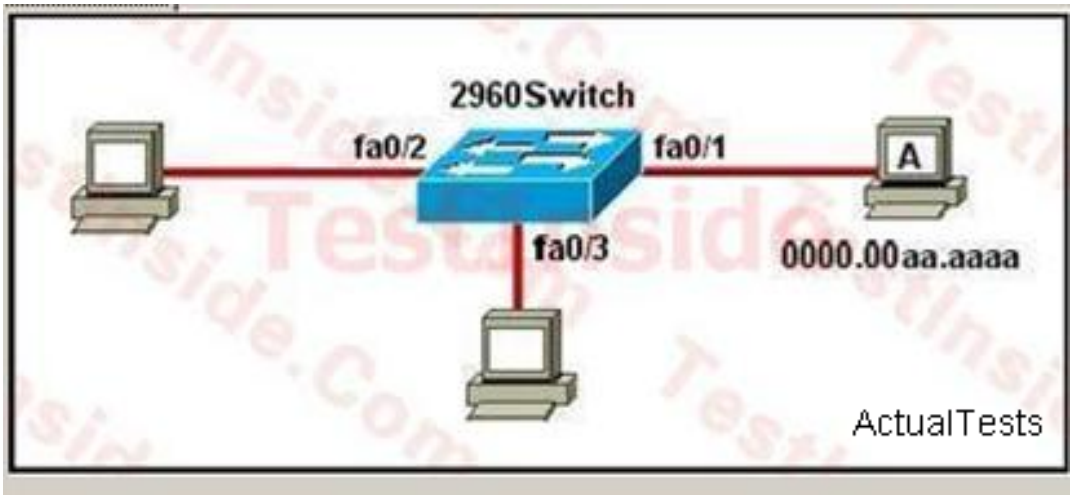
Explanation:
FastEthernet0/1 is up, line protocol down (not connect) indicate that the physical layer has been activated, but layer 2 data link protocol has not been activated. This involves data link layer, it view from the connecting end to maintain activation information (information used to confirm the connectivity available between two devices), here shows the problem of clock frequency (maintain activation information) or frame Packaging types. Maybe the devices in the opposite end are not configured with clock frequency, or package type configuration is not consistent.

QUESTION NO: 99

Second exhibit is of the engine check which one will work.Refer to the exhibit. This command is executed on 2960Switch:
SW(config)# mac-address-table static 0000.00aa.aaaa vlan 10 interface fa0/1

Which two of these statements correctly identify results of executing the command? (Choose two.)





A. MAC address 0000.00aa.aaaa does not need to be learned by this switch.
B. Only MAC address 0000.00aa.aaaa can source frames on the fa0/1 segment.
C. MAC address 0000.00aa.aaaa will be listed in the MAC address table for interface fa0/1 only.
D. Port security is implemented on the fa0/1 interface.

Answer: A,C

QUESTION NO: 100

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

Exhibit:

```
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
0010.5cf4.0076         Dynamic        1       FastEthernet0/1
0010.5cf4.0077         Dynamic        3       FastEthernet0/1
0010.5cf4.1315         Dynamic        1       FastEthernet0/1
0010.70cb.f301         Dynamic        2       FastEthernet0/1
0010.70cb.3f01         Dynamic        5       FastEthernet0/2
0010.1e42.9978         Dynamic        4       FastEthernet0/1
0010.1e9f.3900         Dynamic        3       FastEthernet0/1
0010.70cb.33f1         Dynamic        6       FastEthernet0/3
0010.70cb.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
                                                                ActualTests

Switch1#
```

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

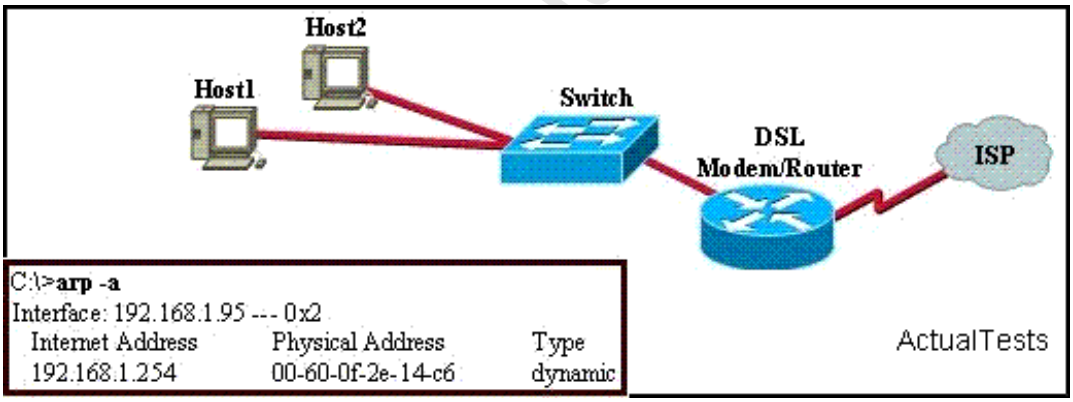
Answer: C,F

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: 101

The user of Host1 wants to ping the DSL modem/router at 192.168.1.254. Based on the Host1 ARP table that is shown in the exhibit, what will Host1 do?



A. send a unicast ARP packet to the DSL modem/router
B. send a Layer 2 broadcast that is received by Host2, the switch, and the DSL modem/router
C. send Layer 3 broadcast packets to which the DSL modem/router responds
D. send unicast ICMP packets to the DSL modem/router

Answer: D

Explanation:

When Host1 sends ICMP packets to the DSL modem/router for the first time, Host1 checks the mapping between the target IP address and the MAC with APP cache and sends unicast ICMP packets. If Host1 cannot find the mapping between the target IP address and the MAC, Host1 sends broadcast packets to find the MAC mapping the target IP address.
The ARP cache contains the MAC mapping the target IP address 192.168.1.254, so Host1 sends unicast ICMP packets to the DSL modem/router.

When Host1 sends ICMP packets to the DSL modem/router

QUESTION NO: 102

A network administrator issues the ping 192.168.2.5 command and successfully tests connectivity to a host that has been newly connected to the network. Which protocols were used during the test? (Choose two.)

A. ICMP
B. ARP
C. DHCP
D. DNS

Answer: A,B

Explanation:
PING (Packet Internet Grope) is program to test network connection amount. Ping sends an ICMP echo request message to the destination and reports whether an expected ICMP echo response is received or not. It is a command used to check whether the network is connected or network connection speed. As a network administrator or a hacker, ping is the first DOS command that one should master. Its operation principle is: the machines on the network are identified by unique IP addresses; when we send a data packet to our destination IP address, it will return a same-sized data packet. With this packet, we can determine the existence of the target host, and the operating system of the host.

ARP finds the hardware address of a host from a known IP address. Here's how it works: when IP has a datagram to send, it must inform a Network Access protocol, such as Ethernet or Token Ring, of the destination's hardware address on the local network. (It has already been informed by upper-layer protocols of the destination's IP address.) If IP doesn't find the destination host's hardware address in the ARP cache, it uses ARP to find this information.

ICMP works at the Network layer and is used by IP for many different services. ICMP is a management protocol and messaging service provider for IP. Its messages are carried as IP datagrams. RFC 1256 is an annex to ICMP, which affords hosts' extended capability in discovering routes to gateways. Periodically, router advertisements are announced over the

network, reporting IP addresses for the router's network interfaces. Hosts listen for these network infomercials to acquire route information. A router solicitation is a request for immediate advertisements and may be sent by a host when it starts up.

QUESTION NO: 103

As the network administrator, you are troubleshooting network issues, which following commands will allow you to find the ip address associated with each MAC address? (Choose two)

A. show hosts
B. show address
C. show interface
D. show arp

Answer: C,D

Explanation:
Use the command "show arp" to display the MAC addresses of Layer2 and the IP addresses of Layer3 contained in the ARP table:
Router # show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.0.0.2 0 0005.dc0c.ffab ARPA Ethernet01
Internet 10.0.0.4 - 0005.dc0c.ff76 ARPA Ethernet0
In the same way, use the command "show interface" on router to display the related information of the MAC addresses of Layer2 and the IP addresses of Layer3
Router# show interfaces
Ethernet 0 is up, line protocol is up
Hardware is MCI Ethernet, address is 0000.0d00.640c (bia 0000.0d00.640c)
Internet address is 10.112.12.85, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
----more----

The "show arp" command Displays the entries in the ARP table, including their layer 2 MAC address and layer 3 IP address.
Example:
The following is the output for the show arp command on Router 1:

TK1 # show arp

Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.0.0.3 0 0004.dd0c.ffcb ARPA Ethernet01
Internet 10.0.0.1 - 0004.dd0c.ff86 ARPA Ethernet0

To see the MAC (hardware) address of the router interfaces as well as their IP addresses, use the "show interfaces" command as shown in the example below:

TK1# show interfaces

Ethernet 0 is up, line protocol is up
Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
Internet address is 10.108.28.8 , subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255

QUESTION NO: 104

While troubleshooting a connectivity problem, a network administrator notices that a port status LED on a Cisco Catalyst series switch is alternating green and amber. Which condition could this indicate?

A. The port is blocked by spanning tree.
B. The port is experiencing errors.
C. The port is administratively disabled.
D. The port has an active link with normal traffic activity.

Answer: B

Explanation:
Here are some Port status LEDs and their meanings:

Port Mode	LED Color	Meaning
STAT (port status)	Off	No link, or port was administratively shut down.
	Green	Link present.
	Flashing green	Activity. Port is transmitting or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data. Note After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
	Flashing amber	Port is blocked by STP and is transmitting or receiving packets.
DUPLX (duplex)	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.
SPEED	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	Flashing green	Port is operating at 1000 Mbps. ActualTests

QUESTION NO: 105

What is the purpose of using the traceroute command?

A. to display the current TCP/IP configuration values
B. to see how a device MAC address is mapped to its IP address
C. to see the path a packet will take when traveling to a specified destination
D. to display the MTU values for each router in a specified network path from a source to a destination
E. to map all the devices on a network

Answer: C

Explanation:
The traceroute command traces the network path of Internet routers that packets take as they are forwarded from your computer to a destination address. The "length" of the network connection is indicated by the number of Internet routers in the traceroute path. This command is useful for troubleshooting purposes and shows the router hops as well as the latency.

QUESTION NO: 106

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

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	192.168.40.5

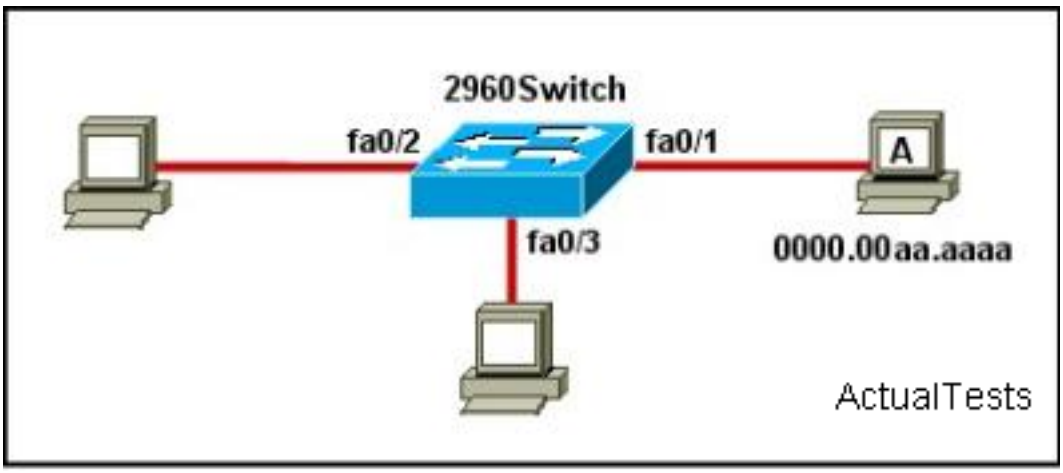
ActualTests

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

QUESTION NO: 107

Refer to the exhibit.



This command is executed on 2960Switch:

2960Switch(config)# mac-address-table static 0000.00aa.aaaa vlan 10 interface fa0/1

Which two of these statements correctly identify results of executing the command? (Choose two.)

A. Port security is implemented on the fa0/1 interface.
B. MAC address 0000.00aa.aaaa does not need to be learned by this switch.
C. Only MAC address 0000.00aa.aaaa can source frames on the fa0/1 segment.
D. Frames with a Layer 2 source address of 0000.00aa.aaaa will be forwarded out fa0/1.
E. MAC address 0000.00aa.aaaa will be listed in the MAC address table for interface fa0/1 only.

Answer: B,E

Explanation:
To add static entries to the MAC address table, use the mac - address - table static command in global configuration mode. Static entries will automatically be added to the MAC address table and do not need to be learned dynamically. In this example, interface fa0/1 was specified so this static entry only applies to that interface.

QUESTION NO: 108

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

QUESTION NO: 109

Which command is used to see the path taken by packets across an IP network?

A. show ip route
B. show route
C. traceroute
D. trace ip route

Answer: C

Explanation:
Section 7: Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures (4 questions)

QUESTION NO: 110

Recently, associates have noticed extremely slow network performance, intermittent connectivity, and connection losses. After entering the "show interfaces" command, you notice that the Ethernet interface is configured as 100 Mbps full-duplex and that there is evidence of late collisions. What could be the cause of this problem?

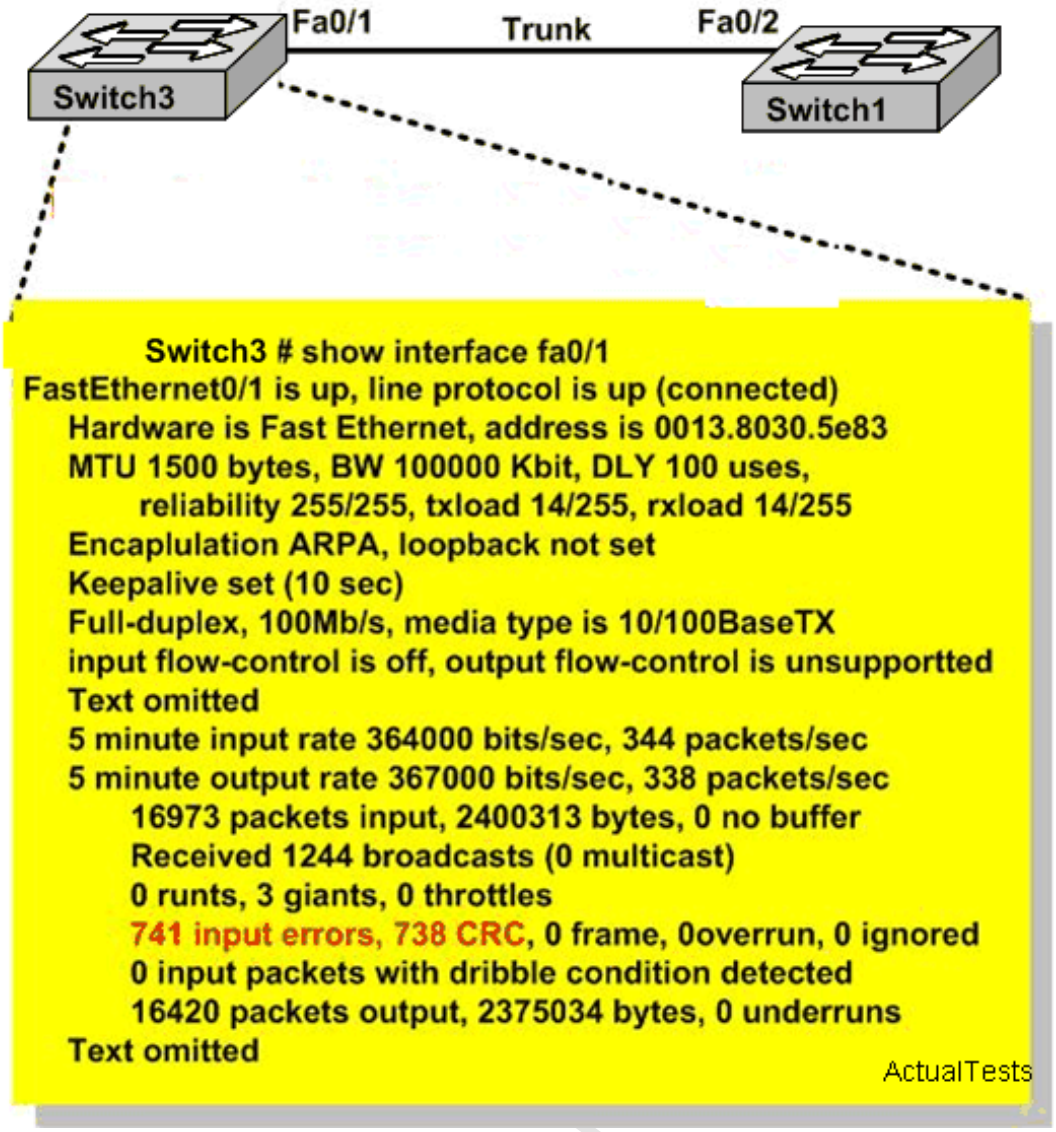
A. A routing loop
B. Duplex mismatch
C. Trunking mode mismatch
D. Improperly configured root bridge

Answer: B

Explanation:
A duplex mismatch may result in performance issues, intermittent connectivity, and loss of communication. When troubleshooting NIC issues, verify that the NIC and switch are using a valid configuration. Some third-party NIC cards may fall back to half-duplex operation mode, even though both the switchport and NIC configuration have been manually configured for 100 Mbps, full-duplex. This behavior is due to the fact that NIC autonegotiation link detection is still operating when the NIC has been manually configured. This causes duplex inconsistency between the switchport and the NIC. Symptoms include poor port performance and frame check sequence (FCS) errors that increment on the switchport. To troubleshoot this issue, try manually configuring the switchport to 100 Mbps, half-duplex. If this action resolves the connectivity problems,you may be running into this NIC issue. Try updating to the latest drivers for your NIC, or contact your NIC card vendor for additional support.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a00800a7af0.shtml

QUESTION NO: 111

Refer to the exhibit. Given this output for SWITCH3, what should the network administrator's next action be?



A. Check the trunk encapsulation mode for SWITCH3's fa0/1 port.
B. Check the trunk encapsulation mode for SWITCH1's fa0/2 port.
C. Check the duplex mode for SWITCH3's fa0/1 port.
D. Check the duplex mode for SWITCH1's fa0/2 port.

Answer: D

QUESTION NO: 112

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

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

Answer: B,C,D

Explanation:
Both the auto and on modes can be automatically switched to the desirable mode based on the topology.

A trunk port can be configured as one of the following 5 different modes: on, off, desirable, auto, or nonegotiate.
The table below is a summary of the configuration modes.

Mode	Function	DTP Frames Transmitted	Final State (Local Port)
Auto(default)	Makes the port willing to convert the link to a trunk. The port becomes a trunk port if the neighboring port is set to on or desirable mode.	Yes, periodic.	Trunking
On	Puts the port into permanent trunking mode and negotiates to convert the link into a trunk. The port becomes a trunk port even if the neighboring port does not agree to the change.	Yes, periodic.	Trunking, **unconditionally**.
Nonegotiate	Puts the port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link. This is useful for devices that do not support DTP.	No	Trunking, **unconditionally**.
Desirable	Makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to on, desirable, or auto mode.	Yes, periodic.	It will end up in trunking state only if the remote mode is on, auto, or desirable.
Off	Puts the port into permanent non-trunking mode and negotiates to convert the link into a non-trunk link. The port becomes a non-trunk port even if the neighboring port does not agree to the change.	No in steady state, but will transmit informs to speed up remote end detection after the change from on.	Non-trunking

QUESTION NO: 113

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?

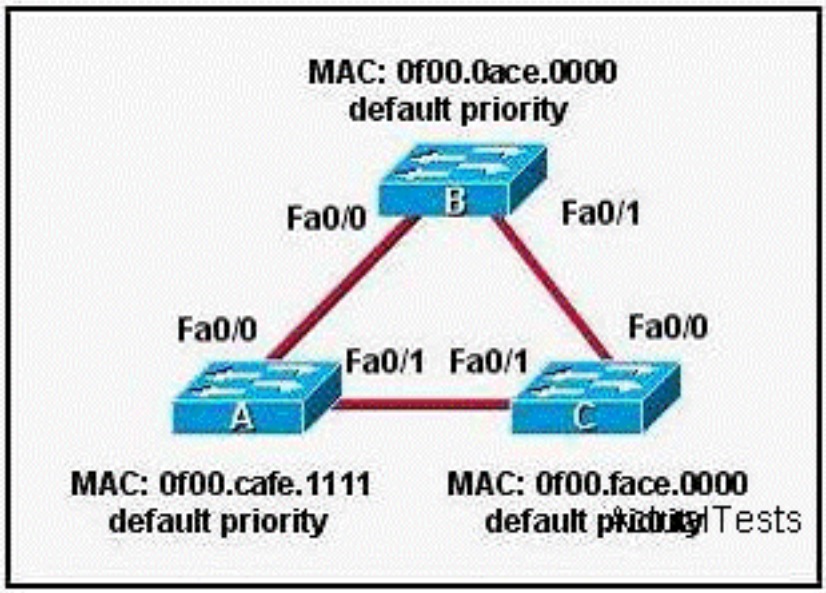
A. This is a port on a network interface card in a PC.
B. This is a 100 Mb/s switch port.
C. This is a 10 Mb/s switch port.
D. This is an Ethernet port operating at full duplex.
E. This is an Ethernet port operating at half duplex.

Answer: E

Explanation:
CSMA/CD is the basic way that the traditional Ethernet operates. 10M interface is the way that an Ethernet operates at half duplex.
Section 8: Describe enhanced switching technologies (including: VTP, RSTP, VLAN, PVSTP, 802.1q) (17 questions)

QUESTION NO: 114

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:
1) Switch B will become the ROOT BRIDGE because it has the lowest MAC address as you can see in the picture.Its both ports will become STP designated ports so choice C and D are right . 2) Next Election will be of Designated Ports on the segment connecting A and C. Switch A has lower MAC address so, its port FA0/1 will become designated port and FA0/1 of switch C will be placed in a BLOCKING state to avoid switching LOOPS. This makes option B right. .So,ultimately B,C & D are correct.

QUESTION NO: 115

A switch is configured with all ports assigned to VLAN 2. In addition, all ports are configured as full-duplex FastEthernet. What is the effect of adding switch ports to a new VLAN on this switch?

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

Answer: B

Explanation:
A VLAN is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment.
Networks that use the campus-wide or end-to-end VLANs logically segment a switched network based on the functions of an organization, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup can be connected to the same VLAN, regardless of their physical network connections or interaction with other workgroups. Network reconfiguration can be done through software instead of physically relocating devices.
Cisco recommends the use of local or geographic VLANs that segment the network based on IP subnets. Each wiring closet switch is on its own VLAN or subnet and traffic between each switch is routed by the router. The reasons for the Distribution Layer 3 switch and examples of a larger network using both the campus-wide and local VLAN models will be discussed later.
A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. Ports on a switch can be grouped into VLANs in order to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out ports belonging to that VLAN, including trunk ports, so a switch that connects to another switch will normally introduce an additional broadcast domain.

VLAN (Virtual Local Area Network) technology is to solve the problem that switches can't limit broadcast within the LAN interconnection. This technology can divide a LAN into more logical LAN- VLAN, each VLAN is a broadcast domain, the communication between the hosts within a VLAN is like that of the hosts in a LAN, while the communication can't be achieved between VLANs directly. Thus the broadcast datagram is limited within a LAN. So, creating a new VLAN on switch is the same as adding a new broadcast domain.

QUESTION NO: 116

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

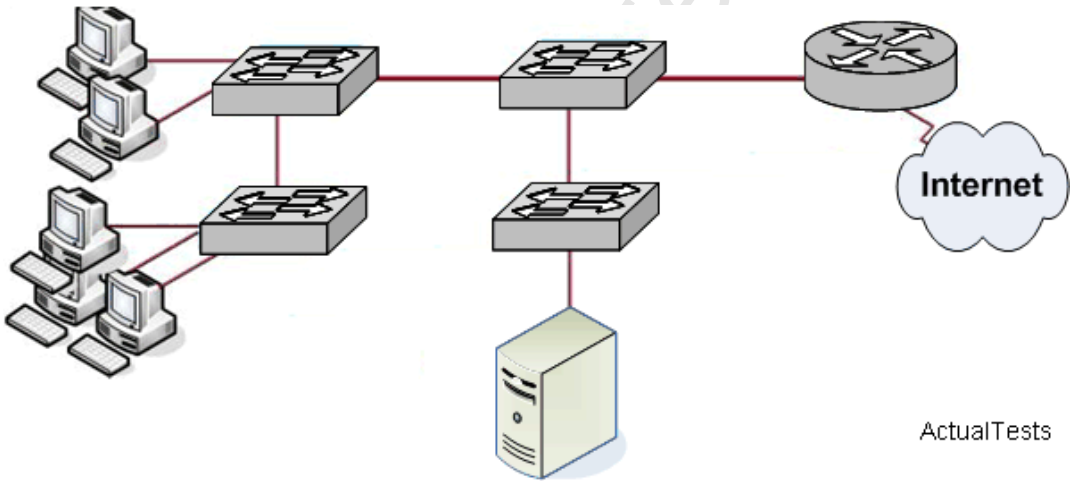
A. It is a Layer 2 messaging protocol which maintains VLAN configurations across networks.
B. It is a trunking protocol capable of carrying untagged frames.
C. It modifies the 802.3 frame header, and thus requires that the FCS be recomputed.
D. It includes an 8-bit field which specifies the priority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

Answer: B,C

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: 117

Refer to the exhibit. When the hosts boot, hosts that are connected to the switches are having trouble getting a DHCP address from the DHCP server. Which STP feature could minimize the effects of STP convergence for the hosts?



A. path cost
B. port priority
C. BID
D. PortFast

Answer: D

Explanation:
The purpose of PortFast is to shorten the time to access port and STP convergence. The advantages of PortFast are to prevent DHCP overtime, Novell login issue, Apple Talk address

finding, and so on. In addition to the specific network design, it is generally used when accessing to ports. If startup PostFast when connecting to other switch ports, it may result in bridge loop.

QUESTION NO: 118

Which statement accurately describes a benefit provided by VTP?

A. VTP allows switches to share VLAN configuration information.
B. VTP allows physically redundant links while preventing switching loops.
C. VTP allows a single port to carry information to more than one VLAN.
D. VTP allows routing between VLANs.

Answer: A

Explanation:
Trunking Protocol (VTP) are to manage all configured VLANs across a switched internetwork and to maintain consistency throughout that network VTP allows you to add, delete, and rename VLANs-information that is then propagated to all other switches in the VTP domain.

Here's a list of some features of VTP:

* Consistent VLAN configuration across all switches in the network
* VLAN trunking over mixed networks, such as Ethernet to ATM LANE or even FDDI
* Accurate tracking and monitoring of VLANs
* Dynamic reporting of added VLANs to all switches in the VTP domain
* Plug and Play VLAN adding

Administration of network environments that consists of many interconnected switches is complicated. Cisco has developed a propriety solution to manage VLANs across such networks using the VLAN Trunking Protocol (VTP) to exchange VLAN configuration information between switches. VTP uses Layer 2 trunk frames to exchange VLAN information so that the VLAN configuration stays consistent throughout a network. VTP also manages the additions, deletions, and name changes of VLANs across multiple switches from a central point, minimizing misconfigurations and configuration inconsistencies that can cause problems, such as duplicate VLAN names or incorrect VLANtype settings.
VTP is organized into management domains or areas with common VLAN requirements. A switch can belong to only one VTP domain. Switches in different VTP domains do not share VTP information. Switches in a VTP domain advertise several attributes to their domain neighbors. Each advertisement contains information about the VTP management domain, VTP configuration revision number, known VLANs, and specific VLAN parameters.
The VTP process begins with VLAN creation on a switch called a VTP server. VTP floods advertisements throughout the VTP domain every 5 minutes, or whenever there is a change in

VLAN configuration. The VTP advertisement includes a configuration revision number, VLAN names and numbers, and information about which switches have ports assigned to each VLAN. By configuring the details on one or more VTP server and propagating the information through advertisements, all switches configuration know the names and numbers of all VLANs.

QUESTION NO: 119

As the network administrator. You need to configure two switches to exchange VLAN information. Which protocol provides a method of sharing VLAN configuration information between these two switches?

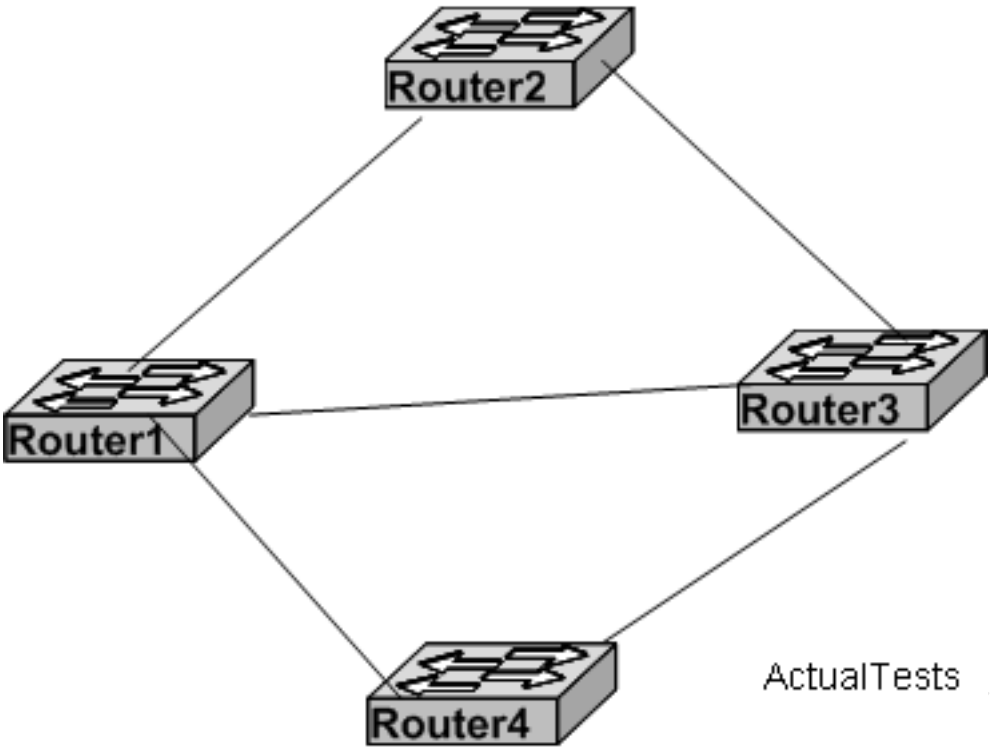
A. 802.1Q
B. STP
C. VLSM
D. VTP

Answer: D

Explanation:
VLAN Trunking Protocol (VTP) is Cisco level 2 information transfer protocol, mainly controls the VLANs add, delete, and rename within network. VTP reduce the management services in switch network. When a user prepares to configure new VLAN for VTP server, he may implement VLAN distribution through all the switches, to avoid identical VLAN configuration. VTP is a Cisco private protocol, which support the majority of Cisco Catalyst Series products.
Through VTP, all switches within its domain have a clear idea of all the VLANs, except when VTP can create extra traffic. At this time, all unknown unicast and broadcast spread throughout the VLAN, making all the switches in the network receive all broadcasts, even if no user is connected in the VLAN, the situation is no exception. And VTP Pruning is able remove the extra traffic.

QUESTION NO: 120

Refer to the exhibit. Spanning Tree Protocol has created a loop-free logical topology in the network that is pictured. How many ports have been placed in the blocking mode?



A. three
B. one
C. none
D. two

Answer: D

Explanation:
Spanning Tree maintains a loop free topology. Regardless of which switch is elected the root switch, two of the five links will not be used as they would create a redundant path.

QUESTION NO: 121

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

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

Answer: B,C,D

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: 122

A network administrator needs to force a high-performance switch that is located in the MDF to become the root bridge for a redundant path switched network. What can be done to ensure that this switch assumes the role as root bridge?

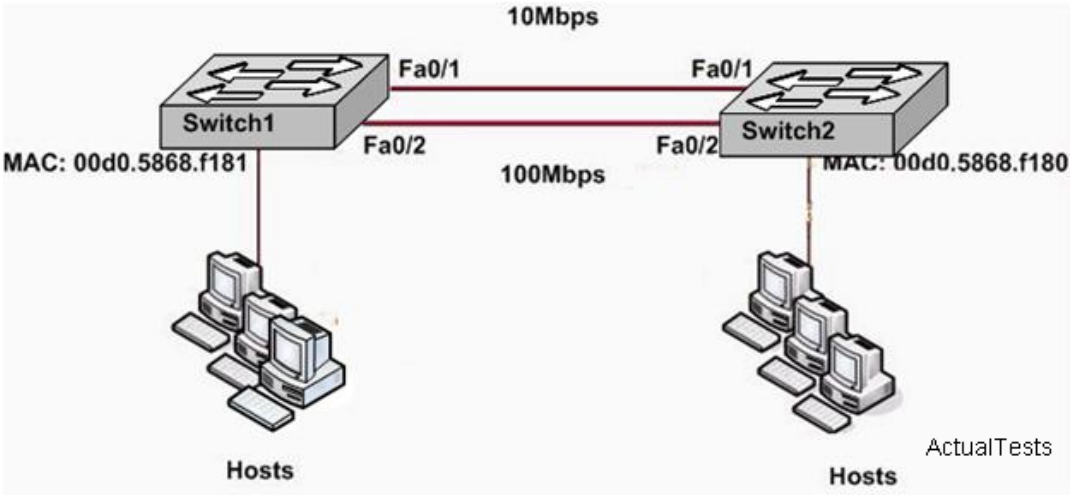
A. Connect the switch directly to the MDF router, which will force the switch to assume the role of root bridge.
B. Configure the switch for full-duplex operation and configure the other switches for half-duplex operation.
C. Establish a direct link from the switch to all other switches in the network.
D. Assign the switch a higher MAC address than the other switches in the network have.
E. Configure the switch so that it has a lower priority than other switches in the network.

Answer: E

Explanation:
For all switches in a network to agree on a loop-free topology, a common frame of reference must exist. This reference point is called the Root Bridge . The Root Bridge is chosen by an election process among all connected switches. Each switch has a unique Bridge ID (also known as the bridge priority) that it uses to identify itself to other switches. The Bridge ID is an 8-byte value. 2 bytes of the Bridge ID is used for a Bridge Priority field, which is the priority or weight of a switch in relation to all other switches. The other 6 bytes of the Bridge ID is used for the MAC Address field, which can come from the Supervisor module, the backplane, or a pool of 1024 addresses that are assigned to every Supervisor or backplane depending on the switch model. This address is hard coded, unique, and cannot be changed.
The election process begins with every switch sending out BPDUs with a Root Bridge ID equal to its own Bridge ID as well as a Sender Bridge ID. The latter is used to identify the source of the BPDU message. Received BPDU messages are analyzed for a lower Root Bridge ID value. If the BPDU message has a Root Bridge ID (priority) of the lower value than the switch's own Root Bridge ID, it replaces its own Root Bridge ID with the Root Bridge ID announced in the BPDU. If two Bridge Priority values are equal, then the lower MAC address takes preference.

QUESTION NO: 123

The exhibited network is stable and operating properly. Assuming that default STP configurations are running on both switches, which port will be in blocking mode?

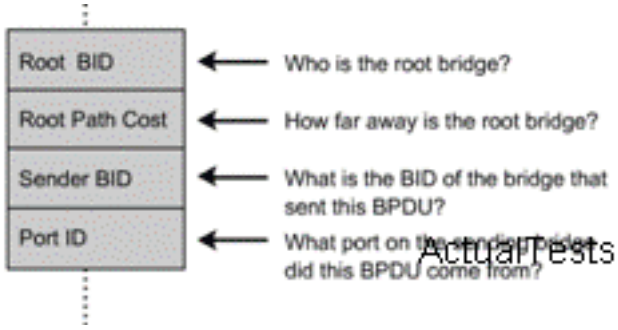


A. Port Fa0/2 on Switch1
B. Port Fa0/1 on Switch2
C. Port Fa0/1 on Switch1
D. Port Fa0/2 on Switch2

Answer: C

Explanation:
First find out which switch port will become blocking mode through root-bridge election.
Root-bridge election:
Bridge ID = Bridge Priority + Bridge MAC address
The default bridge priority is 32,768. In this case, you only need to compare two switch MAC addresses. The MAC address of Switch2 is the smallest one. Therefore it will be the root-bridge of this switching network.
As a non-root bridge, an interface of Switch1 will be blocked by STP. Compare the speed of the links that Fa0/1 and Fa0/2 connect, you'll find that the link that Fa0/1 connects needs much higher cost. Therefore Fa0/1 will be blocked.

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.



The switches move on to selecting Root Ports. The Root Port of a bridge is the port that is closest to the Root Bridge in terms of Path Cost. Every non-Root Bridge must select one Root Port. Again, bridges use the concept of cost to measure closeness. As with some routing metrics, the measure of closeness using STP is not necessarily reflected by hop count. Specifically, bridges track what is referred to as Root Path Cost, which is the cumulative cost of all links to the Root Bridge . So, Answer A is correct.

QUESTION NO: 124

What is the purpose of Spanning Tree Protocol?

A. to provide multiple gateways for hosts
B. to maintain a loop-free Layer 2 network topology
C. to prevent routing loops
D. to create a default route

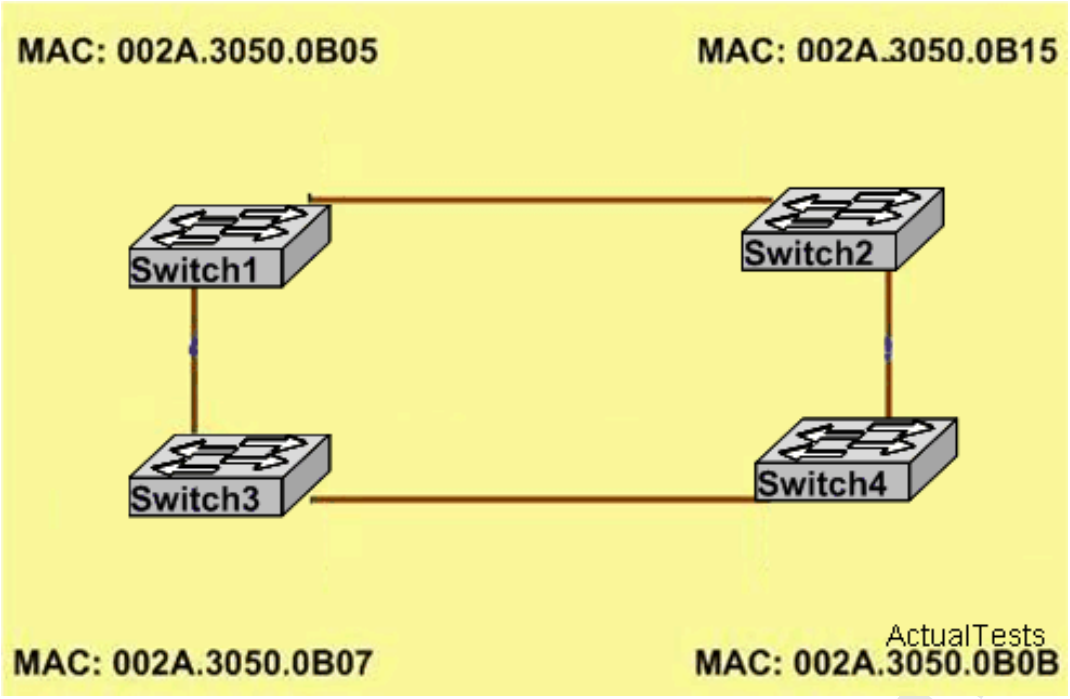
Answer: B

Explanation:
STP (Spanning Tree protocol) is able to overcome transparent bridge in network redundancy. Through the use of non-loop path, STP is able to avoid and eliminate network loops. It may locate the loop and cut off link redundancy.

STP's main task is to stop network loops from occurring on your Layer 2 network (bridges or switches). It vigilantly monitors the network to find all links, making sure that no loops occur by shutting down any redundant ones. STP uses the spanning-tree algorithm (STA) to first create a topology database, then search out and destroy redundant links. With STP running, frames will only be forwarded on the premium, STP-picked links.

QUESTION NO: 125

Refer to the exhibit. Three Cisco 2950 switches are set to their default priority settings. During the spanning-tree process, which switch will be elected as the root bridge?



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

Answer: A

Explanation:
The first step of STP is root-bridge election. BPDU is used in this election process. When device advertises BPDU, it will put its own switch ID in BPDU. Switch ID is used for the election of root switch. Switch with a minimum switch ID is selected as root. Switch ID is composed of two components:
1. Switch Priority: the default priority on Cisco switches is 32,768 (two bytes in length)
2. Switches MAC address (6 bytes in length)
By default, the switch with the lowest MAC address in switching network will be root-bridge.

QUESTION NO: 126

Which of the protocols operates at Layer 2 of the OSI model, and is used to maintain a loop-free network?

A. VTP
B. IGRP
C. RIP
D. STP

Answer: D

Explanation:
A Layer 2 switch, which functions as a transparent bridge, offers no additional links for redundancy purposes. To add redundancy, a second switch must be added. Now two switches offer the transparent bridging function in parallel. LAN designs with redundant links introduce the possibility that frames might loop around the network forever. These looping frames would cause network performance problems. For example, when the switches receive an unknown unicast, both will flood the frame out all their available ports, including the ports that link to the other switch, resulting in what is known as a bridging loop, as the frame is forwarded around and around between two switches. This occurs because parallel switches are unaware of each other. The Spanning Tree Protocol (STP), which allows the redundant LAN links to be used while preventing frames from looping around the LAN indefinitely through those redundant links, was developed to overcome the possibility of bridging loops. It enables switches to become aware of each other so that they can negotiate a loop-free path through the network. Loops are discovered before they are opened for use, and redundant links are shut down to prevent the loops from forming. STP is communicated between all connected switches on a network. Each switch executes the Spanning-Tree Algorithm (STA) based on information received from other neighboring switches. The algorithm chooses a reference point in the network and calculates all the redundant paths to that reference point. When redundant paths are found, STA picks one path to forward frames with and disables or blocks forwarding on the other redundant paths. STP computes a tree structure that spans all switches in a subnet or network. Redundant paths are placed in a blocking or standby state to prevent frame forwarding. The switched network is then in a loop-free condition. However, if a forwarding port fails or becomes disconnected, the STA will run again to recompute the Spanning-Tree topology so that blocked links can be reactivated.

STP (spanning tree protocol) operates on layer 2 to prevent loops in switches and bridges.
Incorrect Answers:
A: VTP is the VLAN Trunking Protocol, used to pass VLAN information through switches. It relies on the STP mechanism to provide a loop free network.
B: RIP and IGRP are routing protocols, which are used at layer 3 to maintain a loop free routed environment.
C: RIP and IGRP are routing protocols, which are used at layer 3 to maintain a loop free routed environment.

QUESTION NO: 127

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

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

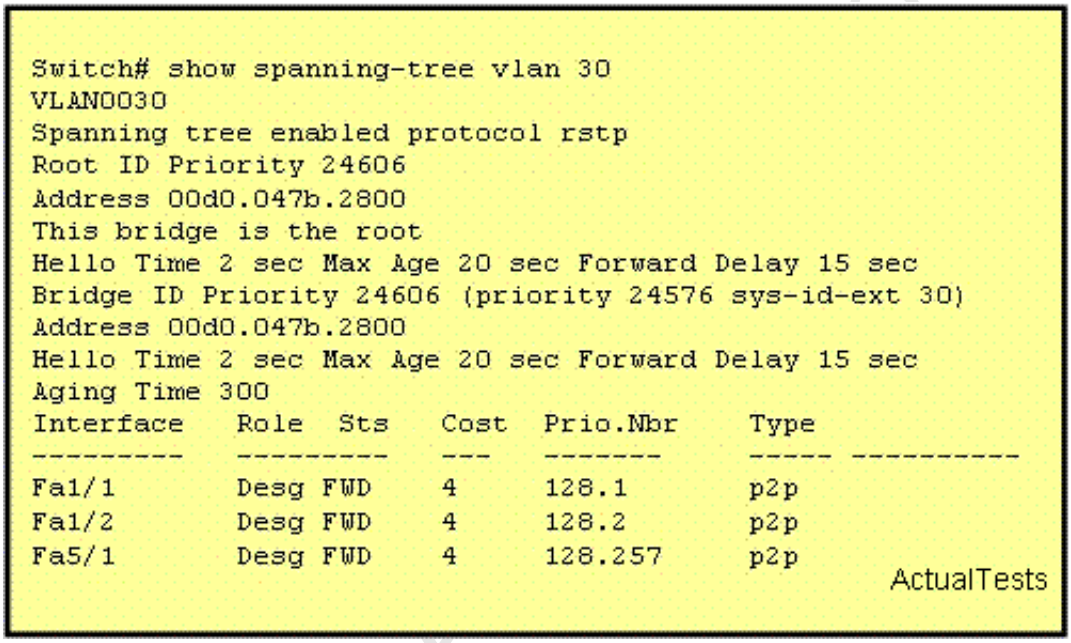
Answer: A,B

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: 128

Refer to the exhibit. The output that is shown is generated at a switch. Which three of these statements are true? (Choose three.)



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

Answer: A,B,F

Explanation:
Root bridge election succeeds, switches stop flooding, and all ports have experienced discarding, learning or forwarding status. The default priority for the bridge is 32768; it shows in Role and Sts that all designated ports are in forward state.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) enhances the 802.1d standard with one goal in mind: improving STP convergence. To do so, RSTP defines new variations on BPDUs between switches, new port states, and new port roles, all with the capability to operate backwardly compatible with 802.1d switches.

The default priority value of spanning is 32,768 but shown value is lower than default value.

In RSTP new port state is defined as:

STP State (802.1d)	RSTP State (802.1w)
Disabled	Discarding
Blocking	Discarding
Listening	Discarding
Learning	Learning
Forwarding	Forwarding

QUESTION NO: 129

What is the purpose of the Cisco VLAN Trunking Protocol?

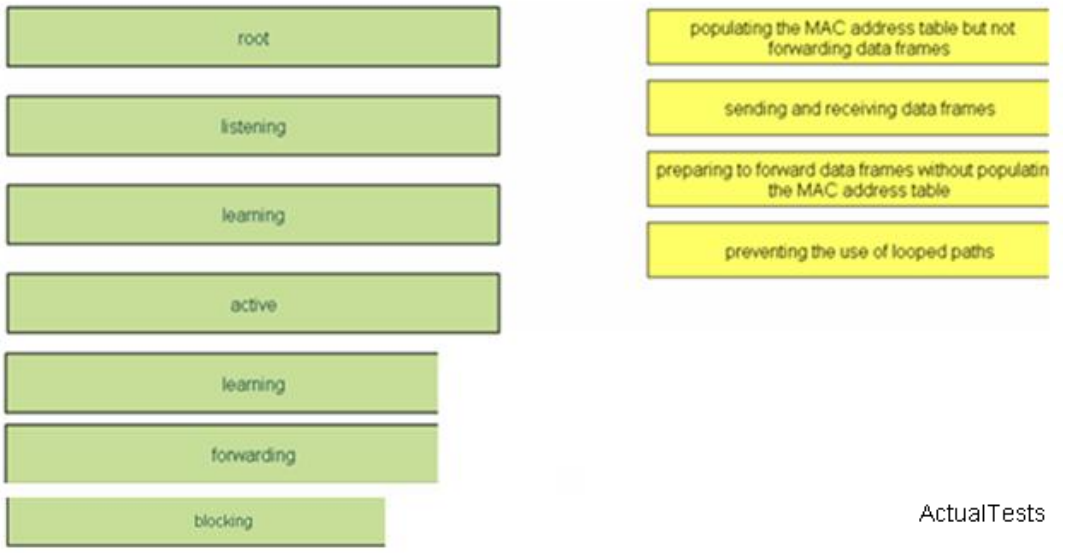
A. to provide a mechanism to dynamically assign VLAN membership to switch ports
B. to allow for managing the additions, deletions, and changes of VLANs between switches
C. to provide a mechanism to manually assign VLAN membership to switch ports
D. to allow native VLAN information to be carried over a trunk link
E. to allow traffic to be carried from multiple VLANs over a single link between switches

Answer: B

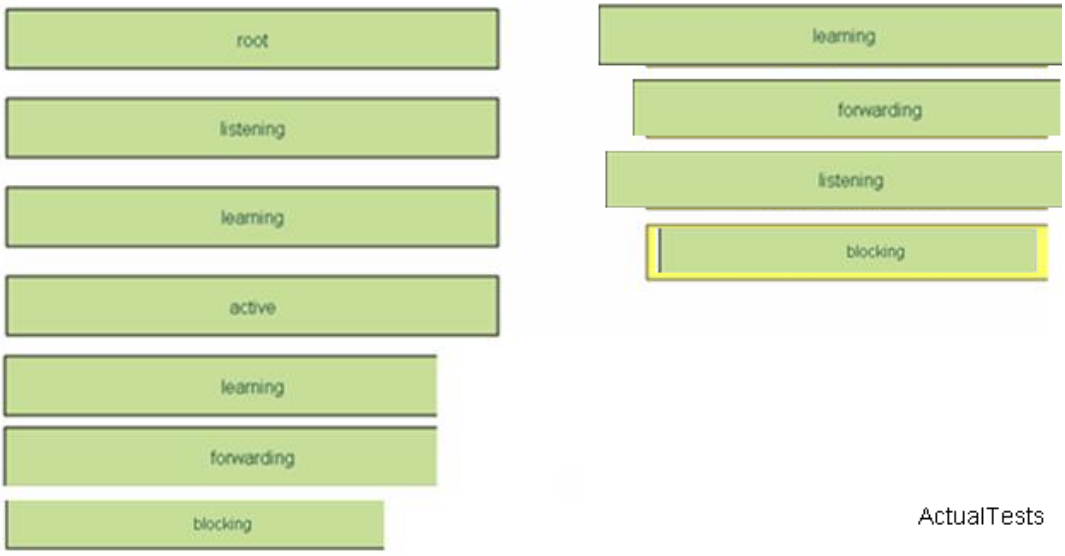
Explanation:
The basic goals of the VLAN Trunking Protocol (VTP) are to manage all configured VLANs across a switched internetwork and to maintain consistency throughout that network VTP allows you to add, delete, and rename VLANs-information that is then propagated to all other switches in the VTP domain.

QUESTION NO: 130 DRAG DROP

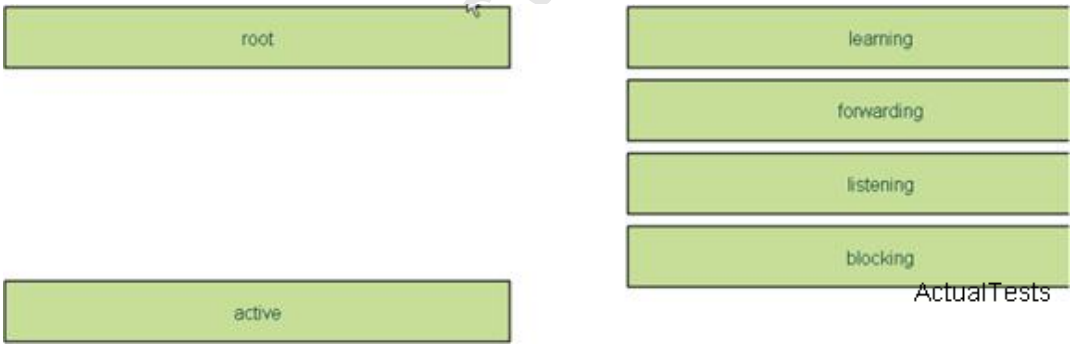
Place the Spanning-Tree Protocol port state on its function by dragging the state on the left to the correct target on the right. (Not all options on the left are used.)



Answer:



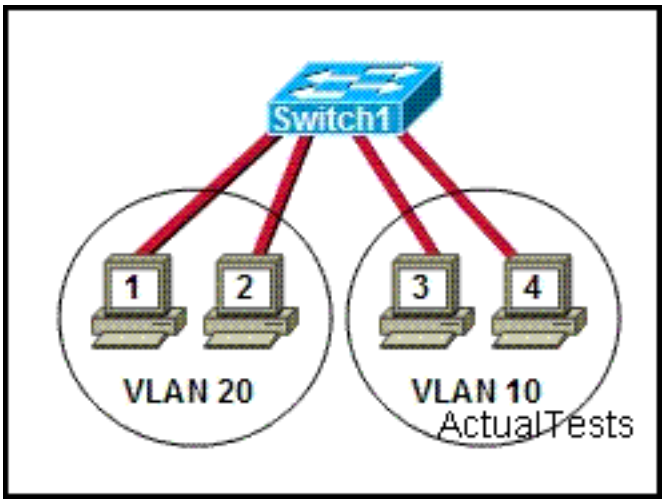
Explanation:



Section 9: Describe how VLANs create logically separate networks and the need for routing between them (4 questions)

QUESTION NO: 131

Refer to the exhibit. Hosts on the same VLAN can communicate with each other but are unable to communicate with hosts on different VLANs. What is needed to allow communication between VLANs?



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

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: 132

Which three statements are typical characteristics of VLAN arrangements? (Choose three.)

A. A new switch has no VLANs configured.
B. Connectivity between VLANs requires a Layer 3 device.
C. VLANs typically decrease the number of collision domains.
D. Each VLAN uses a separate address space.
E. A switch maintains a separate bridging table for each VLAN.
F. VLANs cannot span multiple switches.

Answer: B,D,E

QUESTION NO: 133

Which three benefits are 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 number of broadcast domains while decreasing the size of the broadcast domains.

Answer: B,C,D

QUESTION NO: 134

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:
Section 10: Configure, verify, and troubleshoot VLANs (4 questions)

QUESTION NO: 135

Refer to the exhibit.

Which two statements about the configuration of the switch interface are correct? (Choose two)

```
SwitchA(config)# interface fa0/0
SwitchA(config-if)# switchport access vlan 2
```

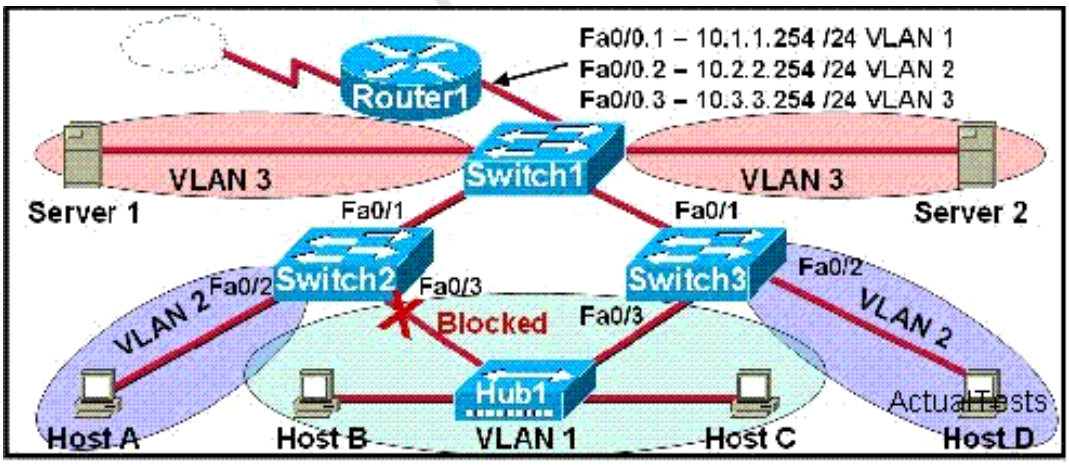

A. A network host can be connected to this interface.
B. The switchport belongs only to VLAN 2
C. The exhibit shows interface fa0/0 to be dynamically mapped to VLAN 2
D. Interface fa0/0 will be in both VLAN 1 (by default) and VLAN 2

Answer: A,B

Explanation:
On a Cisco switch, ports are assigned to a single VLAN. These ports are referred to as access ports and provide a connection for end users or node devices, such as a router or server. By default all devices are assigned to VLAN 1, known as the default VLAN . After creating a VLAN, you can manually assign a port to that VLAN and it will be able to communicate only with or through other devices in the VLAN. In this case, the port has been manually assigned to VLAN 2, not the default value of VLAN 1.

QUESTION NO: 136

Which statement is correct about the internetwork shown in the diagram?



A. If Fa0/0 is down on Router 1, Host A cannot access Server 1.

B. If Fa0/1 is down on Switch 3, Host C cannot access Server 2.
C. No collisions can occur in traffic between Host B and Host C.
D. Spanning Tree is not running.
E. Switch 2 is the root bridge.
F. Host D and Server 1 are in the same network.

Answer: B

Explanation:
Host A is on VLAN1 and Server1 is on VLAN3. Router 1 routes data between VLANs through the interface of FA0/0. If FA0/0 is down, there is no routing between VLANs, so Host A cannot access Server 1.

A VLAN is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment.
The above diagram is configured with inter-VLAN communication so the router has a great role to make communication between different VLAN. When router's port configured with trunk goes down all host can't communicate with other host in different VLAN as it is the router that directs traffic between the separate VLANs.

QUESTION NO: 137

Which two statements describe the Cisco implementation of VLANs? (Choose two.)

A. VLAN 1 is the default Ethernet VLAN.
B. VLANs 1002 through 1005 are automatically created and cannot be deleted.
C. CDP advertisements are only sent on VLAN 1002.
D. By default, the switch IP address is in VLAN 1005.

Answer: A,B

QUESTION NO: 138

To configure the VLAN trunking protocol to communicate VLAN information between two switches, what two requirements must be met? (Choose two.)

A. Each end of the trunk line must be set to IEEE 802.1E encapsulation.
B. The VTP management domain name of both switches must be set the same.
C. All ports on both the switches must be set as access ports.

D. One of the two switches must be configured as a VTP server.
E. A rollover cable is required to connect the two switches together.
F. A router must be used to forward VTP traffic between VLANs.

Answer: B,D

Explanation:
Section 11: Configure, verify, and troubleshoot trunking on Cisco switches (8 questions)

QUESTION NO: 139

As the network administrator, you are required to redesign the network. You choice a new switch to install into an existing LAN and a new VTP trunk is set up with an existing switch. Which VLANs will be allowed on this new trunk?

A. Each single VLAN, or VLAN range, must be specified with the switch port mode command.
B. Each single VLAN, or VLAN range, must be specified with the vtp domain command.
C. Each single VLAN, or VLAN range, must be specified with the vlan dataBased command.
D. By default, all defined VLANs are allowed on the trunk.

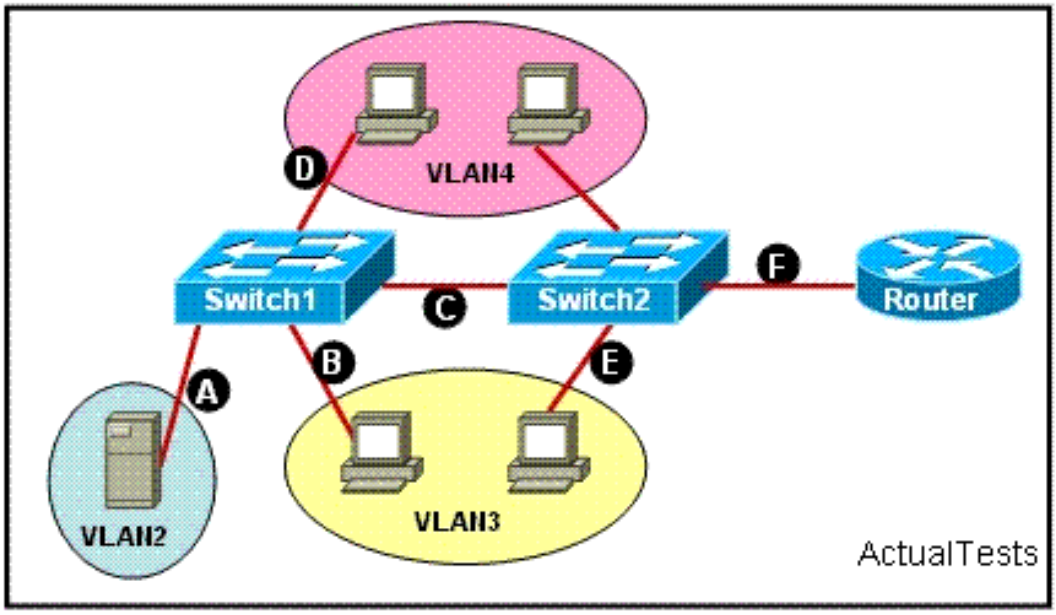
Answer: D

Explanation:
The question does not state that there are multiple VTP Domains meaning that all defined VLANs are allowed on the trunk until a vtp domain command is issued.

Trunk is a kind of port aggregating protocol, mainly used to undertake multi-VLAN flux link. Thus the device in the newly designed network allows only default vlan and vlans that are defined to be allowed on this trunk.

QUESTION NO: 140

Refer to the exhibit. A network associate needs to configure the switches and router in the graphic so that the hosts in VLAN3 and VLAN4 can communicate with the enterprise server in VLAN2. Which two Ethernet segments would need to be configured as trunk links? (Choose two.)



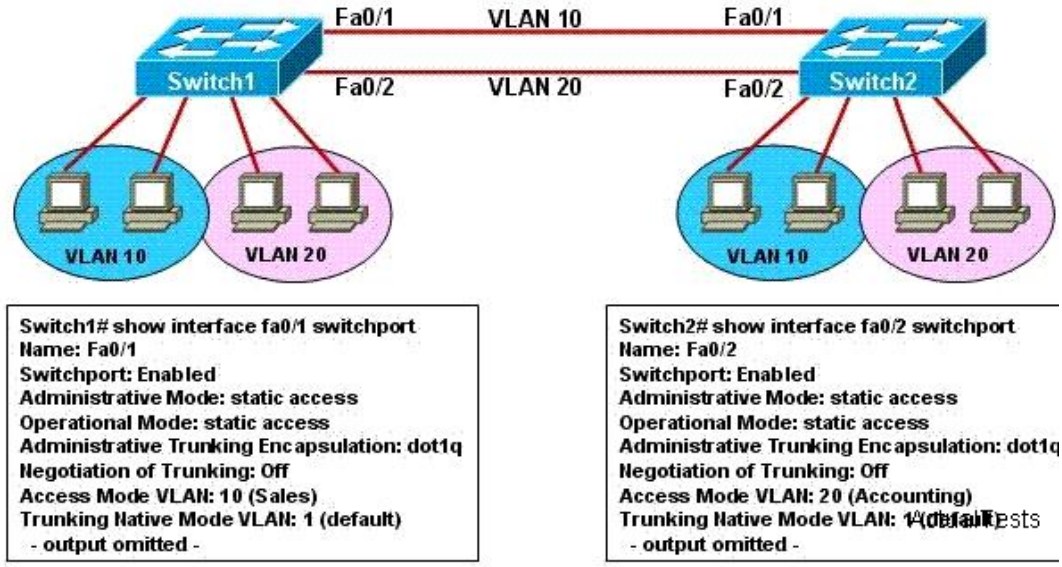
A. A
B. B
C. C
D. D
E. E
F. F

Answer: C,F

Explanation:
Layer 3 routing is needed to implement communication between VLANs, so a trunk link is configured between ROuter and Switch2. Both Switch1 and Switch2own VLAN3 and VLAN4 members, so a trunk link is configured between Switch1 and Switch2.

QUESTION NO: 141

Refer to the exhibit. An organization connects two locations, supporting two VLANs, through two switches as shown. Inter-VLAN communication is not required. The network is working properly and there is full connectivity. The organization needs to add additional VLANs, so it has been decided to implement VTP. Both switches are configured as VTP servers in the same VTP domain. VLANs added to Switch1 are not learned by Switch2. Based on this information and the partial configurations in the exhibit, what is the problem?



A. VTP is Cisco proprietary and requires a different trunking encapsulation.
B. Switch2 should be configured as a VTP client.
C. A router is required to route VTP advertisements between the switches.
D. STP has blocked one of the links between the switches, limiting connectivity.
E. The links between the switches are access links.

Answer: D

Explanation:
A trunk link is a special connection; the key difference between an ordinary connection (access port) and a trunk port is that although an Access port is only in one VLAN at a time, a trunk port has the job of carrying traffic for all VLANs from one switch to another. Any time you connect a switch to another switch and want to make sure that all VLANs will be carried across the switches, you want to make it a trunk.

To carry on the data frames for all VLANs, you need to create the Trunk link on switch port as well as you need to select the encapsulation type.

Switchport mode trunk
Switchport trunk encapsulation dot1q or isl

In the above topology the switches are connected on access ports. Making them trunk ports should solve this issue.

QUESTION NO: 142

When a new trunk is configured on a 2950 switch, which VLANs by default are allowed over the trunk link?

A. no VLANs
B. all VLANs
C. only VLANs 1 - 64
D. only the VLANs that are specified when creating the trunk

Answer: B

Explanation:
By default, all VLANs are allowed over the trunk link.

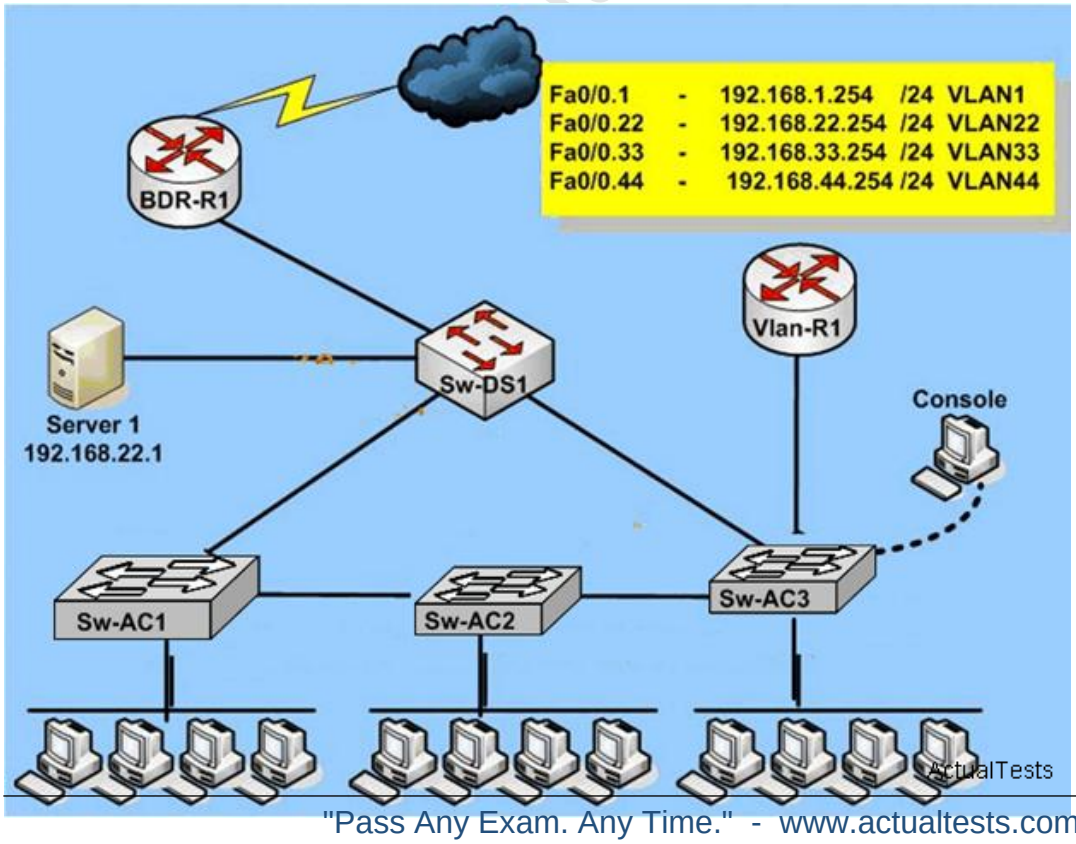
Trunk ports send and receive information from all VLANs by default, and if a frame is untagged, it's sent to the management VLAN. This applies to the extended range VLANs as well. But we can remove VLANs from the allowed list to prevent traffic from certain VLANs from traversing a trunked link.

Here is example:
RouterA(config)#int f0/1
RouterA(config-if)# switchport mode trunk
RouterA(config-if)#switchport trunk allowed vlan VLANID

RouterA(config-if)#switchport trunk allowed vlan remove VLANID

QUESTION NO: 143

What ports on Sw-AC3 are operating as trunks?(Choose three)



Sw-AC3#show trunk

```
Sw-Ac3#show int trunk
Port        Mode         Encapsulation  Status       Native vlan
Fa0/3       on           802.1q         trunking      1
Fa0/9       desirable    802.1q         trunking      1
Fa0/12      desirable    802.1q         trunking      1
```


A. Fa0/12
B. Fa0/3
C. Fa0/1
D. Fa0/9

Answer: A,D

Explanation:
Based on the output of Sw-AC3#show trunk provided in the exhibit, we know that the status of port Fa0/3, Fa0/9, Fa0/12 on Sw-Ac3 is trunking.

QUESTION NO: 144

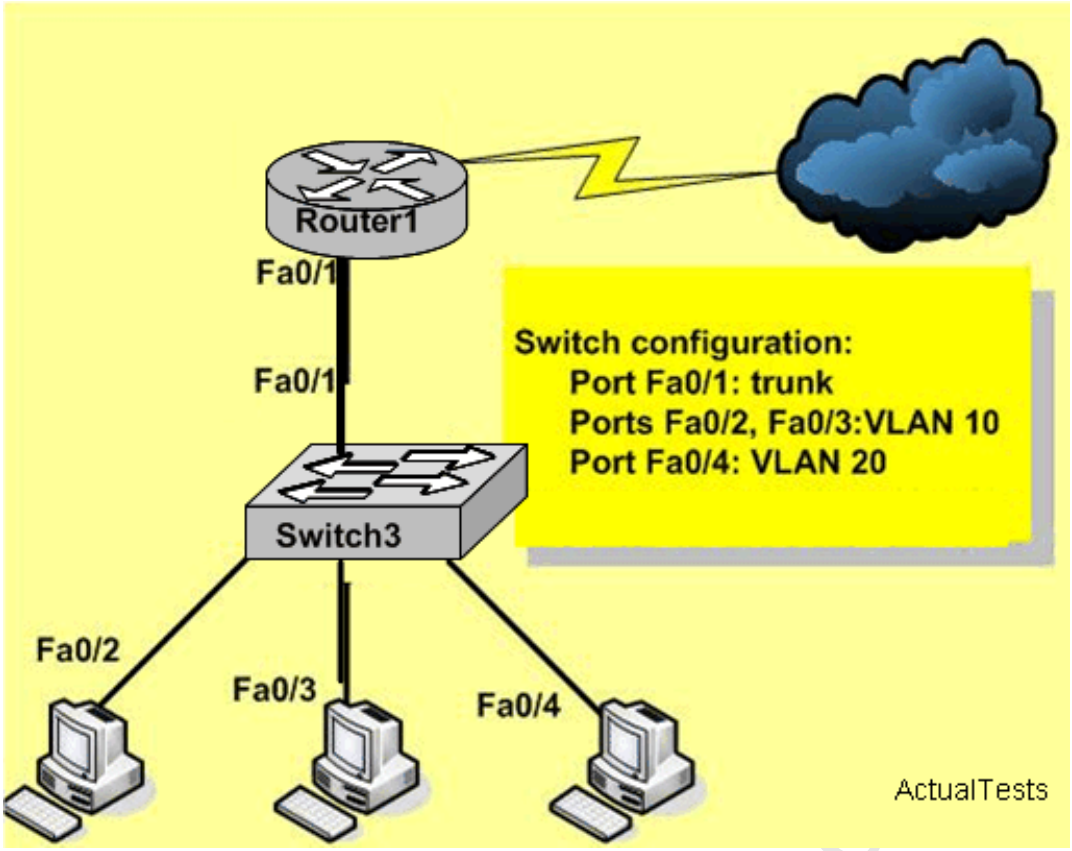
Which interface commands would you enter on a Catalyst 2900 switch, if your goal was to bring all VLAN traffic to another directly connected switch?(Choose two)

A. Switch(config-if)# switchport access vlan all
B. Switch(config-if)# switchport mode trunk
C. Switch(config-if)# switchport trunk encapsulation dot1q
D. Switch(config-if)# vlan all

Answer: B,C

QUESTION NO: 145

Refer to the topology and configuration information shown in the graphic. Router1 has been configured to provide communication between the VLANs. Which IOS commands are required to configure switch port fa0/1 to establish a link with router Router1 -R1 using the IEEE standard protocol? (Choose three.)



A. Switch3(config-if)# switchport mode trunk
B. Switch3(config)# interface fastethernet 0/1
C. Switch3(config-if)# switchport trunk encapsulation dot1q
D. Switch3(config-if)# switchport access vlan 1

Answer: A,B,C

Explanation:
Enable trunk on Fa0/1 interface of the router Router1.

QUESTION NO: 146

When a new trunk link is configured on an IOS based switch, which VLANs are allowed over the link?

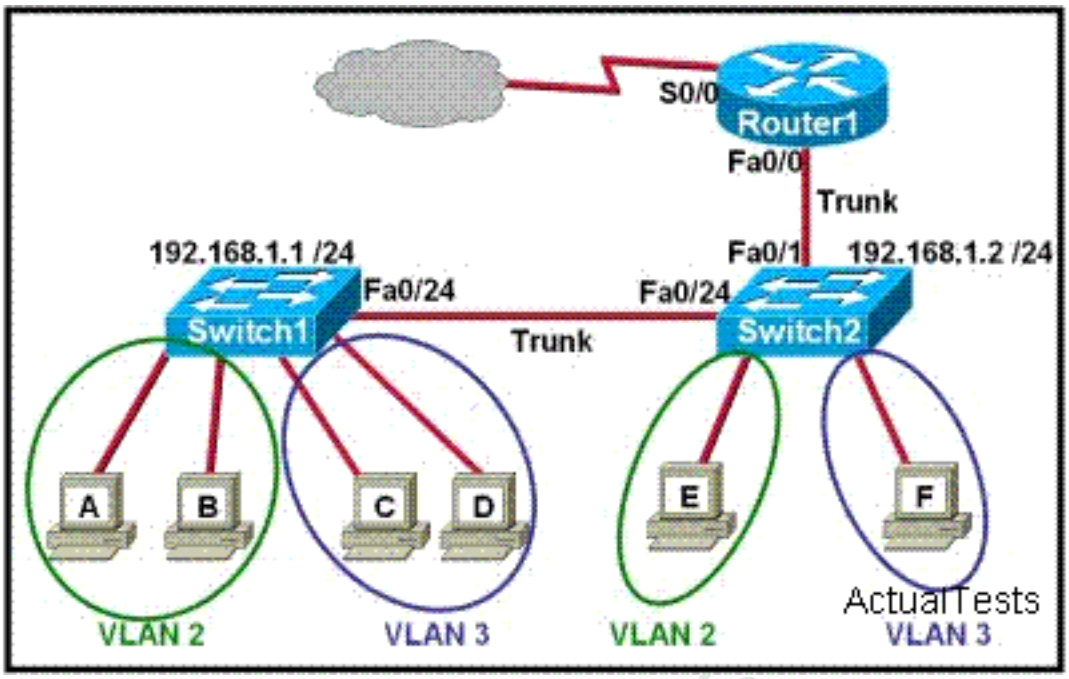
A. By default, all defined VLANs are allowed on the trunk.
B. Each single VLAN, or VLAN range, must be specified with the switchport mode command.
C. Each single VLAN, or VLAN range, must be specified with the vtp domain command.
D. Each single VLAN, or VLAN range, must be specified with the vlan database command.

Answer: A

Explanation:
All VLANs are allowed over the trunk link regardless of the switch mode.
Section 12: Configure, verify, and troubleshoot interVLAN routing (4 questions)

QUESTION NO: 147

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



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

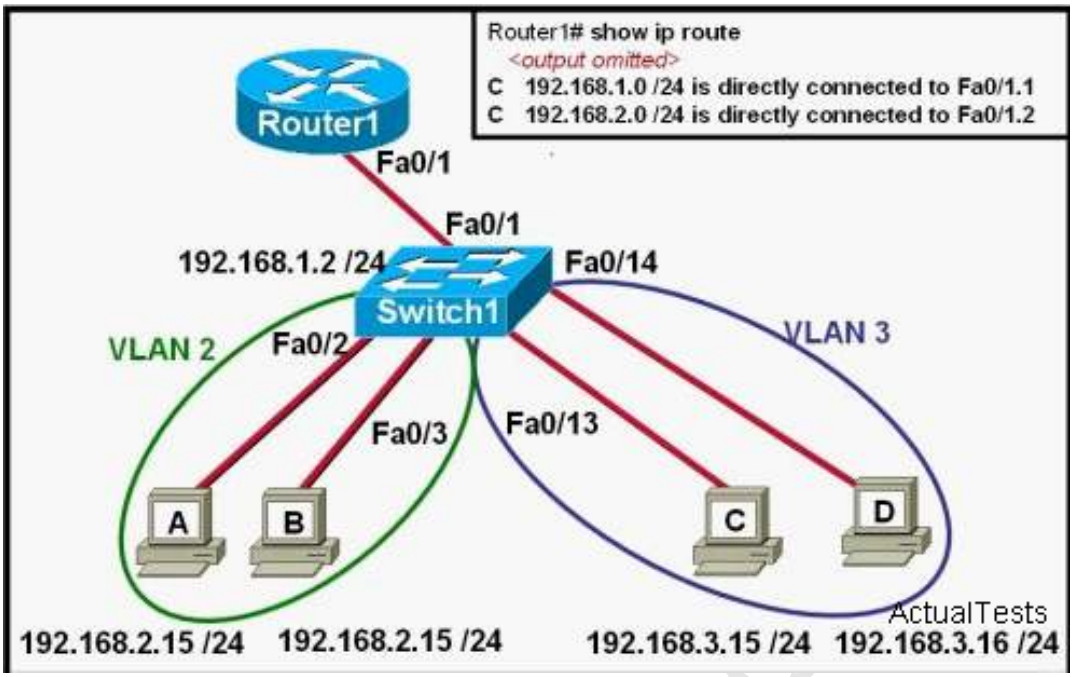
Answer: A,D

Explanation:
This scenario requires inter-VLAN routing, which requires a layer three device. Based on the information above, a trunk has indeed been set up to route traffic between VLAN's so the problem is that default gateway has been specified in the switch, so traffic will not be forwarded to the router from the switch from one VLAN to the other.

Different VLANs can't communicate with each other, it is needed to configure sub-interface between the router and the switch and set up trunk link , requiring matched encapsulation type.

QUESTION NO: 148

Refer to the exhibit. The network administrator has created a new VLAN on Switch1 and added host C and host D. The administrator has properly configured switch interfaces FastEthernet0/13 through FastEthernet0/24 to be members of the new VLAN. However, after the network administrator completed the configuration, host A could communicate with host B, but host A could not communicate with host C or host D. Which commands are required to resolve this problem?



A. Switch1# vlan database
Switch1(vlan)# vtp v2-mode
Switch1(vlan)# vtp domain cisco
Switch1(vlan)# vtp server
B. Router(config)# router rip
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# network 192.168.3.0
C. Switch1(config)# interface fastethernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk encapsulation isl
D. Router(config)# interface fastethernet 0/1.3
Router(config-if)# encapsulation dot1q 3
Router(config-if)# ip address 192.168.3.1 255.255.255.0

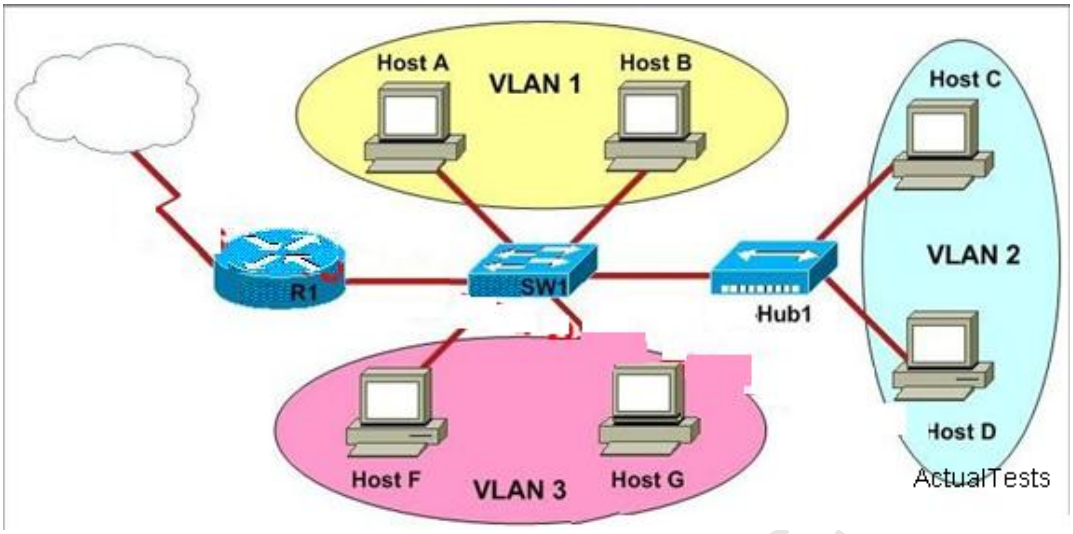
Answer: D

Explanation:
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: 149

Which three descriptions are true about the R1 port configuration and the SW1 port configuration as displayed in the topology? (Choose three.)

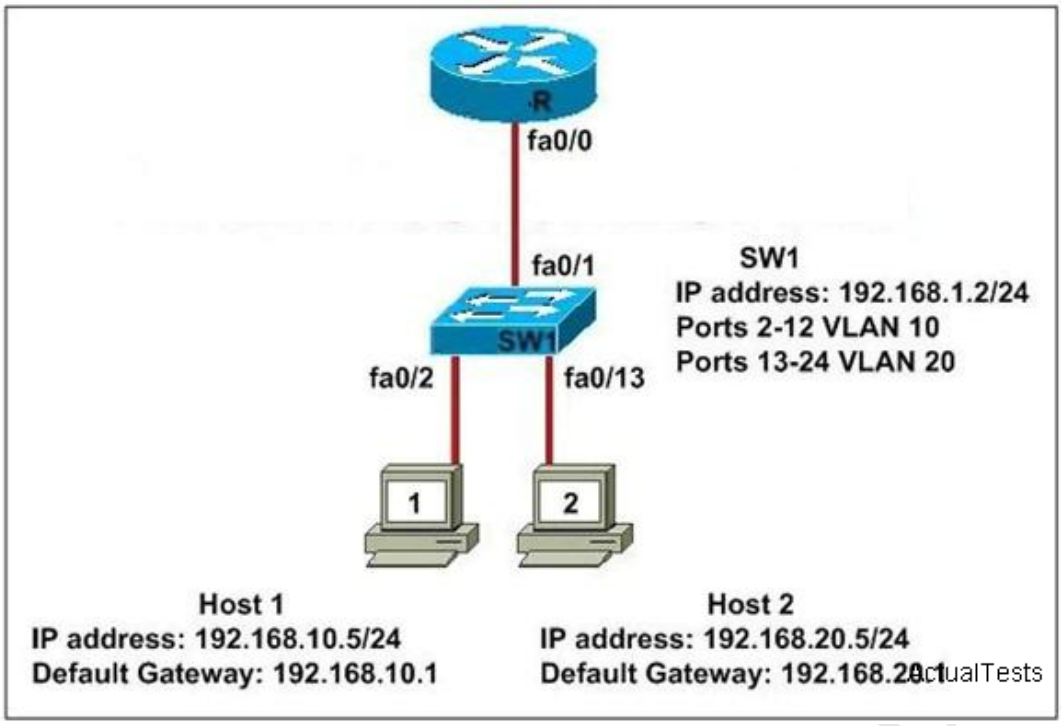


A. The SW1 port connected to Hubl is configured as full duplex.
B. The R1 port connected to SW1 is configured using subinterfaces.
C. The SW1 port connected to Host B is configured as an access port.
D. The SW1 port connection to R1 is configured as a trunking port.

Answer: B,C,D

QUESTION NO: 150

Which commands should be configured on the 2950 switch SW1 and the router R to allow communication between host 1 and host 2? (Choose two.)



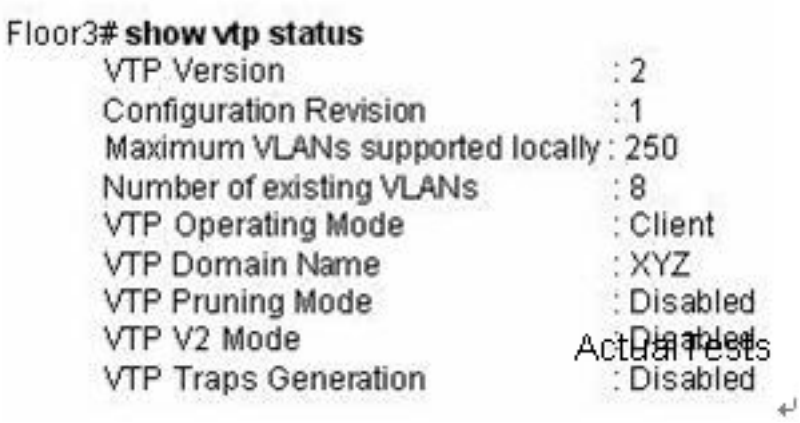
A. R(config)# interface fastethernet 0/0
R(config-if)# ip address 192.168.1.1 255.255.255.0
R(config-if)# no shut down
B. R(config)# interface fastethernet 0/0
R(config-if)# no shut down
R(config)# interface fastethernet 0/0.1
R(config-subif)# encapsulation dot1q 10
R(config-subif)# ip address 192.168.10.1 255.255.255.0
R(config)# interface fastethernet 0/0.2
R(config-subif)# encapsulation dot1q 20
R(config-subif)# ip address 192.168.20.1 255.255.255.0
C. SW1(config)# vlan database
SW1(config-vlan)# vtp domain XYZ
SW1(config-vlan)# vtp server
D. SW1(config)# interface fastethernet 0/1
SW1(config-if)# switchport mode trunk

Answer: B,D

Explanation:
Section 13: Configure, verify, and troubleshoot VTP (11 questions)

QUESTION NO: 151

Given the output of the Floor3 switch shown above, which statement best describes the operation of this switch?



A. The switch learns VLAN information but does not save it to NVRAM.
B. The switchs can create VLANs locally but will not forward this information to other switches.
C. The switchs can create, change, and delete VLANs.
D. VTP is disabled on this switchs.

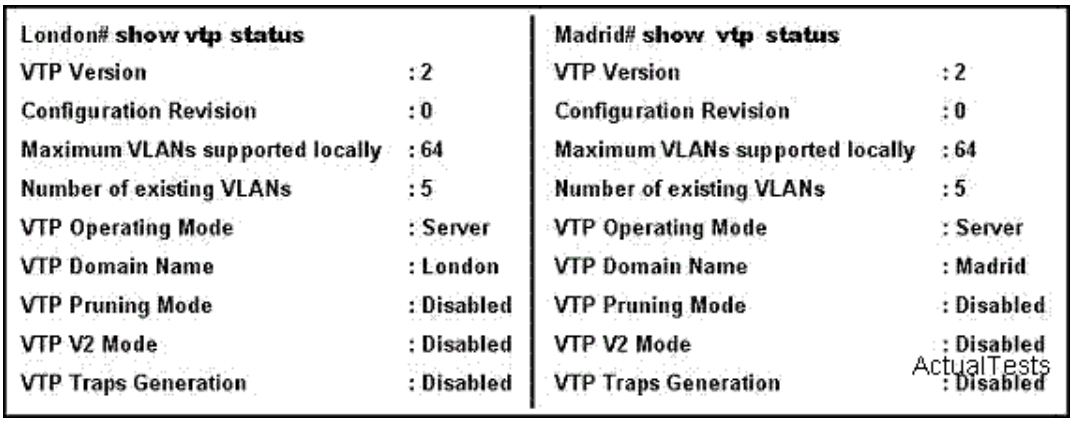
Answer: A

Explanation:
On the basis of the exhibit, we know that the switch Floor3 is configured with VTP and the VTP Mode is Client mode.
Client mode: Client mode is a passive listening mode. Switches listens to VTP advertisements from other switches and modify their VLAN configurations accordingly but does not save it to NVRAM. Thus the administrator is not allowed to create, change, or delete any VLANs. If other switches are in the management domain, a new switch should be configured for client mode operation. In this way, the switch will learn any existing VTP information from a server. If this switch will be used as a redundant server, it should start out in client mode to learn all VTP information from reliable sources. If the switch was initially configured for server mode instead, it might propagate incorrect information to the other domain switches. Once the switch has learned the current VTP information, it can be reconfigured for server mode.

This switch is operated on client VTP mode.
In client mode, switches receive information from VTP servers, but they also send and receive updates, so in this way, they behave like VTP servers. The difference is that they can't create, change, or delete VLANs. Plus, none of the ports on a client switch can be added to a new VLAN before the VTP server notifies the client switch of the new VLAN. Also good to know is that VLAN information sent from a VTP server isn't stored in NVRAM, which is important because it means that if the switch is reset or reloaded, the VLAN information will be deleted. Here's a hint: If you want a switch to become a server, first make it a client so it receives all the correct VLAN information, then change it to a server.

QUESTION NO: 152

A network administrator has configured two switches, named London and Madrid, to use VTP. However, the switches are not sharing VTP messages. Given the command output shown in the graphic, why are these switches not sharing VTP messages?



London# **show vtp status**	
VTP Version	: 2
Configuration Revision	: 0
Maximum VLANs supported locally	: 64
Number of existing VLANs	: 5
VTP Operating Mode	: Server
VTP Domain Name	: London
VTP Pruning Mode	: Disabled
VTP V2 Mode	: Disabled
VTP Traps Generation	: Disabled

Madrid# **show vtp status**	
VTP Version	: 2
Configuration Revision	: 0
Maximum VLANs supported locally	: 64
Number of existing VLANs	: 5
VTP Operating Mode	: Server
VTP Domain Name	: Madrid
VTP Pruning Mode	: Disabled
VTP V2 Mode	: Disabled
VTP Traps Generation	: Disabled

A. VTP traps generation is disabled.
B. The VTP operating mode is not correctly configured.
C. The VTP version is not correctly configured.
D. The VTP domain name is not correctly configured.
E. VTP pruning mode is disabled.
F. VTP V2 mode is disabled.

Answer: D

Explanation:
When you create the VTP domain, you have a bunch of options, including setting the domain name, password, operating mode, and pruning capabilities of the switch. Use the vtp global configuration mode command to set all this information.

To share the VTP messages switches should have same domain name and password. Mode can be either Server, Transparent, Client.

In the Exhibit one switch has London and another has Madrid domain name, so to exchange VTP message both should have same domain name.

QUESTION NO: 153

What is the purpose of the command shown below?

vtp password Fl0r1da

A. It is the password required when promoting a switch from VTP client mode to VTP server mode.
B. It is used to access the VTP server to make changes to the VTP configuration.
C. It is used to prevent a switch newly added to the network from sending incorrect VLAN information to the other switches in the domain.

D. It is used to validate the sources of VTP advertisements sent between switches.
E. It allows two VTP servers to exist in the same domain, each configured with different passwords.

Answer: D

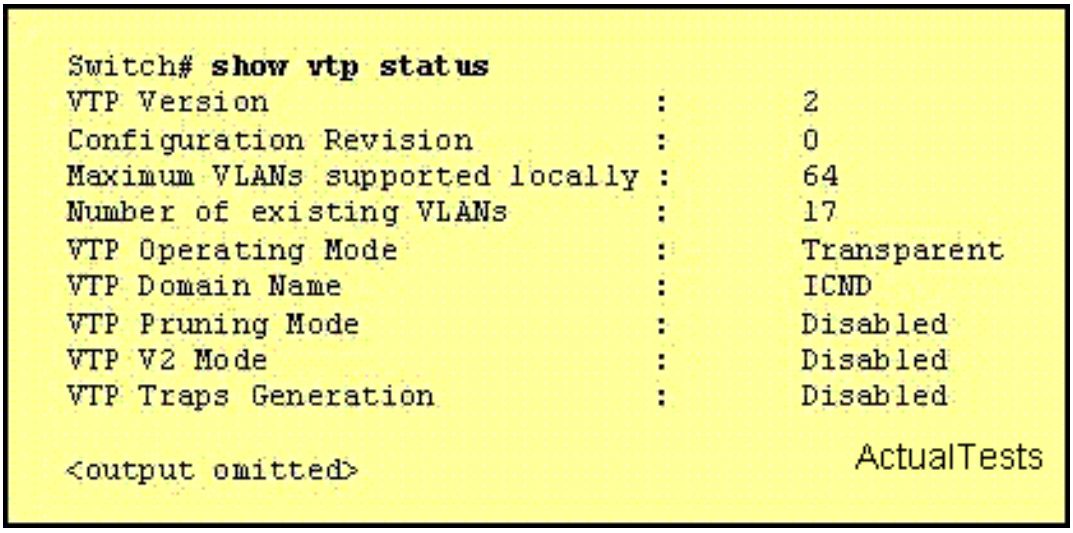
Explanation:
When you create the VTP domain, you have a bunch of options, including setting the domain name, password, operating mode, and pruning capabilities of the switch. Use the vtp global configuration mode command to set all this information.
The purpose of setting password on VTP is to validate the sources of VTP advertisements sent between switches belonging to same VTP domain.

VTP password is used to authenticate the VTP members in the same VTP domain. When VTP Server sends VTP advertise to VTP client, it is required that the VTP domain name of the VTP server and the VTP client agree with VTP password.
VTP: VTP is organized into management domains or areas with common VLAN requirements. A switch can belong to only one VTP domain. Switches in different VTP domains do not share VTP information. Switches in a VTP domain advertise several attributes to their domain neighbors. Each advertisement contains information about the VTP management domain, VTP configuration revision number, known VLANs, and specific VLAN parameters.

The VTP process begins with VLAN creation on a switch called a VTP server. VTP floods advertisements throughout the VTP domain every 5 minutes, or whenever there is a change in VLAN configuration. The VTP advertisement includes a configuration revision number, VLAN names and numbers, and information about which switches have ports assigned to each VLAN. By configuring the details on one or more VTP server and propagating the information through advertisements, all switches configuration know the names and numbers of all VLANs.

QUESTION NO: 154

Refer to the exhibit. The show vtp status command is executed at a switch that is generating the exhibited output. Which statement is true for this switch?



A. The switch forwards its VLAN database to other switches in the ICND VTP domain.
B. The VLAN database is updated when VTP information is received from other switches.
C. The configuration revision number increments each time the VLAN database is updated.
D. The switch forwards VTP updates that are sent by other switches in the ICND domain.

Answer: D

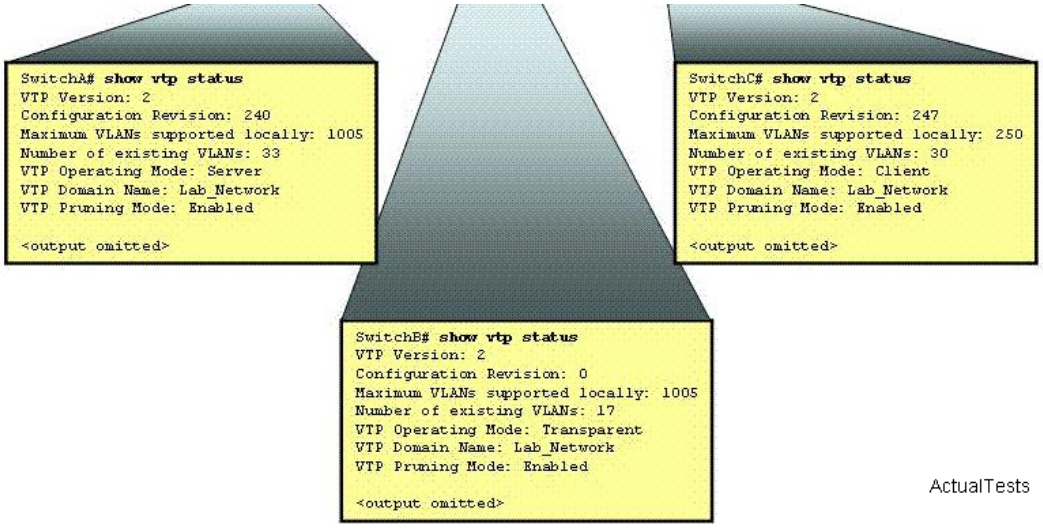
Explanation:
Switches in transparent mode don't participate in the VTP domain or share its VLAN database, but they'll still forward VTP advertisements through any configured trunk links.

VTP is organized into management domains or areas with common VLAN requirements. A switch can belong to only one VTP domain. Switches in different VTP domains do not share VTP information. Switches in a VTP domain advertise several attributes to their domain neighbors. Each advertisement contains information about the VTP management domain, VTP configuration revision number, known VLANs, and specific VLAN parameters.
From the output of the command how vtp status provided in the exhibit, we know that the VTP mode of the switch is the transparent mode.

Transparent mode does not allow the switch to participate in VTP negotiations. Thus, a switch does not advertise its own VLAN configuration, and a switch does not synchronize its VLAN database with received advertisements. VLANs can still be created, deleted, and renamed on the transparent switch. However, they will not be advertised to other neighboring switches. VTP advertisements received by a transparent switch will be forwarded on to other switches on trunk links.

QUESTION NO: 155

Refer to the exhibit. The network administrator has discovered that the VLAN configuration of SwitchC is not synchronized with the rest of the switched network. Why is SwitchC not receiving VTP updates?



A. SwitchA supports a greater number of VLANs than does SwitchC.
B. SwitchC has fewer existing VLANs than does SwitchA.
C. SwitchC has a revision number higher than that being advertised.
D. SwitchC should be operating in VTP server mode to receive VTP updates.
E. SwitchB is not relaying VTP advertisements to SwitchC.
F. SwitchB should be operating in VTP server or client mode to relay VTP updates.

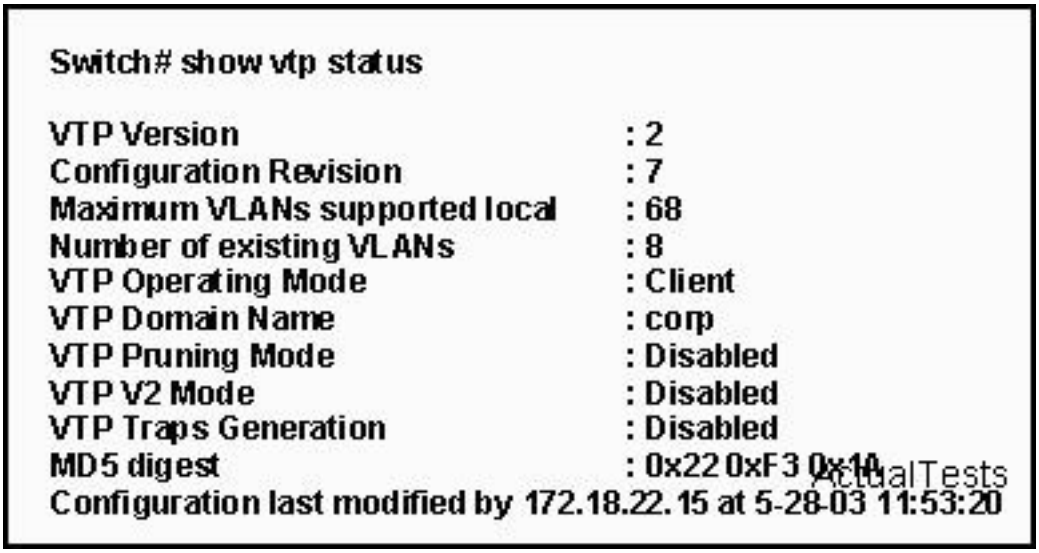
Answer: C

Explanation:
VTP revision number is to indicate the modified version that VTP configured is a 32-bit value, which begins with 0. If VLAN information changes, the revision number will plus 1 until 4294967295. Then circulate and then return 0, re-start and increase.
When the monitoring switch receives notices bigger than the revision number they stored, this notice will override the stored VLAN information, and thus it is very important to set the added revision number of the switch to default 0.
To set the revision number to default 0, the following methods may be used:
1> change the mode of switch VTP to transparent mode, and then return to the server mode
2> make changes to switch VTP domain name, and revert to the original domain name

Reference:
http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml

QUESTION NO: 156

An administrator is unsuccessful in adding VLAN 50 to a switch. While troubleshooting the problem, the administrator views the output of the show vtp status command, which is displayed in the graphic. What commands must be issued on this switch to add VLAN 50 to the database? (Choose two.)

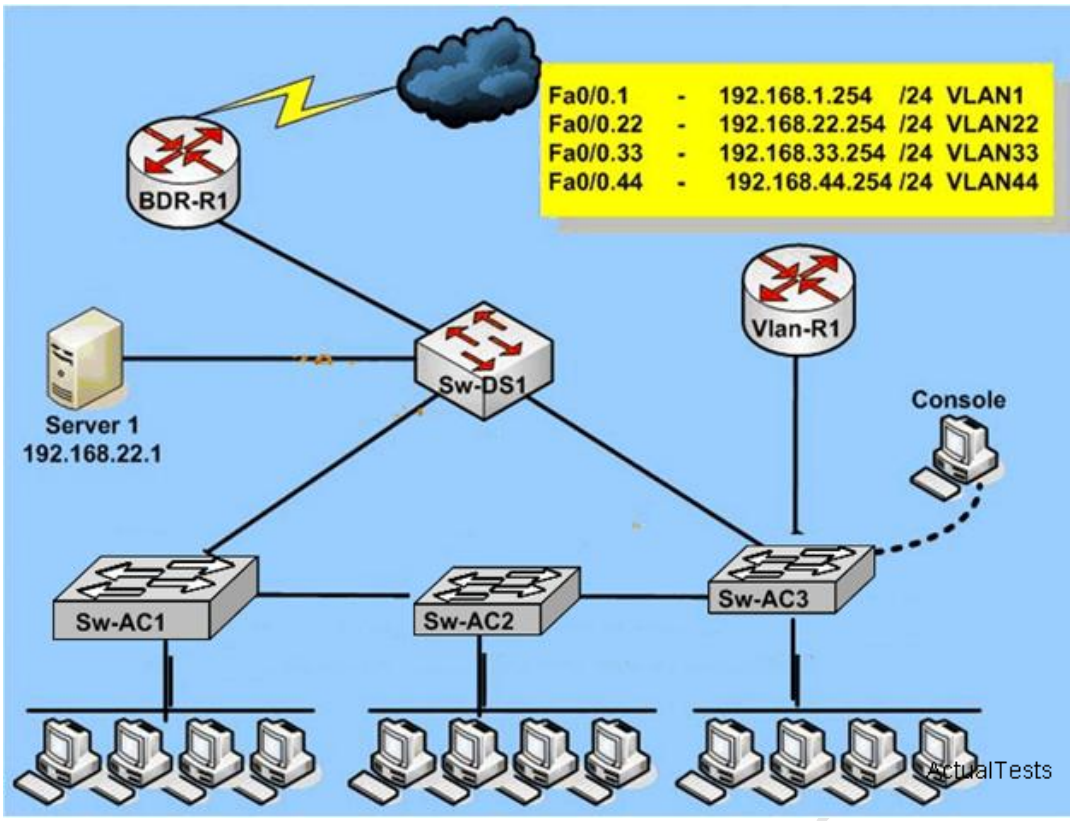


A. Switch(config-if)# switchport access vlan 50
B. Switch(vlan)# vtp server
C. Switch(config)# config-revision 20
D. Switch(config)# vlan 50 name Tech
E. Switch(vlan)# vlan 50
F. Switch(vlan)# switchport trunk vlan 50

Answer: B,E

QUESTION NO: 157

Refer to the exhibit. SwX was taken out of the production network for maintenance.
It will be reconnected to the Fa0/16 port of Sw-AC3. What happens to the network when it is reconnected and a trunk exists between the two switches?



SwX#show vlan | SwX#show vtp stat

```
SwX#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
                   Gi0/1, Gi0/2
2   students   active
3   admin      active
4   faculty    active
```

```
SwX#  show vtp stat
VTP Version                 : 2
Configuration Revision      : 6
Maximum VLANs supported locally : 250
Number of existing VLANs    : 8
VTP Operating Mode          : Server
VTP Domain Name             : home-office
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xD8 0xD8 0x38 0x22
                              0x98 0xE3 0xAC 0x65
Configuration last modified by 0.0.0.0 at
                              3-28-99  01:24:88
```


Sw-AC3#show vtp stat

```
Sw-Ac3#show vtp status
VTP Version                     :   2
Configuration Revision          :   5
Maximum VLANs supported locally :   250
Number of existing VLANs        :   9
VTP Operating Mode              :   Client
VTP Domain Name                 :   home-office
VTP Pruning Mode                :   Disabled
VTP V2 Mode                     :   Disabled
VTP Traps Generation            :   Disabled
MD5 digest                      :   0xD8 0xD8 0x38 0x22 0x98 0xE3 0xAC 0x65
Configuration last modified by 192.168.1.249 at 3-2-93 21:29:08
Sw-Ac3#
```


Sw-AC3#show vlan

```
Sw-Ac3#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16
22   Servers                          active
33   Management                       active    Fa0/1, Fa0/2, Fa0/5, Fa0/6, Fa0/7
44   Production                       active    Fa0/4, Fa0/8, Fa0/10, Fa0/11
99   no-where                         active    Fa0/13, Fa0/14, Fa0/15, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                F0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```


A. The VLANs Servers, Managements, Production and no-where will be removed from existing switches.
B. The VLANs Servers, Management, Production and no-where will replace the VLANs on SwX.
C. All VLANs except the default VLAN will be removed from all switches.
D. All existing switches will have the students, admin, faculty, Servers, Management, Production and no-where VLANs.

Answer: A

Explanation:
On the basis of the output of SwX#show vtp stat, we know that the VTP mode configured on SwX is the Server mode, through the output of the Sw-AC3#show vtp stat, we know that the VTP mode configured on Sw-AC3 is the client mode, both are in the same VTP Domain Home-office.
Based on the output of the SwX#show vlan, we know that VTP Server has four types of VLAN : Default, students, admin, faculty. Through the output of Sw-AC3#show vlan, we know that there are Default, Servers, Managements, Production, and no-where five VLANs existed. As VTP client, it will learn the VLAN information on VTP Server and clear non-exist VLANS information on VTP server.

VTP operates in one of three modes:1:server;2:client;3:transparent .
Server Mode.In this VTP mode you can create, remove, and modify VLANs. You can also set other configuration options like the VTP version and also turn on/off VTP pruning for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on messages received over trunk links. VTP server is the default mode. The VLANs information are stored on NVRAM and they are not lost after a reboot.
Client Mode VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on the local device.
Transparent Mode.When you set the VTP mode to transparent, then the switches do not participate in VTP. A VTP transparent switch will not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received messages. VLANS can be created, changed or deleted when in transparent mode. In VTP version 2, transparent switches do forward

VTP messages that they receive out their trunk ports.

QUESTION NO: 158

What are two results of entering the Switch(config)# vtp mode client command on a Catalyst switch? (Choose two.)

A. The switch will originate VTP summary advertisements.
B. The switch will process VTP summary advertisements.
C. The switch will ignore VTP summary advertisements.
D. The switch will forward VTP summary advertisements.

Answer: B,D

Explanation:
Server Mode Once VTP is configured on a Cisco switch, the default mode used is Server Mode. In any given VTP management domain, at least one switch must be in Server Mode. When in Server Mode, a switch can be used to add, delete, and modify VLANs, and this information will be passed to all other switches in the VTP management domain.
Client Mode When a switch is configured to use VTP Client Mode, it is simply the recipient of any VLANs added, deleted, or modified by a switch in Server Mode within the same management domain. A switch in VTP client mode cannot make any changes to VLAN information.
Transparent Mode A switch in VTP Transparent Mode will pass VTP updates received by switches in Server Mode to other switches in the VTP management domain, but will not actually process the contents of these messages. When individual VLANs are added, deleted, or modified on a switch running in transparent mode, the changes are local to that particular switch only, and are not passed to other switches in the VTP management domain.
Based on the roles of each VTP mode, the use of each should be more or less obvious. For example, if you had 15 Cisco switches on your network, you could configure each of them to be in the same VTP management domain. Although each could theoretically be left in the default Server Mode, it would probably be easier to leave only one switch in this configuration, and then configure all remaining switches for VTP Client Mode. Then, when you need to add, delete, or modify a VLAN, that change can be carried out on the VTP Server Mode switch and passed to all Client Mode switches automatically. In cases where you need a switch to act in a relatively standalone manner, or dont want it to propagate information about its configured VLANs, use Transparent Mode.

QUESTION NO: 159

What are two benefits of using VTP in a switching environment? (Choose two.)

A. It allows switches to read frame tags.
B. It allows ports to be assigned to VLANs automatically.
C. It maintains VLAN consistency across a switched network.
D. It allows frames from multiple VLANs to use a single interface.
E. It allows VLAN information to be automatically propagated throughout the switching environment.

Answer: C,E

Explanation:
VTP minimizes the possible configuration inconsistencies that arise when changes are made. These inconsistencies can result in security violations, because VLANs can crossconnect when duplicate names are used. They also could become internally disconnected when they are mapped from one LAN type to another, for example, Ethernet to ATM LANE ELANs or FDDI 802.10 VLANs. VTP provides a mapping scheme that enables seamless trunking within a network employing mixed-media technologies.
VTP provides the following benefits:
VLAN configuration consistency across the network Mapping scheme that allows a VLAN to be trunked over mixed media Accurate tracking and monitoring of VLANs Dynamic reporting of added VLANs across the network Plug-and-play configuration when adding new VLANs

QUESTION NO: 160

A network administrator is explaining VTP configuration to a new technician. What should the network administrator tell VTP configuration? (Choose three.)

A. A switch in the VTP client modecannot update its local VLAN database.
B. A trunk link must be configured between the switches to forward VTP updates.
C. A switch in the VTP server mode can update a switch in the VTP transparent mode.
D. A switch in the VTP transparent mode will forward updates that it receives to other switches.
E. A switch in the VTP server mode only updates switches in the VTP client mode that have a higher VTP revision number.
F. A switch in the VTP server mode will update switches in the VTP client mode regardless of the configured VTP domain membership.

Answer: A,B,D

QUESTION NO: 161

Which statements describe two of the benefits of VLAN Trunking Protocol? (Choose two.)

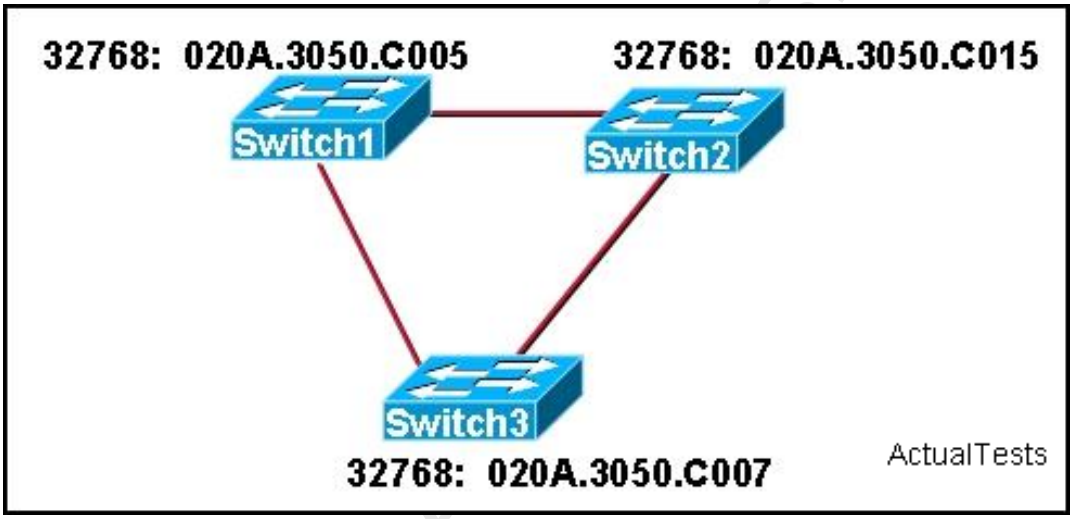
A. VTP allows routing between VLANs.
B. VTP allows a single switch port to carry information to more than one VLAN.
C. VTP allows physically redundant links while preventing switching loops.
D. VTP simplifies switch administration by allowing switches to automatically share VLAN configuration information.
E. VTP helps to limit configuration errors by keeping VLAN naming consistent across the VTP domain.
F. VTP enhances security by preventing unauthorized hosts from connecting to the VTP domain.

Answer: D,E

Explanation:
Section 14: Configure, verify, and troubleshoot RSTP operation (10 questions)

QUESTION NO: 162

Refer to the exhibit. A network administrator wants Switch3 to be the root bridge. What could be done to ensure Switch3 will be the root?

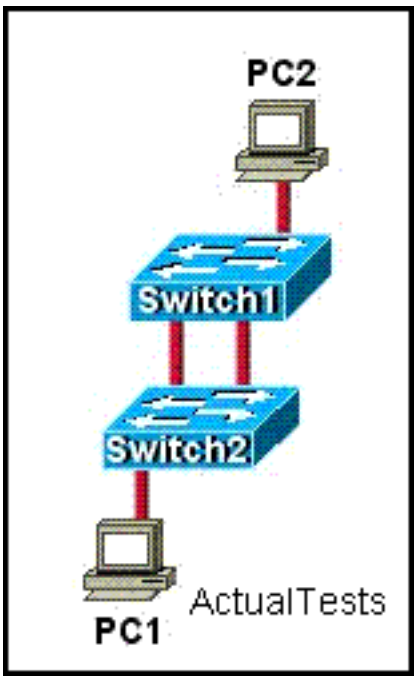


A. Configure the IP address on Switch3 to be higher than the IP addresses of Switch1 and Switch2.
B. Configure the priority value on Switch3 to be higher than the priority values of Switch 1 and Switch2.
C. Configure the BID on Switch3 to be lower than the BIDs of Switch1 and Switch2.
D. Configure the MAC address on Switch3 to be higher than the Switch1 and Switch2 MAC addresses.
E. Configure a loopback interface on Switch3 with an IP address lower than any IP address on Switch1 and Switch2.

Answer: C

QUESTION NO: 163

Refer to the exhibit. When PC1 sends an ARP request for the MAC address of PC2, network performance slows dramatically, and the switches detect an unusually high number of broadcast frames. What is the most likely cause of this?



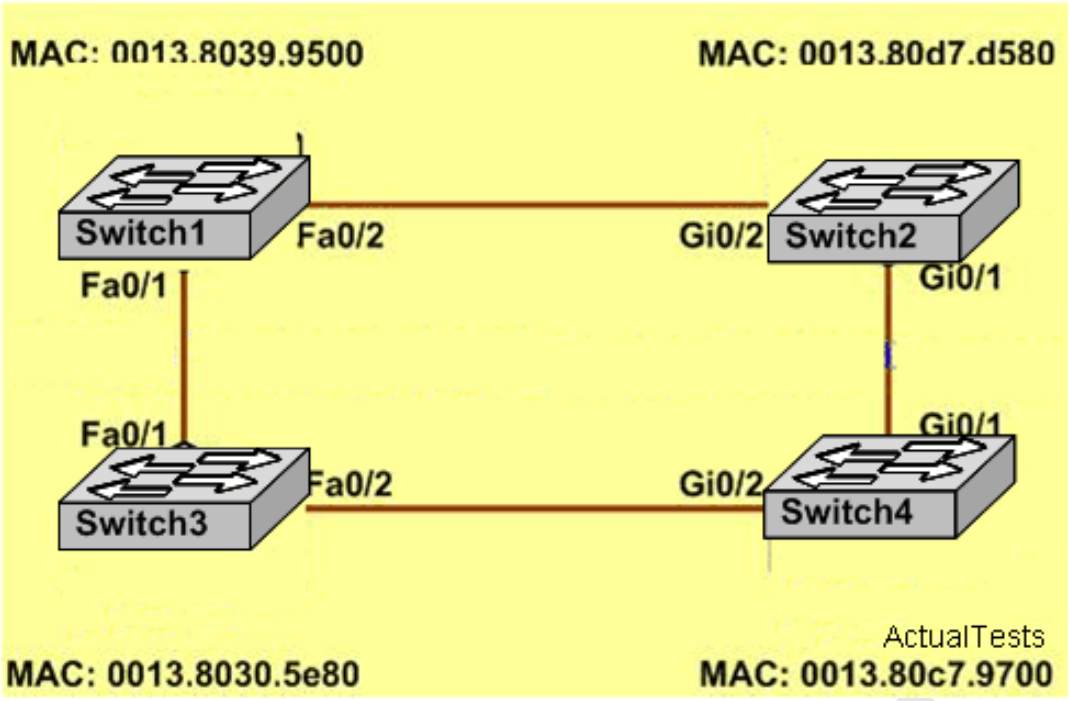
A. PC2 is down and is not able to respond to the request.
B. The VTP versions running on the two switches do not match.
C. The PCs are in two different VLANs.
D. The portfast feature is not enabled on all switch ports.
E. Spanning Tree Protocol is not running on the switches.

Answer: E

Explanation:
As the switches Switch1 and Switch 2 are connected with each other via two links, spanning tree must be enabled on both switches to avoid switching loops and broadcast storms. An ARP request is a broadcast message. If Spanning tree is not running, broadcast loops will form reducing the performance of the network.

QUESTION NO: 164

Study the exhibit carefully. 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 switch will have only one forwarding interface?



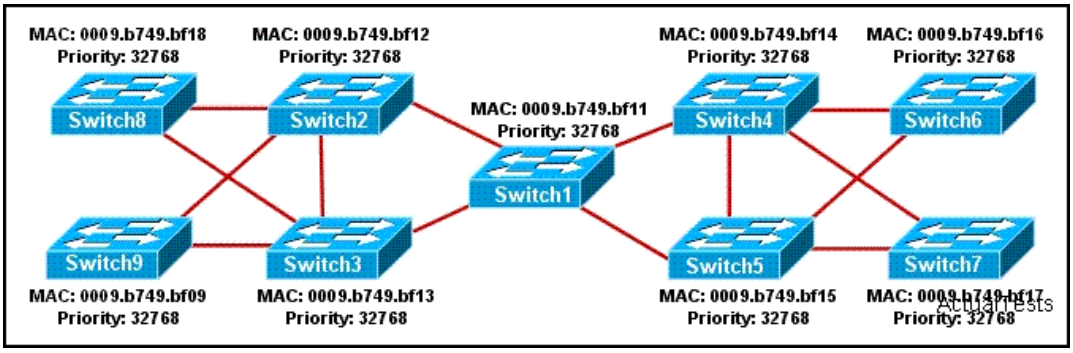
A. Switch 3
B. Switch 4
C. Switch 2
D. Switch 1

Answer: C

Explanation:
1.Judge the root bridge. The election of the root bridge is based on the bridge ID. Bridge ID = Bridge priority + Bridge MAC address. By default, the bridge priority value is 32768. And you can judge the root bridge only by bridge MAC address .The root bridge of this subject is Switch3.
2. Identify the root port. After electing the root bridge, it is needed to select a port of each switch in this network used to reach the root bridge, this port is known as root port (RP) . The port that is nearest to the root bridge is RP of non-root bridge. In this subject, ports F0 / 1 of Switch1, G0 / 1 of Switch2 and G0 / 2 of Switch4 are RPs.
According to the choice of STP, you will eventually find that a port on Switch2 will be blocked ,that is Gi0 / 2.

QUESTION NO: 165

Refer to the exhibit. The switches on a campus network have been interconnected as shown. All of the switches are running Spanning Tree Protocol with its default settings. Unusual traffic patterns are observed and it is discovered that Switch9 is the root bridge. Which change will ensure that Switch1 will be selected as the root bridge instead of Switch9?



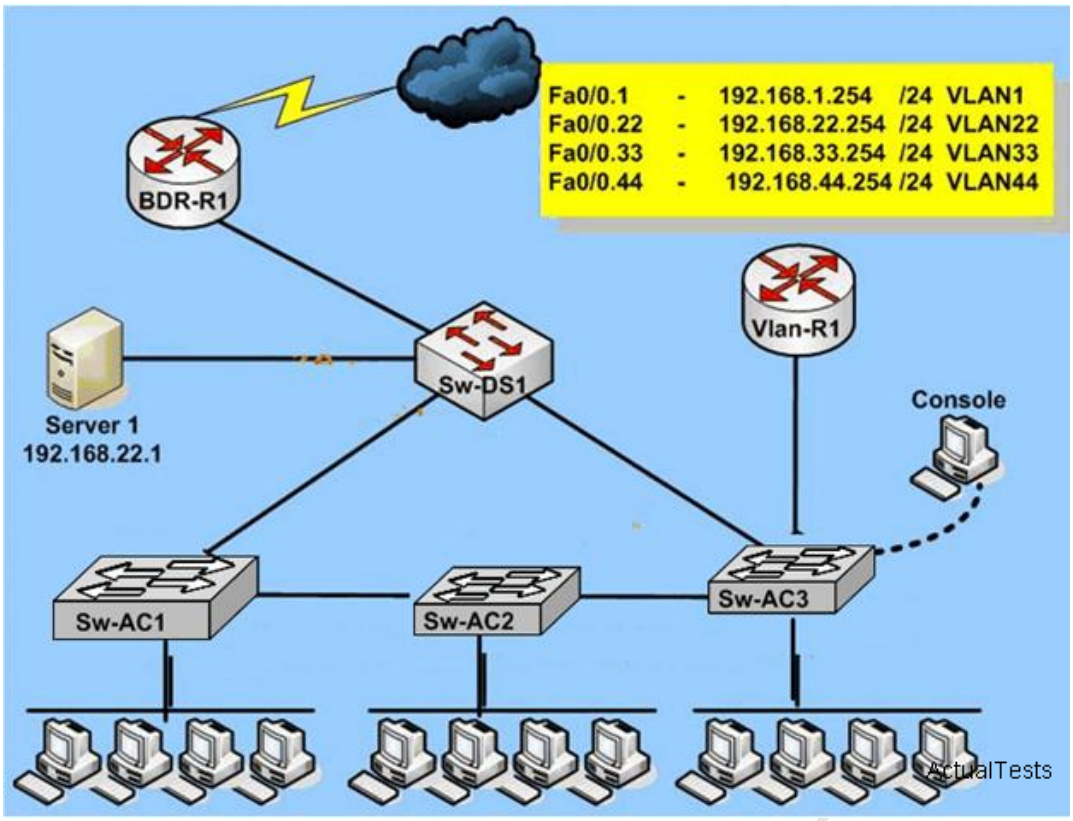
A. Raise the bridge priority on Switch1.
B. Lower the bridge priority on Switch9.
C. Raise the bridge priority on Switch9.
D. Physically replace Switch9 with Switch1 in the topology.
E. Disable spanning tree on Switch9.
F. Lower the bridge priority on Switch1.

Answer: F

Explanation:
The root bridge is the bridge or switch that is the root of the Spanning Tree, with the branches being loop-free paths to the other switches in the system. The Root is the switch with the lowest Bridge ID; the ID is determined by a combination of an administrative Priority and the MAC address of the switch. The Priority is set to 32,768 (8000 hex) by default; if we leave the Priority at the default, whatever switch has the lowest MAC will be the Root. So to elect the Switch1 switch as a root bridge need to set the lowest priority.

QUESTION NO: 166

Network exhibit:



Please refer to the exhibits.

Which switch is the root bridge for VLAN 1?

```
Sw-Ac3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0009.e8b2.c280
              Cost        19
              Port        12 (FastEthernet0/12)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000f.2485.8900
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts  Cost      Prio.Nbr   Type
---------------------------------------------------------------------
Fa0/3            Desg FWD  19        128.3      P2p
Fa0/9            Desg FWD  19        128.9      P2p
Fa0/12           Root FWD  19        128.12     P2p

Sw-Ac3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform      Port ID
Sw-DS1           Fas 0/12           130             S I   WS-C2950G-    Fas 0/12
Sw-AC2           Fas 0/9            176             S I   WS-C2950T-    Fas 0/9
VLAN-R1          Fas 0/3            152             R     2620          Fas 0/0.1
```


A. Sw-AC1

B. Sw-DS1
C. Sw-AC3
D. Sw-AC2

Answer: B

Explanation:
The election of the root bridge of the switching network is based on the bridge ID of each switch involved.

Bridge ID = Bridge priority + Bridge MAC

Bridge priority(by default) = 32768(This value can be adjusted according to different circumstances)

It is obvious that the root bridge is generated in this example, all that we have to do is to find this root bridge,here is a simple rule:

Root Ports(RP) are on the non-root bridges, root bridges have no RPs.

You can use show spanning-tree command on Sw-AC3 to view the root bridge for VLAN1, the results are:

Sw-AC3#show spanning-tree
VLAN001
Spanning tree enabled protocol ieee
Root ID Priority 24577
Address 0009.e8b2.c280
Cost 19
Port 12 (FastEthernet0/12)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
.....

Interface Role Sts Cost Prio.Nbr Type

Fa0/3 Desg FWD 19 128.3 P2p
Fa0/9 Desg FWD 19 128.9 P2p
Fa0/12 Root FWD 19 128.12 P2p

The information of spanning-tree for VLAN1 displays as follows:
1. The RP of Sw-AC3 is FastEthernet0/12.
2. The bridge priority of the root bridge is 24577
3. The root bridge MAC address is 0009.e8b2.c280

The switch connected to the RP Fa0/12 of Sw-AC3 is the root bridge. This switch can be found by use of the show cdp neighbors command on Sw-AC3.

QUESTION NO: 167

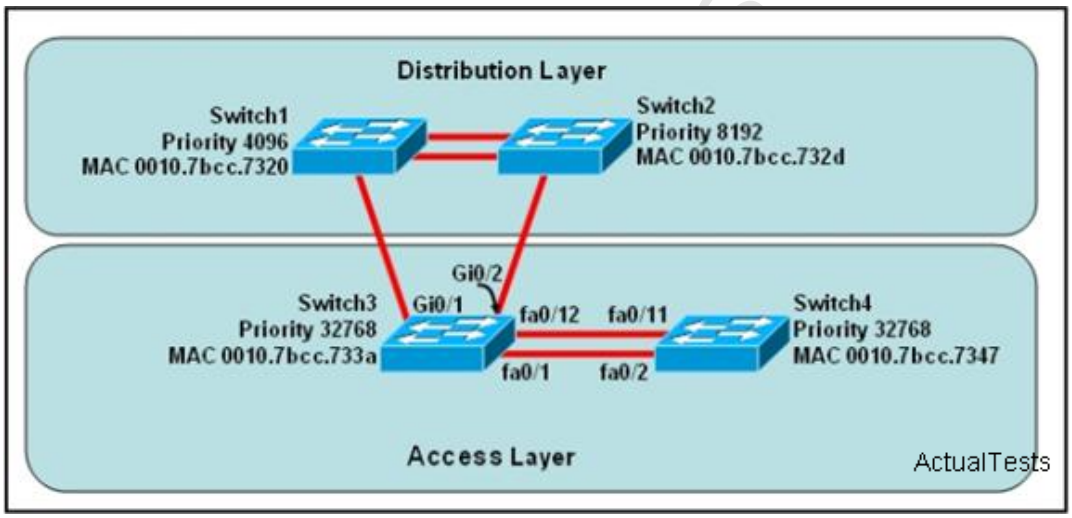
Switch ports operating in which two roles will forward traffic according to the IEEE 802.1w standard? (Choose two.)

A. root
B. designated
C. backup
D. alternate

Answer: A,B

QUESTION NO: 168

Refer to the exhibit.



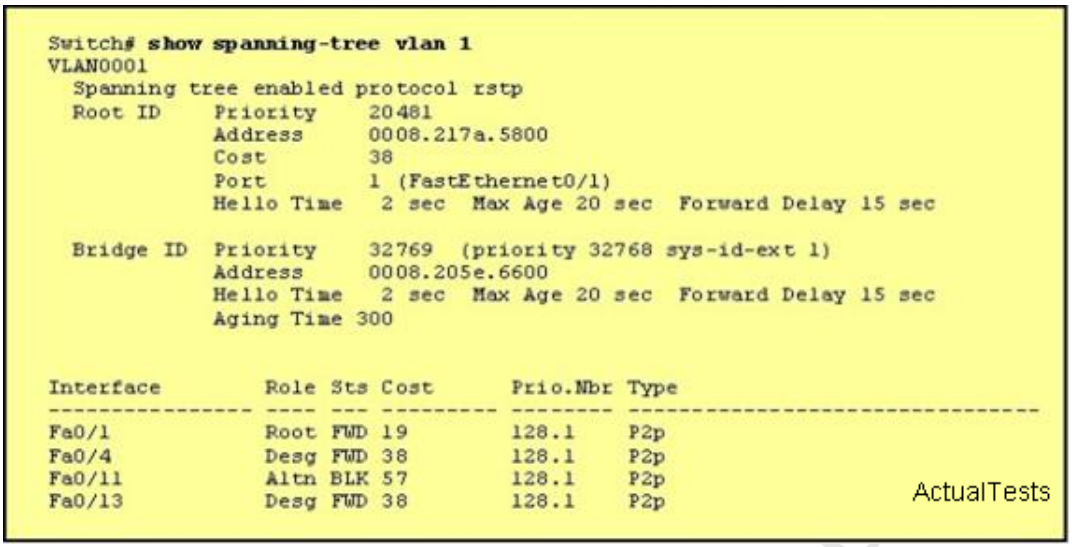
At the end of an RSTP election process, which access layer switch port will assume the discarding role?

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

Answer: C

QUESTION NO: 169

Refer to the exhibit.



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

QUESTION NO: 170

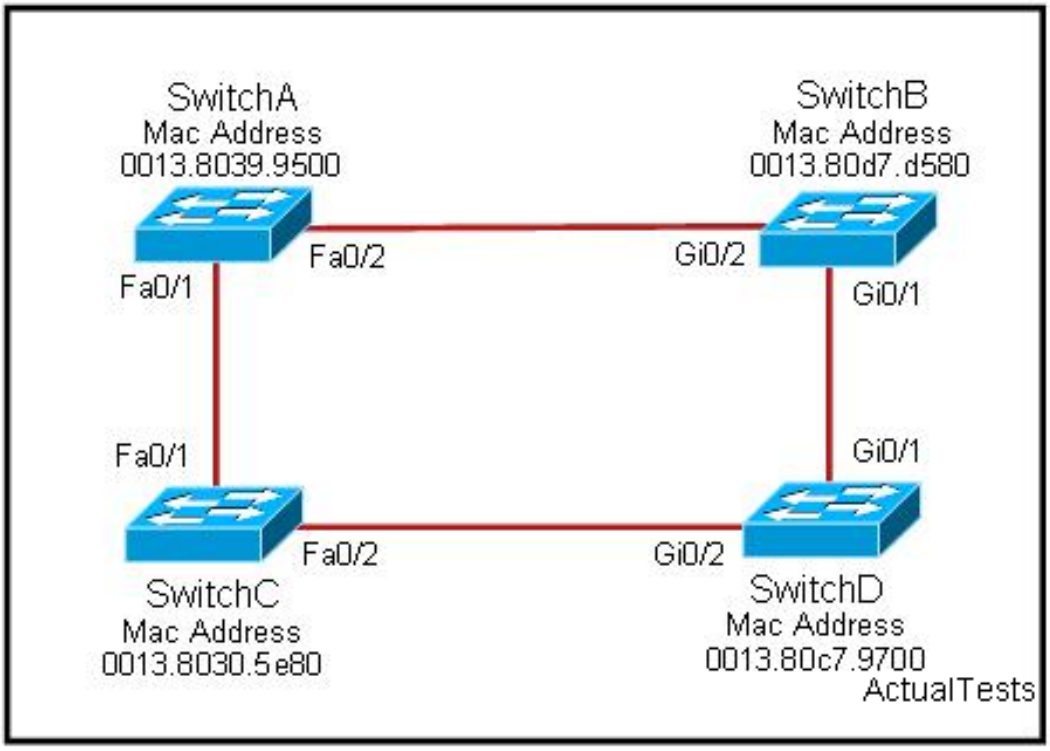
Which two functions of switch ports will forward traffic on the basis of the IEEE 802.1w standard? (Choose two.)

A. alternate
B. backup
C. designated
D. root

Answer: C,D

QUESTION NO: 171

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.)



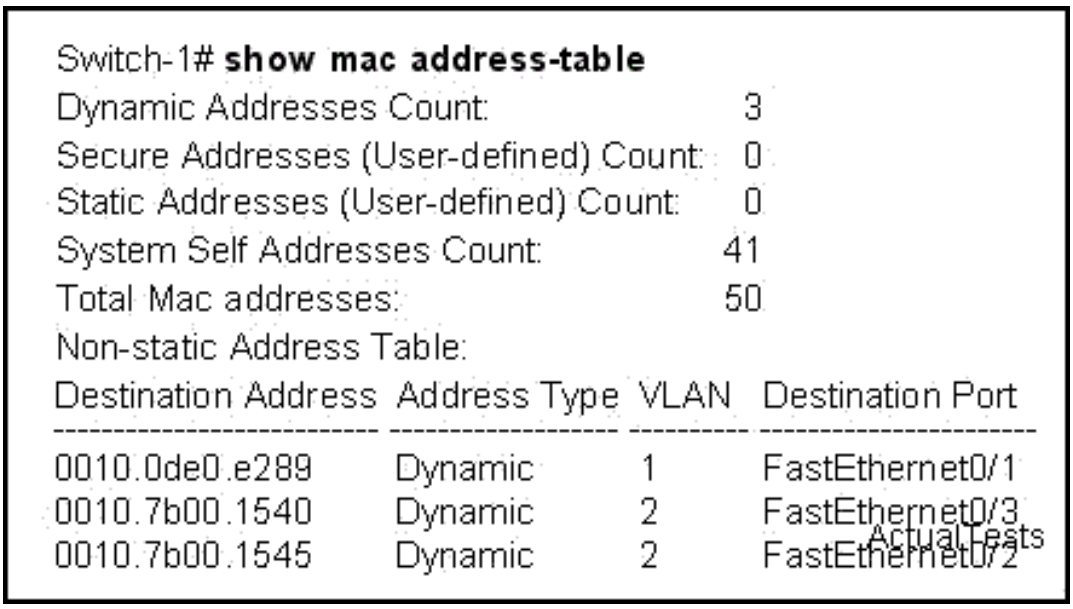
A. SwitchA, Fa0/2, designated
B. SwitchA, Fa0/1, root
C. SwitchB, Gi0/2, root
D. SwitchB, Gi0/1, designated
E. SwitchC, Fa0/2, root
F. SwitchD, Gi0/2, root

Answer: A,B,F

Explanation:
Section 15: Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network. (2 questions)

QUESTION NO: 172

Refer to the exhibit. 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 forward the data to its default gateway.
C. Switch-1 will flood the data out all of its ports except the port from which the data originated.
D. Switch-1 will send an ARP request out all its ports except the port from which the data originated.

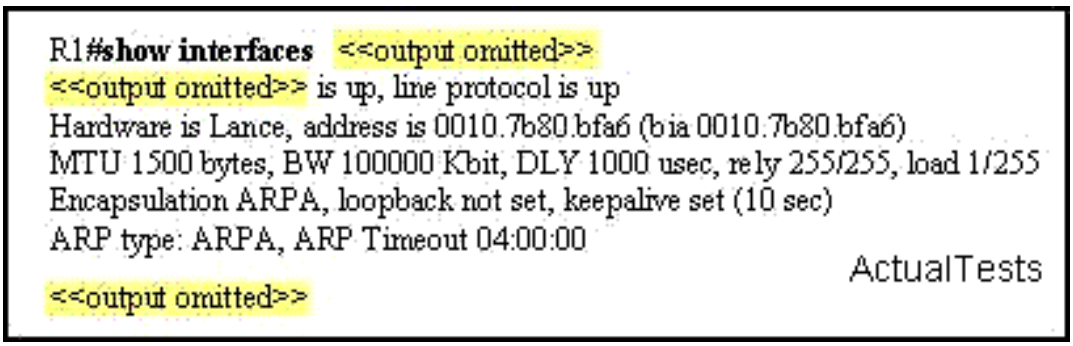
Answer: C

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:
Switches learn the MAC addresses of PCs or workstations that are connected to their switch ports by examining the source address of frames that are received on that port.
Machines may have been removed from a port, turned off, or moved to another port on the same switch or a different switch.
This could cause confusion in frame forwarding.
The MAC address entry is automatically discarded or aged out after 300 seconds
If there is not MAC address of destination host in MAC table, switch sends broadcast to all ports except the source to find out the destination host.
In output there is no MAC address of give host so switch floods to all ports except the source port.

QUESTION NO: 173

Refer to the exhibit. Assuming that the router is configured with the default settings, what type of router interface is this?



A. synchronous serial
B. Gigabit Ethernet
C. Ethernet
D. asynchronous serial
E. FastEthernet

Answer: E

Explanation:
From BW1000000Kbit,Encapsulation ARPA in the command line, we know that the interface is a 100M Ethernet interface.
Section 16: Implement basic switch security (including: port security, trunk access, management vlan other than vlan1, etc.) (9 questions)

QUESTION NO: 174

Why would a network administrator configure port security on a switch?

A. to prevent unauthorized Telnet access to a switch port
B. to limit the number of Layer 2 broadcasts on a particular switch port
C. to prevent unauthorized hosts from accessing the LAN
D. to block unauthorized access to the switch management interfaces over common TCP ports
E. to protect the IP and MAC address of the switch and associated ports

Answer: C

Explanation:
Network administrators can statically set up the legitimate MAC addresses which each port is allowed to connect through port security function to achieve device-level security authorization. Dynamic port security is set up to allow for the number of legitimate MAC addresses and regards the addresses learnt at a certain period as legitimate MAC addresses.
Through configuring Port Security to control the maximum number of MAC addresses across the port ,the MAC addresses learnt by port or cross port, handling with the access devices that exceed the number specified properly.
You can define the MAC addresses which will be allowed to access by ports through static manual configuration and switches learning automatically. The switch will learn the MAC addresses of new

access devices until reaching the desired number of MAC addresses, the MAC addresses that exceed the desired number will be denied. After being restarted , the switch will learn again. There are three methods to deal with the exceeded MAC addresses: Shutdown (shutdown port); Protect (discard illegal traffic without alarm); Restrict (discard illegal traffic with alarm).

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with 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 workstation attached to that port is assured the full bandwidth of the port.
If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00800d6a38.html#86378

QUESTION NO: 175

A network administrator wants to ensure that only the server can connect to port Fa0/1 on a Catalyst switch. The server is plugged into the switch Fa0/1 port and the network administrator is about to bring the server online. What can the administrator do to ensure that only the MAC address of the server is allowed by switch port Fa0/1? (Choose two.)

A. Employ a proprietary connector type on Fa0/1 that is incompatible with other host connectors.
B. Configure port security on Fa0/1 to reject traffic with a source MAC address other than that of the server.
C. Configure the MAC address of the server as a static entry associated with port Fa0/1.
D. Bind the IP address of the server to its MAC address on the switch to prevent other hosts from spoofing the server IP address.
E. Configure port Fa0/1 to accept connections only from the static IP address of the server.
F. Configure an access list on the switch to deny server traffic from entering any port other than Fa0/1.

Answer: B,C

Explanation:
1. Configure the static MAC address of the server on the switch to bind the MAC address of the server to the switch Fa0/1 port. In this way, even if another PC is plugged into this port, this PC

cannot communicate with other devices.
2. Configure port security on Fa0/1 to restrict the number of PCs that can be bound to this port. When the number of plugged PCs exceeds the number, the PCs that are not recorded on the switch cannot communicate with other devices.
Both methods can improve security of a Layer 2 network.

QUESTION NO: 176

The network security policy requires that only one host be permitted to attach dynamically to each switch interface. If that policy is violated, the interface should shut down. Which two commands must the network administrator configure on the 2950 Catalyst switch to meet this policy? (Choose two.)

A. Switch1(config-if)# switchport port-security violation shutdown
B. Switch1(config)# mac-address-table secure
C. Switch1(config-if)# switchport port-security maximum 1
D. Switch1(config)# access-list 10 permit ip host
E. Switch1(config-if)# ip access-group 10

Answer: A,C

Explanation:
Catalyst switches offer the port security feature to control port access based on MAC addresses. To configure port security on an access layer switch port, begin by enabling it with the following interface configuration command:
Switch(config-if)# switchport port-security
Next, you must identify a set of allowed MAC addresses so that the port can grant them access. You can explicitly configure addresses or they can be dynamically learned from port traffic. On each interface that uses port security, specify the maximum number of MAC addresses that will be allowed access using the following interface configuration command:
Switch(config-if)# switchport port-security maximum max-addr

Finally, you must define how each interface using port security should react if a MAC address is in violation by using the following interface configuration command:
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}

A violation occurs if more than the maximum number of MAC addresses are learned, or if an unknown (not statically defined) MAC address attempts to transmit on the port. The switch port takes one of the following configured actions when a violation is detected:
shutdown -The port is immediately put into the errdisable state, which effectively shuts it down. It must be re-enabled manually or through errdisable recovery to be used again.
restrict -The port is allowed to stay up, but all packets from violating MAC addresses are dropped.

The switch keeps a running count of the number of violating packets and can send an SNMP trap and a syslog message as an alert of the violation.
protect -The port is allowed to stay up, as in the restrict mode. Although packets from violating addresses are dropped, no record of the violation is kept.

QUESTION NO: 177

You are a network administrator. In order to improve the security of your company's switching network , refer to the following options. Which two methods are examples of implementing Layer 2 security on a Cisco switch? (Choose two.)

A. enable HTTP access to the switch for security troubleshooting
B. disable trunk negotiation on the switch
C. use only protected Telnet sessions to connect to the Cisco device
D. configure a switch port host where appropriate

Answer: B,D

Explanation:
With the popularity and constantly deepening of network applications, the users?? requirements for Layer 2 switches are not only limited to data forwarding performance and quality of service (QoS), but also philosophy of network security which is becoming an increasingly important consideration of networking products. How to filter user communications and ensure safe and effective data transmission? How to block the illegal users and make network work safely? How to execute secure network management and detect illegal users, illegal activities and security performance of remote network management information in time? The following methods can accomplish network Layer 2 security by working on switches.

Layer 2 filtering.
Now , most new-style switches can achieve various filtering demands by establishing specifications . There are two modes to setup specifications: one is the MAC mode which can effectively achieve data isolation according to the source MAC address or the destination MAC address based on users?? needs; the other is the IP mode(this mode does not belong to Layer2 filtering),which can filter data packets by use of the source IP, the destination IP, protocols, the source ports and the destination ports; the specifications established must be attached to the appropriate receiving or sending port so that when receiving or forwarding data on this port, the switch can filter data packets based on filtering rules and decide to transmit or discard.

802.1X is port-based access control.
In order to prevent illegal users from accessing LAN and guarantee network security, port-based access control protocol 802.1X is widely used in both wired LAN or WLAN.

Traffic control.
The traffic control of switches can prevent abnormal load of switch bandwidth caused by excessive traffic of broadcast data packets, multicast data packet or the wrong destination address of unicast data packet. The traffic control of switches can also improve the whole system performance and maintain security and stability of the network running.

SNMP v3 and SSH
SNMP v3 proposed completely new architecture, concentrating all SNMP standards of various versions together to enhance network management security. The security mode proposed by SNMP v3 is based on the User Security Mode, that is USM. SNMP v3 can effectively prevent non-authorized users from modifying, disguising and eavesdropping management information.

As for the remote network management through the Telnet, because the Telnet services have a fatal weakness it transfers user name and password in the form of plaintext , so it is very easy to steal passwords for those people with ulterior motives. But by use of SSH to communicate, both user name and password are encrypted to effectively prevent eavesdropping the password ,in this way, network administrators can manage remote security network easily.

QUESTION NO: 178

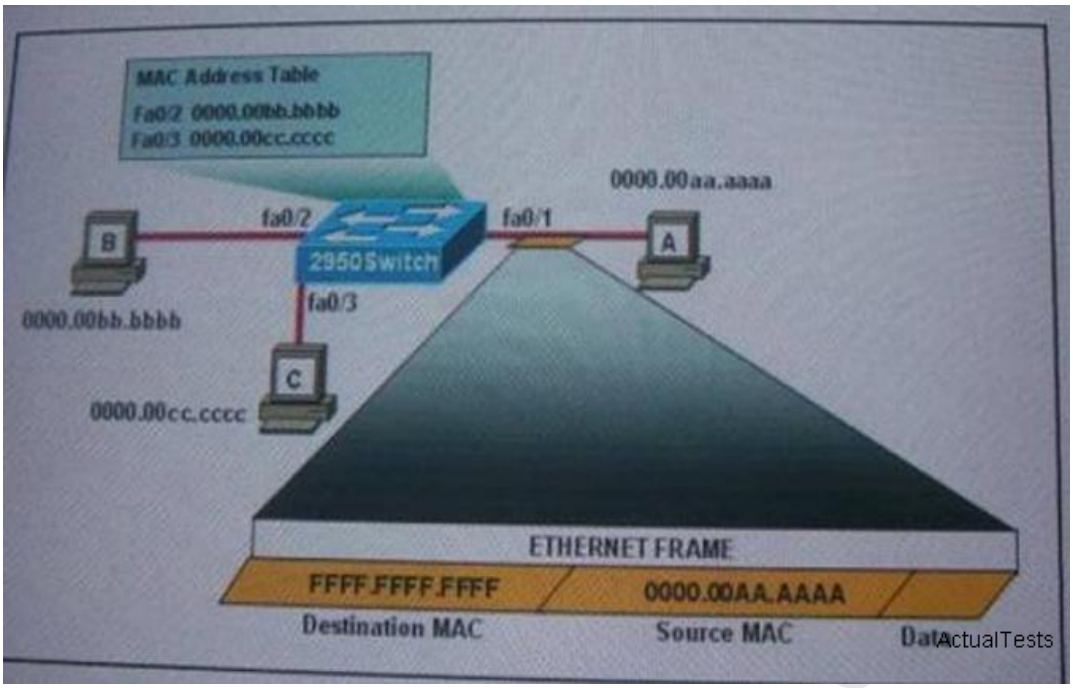
As the network administrator, you are required to configure the network security policy, And the policy requires that only one host be permitted to attach dynamically to each switch interface. If that policy is violated, the interface should shut down. Which two commands must the network administrator configure on the 2950 Catalyst switch to meet this policy? Select two.

A. Switch1(config-if)# switchport port-security maximum 1
B. Switch1(config)# mac-address-table secure
C. Switch1(config)# access-list 10 permit ip host
D. Switch1(config-if)# switchport port-security violation shutdown
E. Switch1(config-if)# ip access-group 10

Answer: A,D

Explanation:
Basically speaking, the function of Port Security is to remember the MAC address of the NIC connected to the switch port and allows this MAC address to use this port. If other NICs attempt to cross this port to connect to the switch, Port Security function will disable this port.
switchport port-security maximum {max # of MAC addresses allowed}: This parameter will allow each port to bind more MAC addresses, not only one.
switchport port-security violation {shutdown | restrict | protect}: This command tells the switch that how to deal with the situation when the number of MAC addresses accessed exceeds the desired maximum number. This port is disabled by default.

QUESTION NO: 179



The following commands are executed on interface fa0/1 of 2950 Switch.

2950Switch (config-if)# switch port port-security
2950Switch (config-if)# switch port port-security mac-address sticky
2950Switch (config-if)# switch port port-security maximum1

The Ethernet frame that is shown arrives on interface fa0/1 .Which 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 frame will 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 forward.
F. Only frames from source 0000.00bb bbbb. the first learned MAC address of 2950Switch, will be forward.

Answer: B,D

QUESTION NO: 180

A network administrator must configure 200 switch ports to accept traffic from only the currently attached host devices. What would be the most efficient way to configure MAC-level security on all these ports?

A. Visually verify the MAC addresses and then telnet to the switches to enter the switchport-port security mac-address command.
B. Have end users e-mail their MAC addresses. Telnet to the switch to enter the switchport-port security mac-address command.
C. Use the switchport port-security MAC address sticky command on all the switch ports that have end devices connected to them.
D. Use show mac-address-table to determine the addresses that are associated with each port and then enter the commands on each switch for MAC address port-security.

Answer: C

QUESTION NO: 181

Select the action that results from executing these commands.

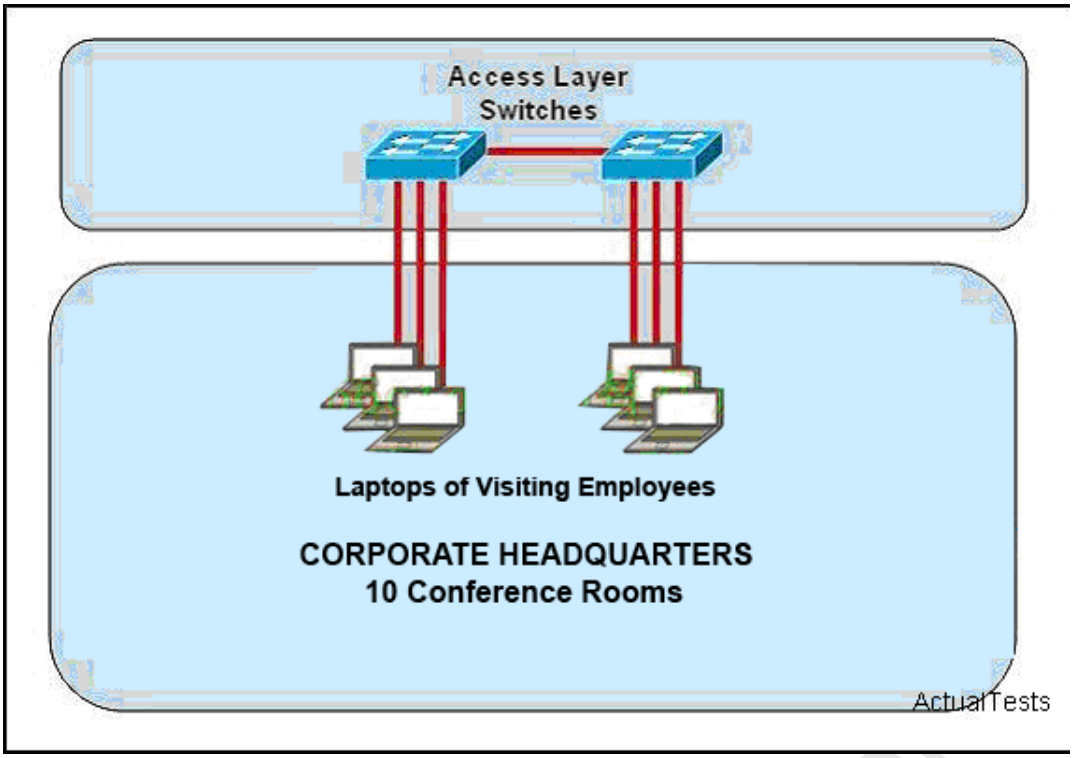
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky

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

QUESTION NO: 182

Refer to the exhibit. Some 2950 series switches are connected to the conference area of the corporate headquarters network. The switches provide two to three jacks per conference room to host laptop connections for employees who visit the headquarters office. When large groups of employees come from other locations, the network administrator often finds that hubs have been connected to wall jacks in the conference area although the ports on the access layer switches were not intended to support multiple workstations.
What action could the network administrator take to prevent access by multiple laptops through a single switch port and still leave the switch functional for its intended use?



A. Configure static entries in the switch MAC address table to include the range of addresses used by visiting employees.
B. Configure an ACL to allow only a single MAC address to connect to the switch at one time.
C. Use the mac-address-table 1 global configuration command to limit each port to one source MAC address.
D. Implement Port Security on all interfaces and use the port-security maximum 1 command to limit port access to a single MAC address.
E. Implement Port Security on all interfaces and use the port-security mac-address sticky command to limit access to a single MAC address.
F. Implement Port Security at global configuration mode and use the port-security maximum 1 command to allow each switch only one attached hub.

Answer: D

QUESTION NO: 183

Which of the following describe private IP addresses? (Choose two.)

A. addresses licensed to enterprises or ISPs by an Internet registry organization
B. addresses that can be routed through the public Internet
C. a scheme to conserve public addresses
D. addresses that cannot be routed through the public Internet
E. addresses chosen by a company to communicate with the Internet

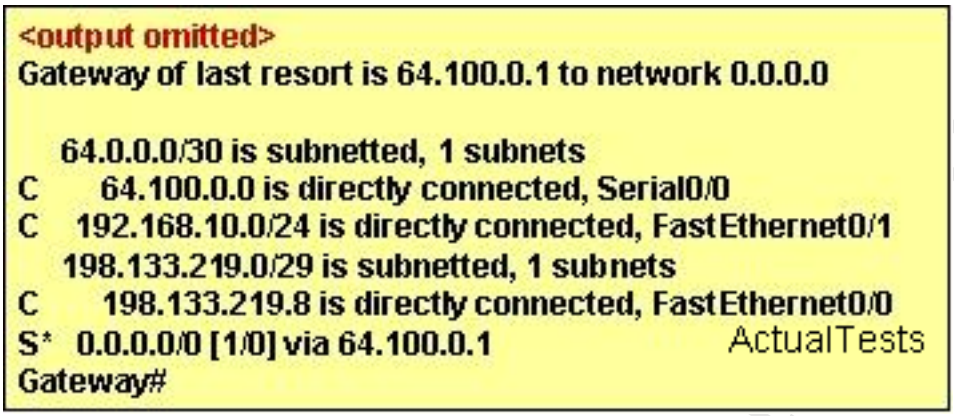
Answer: C,D

Explanation:

Private IP address space has been allocated via RFC 1918. This means the addresses are available for any use by anyone and therefore the same private IP addresses can be reused. However they are defined as not routable on the public Internet. They are used extensively in private networks due to the shortage of publicly registered IP address space and therefore network address translation is required to connect those networks to the Internet.

QUESTION NO: 184

Refer to the exhibit. The router has been configured with these commands.



What are the two results of this configuration? (Choose two.)

```
hostname Gateway
interface FastEthernet 0/0
 ip address 198.133.219.14 255.255.255.248
 no shutdown
interface FastEthernet 0/1
 ip address 192.168.10.254 255.255.255.0
 no shutdown
interface Serial 0/0
 ip address 64.100.0.2 255.255.255.252
 no shutdown
ip route 0.0.0.0 0.0.0.0 64.100.0.1
```

```
interface Serial 0/0
 ip address 64.100.0.2 255.255.255.252
 no shutdown
ip route 0.0.0.0 0.0.0.0 64.100.0.1
```

ActualTests

A. The default route should have a next hop address of 64.100.0.3.

B. Hosts on the LAN that is connected to FastEthemet 0/1 are using public IP addressing.

C. The address of the subnet segment with the WWW server will support seven more servers.

D. The addressing scheme allows users on the Internet to access the WWW server.
E. Hosts on the LAN that is connected to FastEthernet 0/1 will not be able to access the Internet without address translation.

Answer: D,E

Explanation:
Since the hosts on the Fast Ethernet 0/1 network are using private RFC 1918 IP addressing (192.168.10.0/24) their IP addresses will need to be translated into a publicly routable address in order to access the Internet. However, the server is using the 198.133.219.9 IP address, which is publicly routable and so Internet users can indeed access this server (assuming that the 198.133.219.9 IP address has been correctly assigned to the network)

QUESTION NO: 185

Which host addresses are members of networks that can be routed across the public Internet? (Choose three.)

A. 172.16.223.125
B. 172.64.12.29
C. 198.234.12.95
D. 212.193.48.254

Answer: B,C,D

Explanation:
Section 2: Explain the operation and benefits of using DHCP and DNS (8 questions)

QUESTION NO: 186

What TCP/IP stack configuration features can DHCP provide, in addition to assigning an IP address? (Choose three.)

A. DNS servers
B. helper address
C. subnet mask
D. TFTP server
E. default gateway
F. FTP server

Answer: A,C,E

Explanation:
Default gateway refers to router default gateway, which is used to realize access between vlans. When a router receives a destination unknown address packet, it will be sent to the default gateway (such as a router's interface) if default gateway exists, otherwise the packet will be discarded. DNS is Domain Name Server. The conversion between Domain names and IP addresses is called domain analysis, and DNS is the server to process domain analysis. IP addresses use network number and host number to mark network host, and only computers under the same network number can intercommunicate "directly", computers with different networks may intercommunicate only through Gateway. Thus IP networks are divided into smaller networks, known as subnet. Subnet mask is used to determine whether two IP addresses are in the same subnet, then only computers under the same subnet can intercommunicate "directly".

DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon bootup. Since each host needs an IP address to communicate in an IP network, DHCP eases the administrative burden of manually configuring each host with an IP address. Furthermore, if a host moves to a different IP subnet, it has to use a different IP address than the one it was previously using. DHCP takes care of this automatically, by allowing the host to choose an IP address in the correct IP subnet.
Reference:
"Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks"
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml#understanding

QUESTION NO: 187

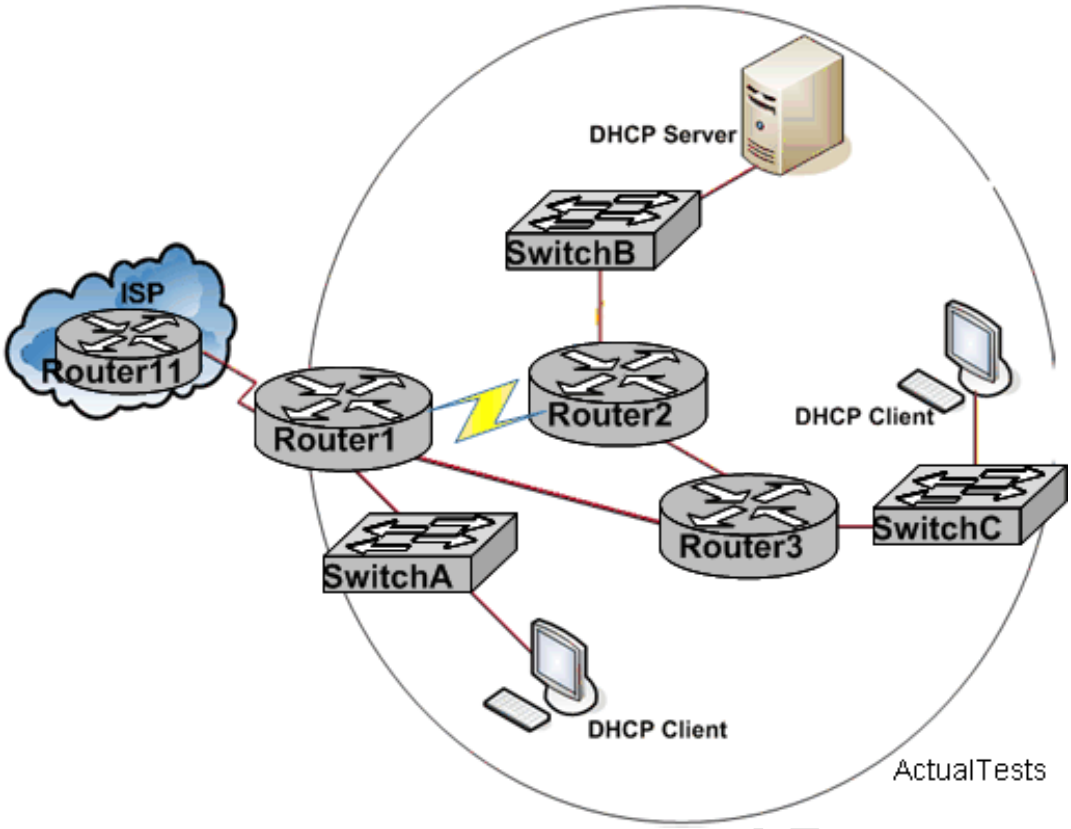
Which statement is correct regarding the operation of DHCP?

A. A DHCP client uses a ping to detect address conficts.
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 detected, 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: E

QUESTION NO: 188

Refer to the exhibit. Using the information shown.



What is the purpose of the DHCP server?

A. to provide storage for email
B. to translate URLs to IP addresses
C. to translate IPv4 addresses to MAC addresses
D. to provide an IP configuration information to hosts

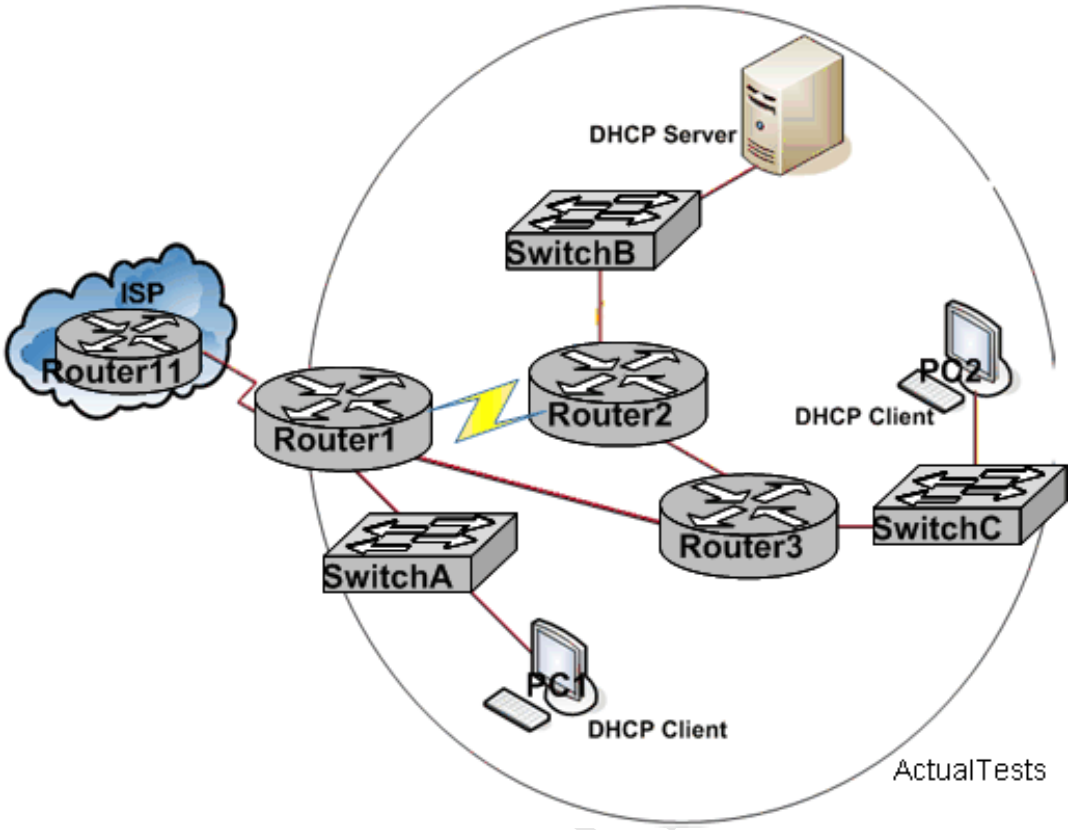
Answer: D

Explanation:
Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain the parameters necessary for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration.
When a DHCP-configured client (be it a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as the default gateway, the domain name, the DNS servers, other servers such as time servers, and so forth. Upon receipt of a valid request the server will assign the computer an IP address, a lease (the length of time for which the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting and must be completed before the client can initiate IP-based communication with other hosts.
So, when the DHCP server is down, clients can be connected normally over a period of time until

the expiration of the lease.

QUESTION NO: 189

Refer to the exhibit. Using the information shown



How is the message sent from a PC2 when is first powers on and attempts to contact the DHCP Server?

A. Layer 3 multicast
B. Without any Layer 3 encapsulation
C. Layer 3 broadcast
D. Layer 3 unicast

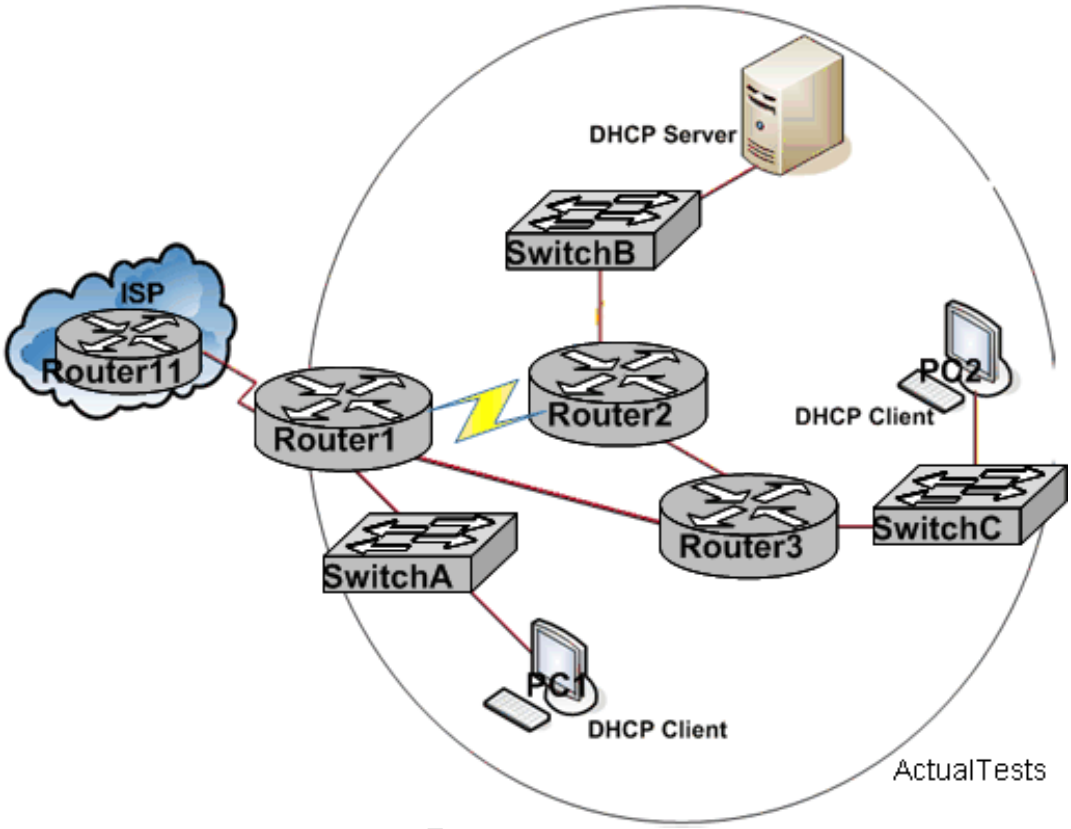
Answer: C

Explanation:
Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain the parameters necessary for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration.
When a DHCP-configured client (be it a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as the default gateway, the domain name, the DNS servers, other

servers such as time servers, and so forth. Upon receipt of a valid request the server will assign the computer an IP address, a lease (the length of time for which the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting and must be completed before the client can initiate IP-based communication with other hosts.
So, when the DHCP server is down, clients can be connected normally over a period of time until the expiration of the lease.

QUESTION NO: 190

Refer to the exhibit. Using the information shown, answer the question.



All hosts in the networks have been operational for several hours when the DHCP server goes down. What happens to the hosts that have obtained service from the DHCP server?

A. The hosts will only be able to communicate with other hosts by IP address not by hostname
B. The hosts will not be able to communicate with any other hosts.
C. The hosts will be able to communicate with hosts outsides their own network
D. The hosts will continue to communicate normally for a period of time.

Answer: D

Explanation:
Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain the parameters necessary for operation in an Internet Protocol network. This protocol

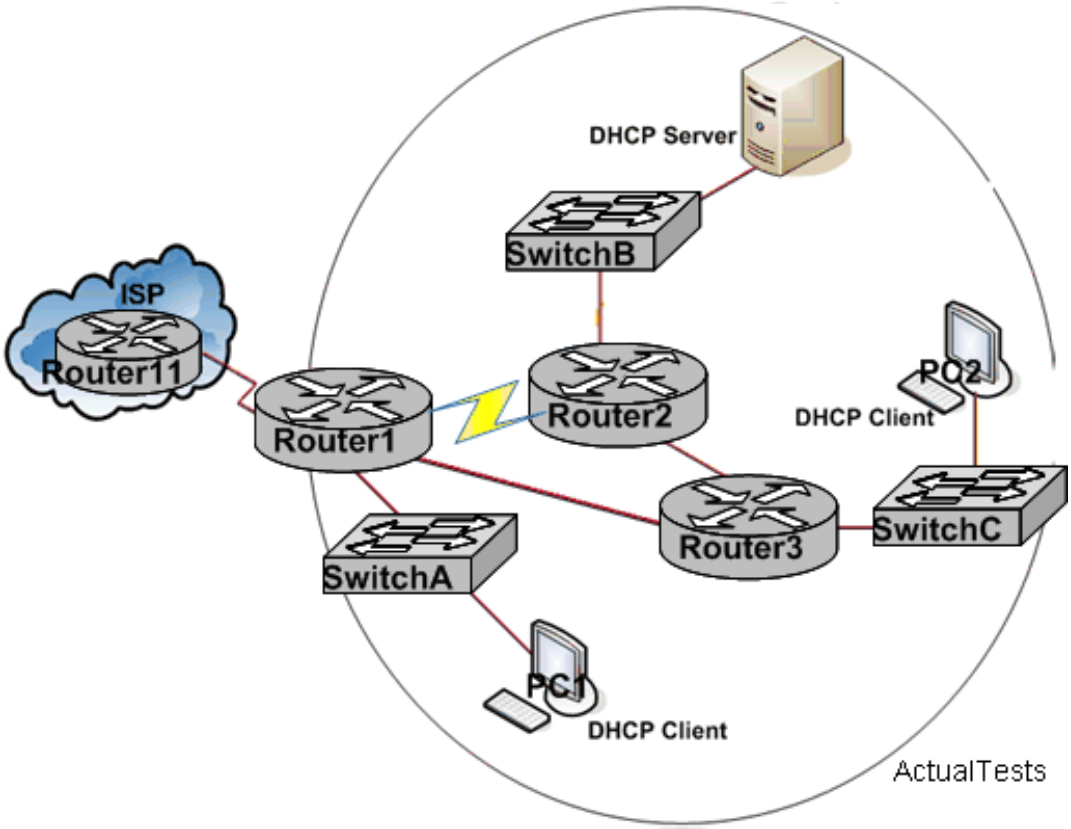
reduces system administration workload, allowing devices to be added to the network with little or no manual configuration.

When a DHCP-configured client (be it a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as the default gateway, the domain name, the DNS servers, other servers such as time servers, and so forth. Upon receipt of a valid request the server will assign the computer an IP address, a lease (the length of time for which the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting and must be completed before the client can initiate IP-based communication with other hosts.

So, when the DHCP server is down, clients can be connected normally over a period of time until the expiration of the lease.

QUESTION NO: 191

Refer to the exhibit. Using the information shown



What is the default behavior of Router1 when PC1 requests service from DHCP server?

A. Drop the request.
B. Broadcast the request to Router2, Router3 and ISP
C. Broadcast the request to Router2 and Router3
D. Forward the request to Router2

Answer: A

Explanation:
DHCP clients send request to DHCP Server in the form of broadcast, while routers will not forward broadcast, it will discard this request packet.
Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain the parameters necessary for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration.
When a DHCP-configured client (be it a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as the default gateway, the domain name, the DNS servers, other servers such as time servers, and so forth. Upon receipt of a valid request the server will assign the computer an IP address, a lease (the length of time for which the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting and must be completed before the client can initiate IP-based communication with other hosts.
So, when the DHCP server is down, clients can be connected normally over a period of time until the expiration of the lease.

QUESTION NO: 192

DNS servers provide what service?

A. They map individual hosts to their specific IP addresses.
B. They convert domain names into IP addresses.
C. They run a spell check on host names to ensure accurate routing.
D. Given an IP address, they determine the name of the host that is sought.

Answer: B

Explanation:
The purpose of DNS is to resolve host names into IP addresses, which is called forward lookup; and IP address to name is called reverse lookup.

ip name-server <DNS Server>

This command is used to configure the IP address of the DNS server on Cisco router. This will allow you to ping, telnet, etc, using the host name instead of the IP address.

QUESTION NO: 193

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 keep the host will usually 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:
As you know, DHCP clients lease their IP addresses from DHCP servers. When this lease expires, that IP address can no longer be utilized by the DHCP client. For that reason, DHCP client must periodically renew their IP address leases, preferably before the lease has expired or is about to expire.
TDHCP client passes through the renewing and rebinding states to renew its IP address lease.
Renewing state: The DHCP client first attempts to renew its lease when 50 percent of the lease time has expired. To renew its lease, the DHCP client sends a directed DHCPREQUEST message to the DHCP server that provided the original lease. If renewal is allowed, the DHCP server automatically renews the lease by responding with a DHCPACK message. This new IP address lease contains not only the original IP address if still available (or another IP address otherwise) but any TCP/IP client configuration information.
Rebinding state: If, for whatever reason, the DHCP client is not able to communicate with the original DHCP server the executed its lease, it attempts another approach called rebinding . Here the DHCP client attempts to contact any available DHCP server when 87.5 percent of the lease time has expired. The leasing process is akin to that detailed over the last several pages.
Reference: http://www.windowsitlibrary.com/Content/329/08/5.html

Section 3: Configure, verify and troubleshoot DHCP and DNS operation on a router. (including: CLI/SDM) (1 question)

QUESTION NO: 194

Refer to the output from the show running-config command in the exhibit. What should the administrator do to allow the workstations connected to the FastEthernet 0/0 interface to obtain an IP address?

A. Configure the IP address of the FastEtherent 0/0 interface to 10.90.201.1.

B. Apply access-group 14 to interface FastEthernet 0/0.

C. Add access-list 14 permit any any to the access list configuration.

D. Add an interface description to the FastEthernet 0/0 interface configuration.

Answer: A

Explanation:

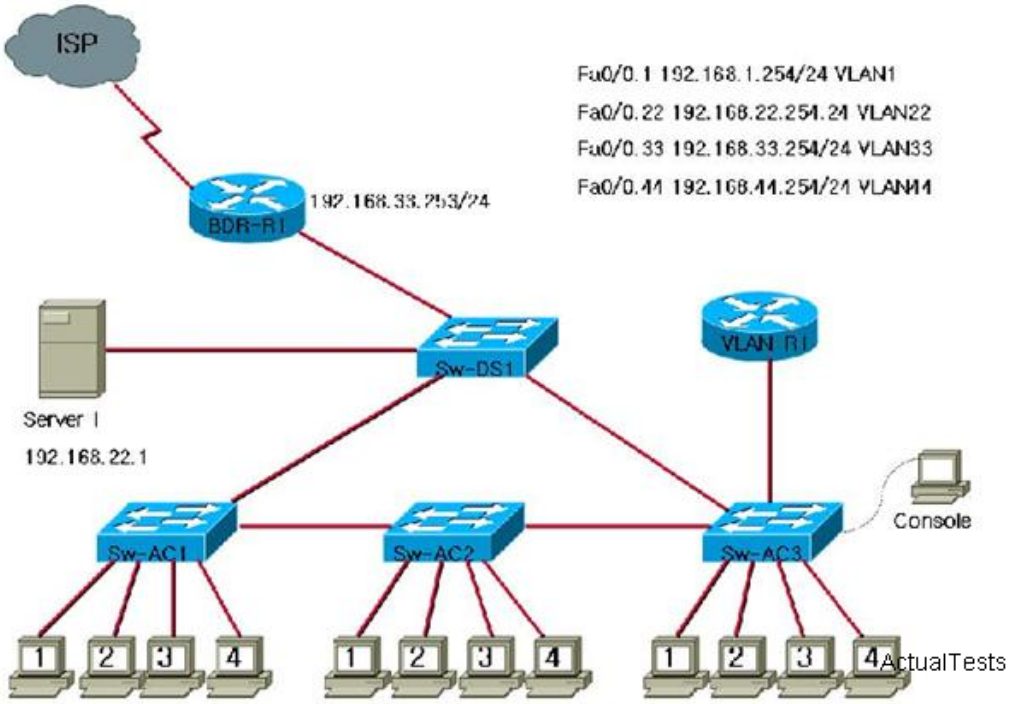
The F0/0 interface of the router is the gateway of the internal network; the administrator must configure an IP address for the interface.

Section 4: Implement static and dynamic addressing services for hosts in a LAN environment (5

questions)

QUESTION NO: 195

What address should be configured as the default-gateway for the host connected to interface Fa0/4 of Sw-AC3?



Sw-AC3#show vlan

```
Sw-Ac3#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16
22   Servers                          active
33   Management                       active    Fa0/1, Fa0/2, Fa0/5, Fa0/6, Fa0/7
44   Production                       active    Fa0/4, Fa0/8, Fa0/10, Fa0/11
99   no-where                         active    Fa0/13, Fa0/14, Fa0/15, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                F0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
```


A. 192.168.1.254
B. 192.168.44.254
C. 192.168.33.254
D. 192.168.22.254

Answer: B

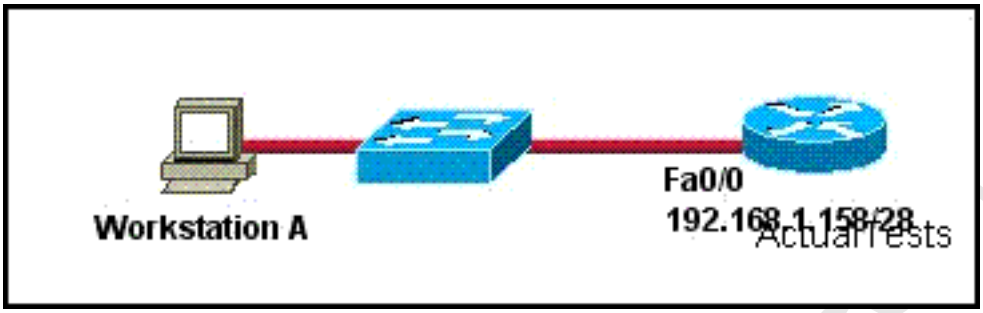
Explanation:

On the basis of the output of "Sw-AC3#show vlan" we know that the interface Fa0/4 on Sw-Ac3 is in VLAN44. Based on the topology provided in the exhibit, we know that the default gateway of VLAN44 is 192.168.44.254.

QUESTION NO: 196

Refer to the exhibit. What IP address should be assigned to Workstation A?

Exhibit:



A. 192.168.1.144/28
B. 192.168.1.145/28
C. 192.168.1.143/28
D. 192.168.1.160/28
E. 192.168.1.159/28

Answer: B

Explanation:
The switch is a Layer 2 device, so the IP address of WorkstationA and that of Fa0/0 are on the same network.
The binary version of 158 is 1001 1110.
The binary version of 145 is 1001 0001.
The sfubnet mask is /28. The binary version of 158 has the same first four bits as that of 145. We can infer that 192.168.1.158/28 and 192.168.1.145/28 have the same subnet number, that is, they are on the same subnet.

The available subnets and IP ranges that are available using a /28 (255.255.255.240) subnet mask is shown below:

/28 IP Bit Mask			
Dotted Decimal Mask: 255.255.255.240 **Hexadecimal Mask:** FF.FF.FF.F0 **Effective Hosts:** 224 **Effective Subnets:** 16			
Network Number	**Broadcast**	**Usable IP Range**	**Usable IPs /subnet**
0	15	1 - 14	14
16	31	17 - 30	14
32	47	33-46	14
48	63	49-62	14
64	79	65-78	14
80	95	81-94	14
96	111	97-110	14
112	127	113-126	14
128	143	129-142	14
144	159	145-158	14
160	175	161-174	14
176	191	177-190	14
192	207	193-206	14
208	223	209-222	14
224	239	225-238	14
240	255	241-254	14

Based on this information, we need to choose an IP address within the 145-158 range, since the IP address of the Fa0/0 on the router is 192.168.1.158, leaving only answer choice C as feasible.
Reference: http://www.more.net/technical/netserv/tcpip/subnet.html#28

QUESTION NO: 197

Which command would correctly configure a serial port on a router with the last usable host address in the 192.216.32.32/29 subnet?

A. router (config-if)# ip address 192.216.32.38 255.255.255.240
B. router (config-if)# ip address 192.216.32.39 255.255.255.224
C. router (config-if)# ip address 192.216.32.63 255.255.255.248

D. router (config-if)# ip address 192.216.32.39 255.255.255.248
E. router (config-if)# ip address 192.216.32.63 255.255.255.248
F. router (config-if)# ip address 192.216.32.38 255.255.255.248

Answer: F

QUESTION NO: 198

The network default gateway applying to a host by DHCP is 192.168.5.33/28. Which option is the valid IP address of this host?

A. 192.168.5.55
B. 192.168.5.47
C. 192.168.5.40
D. 192.168.5.32
E. 192.168.5.14

Answer: C

QUESTION NO: 199

Which two addresses can be assigned to a host with a subnet mask of 255.255.254.0? (Choose two.)

A. 113.10.4.0
B. 186.54.3.0
C. 175.33.3.255
D. 26.35.2.255
E. 17.35.36.0

Answer: B,D

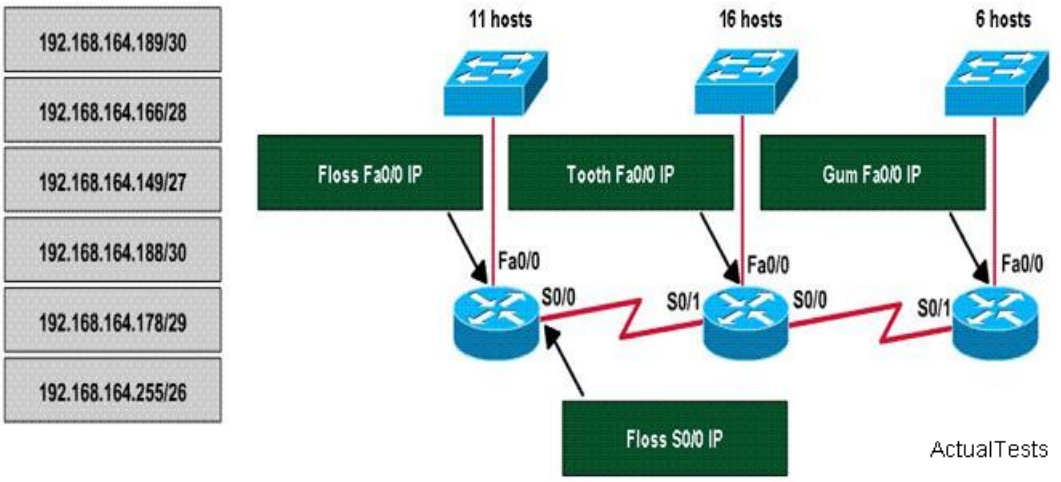
Explanation:
Section 5: Calculate and apply an addressing scheme including VLSM IP addressing design to a network (13 questions)

QUESTION NO: 200 DRAG DROP

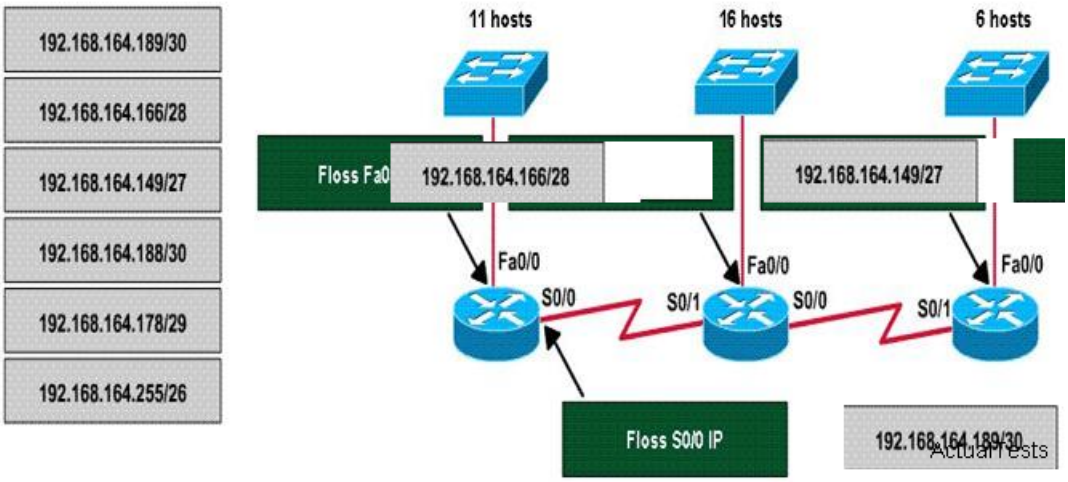
A dental firm is redesigning the network that connects its three locations. The administrator gave the networking team 192.168.164.0 to use for addressing the entire netwok. After subnetting the address, the team is ready to assign the addresses. The administrator plans to configure ip subnet-zero and use RIP v2 as the routing protocol. As a member of the networking team, you

must address the network and at the same time conserver unused addresses for future growth. With those goals in mind, drag the host addresses on the left to the correct router interface. Once of the routers is partially configured. Move your mouse over a router to view its configuration. Not all of the host addresses on the left are necessary.

Exhibit:

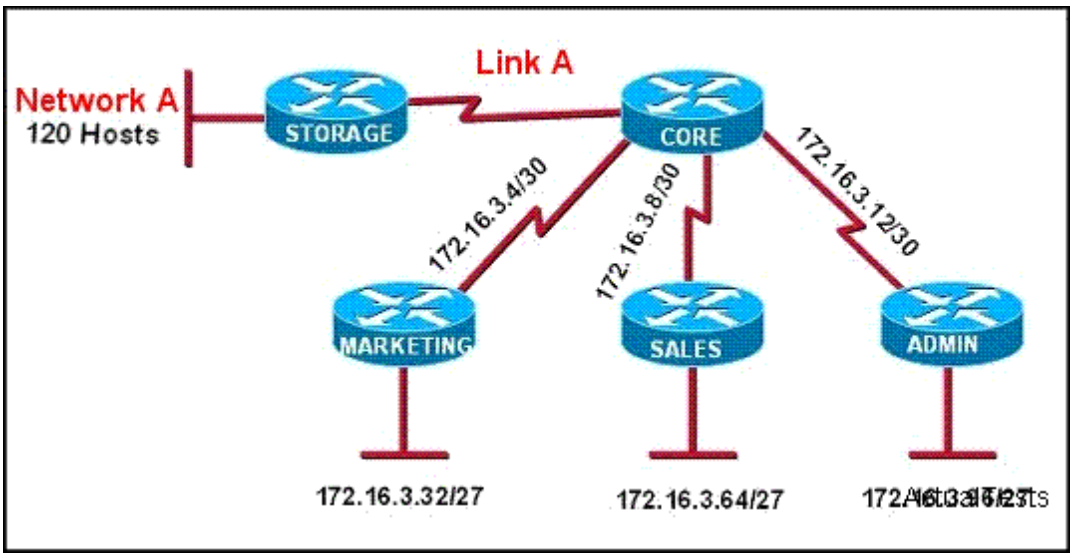


Answer:



QUESTION NO: 201

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. Link A - 172.16.3.40/30
B. Network A - 172.16.3.48/26
C. Network A - 172.16.3.128/25
D. Link A - 172.16.3.0/30
E. Link A - 172.16.3.112/30
F. Network A - 172.16.3.192/26

Answer: C,D

Explanation:
One reserved subnet, the subnetthat has all binary 0s in the subnet field, is called the zero subnet.

Subnet zero, or the zero subnet, is numerically the first subnet, but it is one of the two reserved subnet numbers in a network. You can use the zero subnet on a Cisco router if you configure the global configuration command ip subnet-zero. For the purposes of answering questions on the exam about the number of valid subnets in a network, consider the zero subnet unusable. In real life, do not use the zero subnet if you do not have to.

QUESTION NO: 202

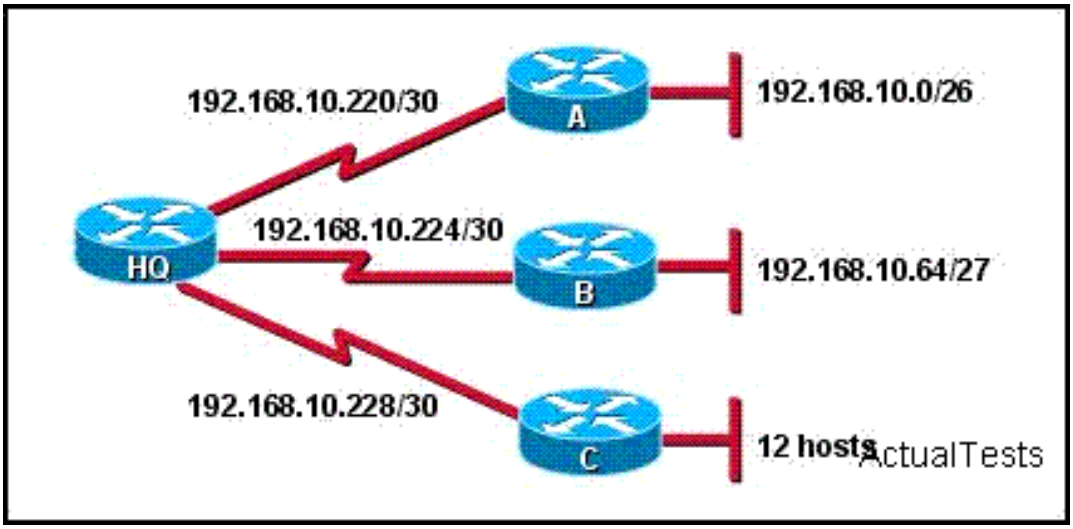
How many subnets can be gained by subnetting 172.17.32.0/23 into a /27 mask, and how many usable host addresses will there be per subnet?

A. 8 subnets, 31 hosts
B. 8 subnets, 32 hosts
C. 16 subnets, 30 hosts
D. A Class B address can't be subnetted into the fourth octet.
E. 16 subnets, 32 hosts

Answer: C

QUESTION NO: 203

Refer to the exhibit. A new subnet with 12 hosts has been added to the network. Which subnet address should this network use to provide enough useable addresses while wasting the fewest addresses?



A. 192.168.10.80/28
B. 192.168.10.96/28
C. 192.168.10.80/29
D. 192.168.10.96/29

Answer: B

Explanation:
This question tests how to choose a subnet address to provide enough useable addresses while wasting the fewest addresses. Because the subnet connected to Router C has only 12 hosts, /28 is the most appropriate. The answer is 192.168.10.96/28.

QUESTION NO: 204

If an ethernet port on a router was assigned an IP address of 172.16.112.1/20, what is the maximum number of hosts allowed on this subnet?

A. 8190
B. 4096
C. 4094
D. 1024
E. 2046

Answer: C

Explanation:
By default, 172.16.112.1/20 is a Class B address.
A Class B address can allow 65534 hosts. 32-16=16 216=65536 65536-2=65534
172.16.112.1 is subnetted. The network can allow 4094 hosts. 32-20=12 212=4096 4096-2=4094
IP addresses with all 0s or all 1s in the host part cannot be used as host addresses; therefore, these two addresses are excluded.

Since a /20 equates to 12 bits used for the subnet mask, 4094 hosts can be uniquely addressed.

QUESTION NO: 205

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. 255.255.255.224
B. 0.0.0.240
C. 255.255.255.252

Answer: A

QUESTION NO: 206

As the network administrator of your company, you have been assigned the task of designing a new Office internetwork. So you need to consider IP addressing scheme, Which two subnetworks would be included in the summarized address of 172.31.80.0 /20? (Choose two.)

A. 172.31.92.0 /22
B. 172.31.51.16 /30
C. 172.31.80.0 /22
D. 172.31.17.4 /30

Answer: A,C

Explanation:
30 bits IP network has relatively small quantities of addresses available, which can not meet the requirements of network design.

QUESTION NO: 207

In the implementation of VLSM techniques on a network using a single Class C IP address, which subnet mask is the most efficient for point-to-point serial links?

A. 255.255.255.240
B. 255.255.255.254
C. 255.255.255.0
D. 255.255.255.252
E. 255.255.255.248

Answer: D

Explanation:
The subnet mask /30 is usually used for point-to-point serial links.

QUESTION NO: 208

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

QUESTION NO: 209

Which two subnetworks would be included in the summarized address of 172.31.80.0/20? (Choose two.)

A. 172.31.17.4/30
B. 172.31.51.16/30
C. 172.31.64.0/18
D. 172.31.80.0/22
E. 172.31.92.0/22
F. 172.31.192.0/18

Answer: D,E

Explanation:
We need to find the range for the 172.31.80.0/20 network. 1) Since this is a /20, convert the third octet to binary: 172.31.0101 0000.0 2) Segregate the network and host address: 172.31. 0101 0000 .0 3) The network address will be: 172.31.80.0 4) The broadcast address will be: [convert all the blue to one (1) plus the red colored] 172.31.95.255 That is now your range 172.31.80.0 - 172.31.95.255

QUESTION NO: 210

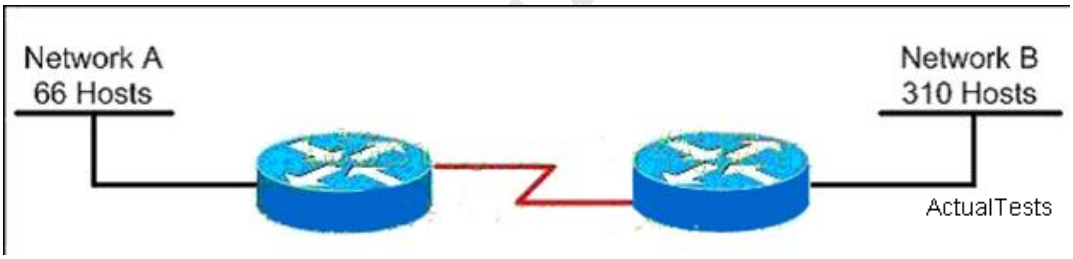
Given the address 192.168.20.19/28, which host addresses are valid on this subnet? (Choose two.)

A. 192.168.20.29
B. 192.168.20.31
C. 192.168.20.17
D. 192.168.20.0

Answer: A,C

QUESTION NO: 211

Refer to the exhibit. Which mask is correct to use for the WAN link between the routers that will provide connectivity while wasting the least amount of addresses?



A. /23
B. /24
C. /25
D. /30

Answer: D

QUESTION NO: 212

The network 172.25.0.0 has been divided into eight equal subnets. Which of the following IP addresses can be assigned to hosts in the third subnet if the ip subnet-zero command is configured on the router? (Choose three.)

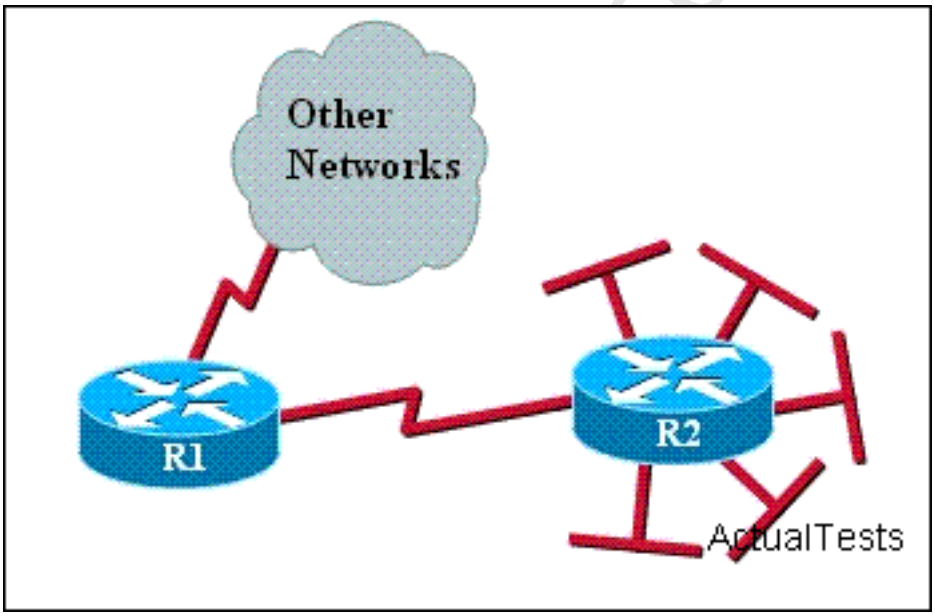
A. 172.25.78.243
B. 172.25.98.16
C. 172.25.72.0
D. 172.25.94.255
E. 172.25.96.17
F. 172.25.100.16

Answer: A,C,D

Explanation:
Section 6: Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment (8 questions)

QUESTION NO: 213

Refer to the exhibit. The networks connected to router R2 have been summarized as a 192.168.176.0/21 route and sent to R1. Which two packet destination addresses will R1 forward to R2? (Choose two.)



A. 192.168.194.160
B. 192.168.159.2
C. 192.168.183.41
D. 192.168.179.4
E. 192.168.183.255
F. 192.168.184.45

Answer: C,D

QUESTION NO: 214

You have a class B network with a 255.255.255.0 mask. Which of the statements below are true of this network? (Choose two)

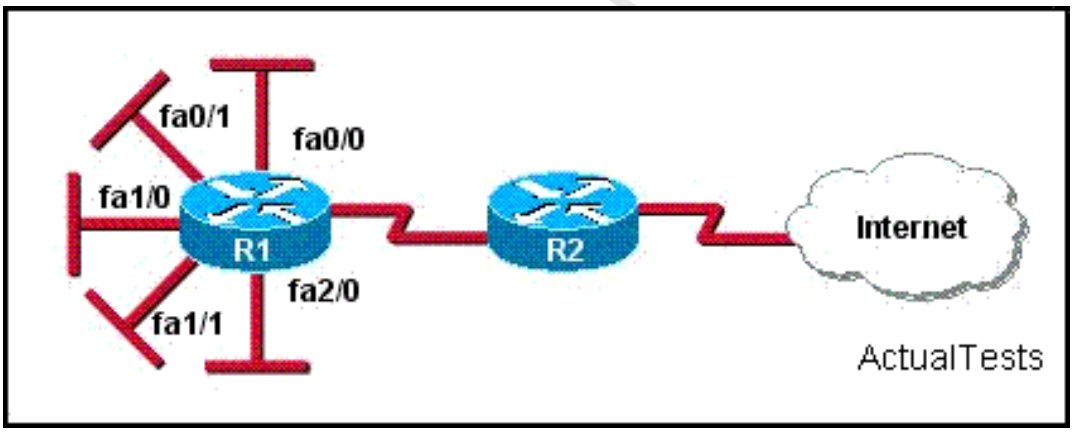
A. There are 24 usable hosts per subnet..
B. There are 254 usable subnets.
C. There are 256 usable hosts per subnet.
D. There are 254 usable hosts per subnet.

Answer: B,D

Explanation:
The mask 255.255.255.0 shows it limits the subnet range to 1-255. Since 255 is broadcast address, so the actual range is 254.

QUESTION NO: 215

The Ethernet networks connected to router R1 in the graphic have been summarized for router R2 as 192.1.144.0/20. Which of the following packet destination addresses will R2 forward to R1, according to this summary? (Choose two.)



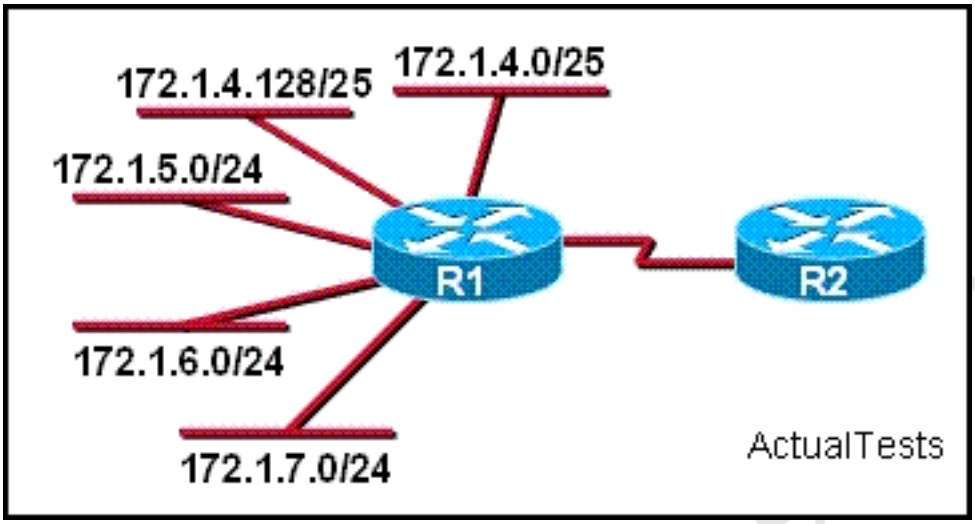
A. 192.1.1.144
B. 192.1.143.145
C. 192.1.160.11
D. 192.1.159.2
E. 192.1.151.254
F. 192.1.138.41

Answer: D,E

Explanation:
The summarized route is 192.1.144.0/20. 192.1.159.2 and 192.1.151.254 are in this range.

QUESTION NO: 216

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



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

Answer: E

Explanation:
When the subnet mask is /22, R1 can advertise its networks to R2.

QUESTION NO: 217

Assume that the subnet mask is /27 and subnet zero is usable, which three of the following IP addresses will be assigned to hosts? (Choose three.)

A. 10.15.32.17
B. 17.15.66.128
C. 66.55.128.1
D. 135.1.64.34

Answer: A,C,D

QUESTION NO: 218

A medium-sized company has a Class C IP address. It has two Cisco routers and one non-Cisco router. All three routers are using RIP version 1. The company network is using the block of 198.133.219.0/24. The company has decided it would be a good idea to split the network into three smaller subnets and create the option of conserving addresses with VLSM. What is the best course of action if the company wants to have 40 hosts in each of the three subnets?

A. Convert all the routers to EIGRP and use 198.133.219.32/27, 198.133.219.64/27, and 198.133.219.92/27 as the new subnetworks.
B. Maintain the use of RIP version 1 and use 198.133.219.32/27, 198.133.219.64/27, and 198.133.219.92/27 as the new subnetworks.
C. Convert all the routers to EIGRP and use 198.133.219.64/26, 198.133.219.128/26, and 198.133.219.192/26 as the new subnetworks.
D. Convert all the routers to RIP version 2 and use 198.133.219.64/26, 198.133.219.128/26, and 198.133.219.192/26 as the new subnetworks.
E. Convert all the routers to OSPF and use 198.133.219.16/28, 198.133.219.32/28, and 198.133.219.48/28 as the new subnetworks.
F. Convert all the routers to static routes and use 98.133.219.16/28, 198.133.219.32/28, and 198.133.219.48/28 as the new subnetworks.

Answer: D

QUESTION NO: 219

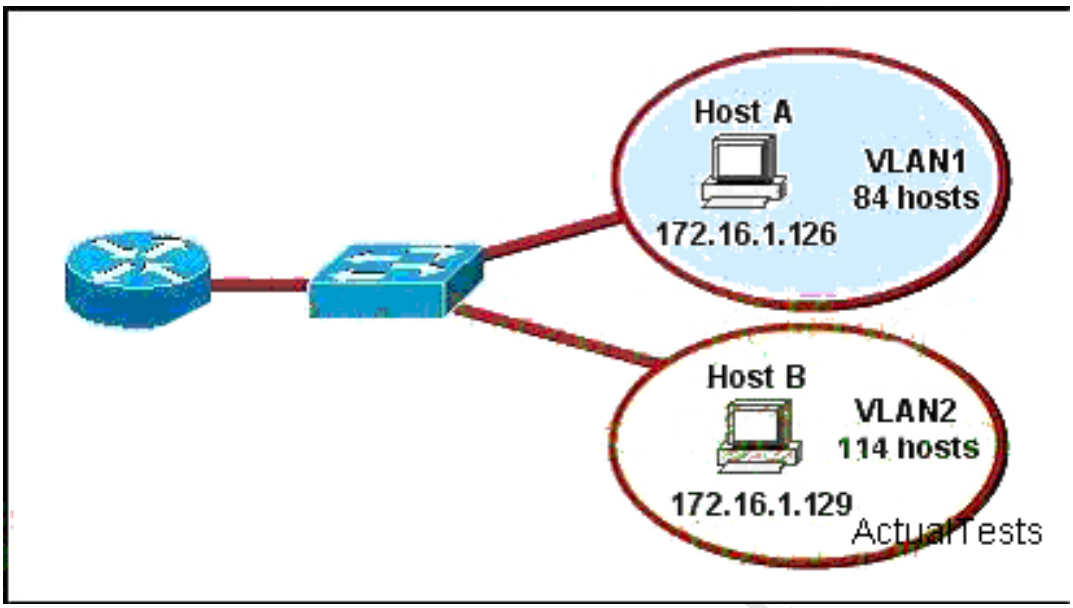
Which of the following IP addresses fall into the CIDR block of 115.64.4.0/22? (Choose three.)

A. 115.64.8.32
B. 115.64.7.64
C. 115.64.6.255
D. 115.64.3.255
E. 115.64.5.128
F. 115.64.12.128

Answer: B,C,E

QUESTION NO: 220

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:
Section 7: Describe the technological requirements for running IPv6 in conjunction with IPv4 (including: protocols, dual stack, tunneling, etc). (2 questions)

QUESTION NO: 221

Running both IPv4 and IPv6 on a router simultaneously is known as what?

A. 4to6 routing
B. 6to4 routing
C. binary routing
D. dual-stack routing

E. NextGen routing

Answer: D

Explanation:
One technique for transitioning to IPv6 is by using dual IPv4 and IPv6 protocol stacks. Using dual stacks enables gradual, one-by-one upgrades to applications running on nodes. Applications that are upgraded to IPv6 use the IPv6 protocol stack, and applications that are not upgraded and support only IPv4 can coexist with upgraded applications on the same node. New and upgraded applications can use both IPv4 and IPv6 protocol stacks. This approach is described in RFC 4213.

QUESTION NO: 222

What are three IPv6 transition mechanisms? (Choose three.)

A. 6to4 tunneling
B. VPN tunneling
C. GRE tunneling
D. ISATAP tunneling
E. PPP tunneling
F. Teredo tunneling

Answer: A,D,F

Explanation:
Section 8: Describe IPv6 addresses (5 questions)

QUESTION NO: 223

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

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

Answer: C

QUESTION NO: 224

Which two of these statements are true of IPV6 address representation? (Choose two)

A. A single interface may be assigned multiple IPV6 addresses of any type
B. Every IPV6 interface contains at least one loopback address.
C. Leading zeros in an IPV6 16 bit hexadecimal field are mandatory.
D. The first 64 bits represent the dynamically created interface ID

Answer: A,B

QUESTION NO: 225

Which two are correct about ipv6 addressing?

A. 2000::/3 is a global unicast address
B. cool.gif ther is only one loopback address ::1
C. FF00::/ is the Link-local address
D. FE00::/ is the unique-local address

Answer: A,B

QUESTION NO: 226

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

QUESTION NO: 227

Select the valid IPv6 addresses. (Choose all apply)

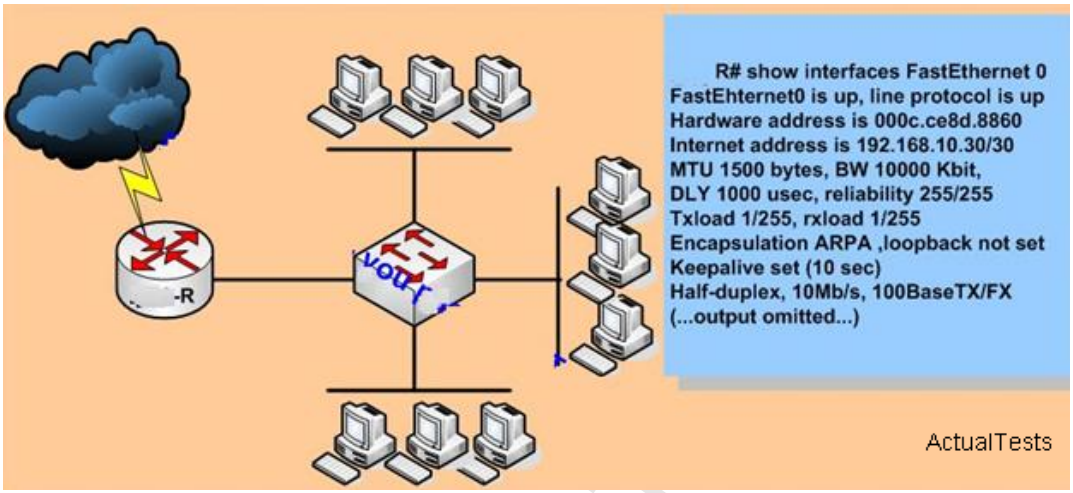
A. ::
B. ::192:168:0:1
C. 2002:c0a8:101::42
D. 2003:dead:beef:4dad:23:46:bb:101

Answer: A,B,C,D

Explanation:
Section 9: Identify and correct common problems associated with IP addressing and host configurations (5 questions)

QUESTION NO: 228

A router has been configured to provide the nine users on the branch office LAN with Internet access, as shown in the diagram. It is found that some of the users on the LAN cannot reach the Internet. Based on the topology and router output shown, which command should be issued on the router to correct the problem?



A. R(config-if)# no shutdown
B. R(config-if)# ip address 192.168.10.30 255.255.255.240
C. R(config-if)# no keepalive
D. R(config-if)# duplex full

Answer: B

Explanation:
From the above R information, we know that IP of Fa0/0 is 192.168.10.30/30. Because mask is 30 bit, it is not qualified for 9 users to access the Internet. Therefore, IP address of Fa0/0 should be reconfigured. The mask that saves address most is 28.

According to the output shown, the subnet mask assigned to the Fast Ethernet interface is /30, which will only allow for up to two hosts. Since there are 9 hosts depicted on the LAN, a subnet mask of /28 (255.255.255.240) will allow for up to 14 hosts.

QUESTION NO: 229

You work as a network technician. Please study the exhibit carefully. After configuring two interfaces on the router, the network administrator notices an error message. What must be done to fix this error?

```
Router# configure terminal
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 192.168.1.17 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface serial 0/0
Router(config-if)# ip address 192.168.1.65 255.255.255.240
Router(config-if)# no shutdown
/ 192.168.1.0 overlaps with FastEthernet0/0
```


A. The serial interface must use the address 192.168.1.2.
B. The subnet mask of the serial interface should be changed to 255.255.255.0.
C. The address of the FastEthernet interface should be changed to 192.168.1.66.
D. The subnet mask of the FastEthernet interface should be changed to 255.255.255.240.

Answer: D

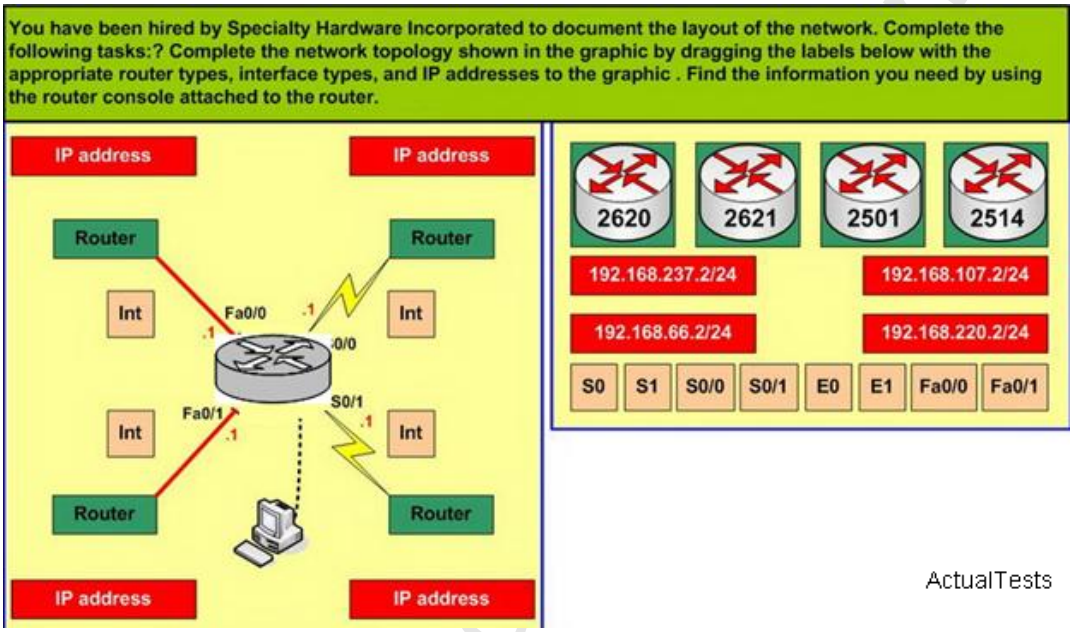
Explanation:
Cisco routers will not allow you to configure two interfaces that belong to the same IP subnet. In this case, by giving the serial 0/0 interface an IP address of 192.168.1.65, it would belong to this /28 subnet but it would also belong to the 192.168.1.17/24 subnet. You need to ensure that two interfaces are given IP addresses and subnet masks so that they belong to different subnets, and given the options only the option of changing the mask of the FE interface to an /28 will accomplish this.

/192.168.1.0 overlaps with FastEthernet0/0 indicates that the IP address repeated, because the 192.168.1.0 mask that Fa0/0 configured is 24 bits, the 28 bit IP of s0/0 192.168.1.0 is unusable.

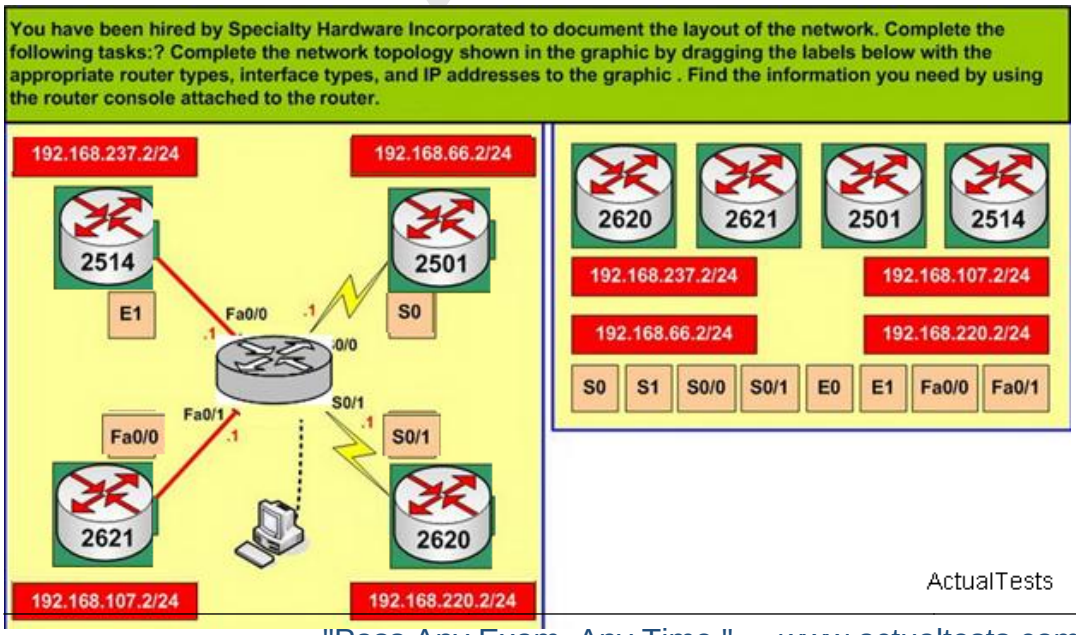
QUESTION NO: 230 DRAG DROP

```
router#show cdp neighbor
...
Device ID     Local Interface   Holdtme   Capability   Platform   Port ID
Birmingham    Fas 0/0           151       R S          2514       E1
Relmap        Fas 0/1           150       R S          2621       Fa0/0
Boaz          Ser 0/0           137       R S          2501       S0/1
Atlanta       Ser 0/1           126       R S          2620       S0/1
```

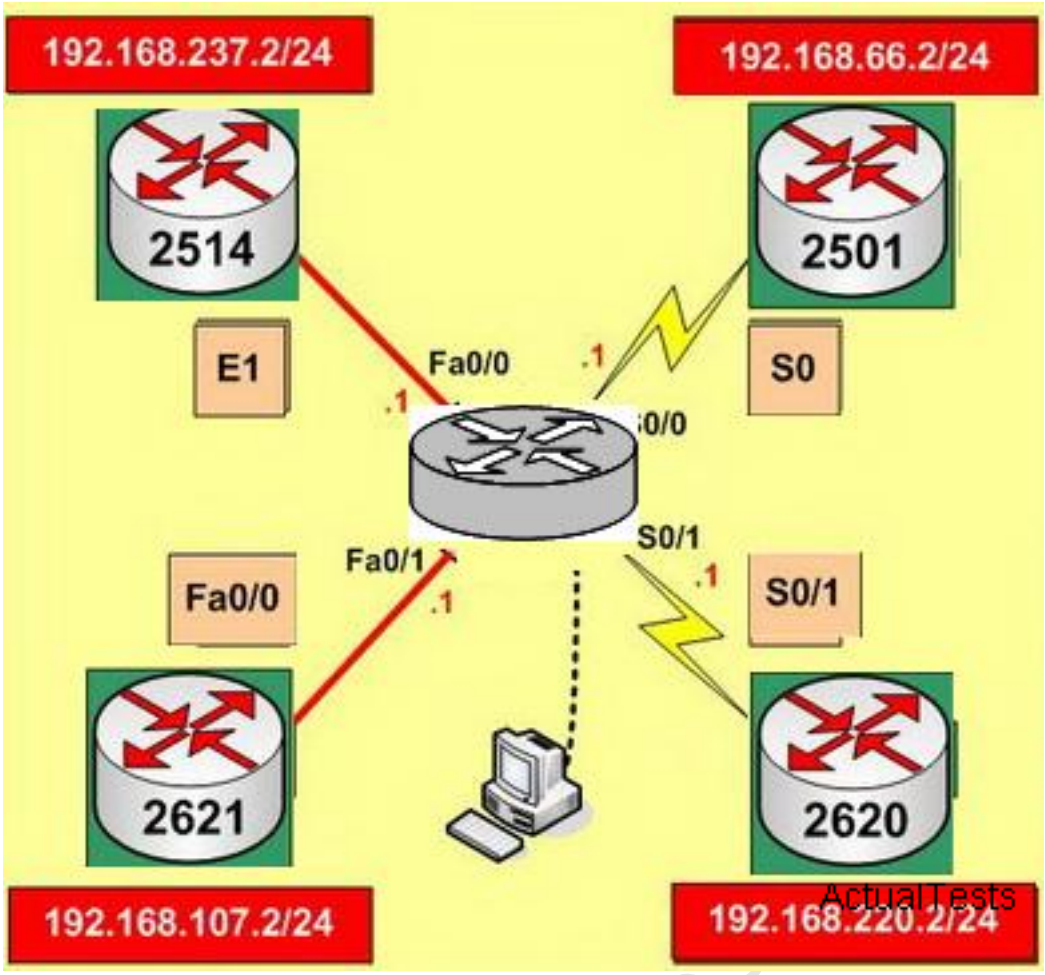
```
Router#show run
!
interface FastEthernet0/0
 ip address 192.168.237.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.107.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.168.66.1 255.255.255.0
!
interface Serial0/1
 ip address 192.168.220.1 255.255.255.0
!
```

Answer:

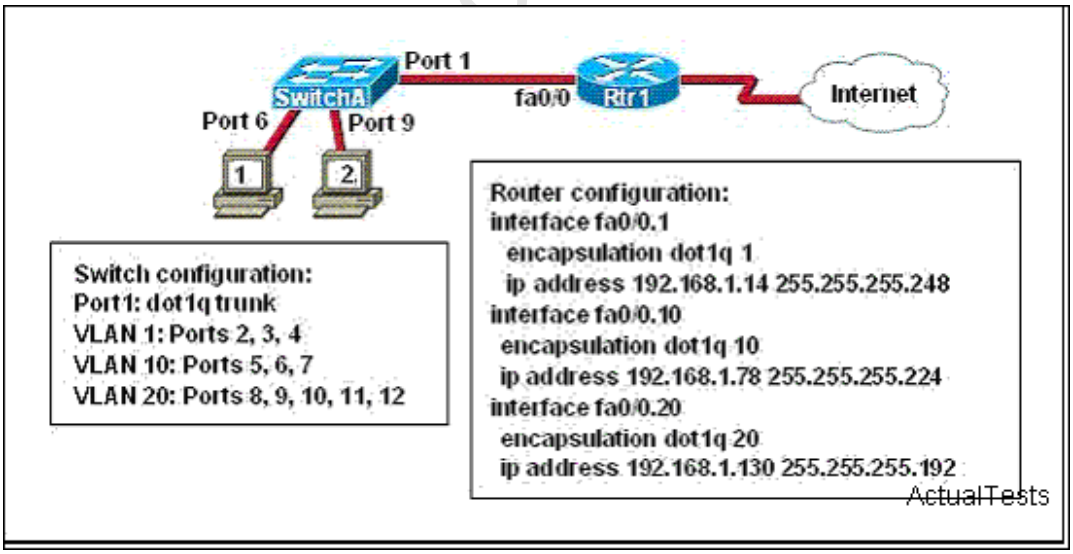


Explanation:



QUESTION NO: 231

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 1 IP address: 192.168.1.79

B. host 2 IP address: 192.168.1.128
C. host 2 default gateway: 192.168.1.129
D. host 2 IP address: 192.168.1.190
E. host 1 IP address: 192.168.1.64
F. host 1 default gateway: 192.168.1.78

Answer: A,D,F

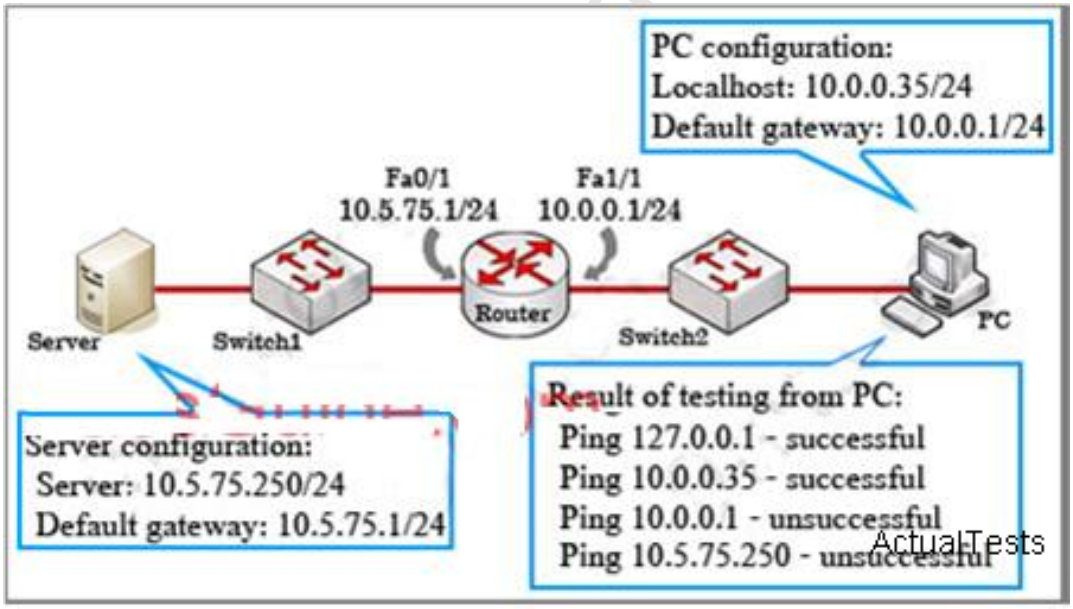
QUESTION NO: 232

While troubleshooting a connectivity issue from a PC you obtain the following information:

Local PC IP address: 10.0.0.35/24
Default Gateway: 10.0.0.1
Remote Sever: 10.5.75.250/24

You then conduct the following tests from the local PC:

Ping 127.0.0.1 - Successful
Ping 10.0.0.35 - Successful
Ping 10.0.0.1 - Unsuccessful
Ping 10.5.75.250 - Unsuccessful



What is the underlying cause of this problem?

A. A remote physical layer problem exists.
B. TCP/IP has not been correctly installed on the host.
C. The host NIC is not functioning.

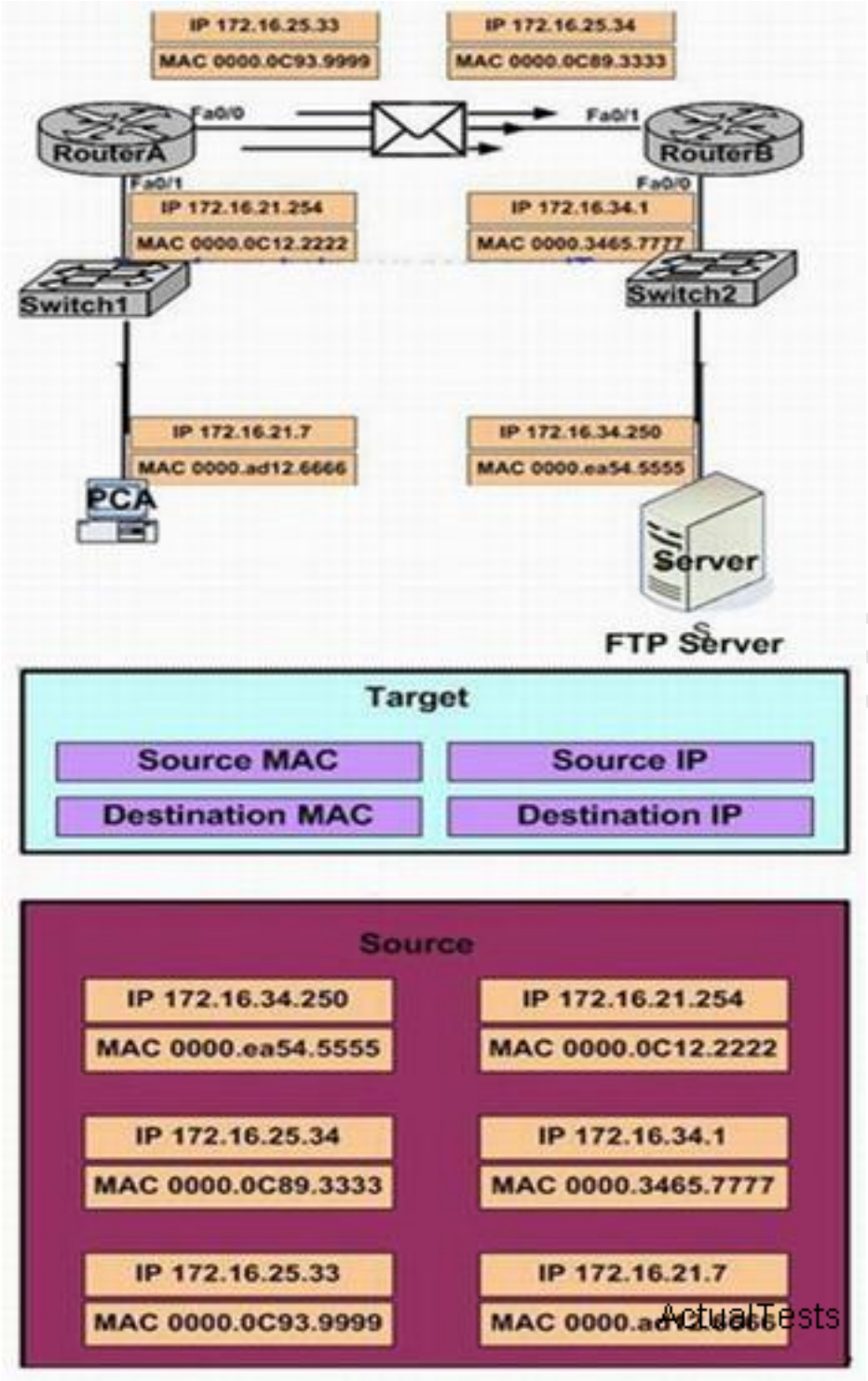
D. A local physical layer problem exists.

Answer: B

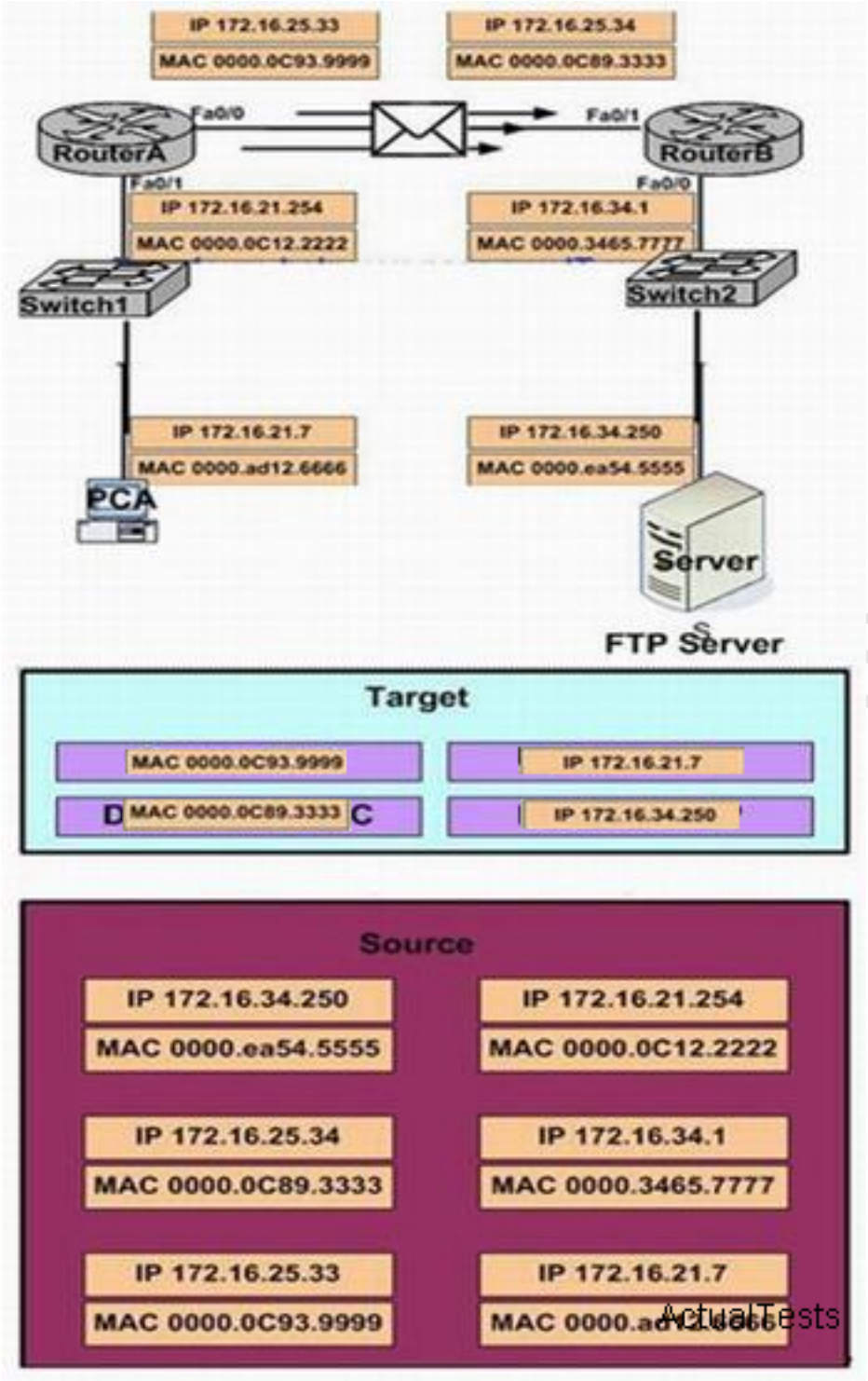
Explanation:
The configuration is correct. The output of the ping command indicates that the fault lies on the F0/0 port or between the host and the router.

QUESTION NO: 233 DRAG DROP

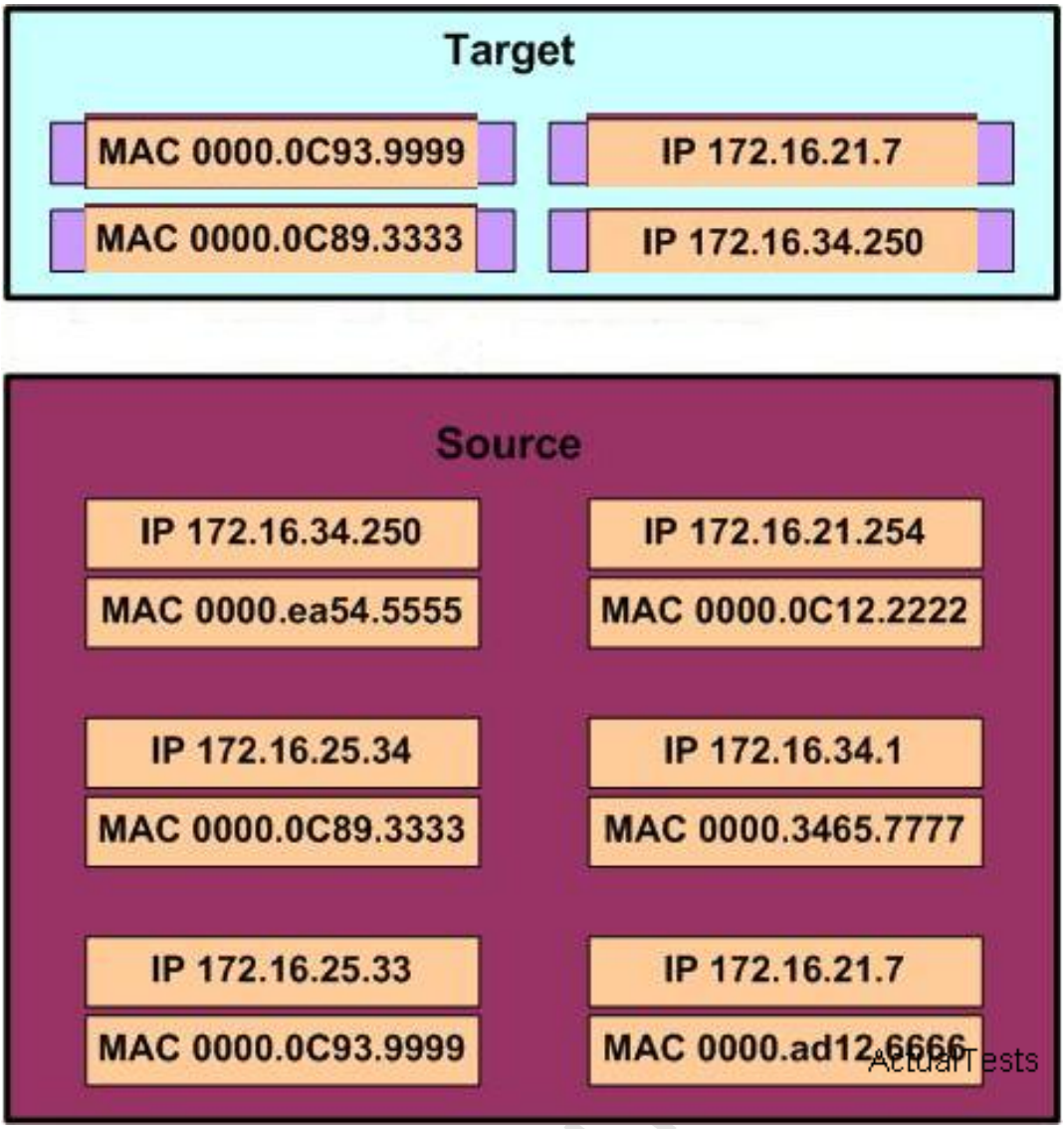
Refer to the exhibit. PCA is sending packets to the FTP server. Consider the packets as they leave out interface Fa0/0 forwards RouterB.Drag the correct frame and packet address to their place in the table.


IP 172.16.25.33
MAC 0000.0C93.9999
IP 172.16.25.34
MAC 0000.0C89.3333
RouterA
Fa0/0
Fa0/1
RouterB
Fa0/1
IP 172.16.21.254
MAC 0000.0C12.2222
Fa0/0
IP 172.16.34.1
MAC 0000.3465.7777
Switch1
Switch2
IP 172.16.21.7
MAC 0000.ad12.6666
IP 172.16.34.250
MAC 0000.ea54.5555
PCA
Server
FTP Server
Target
Source MAC
Source IP
Destination MAC
Destination IP
Source
IP 172.16.34.250
MAC 0000.ea54.5555
IP 172.16.21.254
MAC 0000.0C12.2222
IP 172.16.25.34
MAC 0000.0C89.3333
IP 172.16.34.1
MAC 0000.3465.7777
IP 172.16.25.33
MAC 0000.0C93.9999
IP 172.16.21.7
ActualTests

Answer:



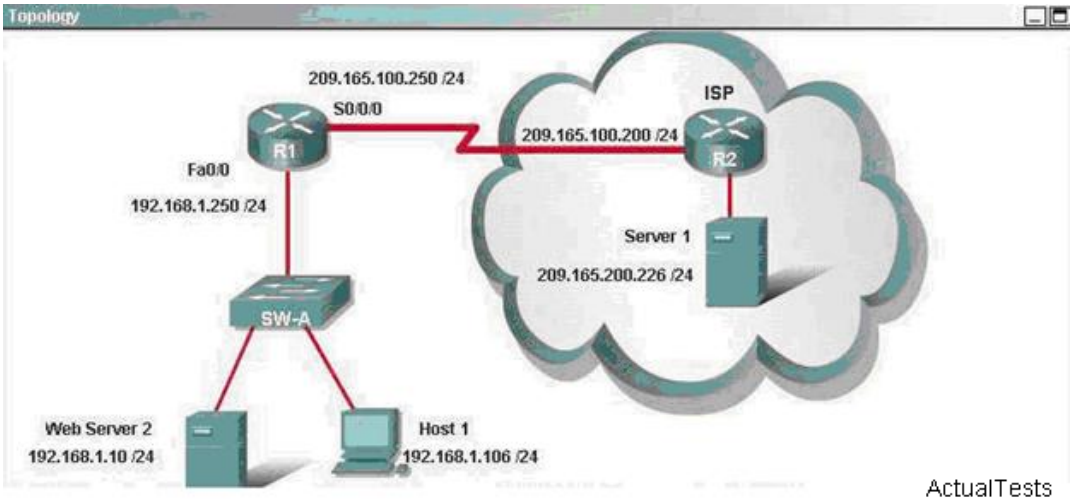
Explanation:



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

QUESTION NO: 234

When a packet is sent from Host 1 to Server1, in how many different frames will the packet be encapsulated as it is sent across the internetwork?



A. 1
B. 3
C. 7
D. 2
E. 0

Answer: B

QUESTION NO: 235

Refer to the exhibit. The partial frame in the graphic represents select header information within a frame arriving at a destination host. What can be determined from this information?

Destination	Source	Destination	Source	Destination	Source	SYN	ACK
000d.56ad.a313	000a.8a47.e612	192.168.14.1	192.168.14.2	23	42335	1	0

ActualTests

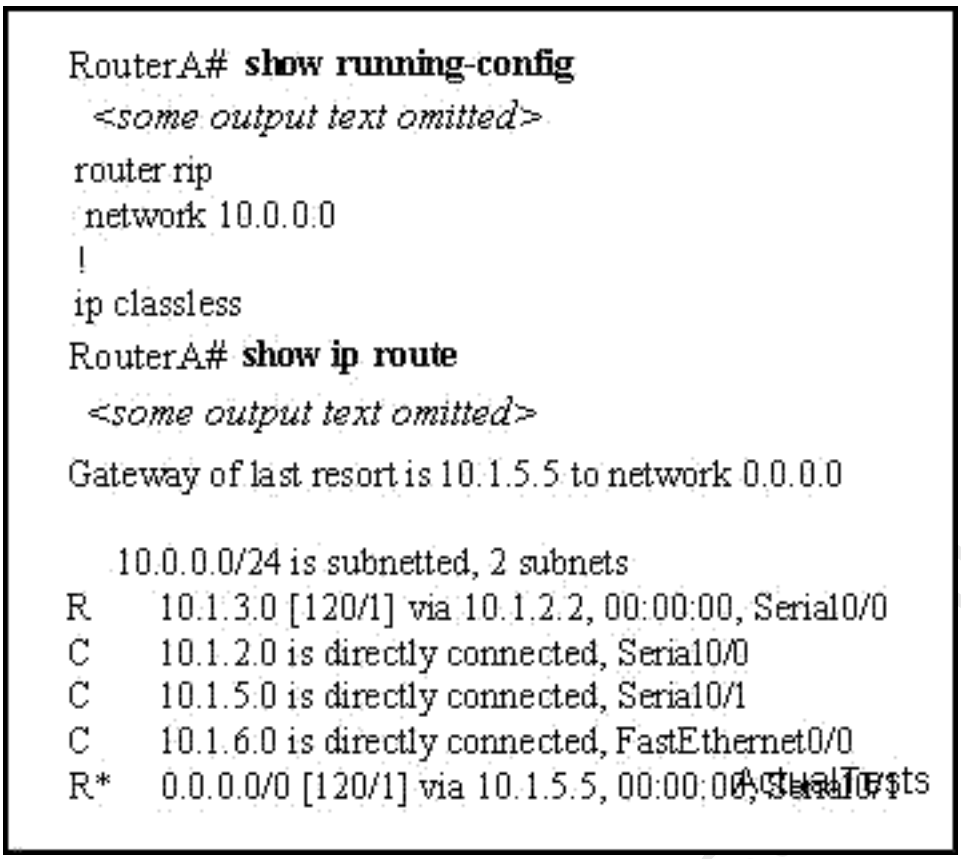
A. The source host is a Telnet server.
B. This frame contains the first segment in a Telnet session.
C. The local host has received 42,335 bytes from the remote host as a part of this conversation.
D. The Layer 2 address of the source host is 192.168.14.2.

Answer: B

Explanation:
From the chart above, we can may source and destination MAC, source and destination IP address, dialog port number, and so on. telnet port number is 23. so this is a frame information concerning TELNET.

QUESTION NO: 236

Refer to the output of the two show commands in the exhibit. If an administrator tries to ping host 10.1.8.5 from host 10.1.6.100, how will the ICMP packets be processed by Router A?



A. The packets will be routed out the Fa0/0 interface.
B. The packets will be routed out the S0/0 interface.
C. The packets will be discarded.
D. The packets will be routed out the S0/1 interface.

Answer: D

Explanation:
Since network 10.1.8.0 does not exist in the routing table, ICMP packet is then sent to default route port S0/1. Default route is a special static route, which will be used when no matching option can be found between the routing tables and package destination address. If there is no default route, the packet whose destination address finds no matching option in the routing table will be discarded. Default route is very effective at certain circumstances, when there is stub network, the default route will greatly simplify router configuration, reducing the workload of administrators and improving network performance. Only one single default route can be configured on Routers.

QUESTION NO: 237

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?

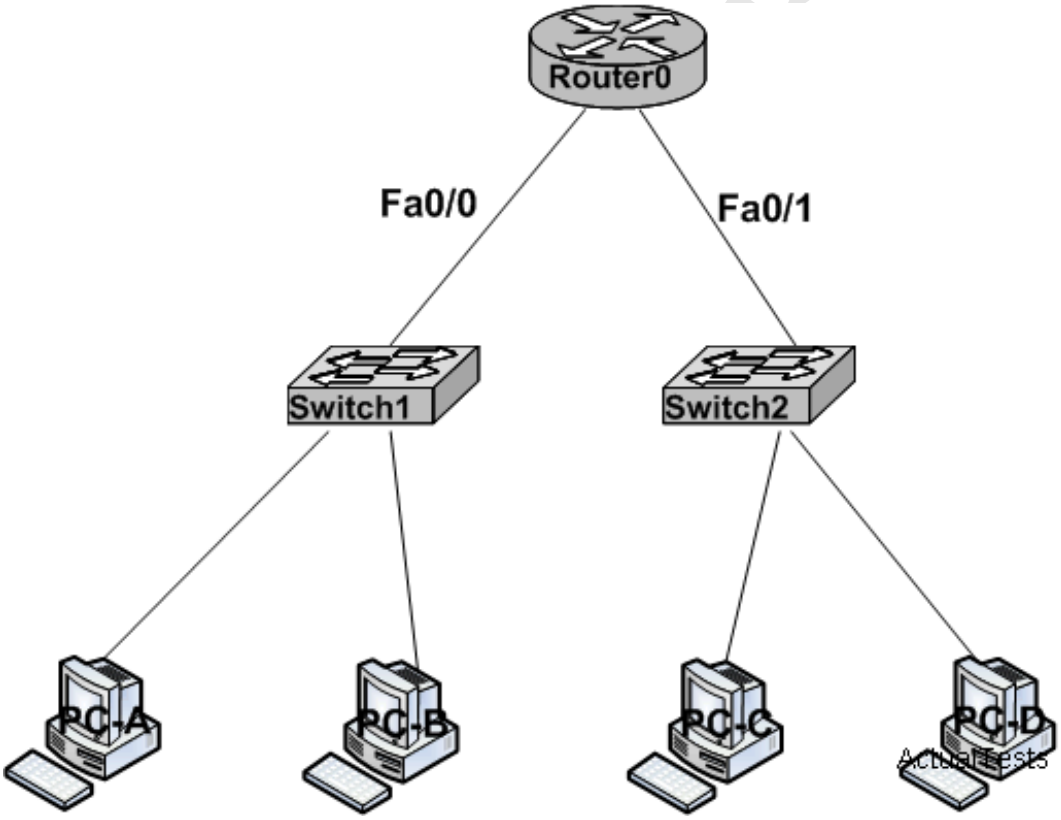
A. a static route to network 192.168.10.0/24 with a local serial interface configured as the next hop
B. a default route with a next hop address of 192.168.10.1
C. a static route to network 192.168.10.0/24
D. a RIP update for network 192.168.10.0/24
E. an OSPF update for network 192.168.0.0/16
F. a directly connected interface with an address of 192.168.10.254/24

Answer: F

Explanation:
Administrative distance refers to the reliability of one routing protocol. Each routing protocol is specified a reliability level from high to low depending on the administrative distance. For the routing information of two different routing protocols to the same destination, the router will make decision on the basis of the administrative distance.

QUESTION NO: 238

Refer to the exhibit. Both switches are using a default configuration. Which two destination addresses will PC-D use to send data to PC-A? (Choose two.)



A. the IP address of PC-A
B. the MAC address of PC-A
C. the MAC address of the Fa0/0 interface of the ROUTER0 router
D. the MAC address of the Fa0/1 interface of the ROUTER0 router

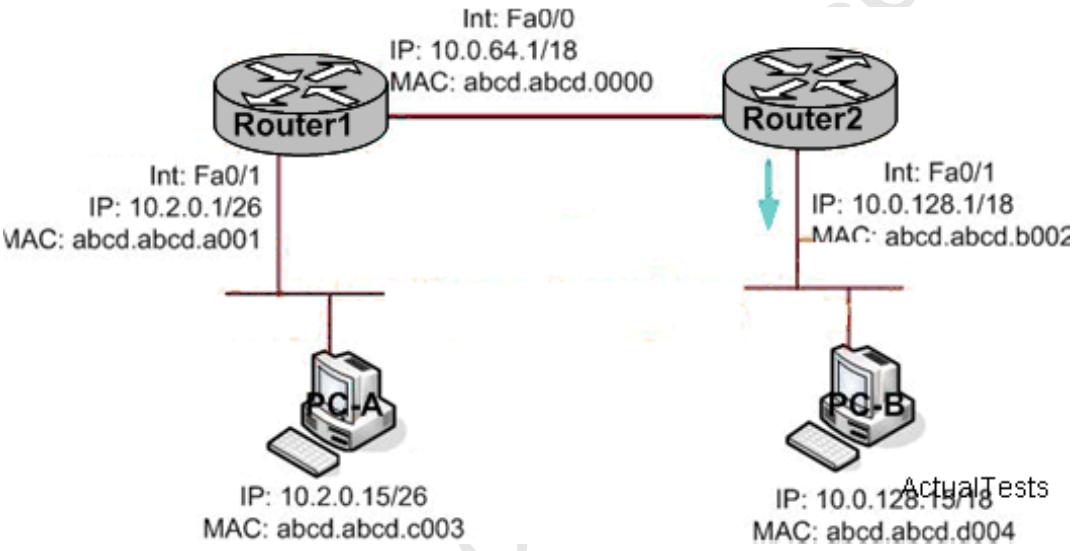
E. the IP address of PC-D
F. the MAC address of PC-D

Answer: A,D

Explanation:
When Host PC-D send data to Host PC-A, because it is communication across subnet, it is necessary to use router. Host PC-D launches ARP request to Router ROUTER0, because ROUTER0 is connected to network PC-A, thus responds to ARP, and use its own Fa0/1 as destination MAC address. So destination address is IP of PC-A, and MAC address is MAC of Fa0/1.

QUESTION NO: 239

Refer to the exhibit. Host PC-A pings Host PC-B. What source MAC address and source IP address are contained in the frame as the frame leaves Router2 destined for host PC-B?



A. abcd.abcd.b002
B. abcd.abcd.a001
C. 10.2.0.1
D. 10.2.0.15

Answer: A,D

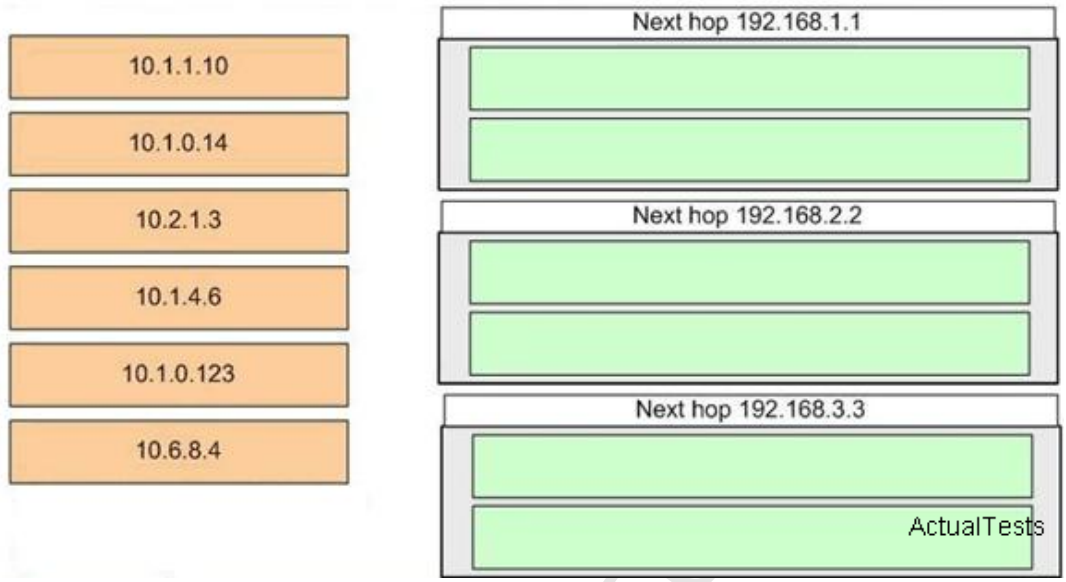
Explanation:
Host use ARP to learn the MAC address of other devices in current subnet, but a router is needed when forwarding to other subnet. Cisco IOS software uses a proxy ARP (RFC 1027) to inform host without routing information host MAC address of other networks or sub-net. Look at the Figure above, the router receives ARP request, if the requested host and host sending the ARP request are connected to different interface, and all the routes in routers heading for this host will pass through other interface, router will generate a proxy ARP response data packet, pointing out its own local MAC address. In this way, the host sends ARP request will send packets to the router,

which again will forward it to the destination host.

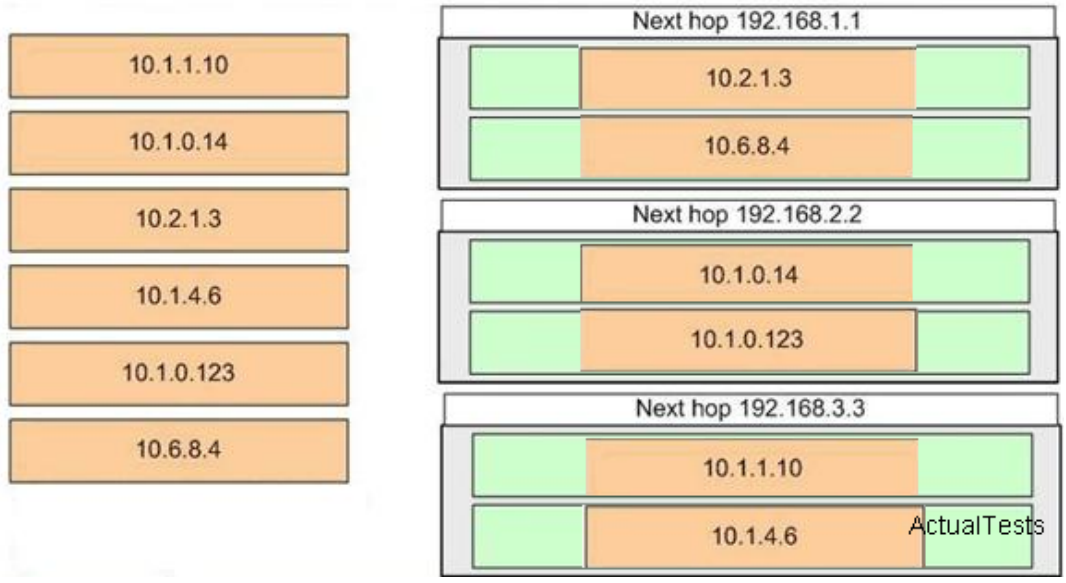
QUESTION NO: 240 DRAG DROP

Drag and Drop question. Drag the items to the proper locations.

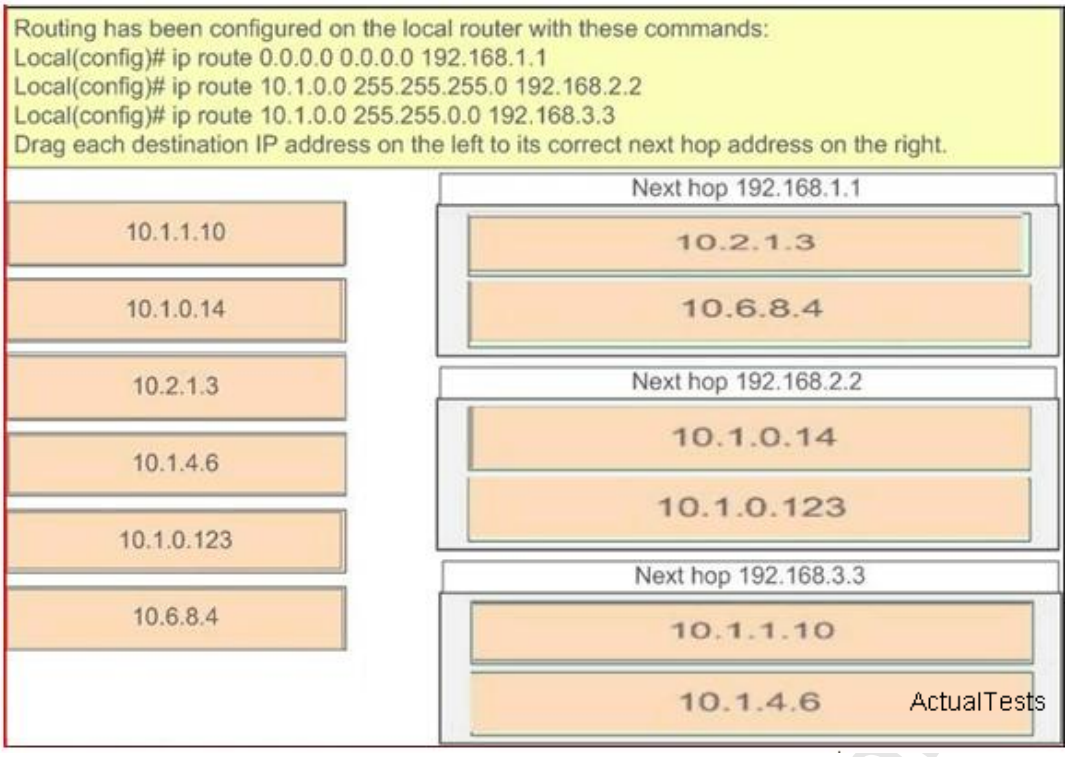
Routing has been configured on the local router with these commands:
Local(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
Local(config)# ip route 10.1.0.0 255.255.255.0 192.168.2.2
Local(config)# ip route 10.1.0.0 255.255.0.0 192.168.3.3
Drag each destination IP address on the left to its correct next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



Answer:

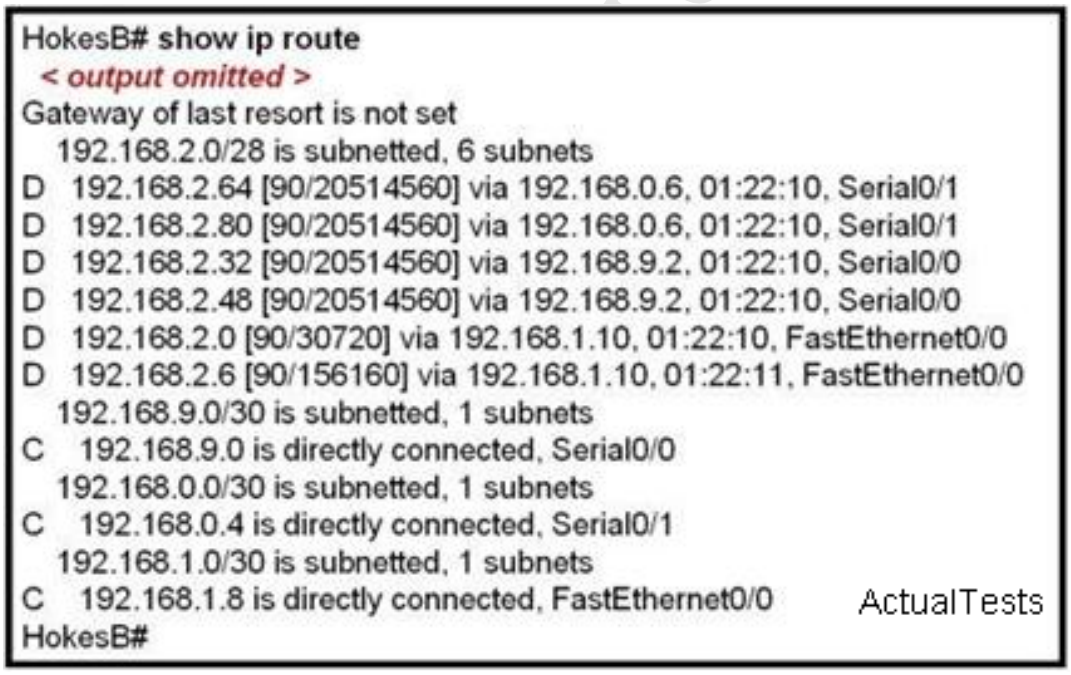


Explanation:



QUESTION NO: 241

Refer to the exhibit. A packet with a source IP address of 192.168.2.4 and a destination IP address of 10.1.1.4 arrives at the HokesB router. What action does the router take?



A. forwards the received packet out the Serial0/0 interface

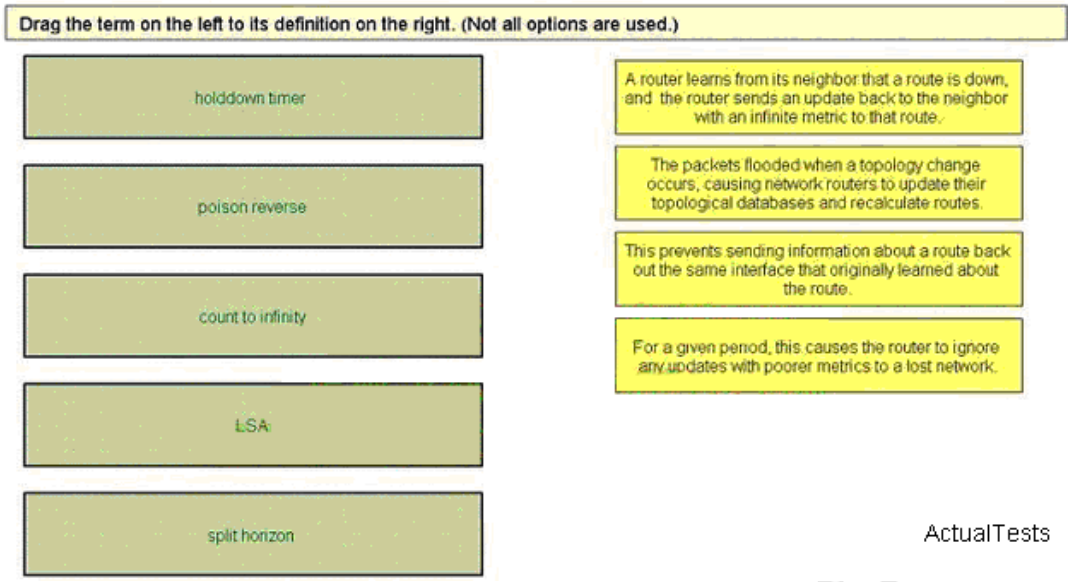
B. forwards a packet containing an EIGRP advertisement out the Serial0/1 interface

C. forwards a packet containing an ICMP message out the FastEthernet0/0 interface

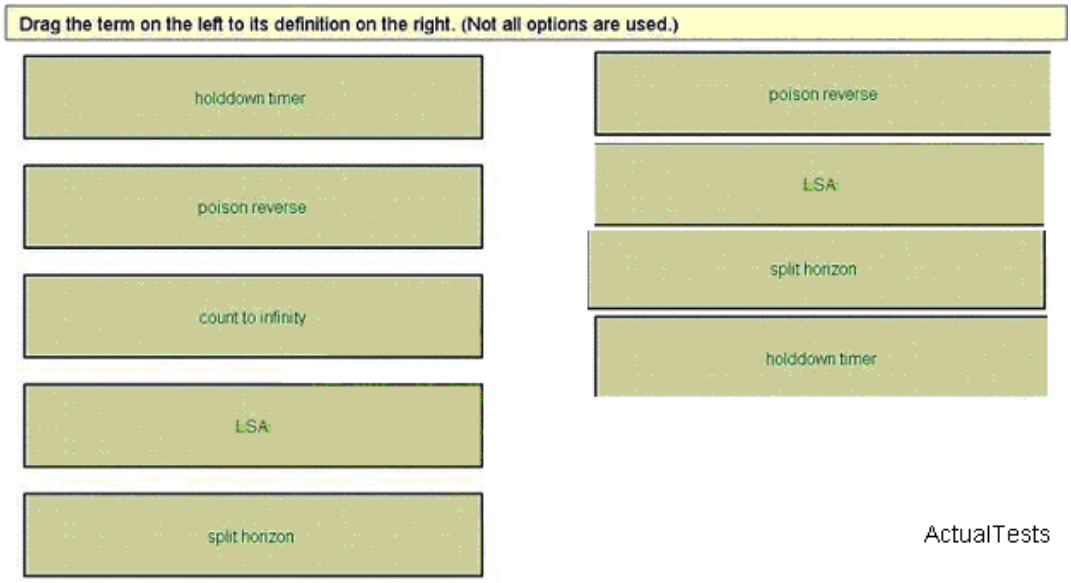
D. forwards a packet containing an ARP request out the FastEthernet0/1 interface

Answer: C

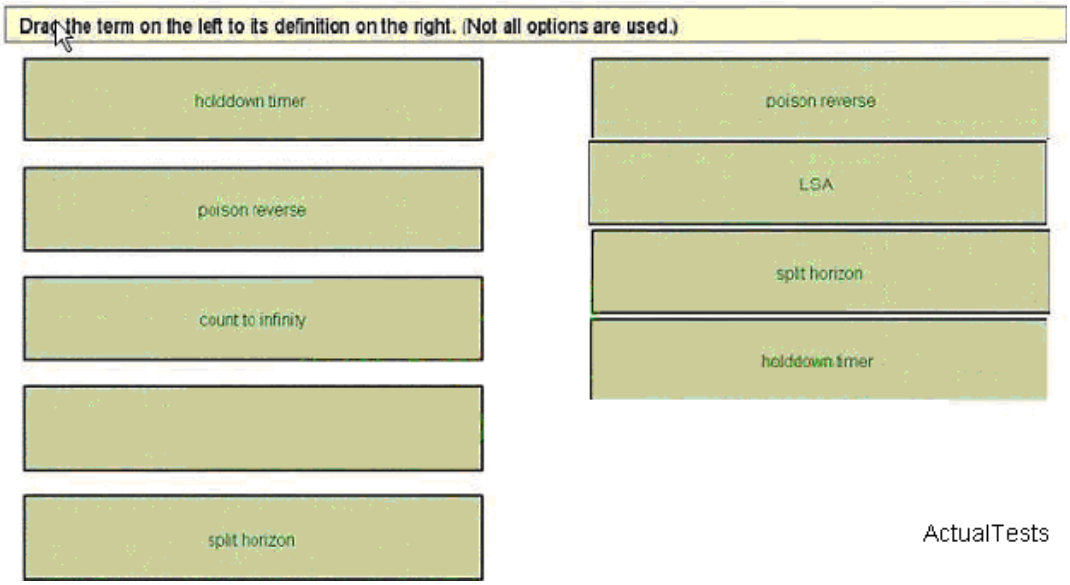
QUESTION NO: 242 DRAG DROP



Answer:



Explanation:



Section 2: Describe the operation of Cisco routers (including: router bootup process, POST, router components) (9 questions)

QUESTION NO: 243

As a CCNA candidate, you will be expected to know the POST process very well. 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 inspects the configuration file in NVRAM for boot instructions.
B. It attempts to boot from a TFTP server.
C. It loads the first image file in flash memory.
D. It checks the configuration register.

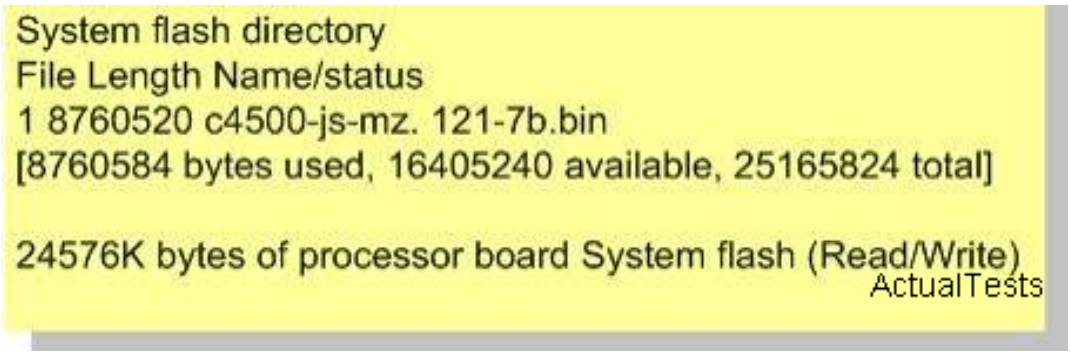
Answer: D

Explanation:
This question tests how a Cisco router is started.
Step 1 The router is booting.
Step 2 The router completes the POST process.
Step 3 The router finds and loads an IOS image.
Step 4 The router checks the configuration register and decides how to load start configuration based on the value of the configuration register.

QUESTION NO: 244

Refer to the graphic. A network associate is planning to copy a new IOS image into the router. This new image requires 8 MB of flash memory and 32 MB of RAM. How will the IOS proceed with the copy process?

Exhibit #sow flash:



A. The new IOS will be copied into flash memory and the current image will remain.
B. IOS will issue an error message because flash memory is not large enough to hold the new image.
C. The current IOS image must be manually erased before IOS will allow the new image to be copied.
D. During the copy process, the current IOS image will be erased.

Answer: A

Explanation:
According to the output shown above, the existing IOS is 8760520 bytes (8M) and the total size of the flash on this device is 24567K (24M). The new IOS only requires an additional 8 MB, so it will be copied on to the flash directly and both images will reside on the flash. The existing IOS is only overwritten it there is insufficient space to hold both.

Through the above chart we can see that the total space of current flash is 25 M , available space being 16 M , so 8M new image will be copied into the flash, while the original image will be preserved.

QUESTION NO: 245

During startup, the router displays the following error message:

boot: cannot open "flash:"

What will the router do next?

A. It will attempt to locate the configuration file from a TFTP server. If this fails, it will initiate the setup dialog.
B. It will attempt to locate the configuration file from a TFTP server. If this fails, it will load a limited configuration fromROM.
C. It will attempt to locate the IOS from a TFTP server. If this fails, it will load a limited IOS fromROM.

D. Because of damaged flash memory, the router will fail the POST.
E. It will attempt to locate the IOS from a TFTP server. If this fails, it will initiate the setup dialog.

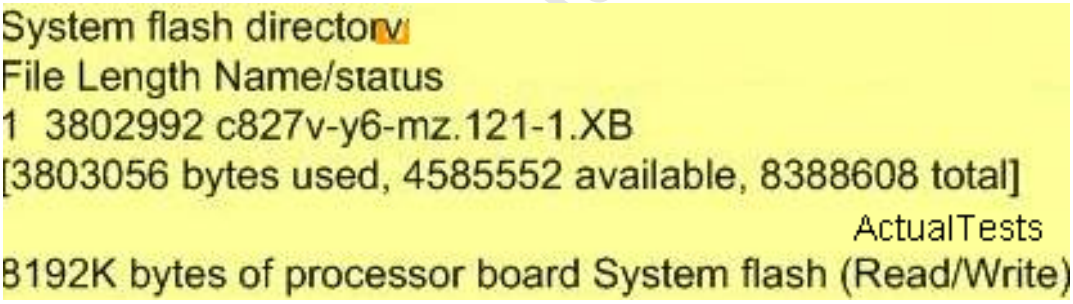
Answer: C

Explanation:
The boot sequence of a Cisco router is shown below:
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. 6. If no IOS can be loaded, the router will get the partial IOS version from ROM

Reference: http://www.svrops.com/svrops/documents/ciscoboot.htm

QUESTION NO: 246

Router#show flash exhibit:



Refer to the exhibit. 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. 5 MB
C. 7 MB
D. 4 MB

Answer: D

Explanation:
Based on the output provided, the total amount of flash memory available is 8388608 bytes (8 MB), but the existing IOS is using up 3803056 bytes (3 MB), so in order to fit both IOS files into the flash the new image must be no greater than the amount of available memory, which is 4585552 bytes (4 MB).

QUESTION NO: 247

There are no boot system commands in the router configuration in NVRAM router. What is the fallback sequence that the router will use to find an IOS during reload?

A. TFTP server, Flash, NVRAM
B. ROM, NVRAM, TFTP server
C. NVRAM, TFTP server, ROM
D. Flash, TFTP server, ROM

Answer: D

Explanation:
Cisco routers can boot Cisco IOS software from these locations:
1. Flash memory
2. TFTP server
3. ROM (not full Cisco IOS)
Multiple source options provide flexibility and fallback alternatives
Locating the Cisco IOS Software
Default boot sequence for Cisco IOS software:
1. NVRAM
2. Flash (sequential)
3. TFTP server (network boot)
4. ROM (partial IOS)
Note: boot system commands can be used to specify the primary IOS source and fallback sequences.
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.

6. If no IOS can be loaded, the router will get the partial IOS version from ROM
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 0x102 to 0x10F to look in NVRAM) - check the startup-config file in NVRAM for boot-system commands (normally there aren't any) - load IOS from Flash.
Boot System Commands
Router(config)# boot system flash IOS filename - boot from FLASH memory Router(config)# boot system tftp IOS filename tftp server ip address - boot from a TFTP server
Router(config)# boot system rom - boot from system ROM
Configuration Register Command
Router(config)# config-register 0x10x (where that last x is 0-F in hex)
When the last x is:
0 = boot into ROM Monitor mode
1 = boot the ROM IOS
2 - 15 = look in startup config file in NVRAM

QUESTION NO: 248

What will a new router do during startup if a configuration file is not located in NVRAM?

A. It will search for the configuration file in flash and if no configuration file is found there, it will enter the setup dialog.
B. It will search for the configuration file on a TFTP server and if no configuration file is found there, it will load a limited configuration file fromROM.
C. It will search for the configuration file on a TFTP server and if no configuration file is found there, it will enter the setup dialog.

D. It will search for the configuration file in flash and if no configuration file is found there, it will load a limited configuration file fromROM.

Answer: C

Explanation:
When a router boots and is able to locate the IOS it begins to load the configuration file. The configuration file, saved in NVRAM, is loaded into main memory and executed one line at a time. These configuration commands start routing processes, supply addresses for interfaces, and set media characteristics. If no configuration file exists in NVRAM, the router attempts a network boot and sends a broadcast request for the file on a TFTP server. If this is also not found, the operating system executes a question-driven initial configuration routine called the system configuration dialog.

QUESTION NO: 249

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

```
Router1> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-J-M), Experimental Version 11.3(19970915:164752)
[hampton-nitro-baseline 249]
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Wed 08-Oct-97 06:39 by hampton
Image text-base: 0x60008900, data-base: 0x60B98000

ROM: System Bootstrap, Version 11.1(11855) [beta 2], INTERIM SOFTWARE
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE (fc1)

Router1 uptime is 23 hours, 33 minutes
System restarted by abort at PC 0x6022322C at 10:50:55 PDT Tue Oct 21 1997
System image file is "tftp://172.16.1.129/hampton/nitro/c7200-j-mz"

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

<output omitted>

Configuration register is 0x2102                                ActualTests
```

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

Answer: A,B

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.
6. If no IOS can be loaded, the router will get the partial IOS version from ROM

QUESTION NO: 250

A network administrator changes the configuration register to 0x2142 and reboots the router. What are two results of making this change? (Choose two.)

A. The IOS image will be ignored.
B. The router will prompt to enter initial configuration mode.
C. The router will boot toROM.
D. Any configuration entries in NVRAM will be ignored.
E. The configuration in flash memory will be booted.

Answer: B,D

QUESTION NO: 251

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:
Section 3: Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts (2 questions)

QUESTION NO: 252

Refer to the exhibit. What could be possible causes for the "Serial0/0 is down" interface status? (Choose two.)

A. The bandwidth is set too low.
B. An incorrect cable is being used.
C. A Layer 1 problem exists.
D. A protocol mismatch exists.

Answer: B,C

Explanation:

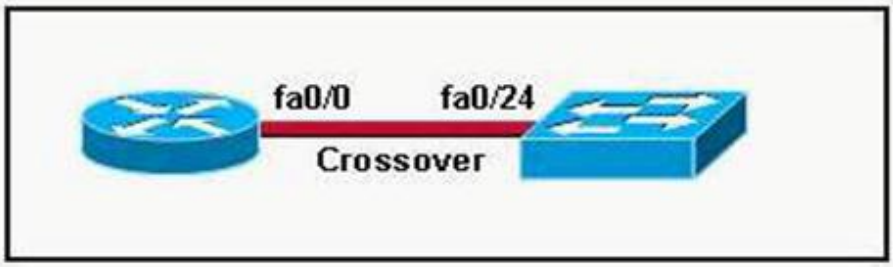
Status Line Condition	Possible Problem	Solution
Serial *x* is up, line protocol is up	—	This is the proper status line condition. No action is required.
Serial *x* is down, line protocol is down (DTE mode)	The router is not sensing a CD signal (that is, the CD is not active). A telephone company problem has occurred—line is down or is not connected to CSU[3]/DSU[4]. Cabling is faulty or incorrect. Hardware failure has occurred (CSU/DSU).	1. Check the LEDs on the CSU/DSU to see whether the CD is active, or insert a breakout box on the line to check for the CD signal. 2. Verify that you are using the proper cable and interface (see your hardware installation documentation). 3. Insert a breakout box and check all control leads. 4. Contact your leased-line or other carrier service to see whether there is a problem. 5. Swap faulty parts. 6. If you suspect faulty router hardware, change the serial line to another port. If the connection comes up, the previously connected interface has a problem.

Reference: http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1915.htm

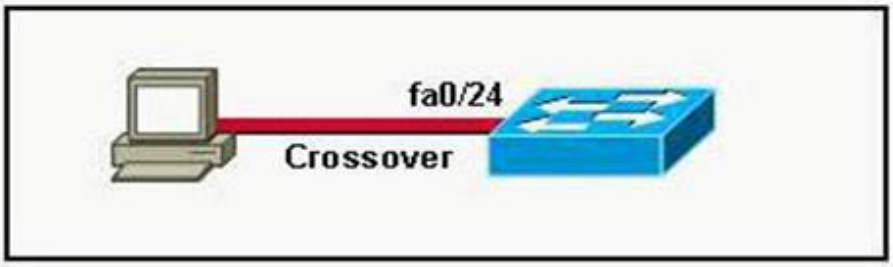
QUESTION NO: 253

Which two topologies are using the correct type of twisted-pair cables? (Choose two.)
Please refer to the exhibit.

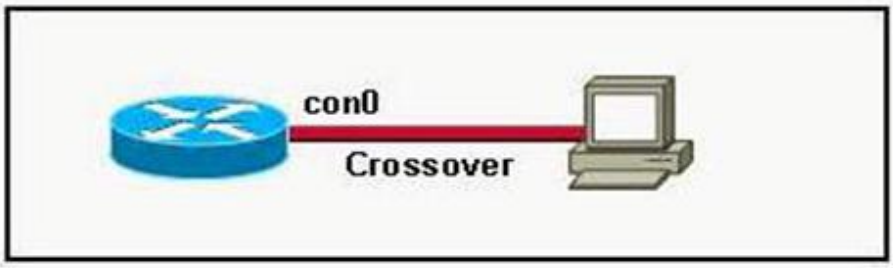
☐ A.



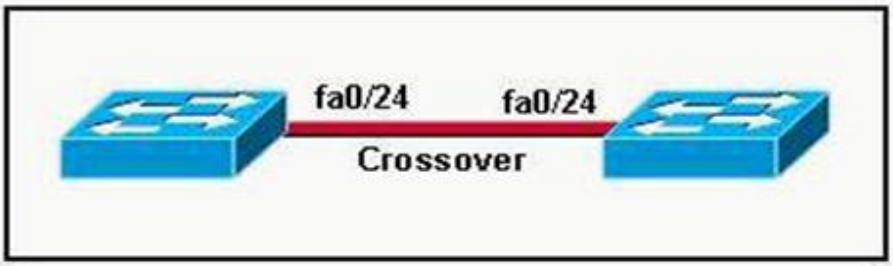
☐ B.



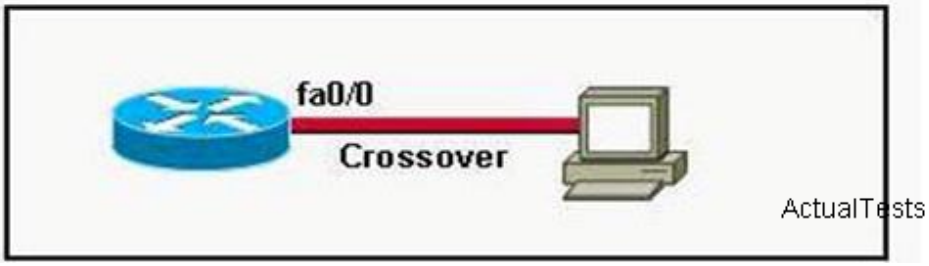
☐ C.



☐ D.



☐ E.



A. A

B. B

C. C

D. D

E. E

Answer: D,E

Explanation:
Section 4: Configure, verify, and troubleshoot RIPv2 (13 questions)

QUESTION NO: 254

The Company WAN is migrating from RIPv1 to RIPv2. Which three statements are correct about RIP version 2? (Choose three)

A. It is a classless routing protocol.
B. It supports authentication.
C. It has a lower default administrative distance than RIP version 1.
D. It uses broadcasts for its routing updates.
E. It has the same maximum hop count as version 1.

Answer: A,B,E

Explanation:
RIPV2 has the maximum hop count as RIPV1(15).
RIPV2 uses multicast for its routing updates while RIPV1 uses broadcast for its routing updates.
RIPV2 has a higher security than RIPV1 because RIPV2 supports authentication.
RIPV2, rather than RIPV1, sends the subnet mask in updates.

RIPV1 is a classful routing protocol , it sends update packets which does not contain subnet mask information every 30 seconds , it does not support VLSM and performs border automatic route summary by default, it can't be shut down, so it does not support non-consecutive networks and authentication, it uses hop counts as metric, the administrative distance is 120. Each packet contains 25 routing information at most , and routing update is broadcast.
RIPV2 is a classless routing protocol, whose transmitted packets contain subnet mask information , it supports VLSM and enables the function of auto-summary . So , it is needed to manually shut down the function of auto-summary in order to send subnet information to the main network .
RIPV2 only supports summarizing routing to the main network instead of summarizing different main networks. So it does not support CIDR. RIPV2 updates routing by use of the multicast address 224.0.0.9, only the corresponding multicast MAC address can reply to packets. Whether reply to packets and support authentication or not can be distinguished at the MAC layer.
Note : Refer to the classful routing protocol, when the subnet of the interface sending routing packets is in the same main network as the subnet associated with the packets, the router can transmit subnet information through this interface assuming that the interface and the subnet of packets use the same subnet mask.
What is the consecutive subnet:

Consecutive subnets belong to the same main network and use the same subnet mask, otherwise it is not. Using the manual summary command on the interface: ip summary-address rip to summarize subnet and subnet mask . RIP uses UDP(User Datagram Protocol)520 port to transmit routing update packets .

QUESTION NO: 255

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local area networks. What is the default routing update period for RIPv2?

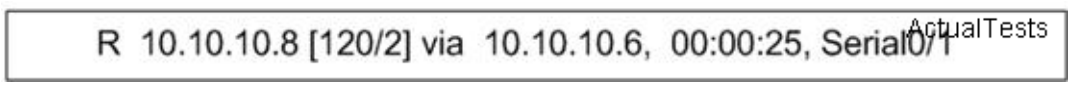
A. 180 seconds
B. 30 seconds
C. 240 seconds
D. 15 seconds

Answer: B

Explanation:
The fact that RIP only records one route for each destination requires RIP to actively maintain the integrity of the routing tables, which can be achieved by asking all active RIP routers to broadcast contents of routing table to adjacent RIP routers in a fixed time interval. All received updated information automatically replaces the information included in the routing table.
RIP maintains routing table depending on three timers.
Update timer.
Routing-timeout timer.
Routing-refresh timer.
Update timer can be used to update initialized routing table on a node. Each RIP node only uses one update timer. On the contrary, both routing-timeout timer and routing-refresh timer are that each router maintains one.
RIP router triggers update every 30 seconds . Update timer is used to record the amount of time. Once the time is up, RIP node will produce a series of datagrams including its own routing table. These datagrams are broadcast to each adjacent node. Therefore, each RIP router will receive update about every 30 seconds from each RIP adjacent node.

QUESTION NO: 256

The following output was shown on router1:



Based on the information shown above, what can be determined from the line of show ip route output shown in the exhibit? (Choose two)

A. This route is using the default administrative distance.
B. The 10.10.10.8 network is two hops away from this router.
C. The IP address 10.10.10.6 is configured on S0/1.
D. The next routing update can be expected in 35 seconds.

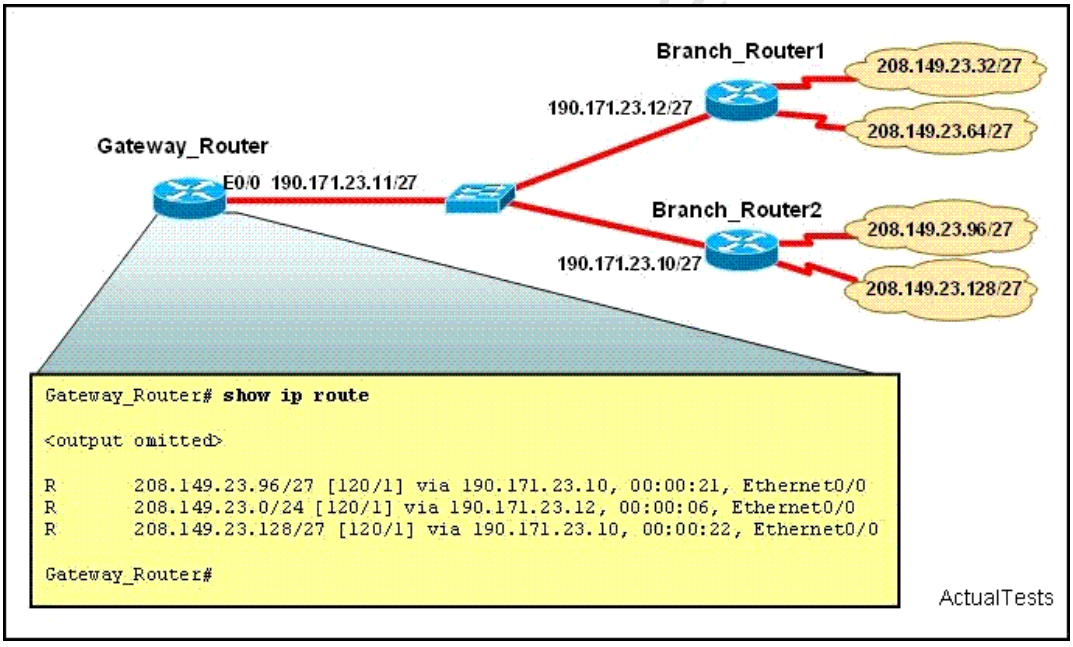
Answer: A,B

Explanation:
The 120 in the RIP route is administrative distance; 2 is metric value, i.e. the route pass through 2 routers.

When issuing the "show ip route" command, the first number in the brackets is the administrative distance of the information source; the second number is the metric for the route. In this case, the value of 120 is the default AD for RIP routes, and the 2 represents the metric, which is the number of router hops in RIP. The 10.10.10.6 IP address belongs to the neighboring router (not the local router) that sent the update in via Serial 0/1.

QUESTION NO: 257

Refer to the exhibit. What is the most likely reason for the disparity between the actual network numbers at the branches and the routes in the routing table on Gateway_Router?



A. Gateway_Router is configured to only receive RIPv2 updates.
B. Branch_Router2 is configured to send both RIPv1 and RIPv2 updates.
C. Gateway_Router is configured to receive only RIPv1 updates.
D. Branch_Router1 is configured to only send RIPv1 updates.

Answer: D

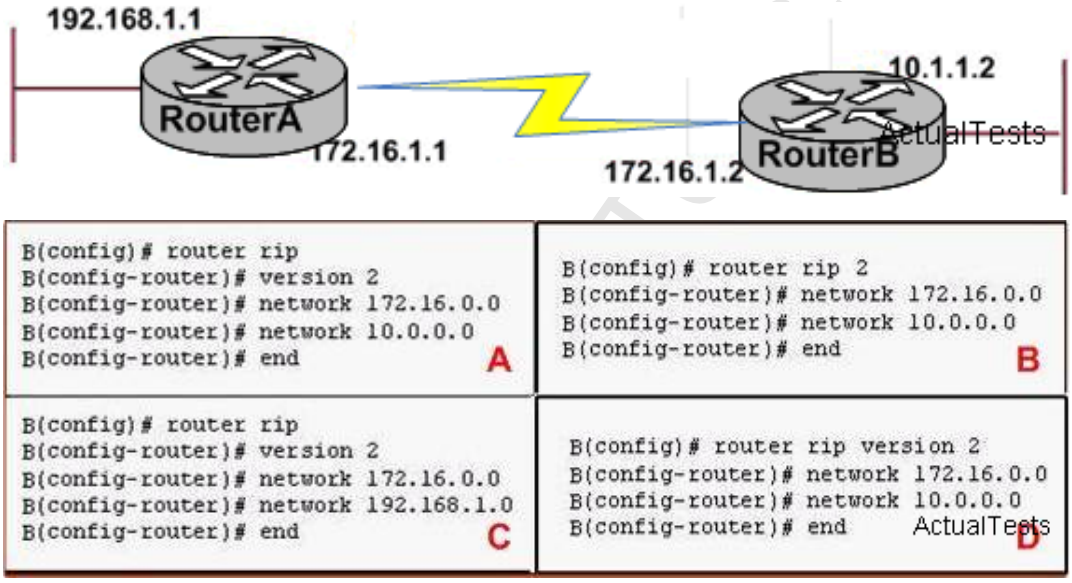
Explanation:
The default version of RIP is version 1, which doesn't supports multicast updates, classless networks, and authentication. It appears that Branch_router1 is configured with RIP v1 so it's sending only v1 packets, which means only the classful network of 208.149.23.0/24 is being advertised. However, it appears that Branch_router2 is indeed using RIPv2 as both the /27 networks are being advertised from that router.

If you wish to enable to RIP version 2 on router use following command:

Router(Config)#router rip
Router(Config-router)#version 2

QUESTION NO: 258

Refer to the exhibit. Router A has interfaces with addresses 192.168.1.1 and 172.16.1.1. Router B, which is connected to router A over a serial link, has interfaces with address 172.16.1.2 and 10.1.1.2. Which sequence of commands will configure RIPv2 on router B?



A. A
B. B
C. C
D. D

Answer: A

Explanation:
The Routing Information Protocol (RIP) is a relatively old, but still commonly used, interior gateway protocol (IGP) created for use in small, homogeneous networks. It is a classical distance-vector routing protocol. RIP is documented in RFC 1058.
RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information.

The Cisco IOS software sends routing information updates every 30 seconds; this process is termed advertising. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the non-updating router as being unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the non-updating router. The metric that RIP uses to rate the value of different routes is hop count. The hop count is the number of routers that can be traversed in a route. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This small range of metrics makes RIP an unsuitable routing protocol for large networks.

If the router has a default network path, RIP advertises a route that links the router to the pseudonetwork 0.0.0.0. The network 0.0.0.0 does not exist; RIP treats 0.0.0.0 as a network to implement the default routing feature. The Cisco IOS software will advertise the default network if a default was learned by RIP, or if the router has a gateway of last resort and RIP is configured with a default metric.

RIP sends updates to the interfaces in the specified networks. If an interface's network is not specified, it will not be advertised in any RIP update.

Cisco's implementation of RIP Version 2 supports plain text and MD5 authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

Enable RIP

To enable RIP, use the following commands, starting in global configuration mode:

Step	Command	Purpose
1	router rip	Enable a RIP routing process, which places you in router configuration mode.
2	network network-number	Associate a network with a RIP routing process.

Because RIP is normally a broadcast protocol, in order for RIP routing updates to reach nonbroadcast networks, you must configure the Cisco IOS software to permit this exchange of routing information. To do so, use the following command in router configuration mode:

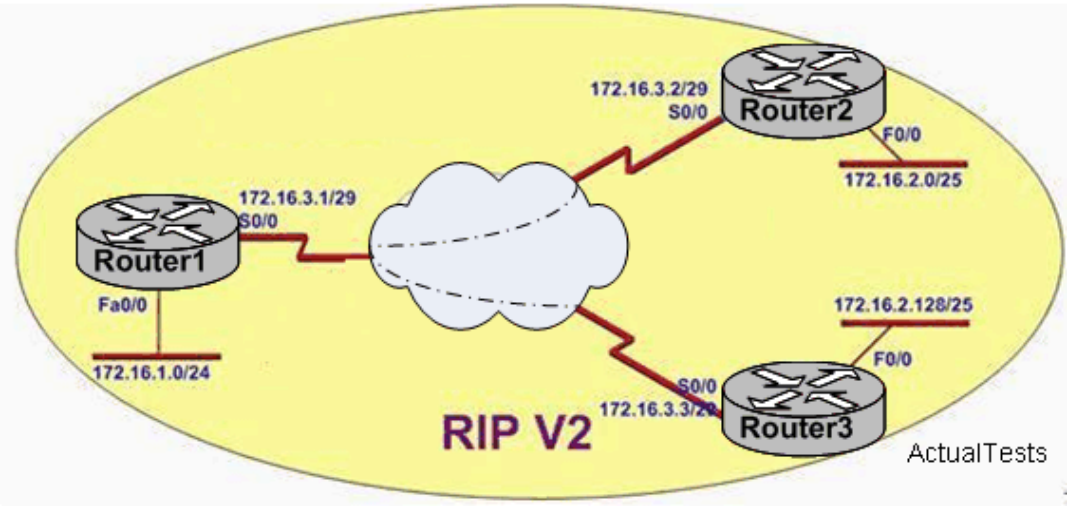
Command	Purpose
neighbor ip-address	Define a neighboring router with which to exchange routing information.

By default, the software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the software to receive and send only Version 1 packets. Alternatively, you can configure the software to receive and send only Version 2 packets. To do so, use the following command in router configuration mode:

Command	Purpose
version {1 | 2}	Configure the software to receive and send only RIP Version 1 or only RIP Version 2 packets.

QUESTION NO: 259

S0/0 on Router1 is configured as a multipoint interface to communicate with Router2 and Router3 in the hub-and-spoke Frame Relay topology shown in the exhibit. Originally, static routes were configured between these routers to successfully route traffic between the attached networks. What will need to be done in order to use RIP v2 in place of the static routes?



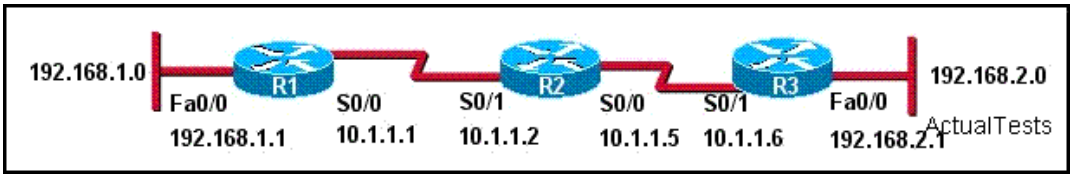
A. Configure the s0/0 interface on Router1 as two sub interfaces and configure point-to-point links to Router2 and Router3.
B. Dynamic routing protocols such as RIP v2 cannot be used across Frame Relay networks.
C. Change the 172.16.2.0/25 and 172.16.2.128/25 subnetworks so that at least two bits are borrowed from the last octet.
D. Configure the no ip subnet-zero command on Router1, Router2, and Router3.

Answer: A

Explanation:
For Dynamic Routing in Hub-and spoke topology, configure the subinterface for each link then define the link as point to point. One reason for the use of subinterfaces is to circumvent the rule of split horizon. Split horizon dictates that a route cannot be advertised out the same interface upon which it was learned in the first place. This can be a problem in hub and spoke frame relay networks, but by using pt-pt subinterfaces this problem will be eliminated.

QUESTION NO: 260

Refer to the exhibit. The network shown in the exhibit is running the RIPv2 routing protocol. The network has converged, and the routers in this network are functioning properly. The FastEthernet0/0 interface on R1 goes down. In which two ways will the routers in this network respond to this change? (Choose two.)



A. R1 will send LSAs to R2 and R3 informing them of this change, and then all routers will send periodic updates at an increased rate until the network again converges.
B. Because of the split-horizon rule, router R2 will be prevented from sending erroneous information to R1 about connectivity to the 192.168.1.0 network.
C. When router R2 learns from R1 that the link to the 192.168.1.0 network has been lost, R2 will respond by sending a route back to R1 with an infinite metric to the 192.168.1.0 network.
D. Routers R2 and R3 mark the route as inaccessible and will not accept any further routing updates from R1 until their hold-down timers expire.
E. All routers will reference their topology database to determine if any backup routes to the 192.168.1.0 network are known.

Answer: B,C

Explanation:
RIP version 2 will send triggered updates when the topology changes like when a link goes down.

The following are the key characteristics of RIPv2 pertaining to this question: Split horizon - RIP doesn't advertise routes back out the interface in which they came. Or put another way, a router won't tell a neighbor about routes that the neighbor presumably already knows about. That would be silly, and could cause a loop in certain circumstances. Triggered update - RIP will send an update out just a soon as the routing table changes. He won't wait for the Update timer to expire. Route poisoning- RIP will tell other routers that a failed route is junk by advertising it with an infinite metric (which is 16 for RIP), effectively poisoning it.
Reference: http://www.ethanbanks.net/?m=200702

QUESTION NO: 261

Which of the following are true regarding the debug output shown in the graphic? (Choose two.)

```
RIP protocol debugging is on
Router1#
1d05h: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (172.16.1.1)
1d05h: RIP: building update entries
1d05h: network 10.0.0.0 metric 1
1d05h: network 192.168.1.0 metric 2
1d05h: RIP: sending v1 update to 255.255.255.255 via Serial0/0 (10.0.8.1)
1d05h: RIP: building update entries
1d05h: network 172.16.0.0 metric 1
Router1#
1d05h: RIP: received v1 update from 10.0.15.2 on Serial0/0
1d05h:    192.168.1.0  in  1  hops
1d05h:    192.168.168.0  in  16  hops (inaccessible)
```

A. Network 10.0.0.0 will be displayed in the routing table.
B. This router was configured with the commands:
ROUTER1(config)# router rip
ROUTER1(config-router)# network 172.16.0.0
ROUTER1(config-router)# network 10.0.0.0

C. This router was configured with the commands:
ROUTER1(config)# router rip
ROUTER1(config-router)# network 192.168.1.0
ROUTER1(config-router)# network 10.0.0.0
ROUTER1(config-router)# network 192.168.168.0

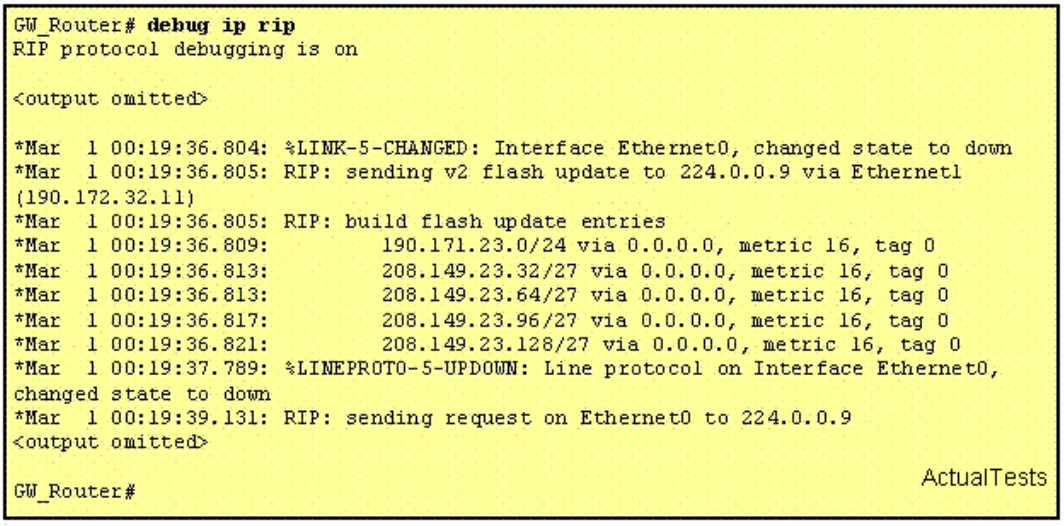
D. This router was configured with the commands:
ROUTER1(config)# router rip
ROUTER1(config-router)# version 2
ROUTER1(config-router)# network 172.16.0.0
ROUTER1(config-router)# network 10.0.0.0

Answer: A,B

Explanation:
Routing Information Protocol (rip) is a distance vector protocol that uses hop as a metric. Rip routing metric: rip uses single routing metric (hops) to measure the distance from source network to destination network. From source to destination, every hop is given a value, which is usually 1. When routers receive route update information of new or changed destination network, the metric value will be added 1 and then stored into a routing table, the ip address of the sender will be used as the next hop address.

QUESTION NO: 262

Refer to the exhibit. Explain how the routes in the table are being affected by the status change on interface Ethernet0.



A. The router is poisoning the routes and multicasting the new path costs via interface Ethernet1.
B. The router is requesting updates for these networks from routers that are connected to interface Ethernet1.
C. The router is poisoning the routes and broadcasting the new path costs via interface Ethernet1.
D. The router is receiving updates about unreachable networks from routers that are connected to interface Ethernet1.

Answer: A

Explanation:
Poison reverse: When path information becomes invalid, routers will not immediately remove them from the routing table, but use 16, an inaccessible metric value, to broadcast it out. Although this increases the size of the routing table, but is helpful for the elimination of routing cycle, it can immediately remove any loop between adjacent routers.

The purpose of route poisoning is to avoid problems caused by inconsistent updates and to prevent network loops. According to exhibit, the interfaces went to the down state so the affected routes were poisoned and removed and an update to the multicast IP address of 224.0.0.9 was sent on interface Ethernet1.

QUESTION NO: 263

Refer to the exhibit. After a RIP route is marked invalid on Router_1, how much time will elapse before that route is removed from the routing table?

```
Router_1# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 8 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  <output omitted>

Router_1#                                                    ActualTests
```

A. 30 seconds
B. 180 seconds
C. 60 seconds
D. 90 seconds
E. 240 seconds

Answer: C

Explanation:
From the condition: After a RIP route is marked invalid on Router_1, we can infer that the RIP route is hold down. By default, the hold-down route will be removed from the routing table in 60 seconds 240-180=60.

QUESTION NO: 264

Which three statements describe the differences between RIP version 1 and RIP version 2? (Choose three.)

A. RIP version 2 sends the subnet mask in updates and RIP version 1 does not.
B. RIP version 1 broadcasts updates whereas RIP version 2 uses multicasts.
C. RIP version 1 multicasts updates while RIP version 2 uses broadcasts.
D. Both RIP version 1 and RIP version 2 are classless routing protocols.
E. Both RIP version 1 and version 2 support authentication.
F. RIP Version 2 is a classless routing protocol whereas RIP version 1 is a classful routing protocol.

Answer: A,B,F

Explanation:
RIP version 1 broadcasts updates whereas RIP version 2 uses multicasts.
RIP Version 2 is a classless routing protocol whereas RIP version 1 is a classful routing protocol.
RIP version 2 sends the subnet mask in updates and RIP version 1 does not.

QUESTION NO: 265

Use the output from the router shown in the graphic above to determine which of the following are correct. (Choose two.)

A. Router John uses a link-state routing protocol.
B. Router John will receive routing updates on the Serial0/0 interface.
C. Router John will receive routing updates on the Serial0/1 interface.
D. Router John will send routing updates out the Serial0/0 interface.

Answer: B,D

QUESTION NO: 266

Refer to the exhibit. Two routers have just been configured by a new technician. All interfaces are up. However, the routers are not sharing their routing tables. What is the problem?

```
Router2# debug ip rip
RIP protocol debugging is on
Router2#RIP: sending  v1 update to 255.255.255.255 via Serial0/0 (192.168.2.2)
RIP: build update entries
   network 192.168.3.0 metric 1
RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.3.1)
RIP: build update entries
   network 192.168.2.0 metric 1
RIP: ignored v2 packet from 192.168.2.1 (illegal version)

Router2#                                                    ActualTests
```

A. Split horizon is preventing Router2 from receiving routing information from Router1.
B. Router1 is configured for RIP version 2, and Router2 is configured for RIP version 1.
C. Router1 has an ACL that is blocking RIP version 2.
D. There is a physical connectivity problem between Router1 and Router2.
E. Router1is using authentication and Router2 is not.

Answer: B

Explanation:
Section 5: Access and utilize the router to set basic parameters. (including: CLI/SDM) (3 questions)

QUESTION NO: 267

Refer to the exhibit. What is the effect of the configuration that is shown?

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


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

Answer: B

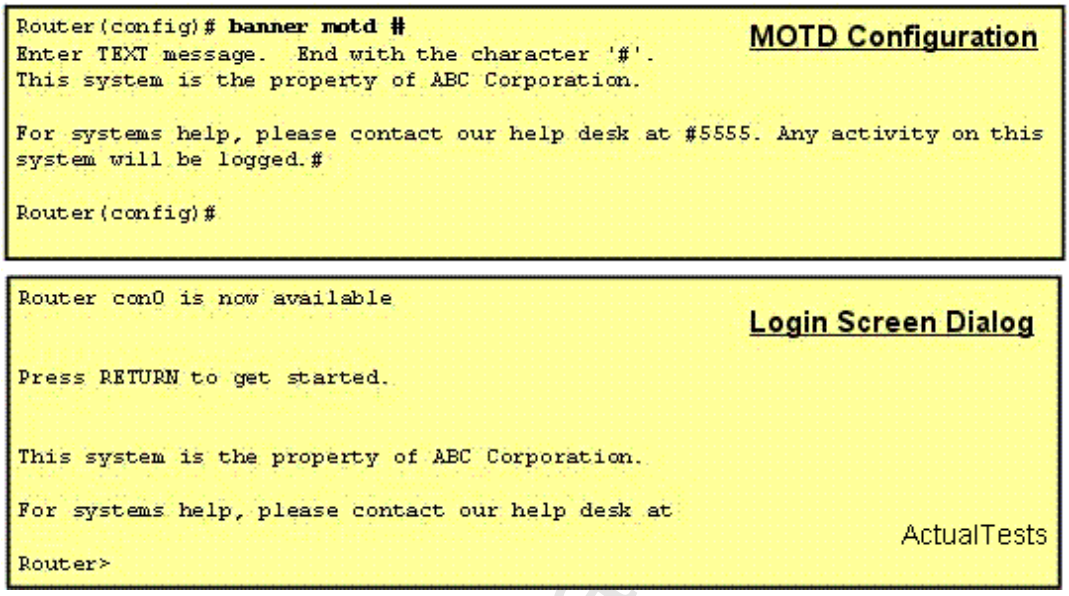
Explanation:
Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. Communication between the client and server is encrypted in both SSH version 1 and SSH version 2. If you want to prevent non-SSH connections, add the "transport input ssh"

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: 268

Refer to the exhibit. On an external corporate router, the network administrator enters the MOTD configuration that is shown in the upper box. The administrator then logs into the router and sees the login screen dialog that is shown in the lower box.

Why does the intended message not display?



A. MOTD banner text may contain only letters and numbers.
B. The network administrator defined an illegal delimiting character in the MOTD command.
C. The banner message exceeds the number of characters allowed.
D. The IOS image on this router does not support the MOTD configuration shown.
E. The MOTD delimiting character appeared in the body of the text.

Answer: E

Explanation:
The banner is displayed whenever anyone logs in to your Cisco router. The syntax is

"banner motd # " . MOTD stands for "Message Of The Day".

symbol signifies the start of the banner message to the router. You will be prompted for the message to be displayed. You need to enter "#" symbol at the end of the message, signifying that the msg has ended. In this case, the # was included in the body of the message, but the router considers it to be the end of the message so only the text preceding the "#" will be displayed.

QUESTION NO: 269

In order to allow the establishment of a Telnet session with a router, which set of commands must be configured?

A. router(config)# line console 0
router(config-line)# enable secret cisco
router(config-line)# login
B. router(config)# line console 0
router(config-line)# enable password cisco
C. router(config)# line console 0
router(config-line)# password cisco
router(config-line)# login
D. router(config)# line vty 0
router(config-line)# password cisco
router(config-line)# login
E. router(config)# line vty 0
router(config-line)# enable password cisco
F. router(config)# line vty 0
router(config-line)# enable secret cisco
router(config-line)# login

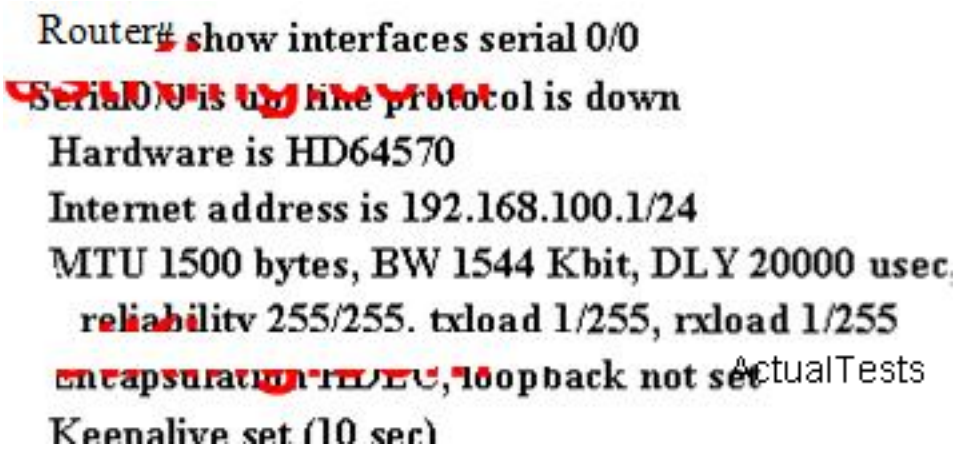
Answer: D

Explanation:
CLI Password Configuration:
Section 6: Connect, configure, and verify operation status of a device interface (3 questions)

QUESTION NO: 270

Refer to the following "show" output:

Router# show interface serial 0/0
Serial 0/0 is up, line protocol is down
Hardware is HD64570
Internet address is 1921.68.100.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 user,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)



What are possible causes for this interface status? (Choose three.)

A. No loopback address is set.
B. No cable is attached to the interface.
C. The clock-rate is not set.
D. There is a mismatch in the encapsulation type.
E. The interface is shut down.
F. No keep-alive messages are received.

Answer: C,D,F

Explanation:
Based on the information provided in the exhibit, we know that Serial0/0 is up, line protocol is down, usually there are three states :
1. serial0/0 up, line protocol is up The interface is up and the link protocol is up.
2. serial0/0 down, line protocol is down The interface is down and there is something wrong with the physical layer .
3. serial0/0 up, line protocol is down The interface is up , but the encapsulation format is not matched correctly.

QUESTION NO: 271

The show interfaces serial 0/0 command resulted in the output shown in the graphic. What are possible causes for this interface status? (Choose three.)

```
Router# show interfaces serial 0/0
Serial0/0 is up, line protocol is down
  Hardware is HD64570
  Internet address is 192.168.100.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
```

ActualTests

A. The interface is shut down.
B. No loopback address is set.
C. The clockrate is not set.
D. There is a mismatch in the encapsulation type.
E. No cable is attached to the interface.
F. No keepalive messages are received.

Answer: C,D,F

Explanation:
According to the description, the possible causes are the following:
1. The clock rate is not set.
2. There is a mismatch in the encapsulation type.
3. No keepalive messages are received.

no shutdown	Enable the interface and the configuration changes you have just made on the interface.

Serial0 is administratively down, line protocol is up.	The possible causes for this state are • The serial interface has been disabled with the **shutdown interface** configuration command. • Different interfaces on the router are using the same IP address.	The following are some steps you can take to isolate the problem: • Use the **show configuration** privileged EXEC command to display the serial port configuration. If "shutdown" is displayed after "interface Serial0," use the **no shutdown** interface configuration command to enable the interface. • Use the **show interface** privileged EXEC command to display the IP addresses for all router interfaces. Use the **ip address** interface configuration command to assign unique IP addresses to the router interfaces.

ActualTests

QUESTION NO: 272 DRAG DROP

This topology contains 3 routers and 1 switch. Complete the topology.
Drag the appropriate device icons to the locations labeled Device.

Drag the appropriate connections to the locations labeled Connections.
Drag the appropriate IP addresses to the locations labeled IP address. (Hint : Use the given host addresses and the Main router information given)
To remove a device or connection , drag it away from the topology.
Use information gathered from the Main router to complete the configuration of any additional routers. No passwords are required to access the Main router. The config terminal command has been disabled for the HQ router. This router does not require configuration.
Configrue each additional router with the following

you should input:
Main>enable
Main#show run
in "terminal" on the right side
to check the address information configured on main-router.
you can see the following information after you input the above command:

Show run 1:

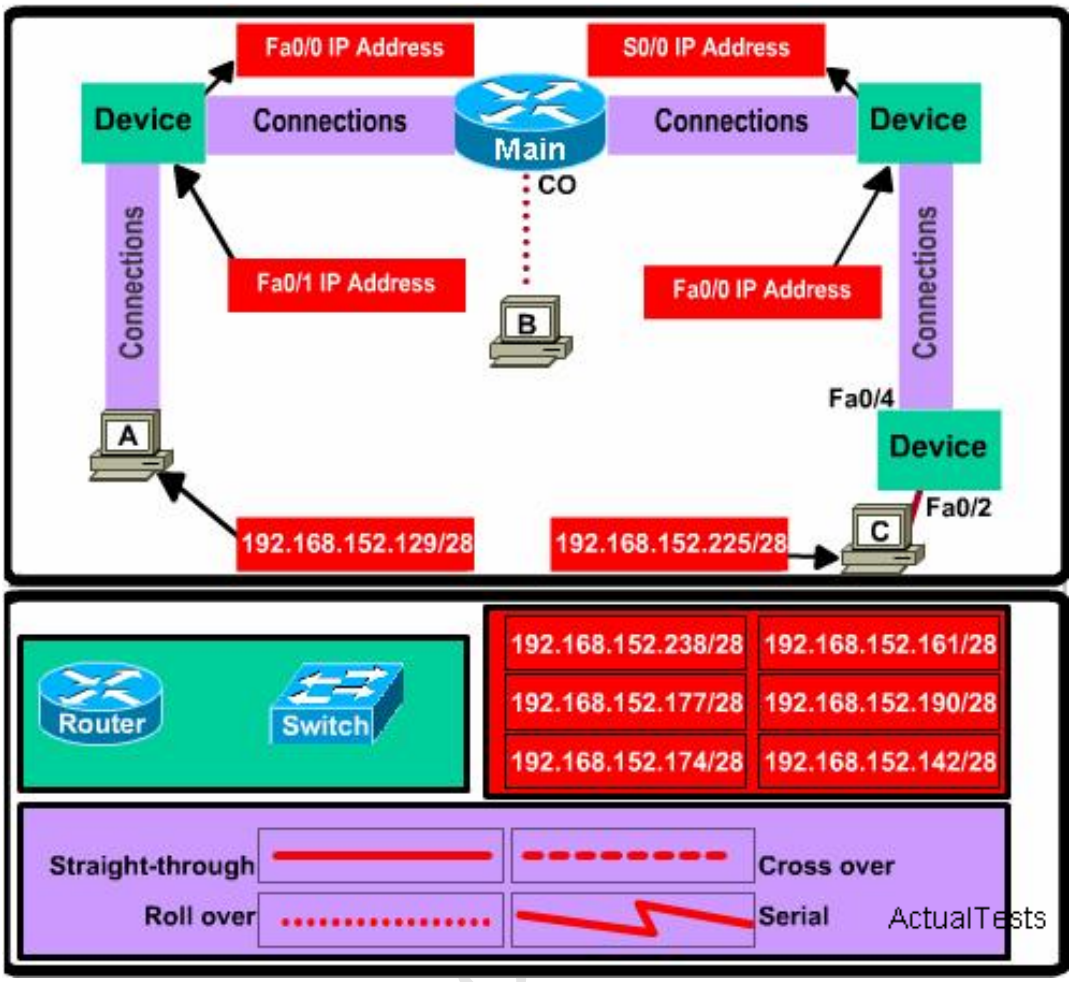
interface FastEthernet0/0
ip address 192.168.152.190 255.255.255.240
!
interface Serial0/0
ip address 192.168.152.174 255.255.255.240
clockrate 64000

Show run 2:

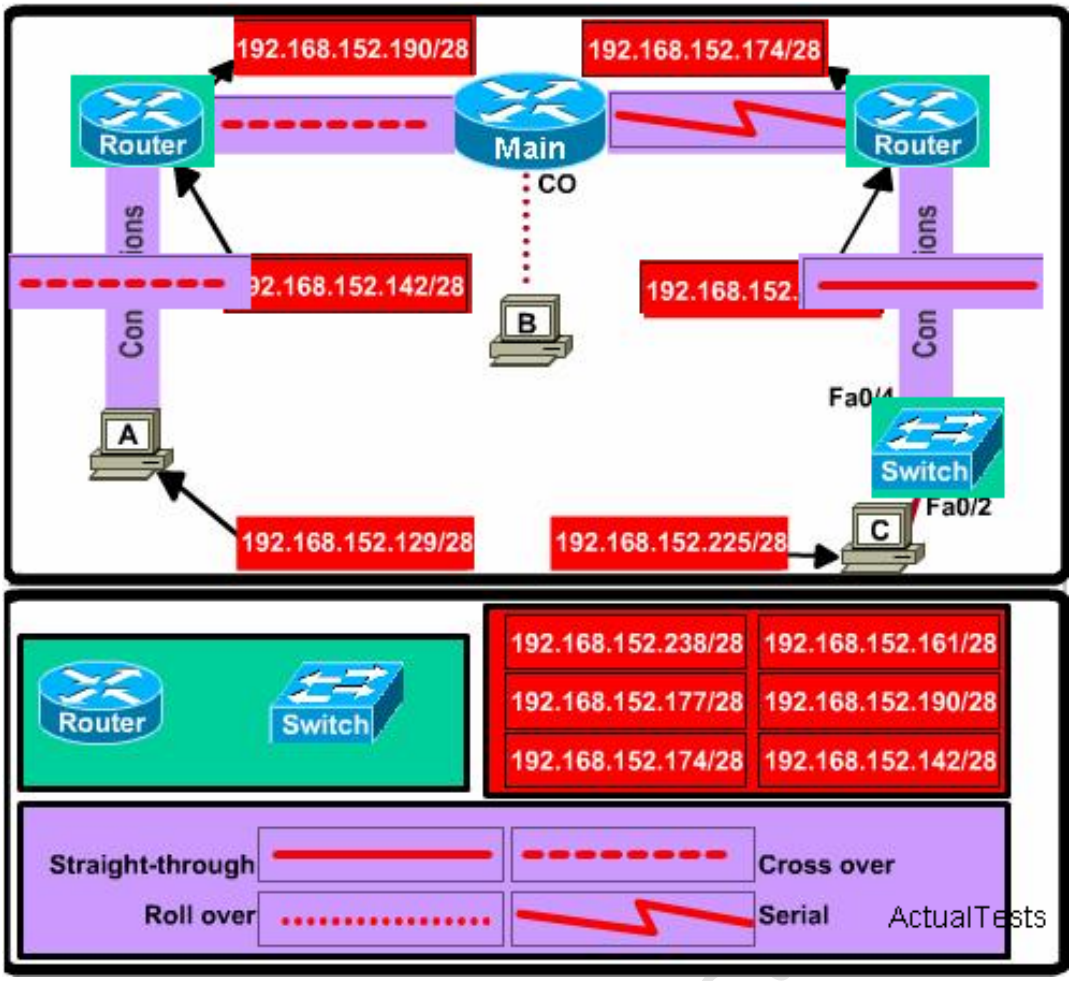
interface FastEthernet0/0
ip address 192.168.152.190 255.255.255.240
!
interface Serial0/0
ip address 192.168.152.174 255.255.255.240
clockrate 64000
!
!
ip classless
ip http server
!
!
!
line con 0
line aux 0

line vty 0 4
login
!
end
Main#

Exhibit:



Answer:



Explanation:
Section 7: Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities (8 questions)

QUESTION NO: 273

An administrator issues the command ping 127.0.0.1 from the command line prompt on a PC. If a reply is received, what does this confirm?

A. The PC has connectivity up to Layer 5 of the OSI model.
B. The PC has the TCP/IP protocol stack correctly installed.
C. The PC has connectivity with a local host.
D. The PC has connectivity with a Layer 3 device.
E. The PC has a default gateway correctly configured.

Answer: B

QUESTION NO: 274

Regarding the extended ping command; which of the statements below are true?(Choose two)

A. With the extended ping command you can specify the TCP and UDP port to be pinged.
B. With the extended ping command you can specify the timeout value.
C. The extended ping command is supported from user EXEC mode.
D. The extended ping command is available from privileged EXEC mode.

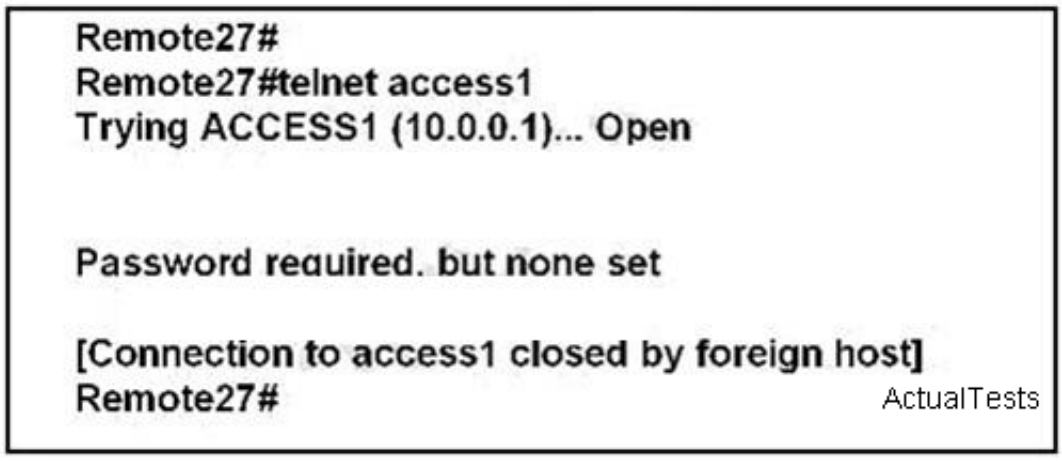
Answer: B,D

Explanation:
The extended ping command works only at the privileged EXEC command line.
Some of the extended ping command values include the datagram size and timeout value as shown:
Datagram size [100]: Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]: Timeout interval. Default: 2 (seconds). The ping is declared successful only if the ECHO REPLY packet is received before this time interval.

The extended ping command works only at the privileged EXEC command line.
Some of the extended ping command values include the datagram size and timeout value as shown:
Datagram size [100]: Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]: Timeout interval. Default: 2 (seconds). The ping is declared successful only if the ECHO REPLY packet is received before this time interval.
Incorrect Answers:
A: Ports can not be specified.
C: Regular pings are available in both user and privileged mode, but not extended pings.

QUESTION NO: 275

The following output was seen on a network device:



This graphic shows the result of an attempt to open a Telnet connection to router access1 From Remote27. Which of the following command sequences will correct this problem?

A. ACCESS1(config)# line vty 0 4
ACCESS1(config-line)# login
ACCESS1(config-line)# password cisco
B. ACCESS1(config)# line console 1
ACCESS1(config-line)# password cisco
C. Remote27(config)# line aux 0
Remote27(config-line)# login
Remote27(config-line)# password cisco
D. Remote27(config)# line vty 0 4
Remote27(config-line)# login
Remote27(config-line)# password cisco

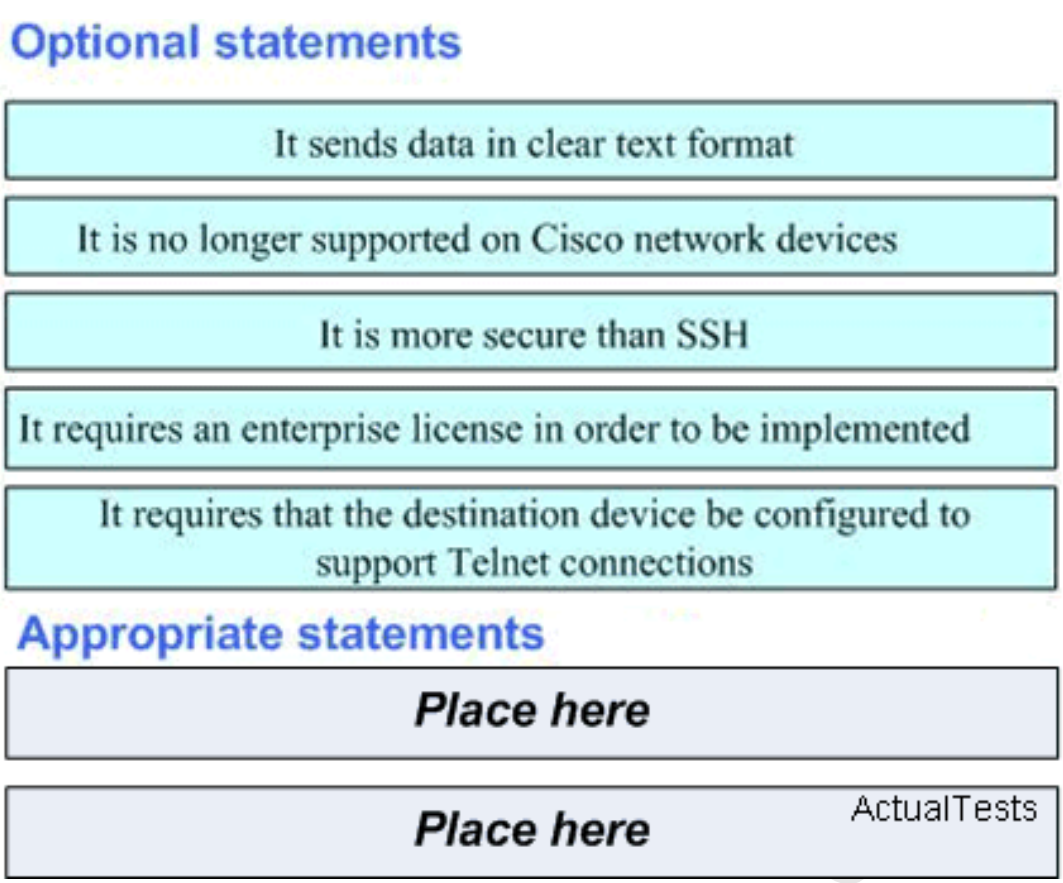
Answer: A

Explanation:
VTY cable can't be used after enabling, it will allow users to access after simply being configured
The picture shows that it is needed to input password in order to connect Remote27 telnet to access 1 , so it is required to configure password to define the logging password on line cable.
The format of the VTP password configuration is as follows:
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password cisco

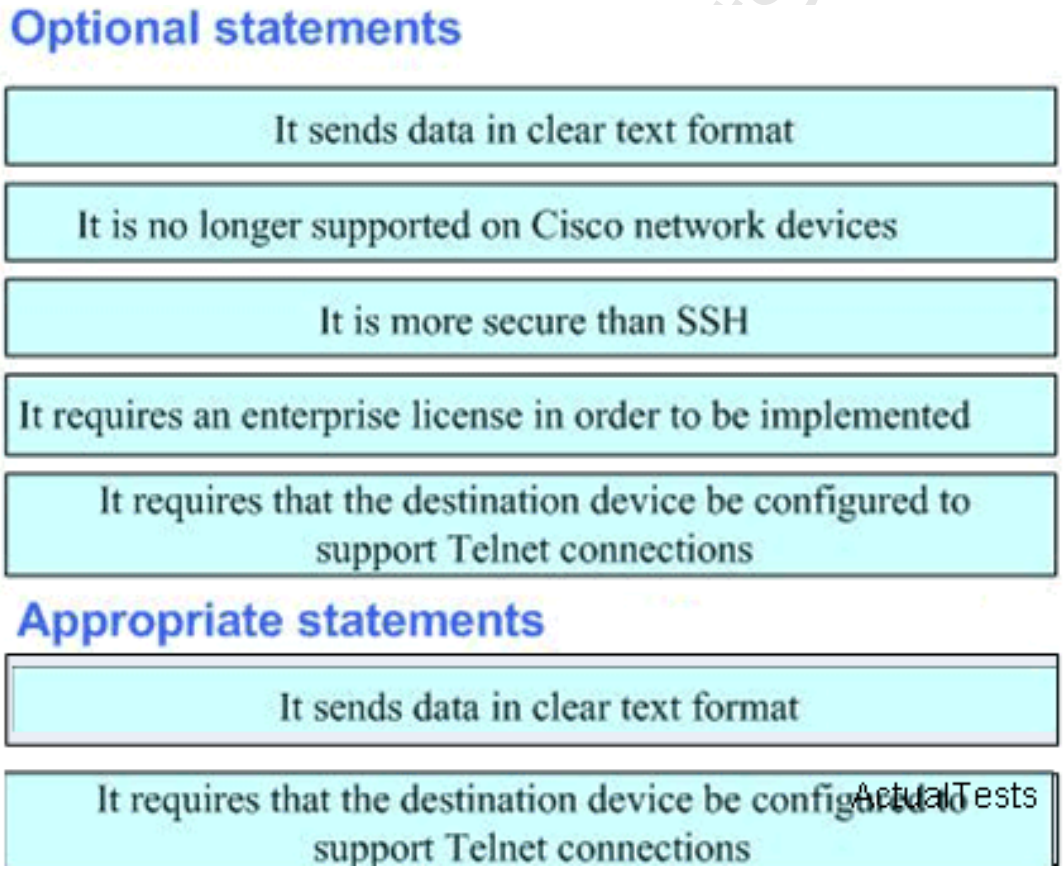
CLI Password Configuration:

QUESTION NO: 276 DRAG DROP

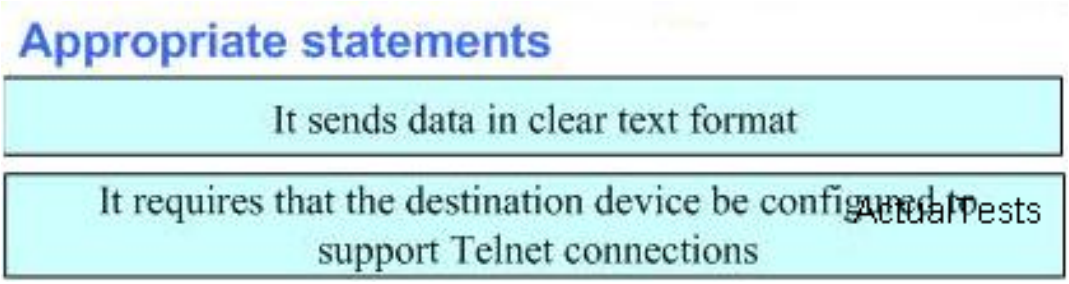
As a CCNA candidate, you need to use a telnet session often. What are two characteristics of Telnet? Please choose two appropriate statements and drag the items to the proper locations.



Answer:



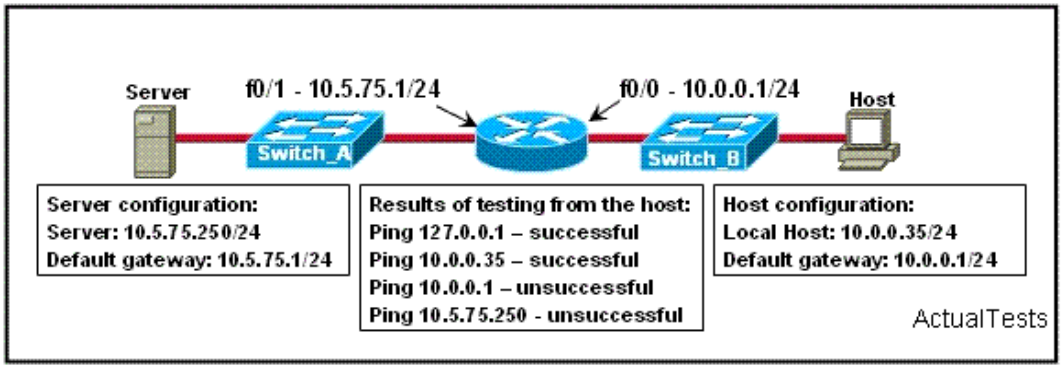
Explanation:



Telnet, by default, does not encrypt any data sent over the connection (including passwords), and so it is often practical to eavesdrop on the communications and use the password later for malicious purposes; anybody who has access to a router, switch, hub or gateway located on the network between the two hosts where Telnet is being used can intercept the packets passing by and obtain login and password information (and whatever else is typed) with any of several common utilities.
If a remote device wants to access the destination device through Telnet, the destination device must be configured to support Telnet connections.

QUESTION NO: 277

Refer to the exhibit. A technician is troubleshooting a host connectivity problem. The host is unable to ping a server connected to Switch_A. Based on the results of the testing, what could be the problem?



A. The host NIC is not functioning.
B. A local physical layer problem exists.
C. A remote physical layer problem exists.
D. TCP/IP has not been correctly installed on the host.

Answer: B

Explanation:
The configuration is correct. The output of the ping command indicates that the fault lies on the F0/0 port or between the host and the router.

QUESTION NO: 278

When you use the ping command to send ICMP messages across a network, what's the most common request/reply pair you'll see?

A. Echo request and Echo reply
B. ICMP hold and ICMP send
C. Echo off and Echo on
D. ICMP request and ICMP reply

Answer: A

Explanation:
The ICMP protocol uses Echo request and Echo reply with the Ping command. The PING utility is the most commonly used message to verify connectivity to a remote device within the network.

QUESTION NO: 279

The network administrator has asked you to check the status of the workstation's IP stack by pinging the loopback address. Which address would you ping to perform this task?

A. 10.1.1.1
B. 127.0.0.1
C. 192.168.0.1
D. 239.1.1.1

Answer: B

QUESTION NO: 280

Which protocol should be used to establish a secure terminal connection to a remote network device? Select the best response.

A. ARP
B. SSH
C. Telnet
D. WEP
E. SNMPv1
F. SNMPv2

Answer: B

Explanation:

Section 8: Perform and verify routing configuration tasks for a static or default route given specific routing requirements (11 questions)

QUESTION NO: 281

Some of the company routers have been configured with default routes. What are some of the advantages of using default routes?(Choose two.)

A. The allow connectivity to remote networks that are not in the routing table.
B. They direct traffic from the Internet into corporate networks.
C. The keep routing tables small.
D. They require a great deal of CPU power.
E. They establish routes that will never go down.

Answer: A,C

Explanation:
Routers use default routing as a last resort when all other methods (directly connected, static, or dynamic) have been exhausted. For stub networks, a single default static route could be used to provide connectivity to the entire network. This is desirable for stub networks where only a single link connects the remote location to the rest of the networks. Because all of the traffic only has one link to use, a single default route will make the routing table as small as possible, while providing for connectivity to networks not in the routing table, since as traffic destined for the Internet.
Incorrect Answers:
B: To influence the way incoming traffic from the Internet gets to a corporation, BGP routing would be used, not default routing.
D: Using static routes, including default routes, is the least CPU-intensive method of routing.
E: Although default routes are normally statically assigned, these routes can still go down. If the interface used as the default route should go down, or the next hop IP address of the default route become unreachable, the static default route will go down.

QUESTION NO: 282

Which two statements are true about the command ip route 172.16.3.0 255.255.255.0 192.168.2.4? (Choose two.)

A. It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4.
B. It is a route that would be used last if other routes to the same destination exist.
C. It establishes a static route to the 192.168.2.0 network.

D. It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network.
E. It uses the default administrative distance.
F. It establishes a static route to the 172.16.3.0 network.

Answer: E,F

Explanation:
The user can specify the path for accessing certain network by configuring static route. In a relatively simple network architecture, and the route to a certain network is unique, the static route will be used.
ip route prefix mask {address | interface} [distance] [tag tag] [permanent]
Prefix :the destination network
mask :subnet mask
address :The IP address of the next hop, that is the address of port on the adjacent router
interface :local network interface
distance : administrative distance(optional)
tag tag : tag value(optional)
permanent :The router is designed as follows : would rather to shut down this port than move.

QUESTION NO: 283

You need to configure a default route on a router. Which command will configure a default route on a router?

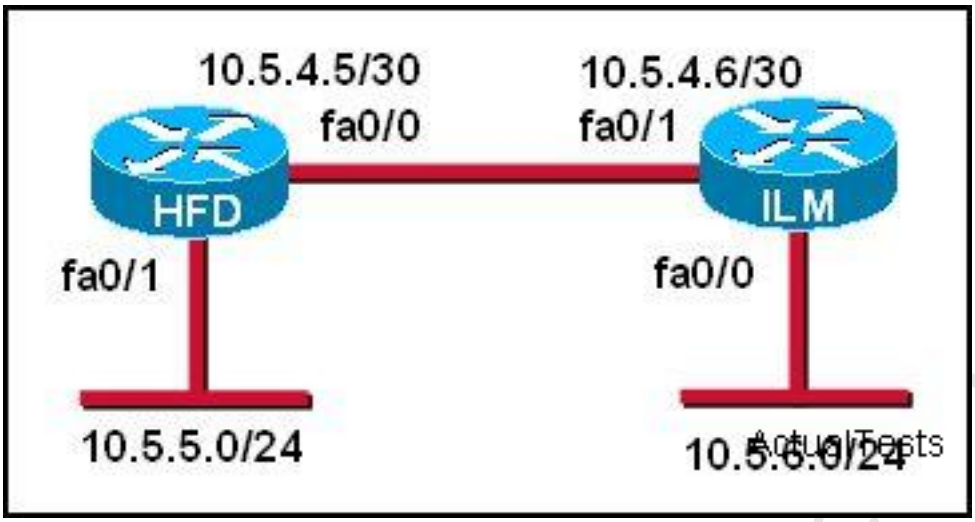
A. Router(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1
B. Router config)# ip default-gateway 10.1.1.0
C. Router(config)# ip default-route 10.1.1.0
D. Router(config)# ip route 0.0.0.0 10.1.1.0 10.1.1.1

Answer: A

Explanation:
The command "IP route 0.0.0.0 0.0.0.0 <ip-address of the interface>" command is used to configure a default route on a router. In this case, a default route with a next hop IP address of 10.1.1.1 was configured.
Incorrect Answers:
B: These commands are invalid. The command "ip default-network" could be used, but not "ip default-route" or "ip default-gateway". IP default-gateway is used on switches, not routers.
C: These commands are invalid. The command "ip default-network" could be used, but not "ip default-route" or "ip default-gateway". IP default-gateway is used on switches, not routers.
D: This will be an invalid route, since the "10.1.1.0" value will specify the network mask, which in this case is invalid.

QUESTION NO: 284

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.)

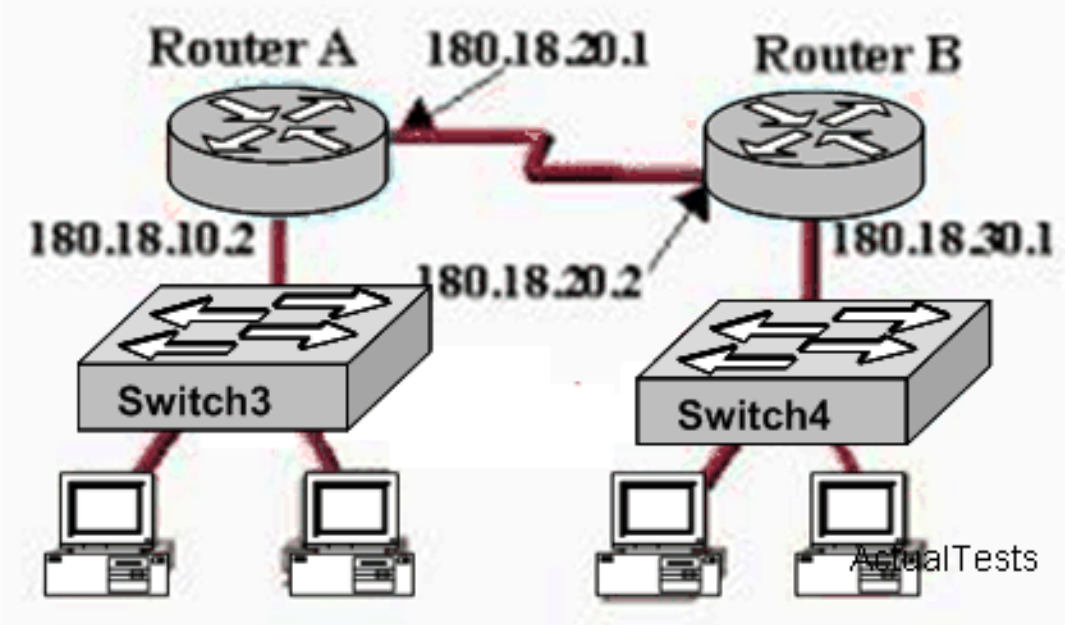


A. HFD(config)# ip route 10.5.6.0 0.0.0.255 fa0/0
B. HFD(config)# ip route 10.5.6.0 0.0.0.255 10.5.4.6
C. HFD(config)# ip route 10.5.6.0 255.255.255.0 fa0/0
D. HFD(config)# ip route 10.5.6.0 255.255.255.0 10.5.4.6
E. HFD(config)# ip route 10.5.4.6 0.0.0.255 10.5.6.0
F. HFD(config)# ip route 10.5.4.6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

Answer: C,D

QUESTION NO: 285

The network is shown below:



Based on this information, which of the following will configure a static route on Router A to network 180.18.30.0/24 with an administrative distance of 90?

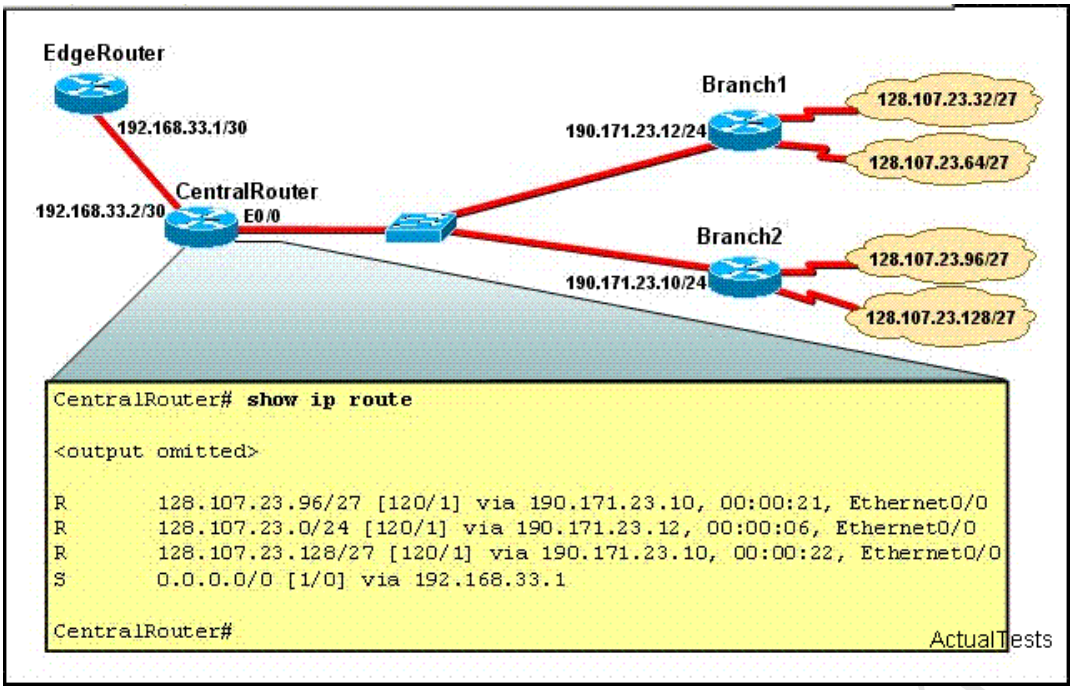
A. Router(config)# ip route 180.18.30.1 255.255.255.0 182.18.20.1 90
B. Router(config)# ip route 180.18.20.1 255.255.255.0 182.18.30.0 90
C. Router(config)# ip route 90 180.18.20.1 255.255.255.0 182.18.20.2
D. Router (config)# ip route 180.18.30.0 255.255.255.0 182.18.20.2 90

Answer: D

Explanation:
Static route entries consist of the destination IP network address, the IP address of the next hop router, and the metric (hop count) for the route. A static route that points to the next hop IP address has an Administrative distance of 1. If the static route points to an outgoing interface, the static route has the Administrative distance of 0.
One common reason to change the administrative distance of a route is when you use Static Routes to backup and existing IGP route. This is normally used to bring up a backup link when the primary fails. In this example, choice E specifies that to reach the 180.18.30.0/24 network, forward this traffic to the router with the next hop IP address of 182.18.20.2 (Router B) using an administrative distance of 90.

QUESTION NO: 286

Refer to the exhibit. RIPv2 is in use on the network with no standard policy in place for summarization. A packet arrives at CentralRouter with a destination IP address of 208.149.23.91. Given the output that is shown, how will CentralRouter process that packet?



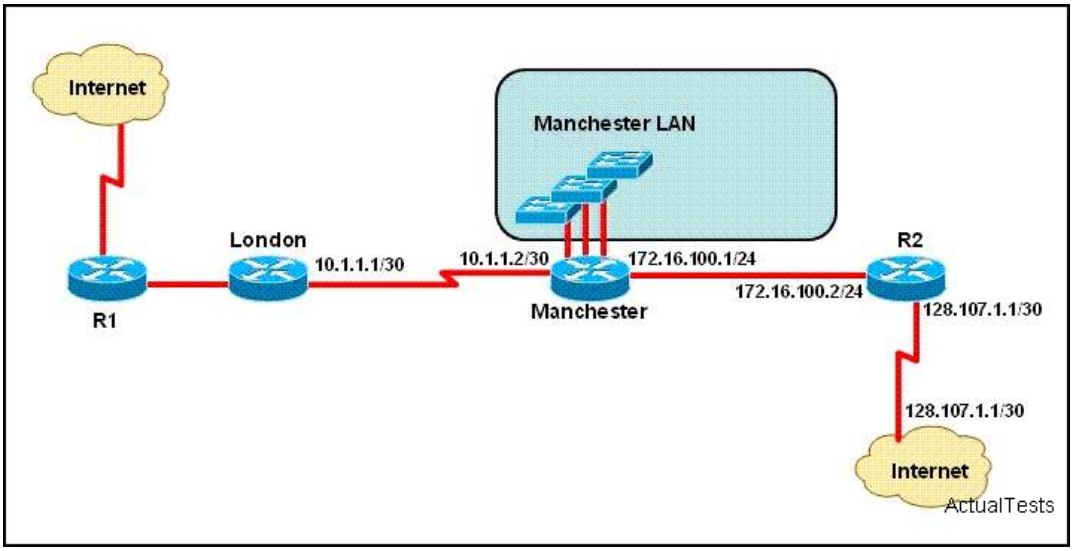
A. It will hold the packet for 22 seconds.
B. It will forward the packet to 190.171.23.10.
C. It will forward the packet to 192.168.33.1.
D. It will forward the packet to 190.171.23.12.
E. It will discard the packet because there is no matching route.
F. It will hold the packet for 21 seconds.

Answer: C

Explanation:
When the packet with the target address 208.149.23.91 reaches CentralRouter, CentralRouter searches its routing table but cannot find the routing entry mapping 208.149.23.91, so the default route is used:
S 0.0.0.0/0 [1/0] via 192.168.33.1
The packet is forwarded by CentralRouter to 192.168.33.1.

QUESTION NO: 287

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 0.0.0.0 172.16.100.2
B. ip route 0.0.0.0 255.255.255.255 172.16.100.2
C. ip route 0.0.0.0 255.255.255.0 172.16.100.2
D. ip route 0.0.0.0 0.0.0.0 128.107.1.1
E. ip route 0.0.0.0 255.255.255.252 128.107.1.1
F. ip route 0.0.0.0 0.0.0.0 172.16.100.1

Answer: A

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: 288

Which of the commands below can you use to configure a default route on router2?(Choose two)

A. ROUTER2(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.21
B. ROUTER2(config)# ip route 0.0.0.0 0.0.0.0 E0
C. ROUTER2(config-interface)# ip route 255.255.255.255 0.0.0.0 192.168.1.21
D. ROUTER2(config)# ip route 0.0.0.0 255.255.255.255 S0

Answer: A,B

Explanation:

There are two ways to specify a default static route. One is to specify the interface to use for forwarding packets, like the example in A. The other way is to specify the IP address of the next hop router, such as the example in D. The ip route 0.0.0.0 0.0.0.0 command uses the fact that network 0.0.0.0 is used by Cisco IOS software to represent the default network.

Reference: CCNA ICND Exam Certification Guide By Wendell Odem Pg.524

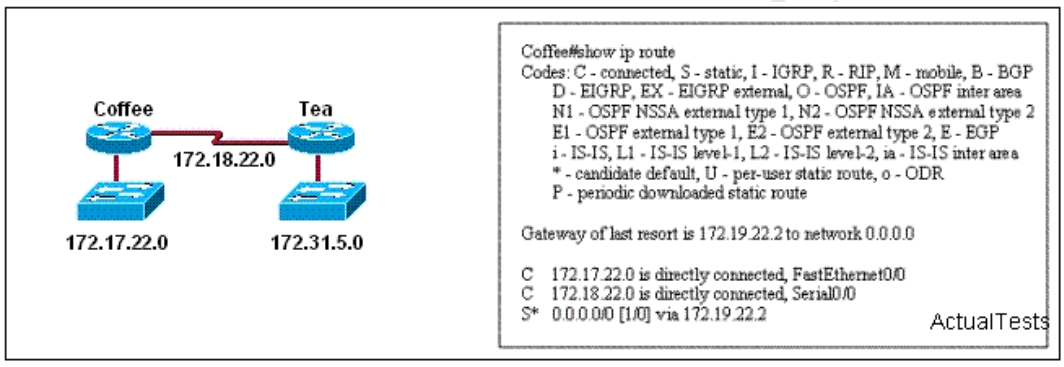
Incorrect Answers:

C: The default route is made in global configuration mode.

D: All zero's must used for the subnet mask of a default route, not all 1's.

QUESTION NO: 289

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. 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 neighbor relationship table is not correctly updated.

B. A static route is configured incorrectly.

C. The routing table on Coffee has not updated .

D. IP routing is not enabled.

E. The FastEthernet interface on Coffee is disabled.

F. The network has not fully converged.

Answer: B

Explanation:

The route S* 0.0.0.0[1/0]VIA 172.19.22.2 is not correct. We can infer that the static route is configured incorrectly and the data cannot reach the external network from this address.

On the bottom line of the command output for 'show ip route' you can see that there is an asterisk by the letter S. The S stands for static route, and the static route is incorrectly configured.

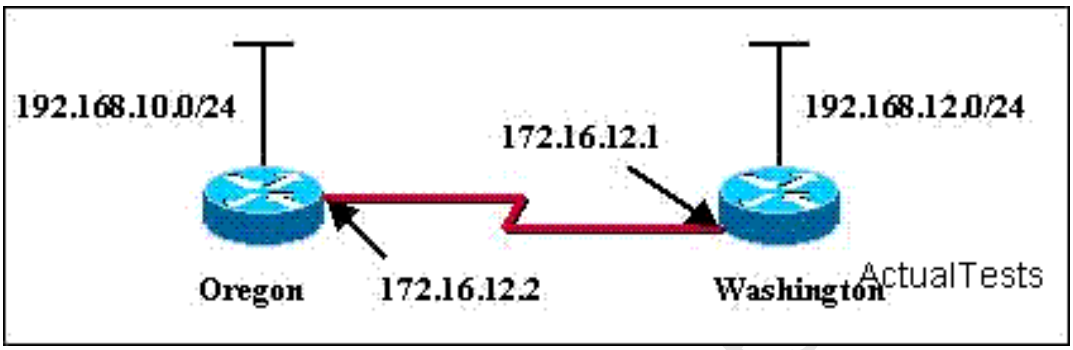
Incorrect Answers:

C: It appears that only a single static route is being used on the Coffee router. Neighbors do not need to be established for static routes.

D: If this were true, then the users on the LAN would be unable to connect to anything outside of their own network.

QUESTION NO: 290

The network administrator of the Oregon router adds the following command to the router configuration: ip route 192.168.12.0 255.255.255.0 172.16.12.1. What are the results of adding this command? (Choose two.)



A. Traffic for all networks is forwarded to 172.16.12.1.

B. This route is automatically propagated throughout the entire network.

C. Traffic for network 172.16.12.0 is forwarded to the 192.168.12.0 network.

D. Traffic for network 192.168.12.0 is forwarded to 172.16.12.1.

E. The command establishes a static route.

F. The command invokes a dynamic routing protocol for 192.168.12.0.

Answer: D,E

Explanation:

In order to configure a static route the router has to be in global configuration mode.

ip route network prefix mask {address | interface} [distance]

network - the destination network

mask - is the subnet mask for that network

address - IP address of the next hop router

interface - or the interface the traffic is to leave by

distance - (optional) the administrative distance of the route

There are other parameters but these have been removed as they are not relevant to the CCNA exam.

In order to configure a static route the router has to be in global configuration mode. ip route network prefix mask { address | interface } [distance] network - the destination network mask - is the subnet mask for that network address - IP address of the next hop router interface - or the

interface the traffic is to leave by distance - (optional) the administrative distance of the route There are other parameters but these have been removed as they are not relevant to the CCNA exam. Example:
ip route 10.0.0.0 255.0.0.0 131.108.3.4 110 10.0.0.0 is the destination network. 255.0.0.0 is the subnet mask for that network and 131.108.3.4 is the next hop for the router to use. The 110 is the administrative distance which we will look at later on.

QUESTION NO: 291

What is an appropriate use of a default route?

A. to provide routing to a local web server
B. to provide routing from an ISP to a stub network
C. to provide routing that will override the configured dynamic routing protocol
D. to provide routing to a destination that is not specified in the routing table and which is outside the local network

Answer: D

Explanation:
Section 9: Manage IOS configuration files. (including: save, edit, upgrade, restore) (5 questions)

QUESTION NO: 292

Which is the correct fallback sequence for loading the Cisco IOS?

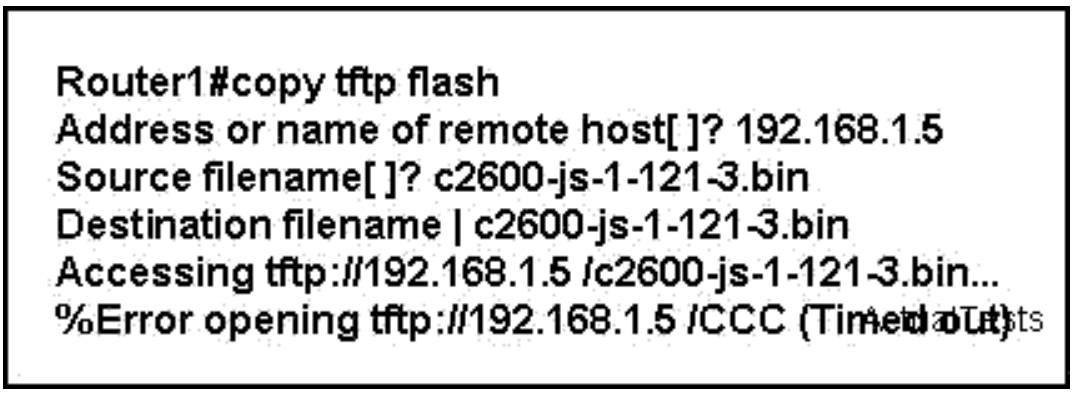
A. Flash, TFTP server, ROM
B. ROM, Flash, NVRAM
C. Flash, NVRAM, RAM
D. ROM, TFTP server, Flash

Answer: A

Explanation:
By default, a Cisco IOS router will normally boot up from flash where the IOS is stored. If the IOS in not found or has become corrupted, the router will then send an all hosts broadcast (255.255.255.255) to find a TFTP server to download the IOS from. Should that fail, the router will boot up in ROM Monitor mode as a last resort.

QUESTION NO: 293

When upgrading the IOS image, the network administrator receives the exhibited error message. What could be the cause of this error?



A. The IOS image on the TFTP server is corrupt.
B. The new IOS image is too large for the router flash memory.
C. The new IOS image is not correct for this router platform.
D. There is not enough disk space on the TFTP server for the IOS image.
E. The TFTP server is unreachable from the router.

Answer: E

Explanation:
The problem shown here is that the destination file is not reachable. When copying files via TFTP the first step is to ensure that there is connectivity to the TFTP server. You should perform the following steps:
1. Verify that the TFTP server has IP connectivity to the router.
2. Check the IP addresses of the TFTP server and the router or access server targeted for the TFTP software upgrade.
3. Ping the router or access server to verify that a network connection exists between them.

QUESTION NO: 294

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. show version
B. the amount of available ROM
C. the version of the bootstrap software present on the router
D. the amount of available flash and RAM memory

Answer: A,D

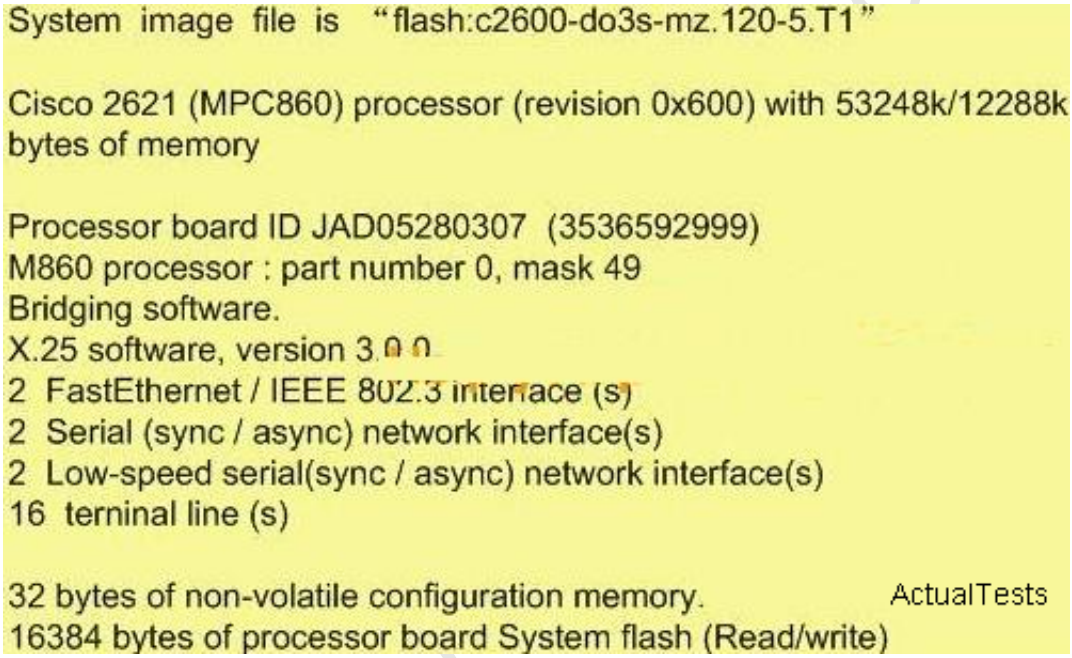
Explanation:
Before the upgrade of IOS, you have to check its current version (you may use show version to check); at the same time you have to ensure that there is sufficient space to store IOS upgrade

(you may use the amount of available flash and RAM memory to check).

To upgrade the IOS, the first two steps are: Download the Cisco IOS software image to your workstation or PC. Install the new Cisco IOS software image in the outbound directory of the TFTP server.
The TFTP server looks for the router's Cisco IOS software image in this directory. Make sure that the image you want to copy to your Flash is in this directory.
Check the memory requirements needed for the Software image being upgraded, which is mentioned in the Downloads download page. Using the show version command, verify that you have enough memory.

QUESTION NO: 295

Refer to the partial command output shown. Which two statements are correct regarding the router hardware? (Choose two.)



A. Total RAM size is 16384 KB (16 MB)
B. Total RAM size is 65536 KB (64 MB).
C. Flash size is 16384 KB (16 MB).
D. Total RAM size is 32 KB.

Answer: B,C

Explanation:
The RAM is found by adding up the memory, so in this case it is 53248K+12288K = 65536K. The Flash is found at the very bottom of the output, which is shown as 16384K

How Do I Know What Platform I Have?

Type the show version command at the enable command prompt of the router to see the platform, RAM, flash memory, and current version of code you are running.
This example shows a Cisco 2600 router with 48 MB of RAM (43617 K + 5534 K), 16 MB of flash memory (16384 K), and a code image called flash:c2600-jk8s-mz.122-6.bin.

```
wilson#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK8S-M), Version 12.2(6), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 07-Nov-01 21:07 by pwade
Image text-base: 0x80008088, data-base: 0x814FF2C4

ROM: System Bootstrap, Version 11.3(2)XA3, PLATFORM SPECIFIC RELEASE SOFTWARE (fc1)

wilson uptime is 1 week, 2 days, 7 hours, 41 minutes
System returned to ROM by power-on
System image file is "flash:c2600-jk8s-mz.122-6.bin"

cisco 2611 (MPC860) processor (revision 0x202) with 43617K/5534K bytes of memory.
Processor board ID JAB03050692 (209339592)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

wilson#
```

ActualTests

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800949e4.shtml

QUESTION NO: 296

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

A. In order for the router to use the new image as the default, it must be the only IOS image in flash.
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. The router cannot verify that the Cisco IOS image currently in flash is valid.

Answer: C

Explanation:
We can keep multiple IOS files on flash memory if there is enough space. When you try to copy the IOS to flash memory, it will ask you to erase current contents of flash memory. If there is enough free space to copy IOS you can type no to erase the contents of flash. If there is not enough space the router will require that the current file is erased first.
Section 10: Manage Cisco IOS. (3 questions)

QUESTION NO: 297

Which of the commands below would you enter if you wanted to see the configuration register of your router?

A. show boot
B. show version
C. show register
D. show config
E. show flash

Answer: B

Explanation:
To display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images, use the show version command in EXEC mode.

Example:
The following is sample output from the show version command:
Router1> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-J-M), Experimental Version 11.3(19970915:164752) [hampton-nitro-baseline 249]
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Wed 08-Oct-97 06:39 by hampton
Image text-base: 0x60008900, data-base: 0x60B98000
ROM: System Bootstrap, Version 11.1(11855) [beta 2], INTERIM SOFTWARE
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE
Router1 uptime is 23 hours, 33 minutes
cisco 7206 (NPE150) processor with 57344K/8192K bytes of memory.
R4700 processor, Implementation 33, Revision 1.0 (512KB Level 2 Cache)
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
8 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
4 Token Ring/IEEE 802.5 interface(s)
4 Serial network interface(s)
1 FDDI network interface(s)
125K bytes of non-volatile configuration memory.
1024K bytes of packet SRAM memory.
20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).

20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).

QUESTION NO: 298

You are a trainee technician. Your instructor tells you to backup an IOS image of a Cisco device to a Windows 2003 server on the network. What should you do first? (Choose three)

A. Assure that the network server has adequate space for the code image.
B. Make sure that the network server can be accessed.
C. Verify any file naming and path requirements.
D. Check that the authentication for access is set.

Answer: A,B,C

Explanation:
More often than not, when backing up IOS files, first , using the command PING to test whether the server is reachable or not and whether the server has enough space to store the IOS backup files or not. When the two needs are satisfied, you can use the command "copy flash tftp" to backup on the router.
Router>enable
Router#copy flash tftp
ip address of remote host:[255.255.255.255]?129.0.0.3
filename to write on tftp hose?c4500-l
writing c4500-l !!!!!!!!!!!!!!!!!!!!!!!!
successful tftp write
After inputting the command "copy flash tftp", the router will require you to input the IP address of the remote TFTP server and IOS mapping name of the server. The router will remind you that backup is successfully completed by a string of exclamation points.

In order to properly back up the Cisco IOS image onto a Windows server, you should ensure that the server is reachable and that you have the proper permissions to save files to the server. In addition to this, the server will need enough space to hold the backup file.

QUESTION NO: 299

You wish to upgrade the IOS of a router without removing the image currently installed. What command will display the amount of memory that is being used by the current IOS image and whether there is enough room available to hold both the current and new images?

A. Router# show version

B. Router# show buffers
C. Router# show flash
D. Router# show memory

Answer: C

Explanation:
The "show flash" command is used to display the layout and contents of the flash memory file system. It will show name of the file system, as well as the number of bytes used and the number available within the flash memory.
Section 11: Compare and contrast methods of routing and routing protocols (16 questions)

QUESTION NO: 300

A routing protocol is required that supports:

1) routing update authentication
2) an addressing scheme that conserves IP addresses
3) multiple vendors
4) a network with over 50 routers

Which routing protocol fulfills these requirements?

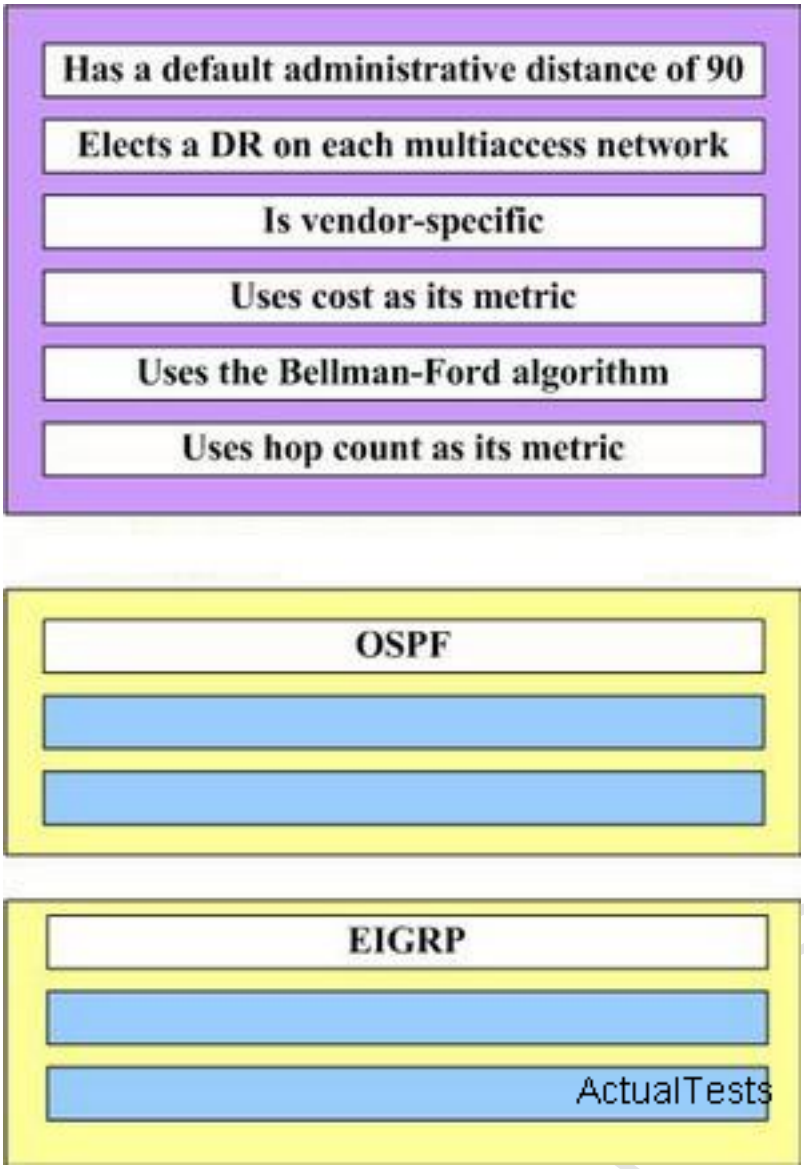
A. RIPv2
B. RIPv1
C. OSPF
D. EIGRP

Answer: C

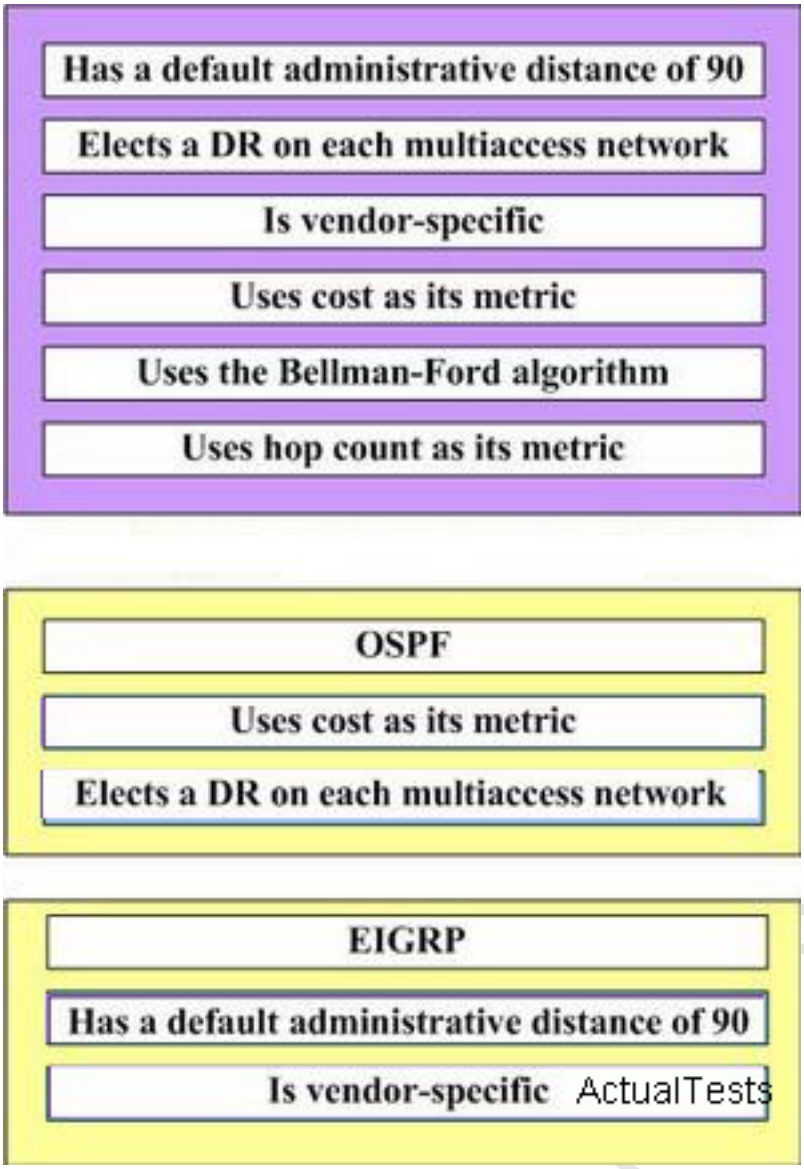
Explanation:
EIGRP is CISCO private agreement, which will not support non-CISCO devices; RIPv1 and RIPv2 are distance vector protocol, supporting up to 15 hop, and 16 hop is inaccessible. RIPv1 does not support routing update verification. Although the convergence rate of OSPF is slower than EIGRP, but OSPF has better expansibility. And OSPF supports multi-vendor devices, and is applicable to large networks.

QUESTION NO: 301 DRAG DROP

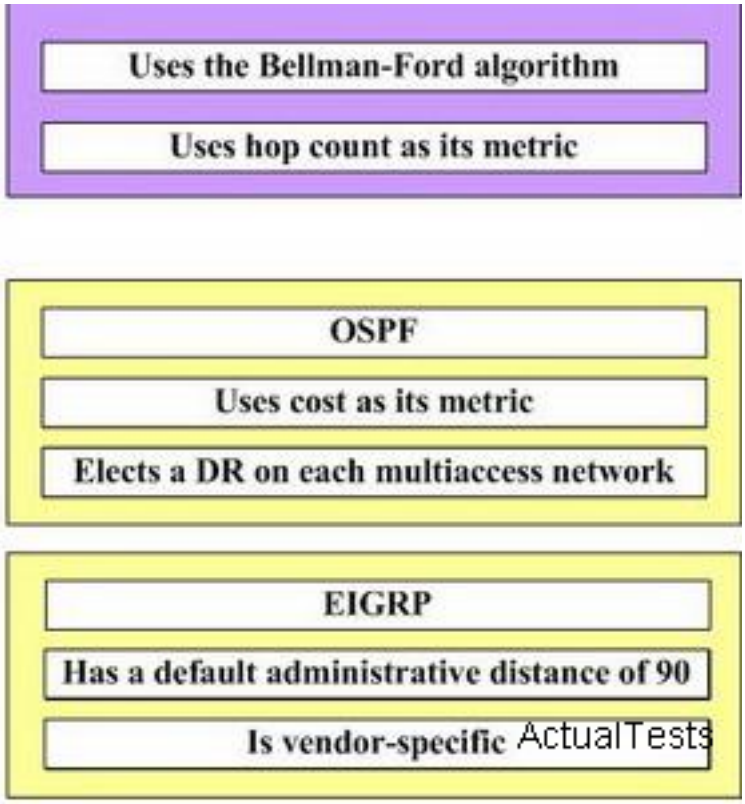
Drag the description on the left to the routing protocol on the right.(Not all options are used.)



Answer:



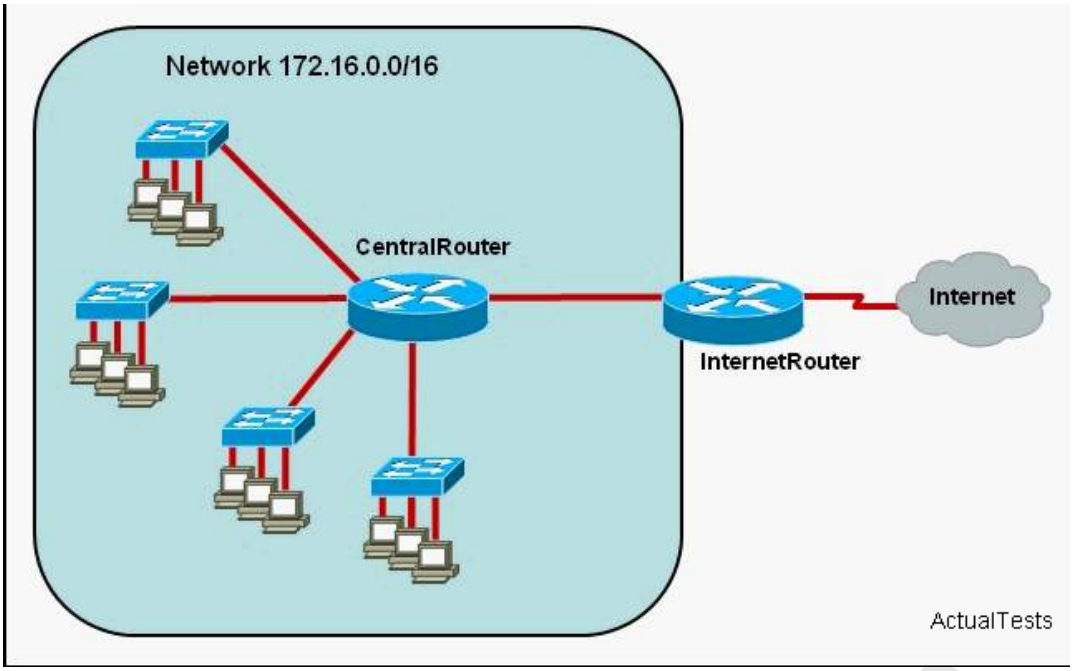
Explanation:



EIGRP is a private CISCO protocol, combining the advantages of the Link State Routing Protocol and the Distance Vector Routing Protocol, the default administrative distance is 90. EIGRP adopts Diffusing Update Algorithm (DUAL) to achieve fast convergence , supports Variable Length Subnet Mask (VLSM) and uses multicast and unicast instead of broadcast to communicate between routers.
OSPF(Open Shortest Path First) is an Interior Gateway Protocol, which can be used for route decision in a single autonomous system. Compared to RIP, OSPF is a Link State Routing Protocol. By default, OSPF calculates the cost based on the bandwidth configured on interface , the higher the bandwidth, the lower the cost.

QUESTION NO: 302

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.)

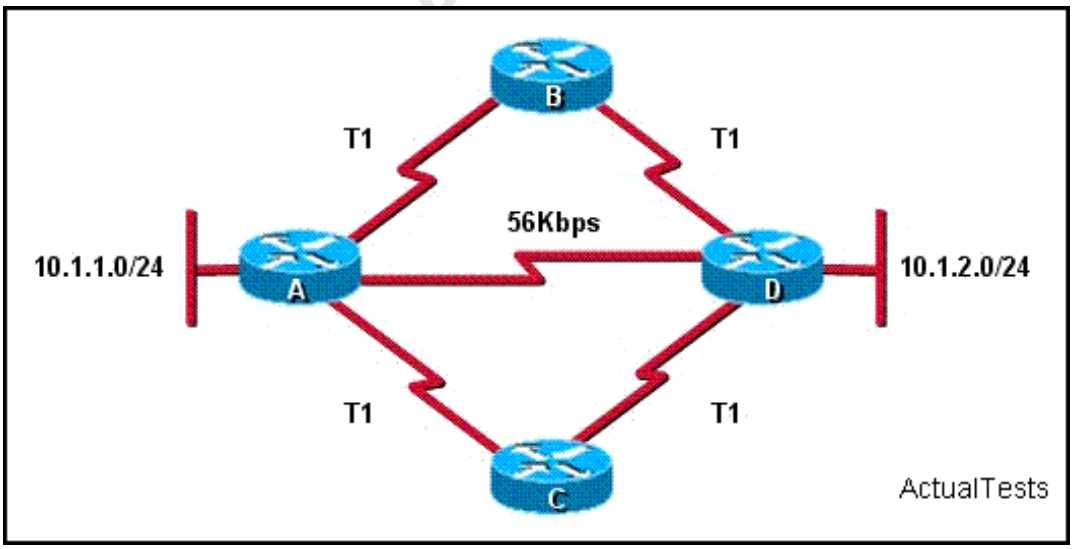


A. a dynamic routing protocol on CentralRouter to advertise summarized routes to InternetRouter.
B. a dynamic routing protocol on CentralRouter to advertise all routes to InternetRouter.
C. a static, default route on CentralRouter that directs traffic to InternetRouter.
D. a dynamic routing protocol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

Answer: C,E

QUESTION NO: 303

Refer to the exhibit. How will router A choose a path to the 10.1.2.0/24 network when different routing protocols are configured? (Choose three.)



A. If EIGRP is the routing protocol, the equal cost paths ABD and ACD will be installed in the routing table by default.
B. If RIPv2 is the routing protocol, the equal cost paths ABD and ACD will be installed in the routing table by default.
C. If EIGRP is the routing protocol, only the path AD will be installed in the routing table by default.
D. If EIGRP and OSPF are both running on the network, the OSPF paths will be installed in the routing table.
E. If EIGRP and OSPF are both running on the network, the EIGRP paths will be installed in the routing table.
F. If RIPv2 is the routing protocol, only the path AD will be installed in the routing table by default.

Answer: A,E,F

Explanation:
Rip uses the hop count to choose the best route. Although the routes ABD and ACD have a higher bandwidth than AD, the hop count of AD is 2; therefore, the route AD is added to the routing table.
EIGRP uses the cost as the metric, so the router chooses both the route ABD and ACD as the best routes and load-balances them.
If multiple routing protocols are running on the network, the router chooses the route whose routing protocol has the lower number. The administrative distance of EIGRP is lower than that of OSPF, so the EIGRP-learned route is added to the routing table.

QUESTION NO: 304

A router learns about a remote network from EIGRP, OSPF, and a static route. Assuming all routing protocols are using their default administrative distance, which route will the router use to forward data to the remote network?

A. The router will use the static route.
B. The router will use the OSPF route.
C. The router will load balance and use all three routes.
D. The router will use the EIGRP route.

Answer: A

Explanation:
When a router learns about the same network via multiple sources, the router will choose the source with the lowest administrative distance (AD). By default, the AD for these routing protocols are:

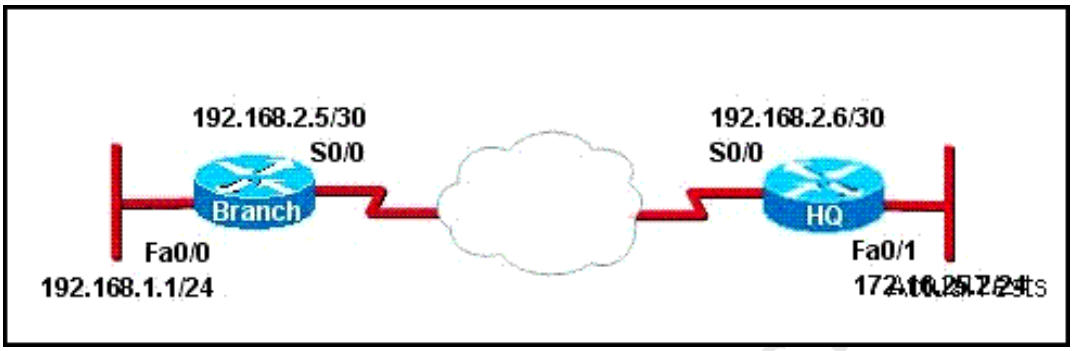
Connected Interface has 0 AD
Static Route : 1
EIGRP : 90

OSPF : 110

So, the static route will be chosen since it has the lowest AD.

QUESTION NO: 305

Refer to the exhibit. A network associate has configured the internetwork that is shown in the exhibit, but has failed to configure routing properly. Which configuration will allow the hosts on the Branch LAN to access resources on the HQ LAN with the least impact on router processing and WAN bandwidth?



A. HQ(config)# router rip
HQ(config-router)# network 192.168.2.0
HQ(config-router)# network 172.16.0.0
Branch(config)# router rip
Branch (config-router)# network 192.168.1.0
Branch (config-router)# network 192.168.2.0
B. HQ(config)# router eigrp 56
HQ(config-router)# network 192.168.2.4
HQ(config-router)# network 172.16.25.0
Branch(config)# router eigrp 56
Branch (config-router)# network 192.168.1.0
Branch (config-router)# network 192.168.2.4
C. HQ(config)# router ospf 1
HQ(config-router)# network 192.168.2.4 0.0.0.3 area 0
HQ(config-router)# network 172.16.25.0 0.0.0.255 area 0
Branch(config)# router ospf 1
Branch (config-router)# network 192.168.1.0 0.0.0.255 area 0
Branch (config-router)# network 192.168.2.4 0.0.0.3 area 0
D. HQ(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.5
Branch(config)# ip route 172.16.25.0 255.255.255.0 192.168.2.6

Answer: D

Explanation:
Static routes can be used to allow Branch LAN to access resources on the HQ LAN with the least impact on router processing and WAN bandwidth.
Compared with dynamic routes, static routes have the following advantages:
1. Control
2. Easy configuration
3. Less WAN bandwidth

QUESTION NO: 306

When designing OSPF networks; what is the purpose of using a hierarchical design?(Choose three)

A. To reduce the complexity of router configuration
B. To confine network instability to single areas of the network
C. To reduce routing overhead
D. To speed up convergence

Answer: B,C,D

Explanation:
The reason for regional structure division in OSPF network is: In a small network, the structure of router is not complicated, it is easy to identify routes to different destinations. However, in large networks, the link structure is complex, the number of the potential paths for different destinations is large. Therefore, the SPF algorithm which compares all possible routes is very complex and requires a very long time.
Link State Routing Protocol often divides network into area structures to reduce the amount of SPF algorithm. The number of routers within the area and diffusing LSA is less, which means that the link-state database is small. The result is that the amount of SPF algorithm is smaller and the time needed is shorter .

An OSPF network designed in a hierarchical fashion with different areas is used because a small change in the topology of a single area won't force every router to run the SPF algorithm. Changes in one area are limited to that area only, not to every router within the entire network. Confining the topology changes to one area reduces the overhead and speeds the convergence of the network.
Reference: CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 194
Incorrect Answers:
A: This choice is incorrect because a hierarchical design actually adds complexity to the router configuration.

QUESTION NO: 307

What are two drawbacks of implementing a link-state routing protocol? (Choose two.)

A. the high volume of link-state advertisements in a converged network
B. the large size of the topology table listing all advertised routes in the converged network
C. the sequencing and acknowledgment of link-state packets
D. the high demand on router resources to run the link-state routing algorithm
E. the requirement for a hierarchical IP addressing scheme for optimal functionality

Answer: D,E

QUESTION NO: 308

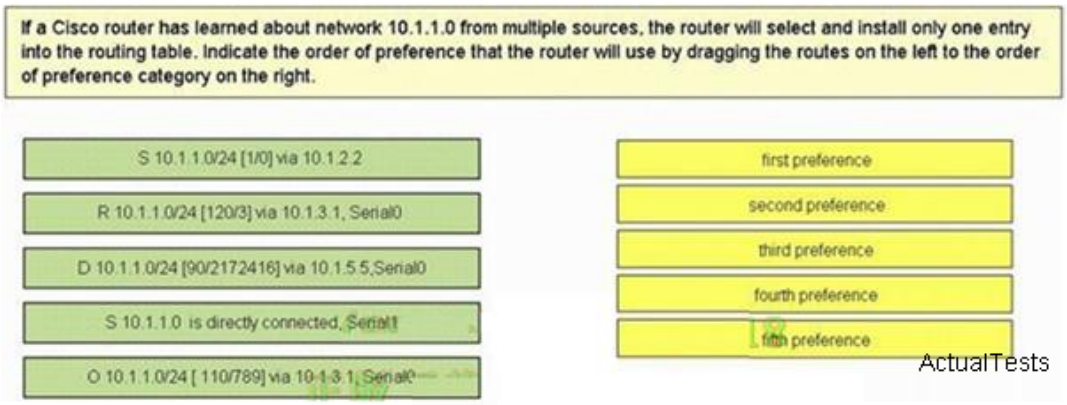
A router has learned three possible routes that could be used to reach a destination network. One route is from EIGRP and has a composite metr of 20514560. Another route is from OSPF with a metric of 782. The last is from RIPv2 and has a metric of 4. Which route or routes will the router install in the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

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

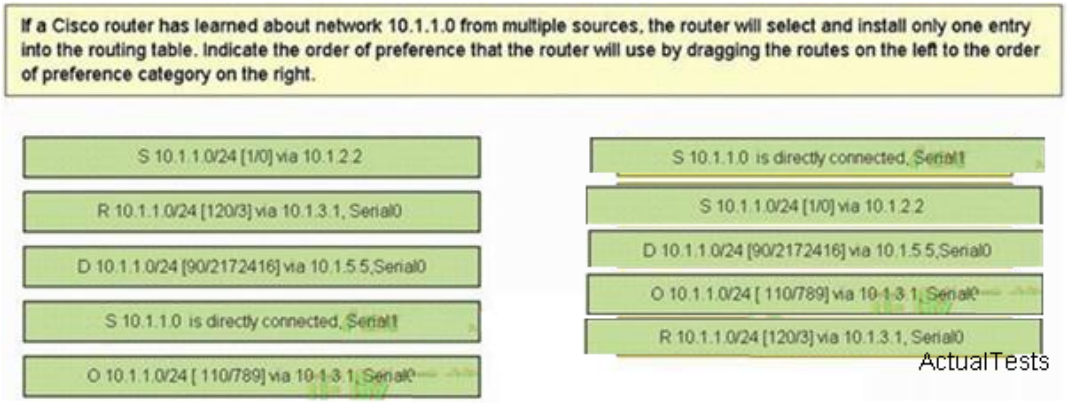
Answer: B

QUESTION NO: 309 DRAG DROP

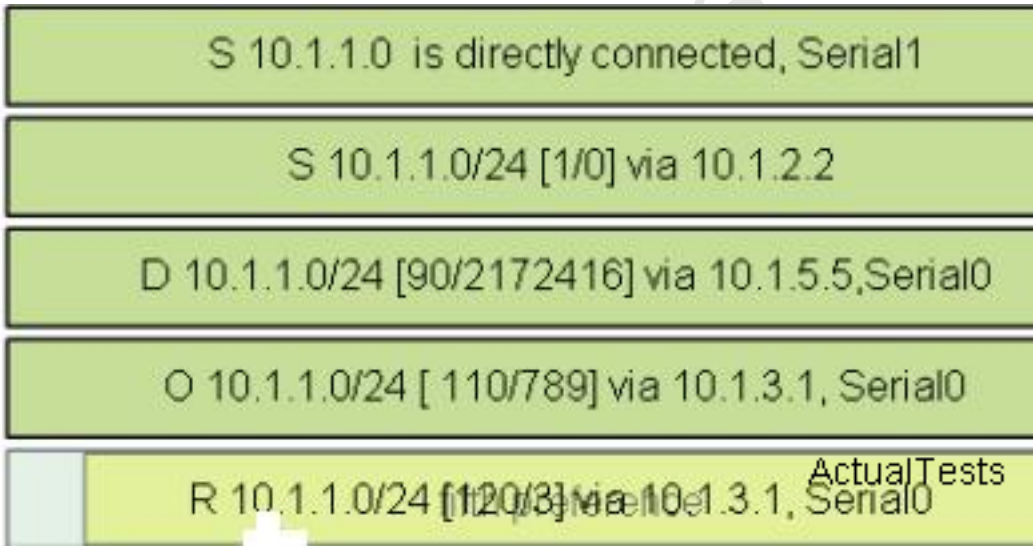
If a Cisco router has learned about network 10.1.1.0 from multiple sources, the router will select and Install only one entry into the routing table. Indicate the order of preference that the router will use by dragging the routes on the left to the -- of preference category on the right.



Answer:

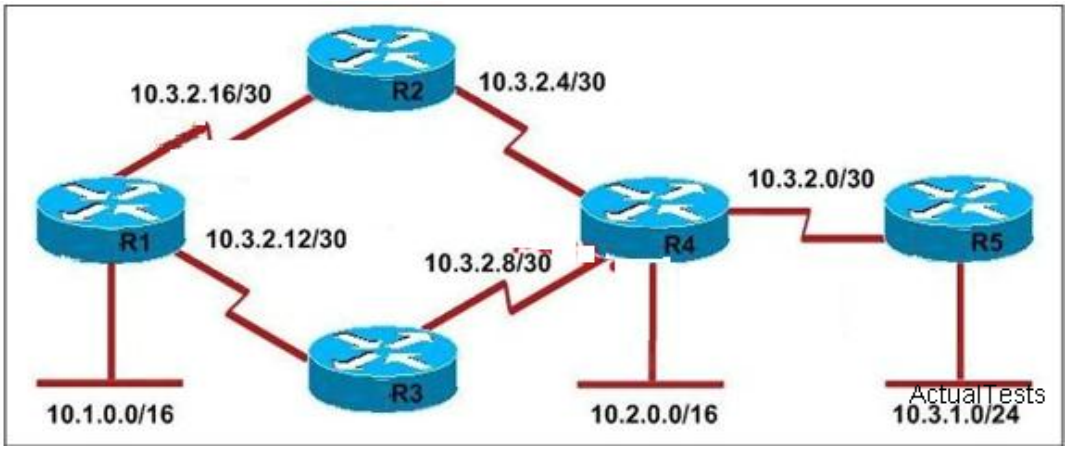


Explanation:



QUESTION NO: 310

Refer to the following routing protocols, which three will you use in the following presented enterprise network? (Choose three.)



A. BGP
B. RIP v2
C. EIGRP
D. OSPF

Answer: B,C,D

QUESTION NO: 311

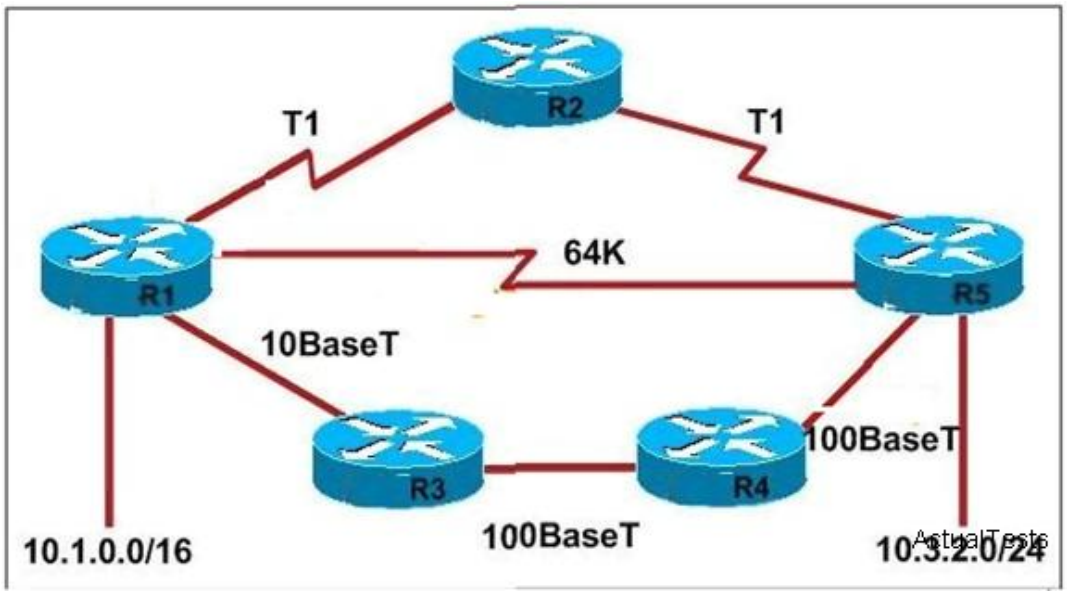
What information can be used by a router running a link-state protocol to build and maintain its topological database? (Choose two.)

A. hello packets
B. beacons received on point-to-point links
C. LSAs from other routers
D. routing tables received from other link-state routers

Answer: A,C

QUESTION NO: 312

Study the following exhibit carefully, if the routing protocol provided in each option below is configured with its default settings and the given routing protocol is working on all the routers. Which two descriptions are correct about the path to be selected between networks 10.1.0.0 and 10.3.2.0 for the routing protocol mentioned? (Choose two.)



A. If OSPF is the routing protocol, the path will be from R1 to R3 to R4 to R5.
B. If OSPF is the routing protocol, the path will be from R1 to R5.
C. If RIPv2 is the routing protocol, the path will be from R1 to R3 to R4 to R5.
D. If RIPv2 is the routing protocol, the path will be from R1 to R5.

Answer: A,D

QUESTION NO: 313

Which routing protocol by default uses bandwidth and delay as metrics?

A. EIGRP
B. RIP
C. BGP
D. OSPF

Answer: A

Explanation:
This question tests the metrics of various routing protocols.
RIP uses hop-count as metrics; BGP uses complicated path attributes as metrics; OSPF uses bandwidth as metrics; and EIGRP uses bandwidth and delay as metrics by default.

QUESTION NO: 314

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

QUESTION NO: 315

Which routing protocols will support the following IP addressing scheme? (Choose three.)

Network 1 - 192.168.10.0 /26
Network 2 - 192.168.10.64 /27
Network 3 - 192.168.10.96 /27
Network 4 - 192.168.10.128 /30
Network 5 - 192.168.10.132 /30

A. RIP version 1
B. RIP version 2
C. IGRP
D. EIGRP
E. OSPF

Answer: B,D,E

Explanation:
Section 12: Configure, verify, and troubleshoot OSPF (19 questions)

QUESTION NO: 316

Refer to the exhibit. Why are two OSPF designated routers identified on Core_Router?

```
Core_Router# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
208.149.23.194    1   FULL/DR         00:00:33    190.172.32.10   Ethernet1
208.149.23.66     1   FULL/BDR        00:00:32    190.171.23.13   Ethernet0
208.149.23.130    1   FULL/DR         00:00:39    190.171.23.10   Ethernet0

Core_Router#                                                  ActualTests
```

A. The DR election is still underway and there are two contenders for the role.
B. The router at 208.149.23.130 is a secondary DR in case the primary fails.
C. Core_Router is connected to more than one multiaccess network.
D. Two router IDs have the same OSPF priority and are therefore tied for DR election.

Answer: C

Explanation:
OSPF neighbors process multicast hello packets upon multicast address 224.0.0.5 to find neighbors dynamically. Default hello packets sending interval is 10 seconds, and dead interval is 40 seconds. In multi-access broadcasting network (such as Ethernet Net and Token Ring), DR/BDR elections are needed. When electing DR/BDR, hello packets priority is considered, the highest priority is DR, then BDR. Default priority is 1. In the circumstances when Priority is the same, RID will be considered, the highest rating RID is DR, and then BDR. When you set the priority 0, OSPF router can not become DR/BDR, it will only turn into DROTHER. From the above OSPF neighbors table, we learn that Ethernet1 and Ethernet0 select DR correspondingly, and Core_Router is connected two multi-access networks.

QUESTION NO: 317

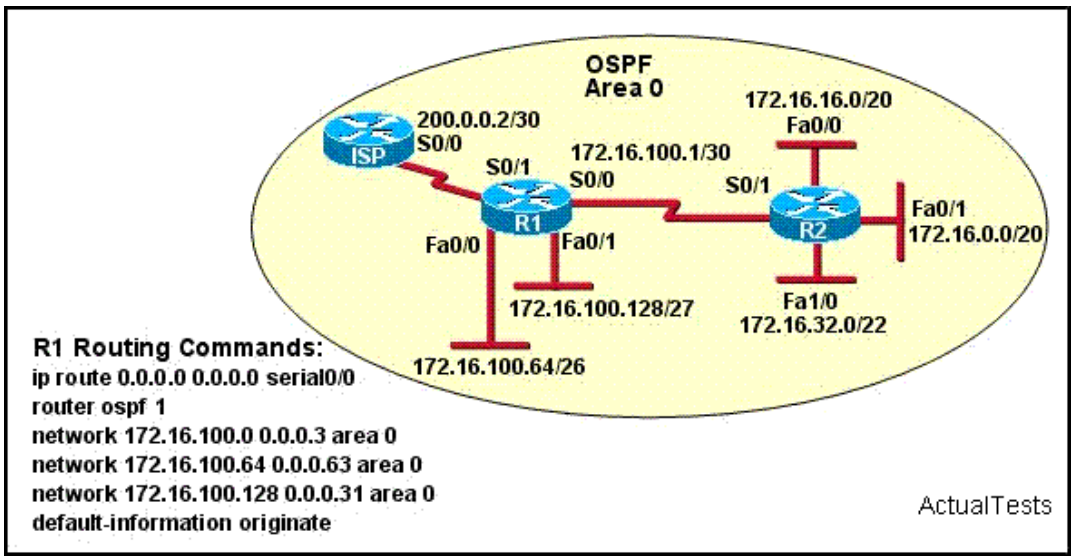
Which of the following describe the process identifier that is used to run OSPF on a router? (Choose two.)

A. It is locally significant.
B. It is needed to identify a unique instance of an OSPF database.
C. All routers in the same OSPF area must have the same process ID if they are to exchange routing information.
D. It is globally significant.
E. It is an optional parameter required only if multiple OSPF processes are running on the router.

Answer: A,B

QUESTION NO: 318

Refer to the exhibit. Assume that all router interfaces are operational and correctly configured. In addition, assume that OSPF has been correctly configured on router R2. How will the default route configured on R1 affect the operation of R2?



A. Any packet destined for a network that is not directly connected to router R2 will be dropped immediately.
B. Any packet destined for a network that is not referenced in the routing table of router R2 will be directed to R1. R1 will then send that packet back to R2 and a routing loop will occur.
C. Any packet destined for a network that is not directly connected to router R1 will be dropped.
D. The networks directly connected to router R2 will not be able to communicate with the 172.16.100.0, 172.16.100.128, and 172.16.100.64 subnetworks.
E. Any packet destined for a network that is not directly connected to router R2 will be dropped immediately because of the lack of a gateway on R1.

Answer: B

QUESTION NO: 319

Which one of the following OSPF network types needs to select a BDR?

A. point-to-multipoint and multiaccess
B. nonbroadcast and broadcast multipoint
C. point-to-point and point-to-multipoint
D. point-to-point and multi-access
E. nonbroadcast and broadcast multiaccess

Answer: E

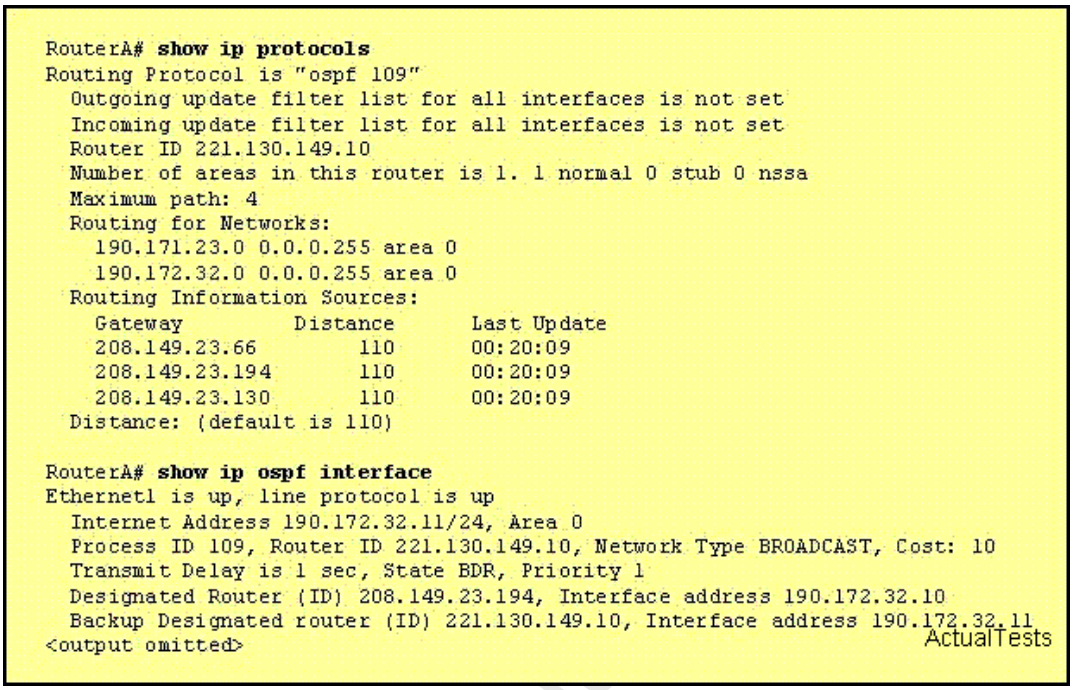
Explanation:
When selecting DR and BDR in the NBMA network, OSPF will use the unicast mode.
By adjusting the hello/dead timers you can make non-compatible OSPF network types appear as neighbors via the "show ip ospf neighbor" but they won't become "adjacent" with each other.
OSPF network types that use a DR (broadcast and non-broadcast) can neighbor with each other and function properly. Likewise OSPF network types (point-to-point and point-to-multipoint) that do not use a DR can neighbor with each other and function properly. But if you mix DR types with

non-DR types they will not function properly (i.e. not fully adjacent). You should see in the OSPF database "Adv Router is not-reachable" messages when you've mixed DR and non-DR types.

OSPF has different Network Types Point-to-Point Point-to-Multipoint Broadcast Multi-Access Non-Broadcast Multi-Access
OSPF will elect a DR and a BDR on Broadcast Multi-Access and Non-broadcast Access.

QUESTION NO: 320

Refer to the exhibit. Why was RouterA not elected as the designated router?



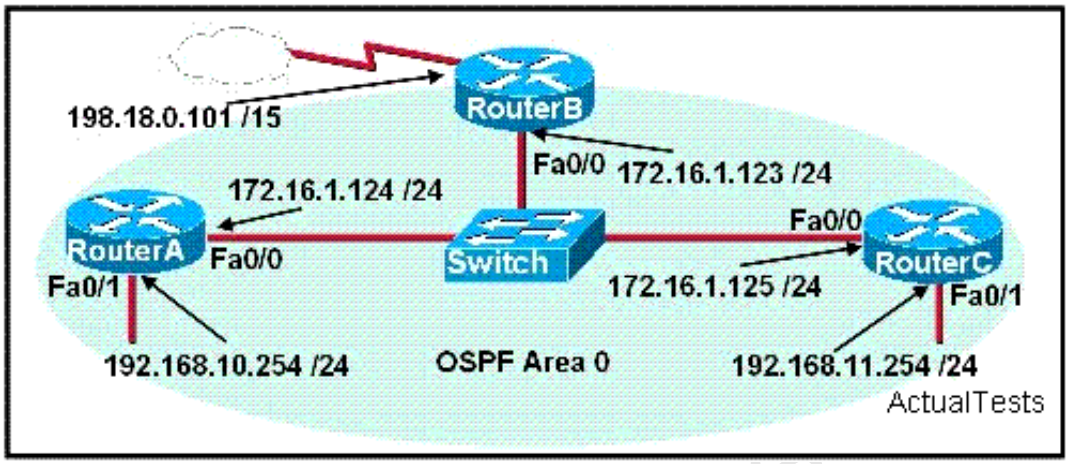
A. The OSPF process ID of RouterA is lower than the process ID of the elected DR.
B. RouterA has a lower OSPF priority value than the router elected as DR.
C. The interface address of RouterA is a higher value than the interface address of the DR.
D. RouterA is not advertising the interface with address 221.130.149.10.

Answer: D

Explanation:
The routeA advertised can be known from the output of 'show ip protocols' provided in the exhibit
190.171.23.0 0.0.0.255 area 0
190.171.32.0 0.0.0.255 area 0
Not advertising the interface of 221.130.149.10.
In broadcast multi-access networks, the routers perform DR and BDR election, more often than not, after being enabled, the routers on the Ethernet will use Hello protocol to select DR and BDR, and the rest routers will attempt to establish neighbor relationships with DR and BDR. If an interface is not advertised, it will not participate in the election.

QUESTION NO: 321

A network administrator is configuring the routers in the graphic for OSPF. The OSPF process has been started and the networks have been configured for Area 0 as shown in the diagram. The network administrator has several options for configuring RouterB to ensure that it will be preferred as the designated router (DR) for the 172.16.1.0 /24 LAN segment. What configuration tasks could be used to establish this preference? (Choose three.)



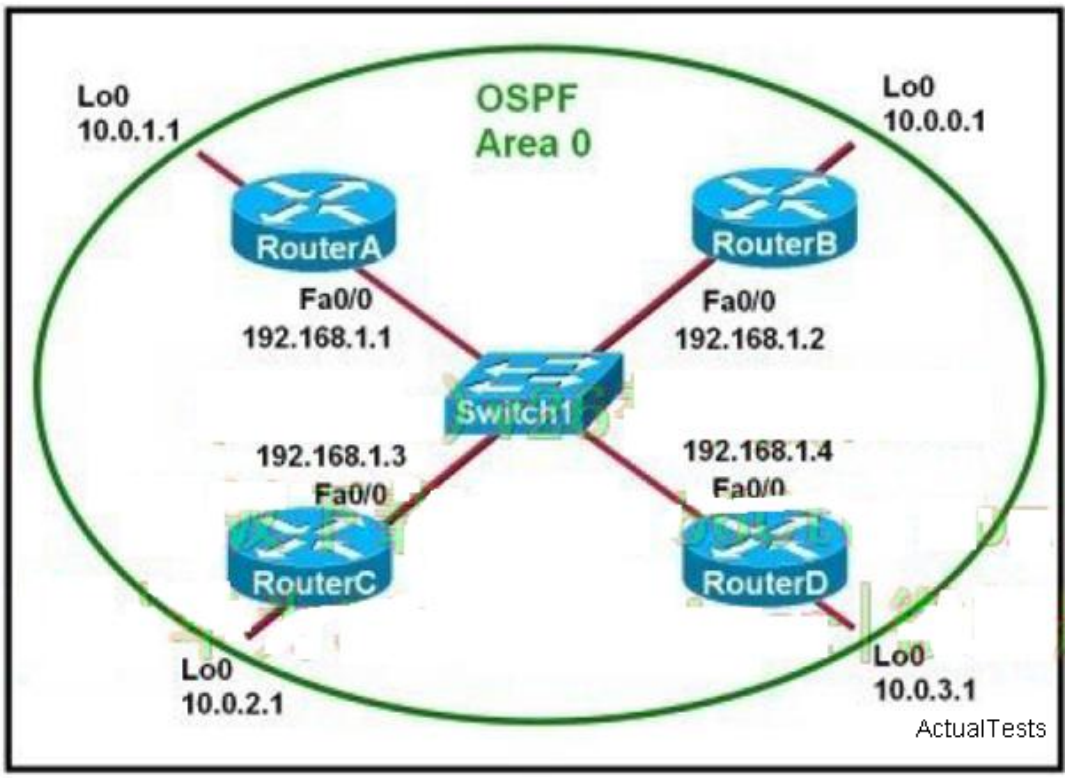
A. Configure the priority value of the Fa0/0 interface of RouterB to a higher value than any other interface on the Ethernet network.
B. Change the priority values of the Fa0/0 interfaces of RouterA and RouterC to zero.
C. Configure a loopback interface on RouterB with an IP address higher than any IP address on the other routers.
D. Change the router id of Router B by assigning the IP address 172.16.1.130/24 to the Fa0/0 interface of RouterB.
E. Change the priority value of the Fa0/0 interface of RouterB to zero.
F. No further configuration is necessary.

Answer: A,B,C

Explanation:
In order to ensure that a router will become the OSPF DR for any given segment, there are a number of options. One way is to manually configure the interface priority as described in option A above using the "ip ospf priority" interface configuration command. The second method is described in option C. OSPF routers will always use the loopback interface IP address as the router ID, when configured, and the router with the highest IP address will be chosen as the DR when the priorities are the same. The final method is to change the priority of the other routers in the segment to zero. When the OSPF priority is set to 0, the router is ineligible to become the DR or the BDR. Important Note: The OSPF DR/BDR election process is not pre-emptive, so any changes to the network regarding the DR/BDR election process will only occur when the routers are restarted.

QUESTION NO: 322

Refer to the exhibit. Which two statements are true about the loopback address that is configured on RouterB? (Choose two.)



A. It specifies that the router ID for RouterB should be 10.0.0.1.
B. It decreases the metric for routes that are advertised from SWITCH2.
C. It provides stability for the OSPF process on RouterB.
D. It ensures that data will be forwarded by SWITCH2.

Answer: A,C

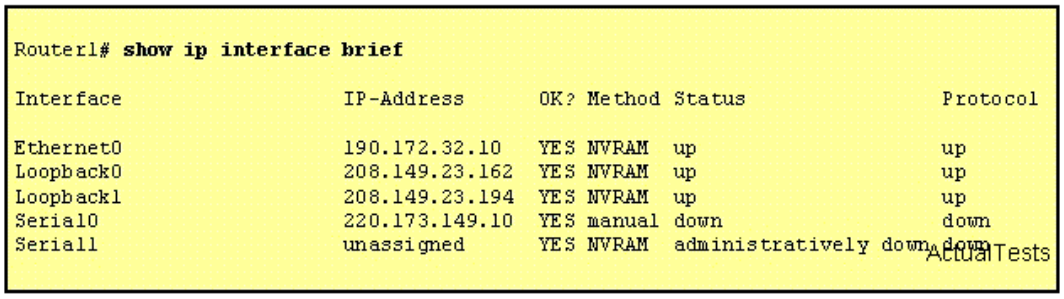
Explanation:
If configure loopback interface on a router with OSPF , the router will use the IP address of this interface as OSPF ROUTER ID, although there may be larger IP address on the router (OSPF optimizes the larger IP address as ROUTER ID) . Because the loopback interface will not be down and it is more stable than other interfaces, OSPF will choose the address of the loopback interface as the ROUTER ID and will use the larger address found first as the ROUTER ID.

A loopback interface is virtual in nature, and thus will never go down as long as the router is powered on. It doesn't rely on any physical network or cable to be plugged in. This makes it a prime choice for any good reference point. That brings us to the "why" about using it. When OSPF routers talk to one another, they all identify themselves. That is done by a RID, or Router ID value. An OSPF router may talk to many neighbors out multiple interfaces, but it only has one Router ID it uses for all conversations. How does a router choose its identifier? Well, there are a couple

ways. Typically, the router chooses its highest IP address of all physical interfaces. However, if there's a loopback interface (seen as a manual intervention), the OSPF process will always use the loopback address as its RID value.
In this network, stability is ensured for SWITCH2 as it will not become the DR or the BDR because the other routers will have a higher router ID since the have a higher loopback IP address. The DR/BDR election process is as follows:
A designated router (DR) is the router elected by the network by elections. The DR is elected based on the following default criteria:
* If the priority setting on a OSPF router is set to 0, that means it can NEVER become a DR or BDR.
* When a DR fails and the BDR takes over, there is another election to see who becomes the replacement BDR.
* The router sending the Hello packets with the highest priority.
* If two or more routers tie with the highest priority setting, the router sending the Hello with the highest RID (Router ID) wins.
* (NOTE) A RID is the highest logical (loopback) IP address configured on a router, if no logical/loopback IP address is set then the Router uses the highest IP address configured on its interfaces. (e.g. 192.168.0.1 would be higher than 10.1.1.2)
* Usually the router with the second highest priority number becomes the BDR (Backup Designated Router)
* The range of priority values range from 1 - 255, with a higher value increasing its chances of becoming DR or BDR.
* IF a HIGHER priority OSPF router comes online AFTER the election has taken place, it will not become DR or BDR until (at least) the DR and BDR fail.

QUESTION NO: 323

Refer to the exhibit. Router1 was just successfully rebooted. Identify the current OSPF router ID for Router1.



```
Router1# show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol

Ethernet0                  190.172.32.10   YES NVRAM  up                    up
Loopback0                  208.149.23.162  YES NVRAM  up                    up
Loopback1                  208.149.23.194  YES NVRAM  up                    up
Serial0                    220.173.149.10  YES manual down                  down
Serial1                    unassigned      YES NVRAM  administratively down down
```


A. 208.149.23.194
B. 208.149.23.162
C. 190.172.32.10
D. 220.173.149.10

Answer: A

Explanation:
To identify the router ID for Router1, do as follows:
Step 1 Choose from all the activated interfaces.
Step 2 Compare the IP addresses of loopback interfaces.
Step 3 If there are no loopback interfaces, compare the IP addresses of all the physical interfaces.

Configures an OSPF router ID.
Description: Router ID is the tie-breaker for OSPF path selection. The path selection process uses a variety of metrics to select a route. If all other metrics (accessibility, administrative weight, local preference, etc.) are equal, OSPF determines the router ID using the following priority:
1.Use the address configured by the ospf router-id command
2.Use the address of the loopback 0 interface
3.Use the highest IP address of any interface
4.If no interface exists, set the router-ID to 0.0.0.0
5.If no OSPF router ID is explicitly configured, OSPF computes the router-ID based on the items 2, 3, and 4 and restarts OSPF (if the process is enabled and router-ID has changed).
WARNING The ospf router-id command causes the OSPF process to restart using the new router-ID (if the processes are enabled and router-ID has changed).
Use ospf router-id ip-address command to set the OSPF router ID for the system.
Use the no ospf router-id to configure the OSPF router ID as the default value (address of the loopback 0 interface).

QUESTION NO: 324

The interface brief message is shown below:

```
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#
```

Please study the exhibit carefully, And you has configured OSPF with the command:

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

After completing the configuration, you 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. Serial0/1.102
B. Serial0/1.104
C. FastEthernet0 /1
D. Serial0/0

Answer: A,C,D

Explanation:
The binary version of 63 is 111111 and the binary version of 64 is 01000000.
The interfaces in the 192.168 .12.64-192.168.12.127 network segment can participate in OSPF.
F0/1 is on the 192.168 .12.65 network.
Serial0/0 is on the 192.168 .12.121 network.
Serial0/1.102 is on the 192.168 .12.125 network.

OSPF uses the concept of wildcard masks much like access list filters. OSPF network matches are done using the network number and wildcard bits. The network number is the network portion of the IP address, with the host bits all set to zero. The wildcard bits determine which portion of the address the access list will act on. Only bits set to zero are acted upon (bits set to one are ignored.) This is the exact opposite of a netmask. Remember that this number is in bits, and you will always have all zeros to the left of the first one, and all ones to the right of the last zero. The table below shows some examples of netmasks and wildcard bits.

Type of network	Netmask	Wildcard Bits
Class A	255.0.0.0	0.255.255.255
Class B	255.255.0.0	0.0.255.255
Class C	255.255.255.0	0.0.0.255
Class C 2-bit subnet	255.255.255.192	0.0.0.63
Class B 4-bit subnet	255.255.240.0	0.0.31.255

In this example, the 192.168.12.64 0.0.0.63 will comprise of all interfaces with an IP address in the 192.168.12.64-127 range.

QUESTION NO: 325

The OSPF Hello protocol performs which of the following tasks? (Choose two.)

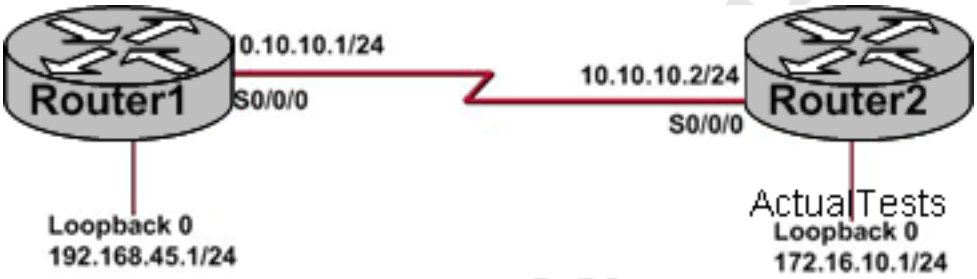
A. It detects unreachable neighbors in 90 second intervals.
B. It uses timers to elect the router with the fastest links as the designated router.
C. It broadcasts hello packets throughout the internetwork to discover all routers that are running OSPF.
D. It negotiates correctness parameters between neighboring interfaces.
E. It maintains neighbor relationships.
F. It provides dynamic neighbor discovery.

Answer: E,F

Explanation:
The Hello protocol performs the following tasks:
Neighbor discovery
Neighbor keepalive

QUESTION NO: 326

Based on this information shown below, when running OSPF, what would cause router Router1 not to form an adjacency with router Router2?



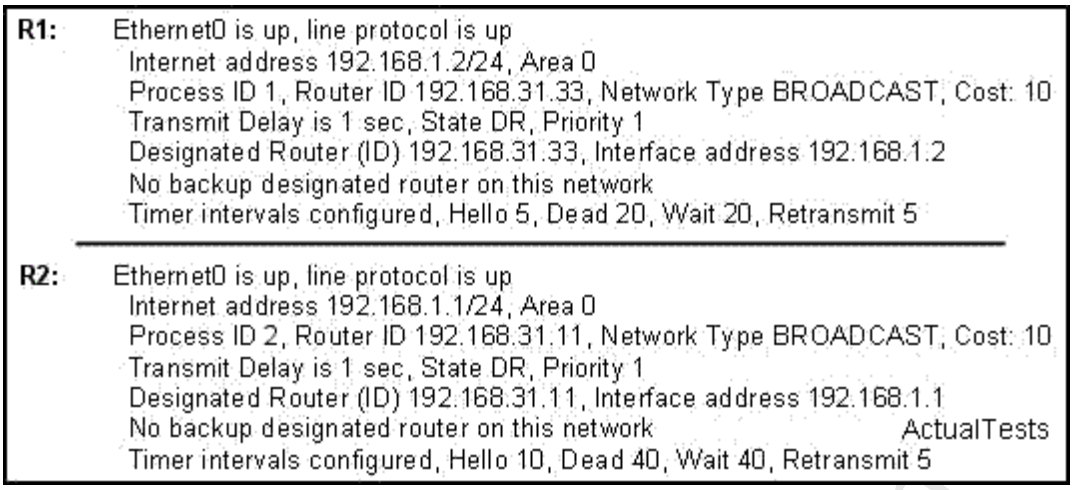
A. The process identifier on Router1 is different than the process identifier on Router2.
B. Route summarization is enabled on both routers.
C. The loopback addresses are on different subnets.
D. The values of the dead timers on the routers are different.

Answer: D

Explanation:
OSPF adjacent relations establishment needs consistent parameters such as AreaID, hello timer, dead timer, authentication, compatible network type, and MTU. In addition that the same type of network could form adjacent relations, networks with the same view upon DR/BDR elections are also able be form adjacent relations, such as broad and non-b.

QUESTION NO: 327

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. 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 priority on R1 should be set higher.
B. The hello and dead timers are not configured properly.
C. The OSPF process ID numbers must match.
D. The cost on R1 should be set higher.
E. A backup designated router needs to be added to the network.
F. The OSPF area is not configured properly.

Answer: B

Explanation:
As can be seen above, the hello interval for R1 has been set to 5 seconds, while it is set to 10 for R2. Also, the dead interval on R1 is set at 20 seconds while on router R2 it is set to 40 seconds. In order for two routers to establish an OSPF neigh adjacency, the hello and dead timers must match

QUESTION NO: 328

On point-to-point networks, OSPF hello packets are addressed to which address?

A. 172.16.0.1
B. 254.255.255.255
C. 224.0.0.5
D. 127.0.0.1
E. 223.0.0.1
F. 192.168.0.5

Answer: C

Explanation:

The multicast IP address 224.0.0.5 is known as 'AllSPFRouters.' All routers running OSPF should be prepared to receive packets sent to this address since hello packets are always sent to this destination. Also, certain OSPF protocol packets are sent to this address during the flooding procedure.

Incorrect Answers:

A: This is the IP address reserved for the internal loopback on PC hosts. All windows based PC's will use this internal IP address, assuming that the TCP/IP stack is correctly installed. B, D. These addresses are part of the range of addresses reserved for internal use, as defined in RFC 1918.

QUESTION NO: 329

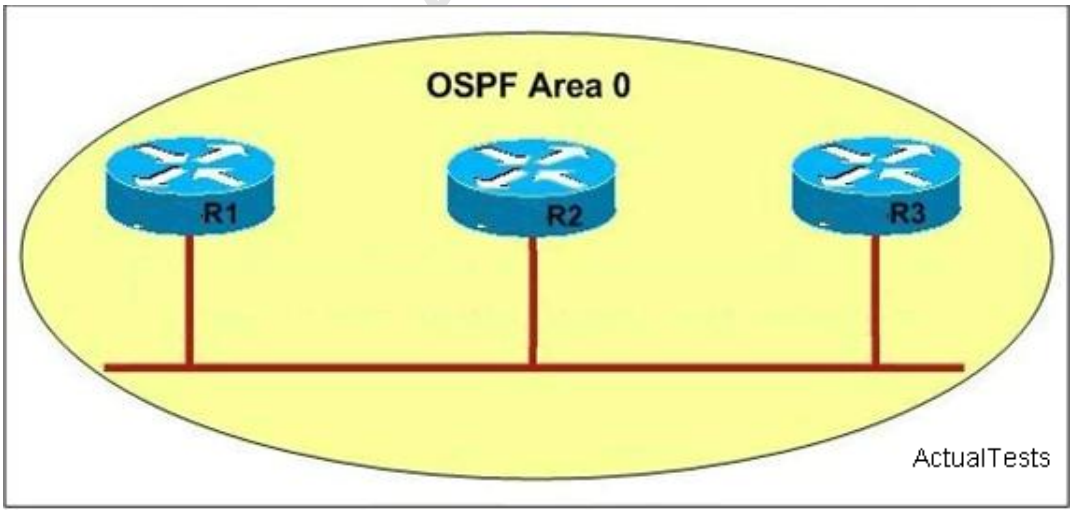
OSPF routing uses the concept of areas. What are the characteristics of OSPF areas? (Choose Three.)

A. Each OSPF area requires a loopback interface to be configured.
B. Areas may be assigned any number from 0 to 65535.
C. Area 0 is called the backbone area.
D. Hierarchical OSPF networks do not require multiple areas.
E. Multiple OSPF areas must connect to area 0.
F. Single area OSPF networks must be configured in area 1.

Answer: B,C,E

QUESTION NO: 330

Why R1 can't establish an OSPF neighbor relationship with R3 according to the following graphic? (Choose two.)



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

B. All of the routers need to be configured for backbone Area 1.
C. R1 and R3 are configured in different areas.
D. The hello and dead interval timers are not set to the same values on R1 and R3.

Answer: C,D

QUESTION NO: 331

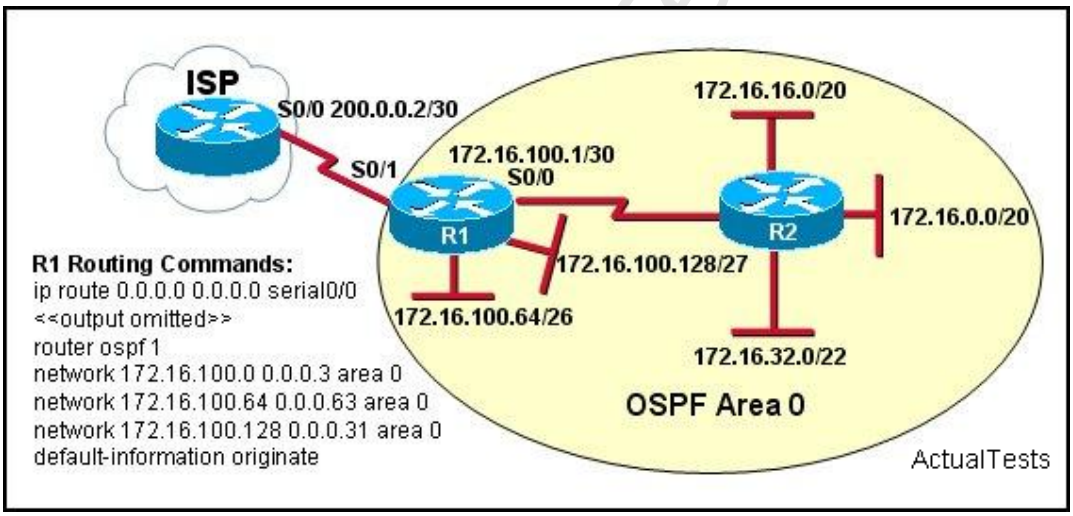
Which items are correct about the routing protocol OSPF? (Choose three.)

A. It supports VLSM.
B. It increases routing overhead on the network.
C. It confines network instability to one area of the network.
D. It allows extensive control of routing updates.

Answer: A,C,D

QUESTION NO: 332

Refer to the exhibit. Assume that all of the router interfaces are operational and configured correctly. How will router R2 be affected by the configuration of R1 that is shown in the exhibit?



A. Router R2 will not form a neighbor relationship with R1.
B. Router R2 will obtain a full routing table, including a default route, from R1.
C. R2 will obtain OSPF updates from R1, but will not obtain a default route from R1.
D. R2 will not have a route for the directly connected serial network, but all other directly connected networks will be present, as well as the two ethernet networks connected to R1.

Answer: A

QUESTION NO: 333

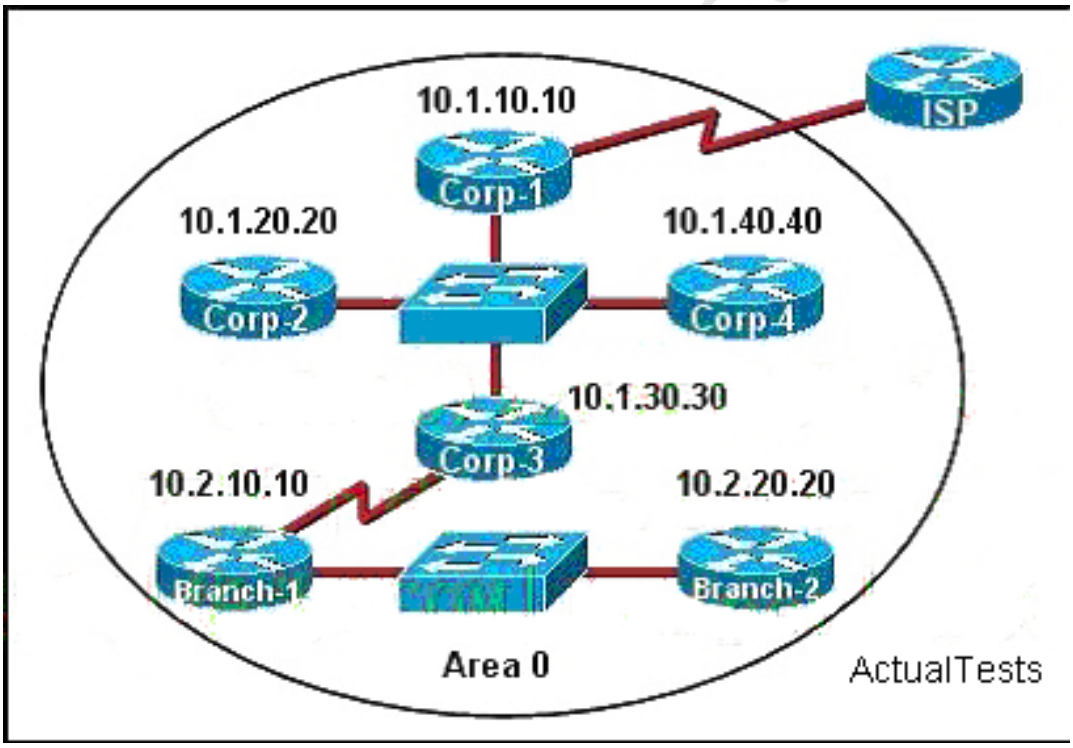
What are three characteristics of the OSPF routing protocol? (Choose three.)

A. It converges quickly.
B. OSPF is a classful routing protocol.
C. It uses cost to determine the best route.
D. It uses the DUAL algorithm to determine the best route.
E. OSPF routers send the complete routing table to all directly attached routers.
F. OSPF routers discover neighbors before exchanging routing information.

Answer: A,C,F

QUESTION NO: 334

The internetwork infrastructure of company XYZ consists of a single OSPF area as shown in the graphic. There is concern that a lack of router resources is impeding internetwork performance. As part of examining the router resources, the OSPF DRs need to be known. All the router OSPF priorities are at the default and the router IDs are shown with each router. Which routers are likely to have been elected as DR? (Choose two.)



A. Corp-1
B. Corp-2
C. Corp-3
D. Corp-4
E. Branch-1

F. Branch-2

Answer: D,F

Explanation:
Section 13: Configure, verify, and troubleshoot EIGRP (14 questions)

QUESTION NO: 335

Which tables of EIGRP route information are held in RAM and maintained through the use of hello and update packets? (Choose two.)

A. RTP table
B. SPF table
C. query table
D. neighbor table
E. DUAL table
F. topology table

Answer: D,F

Explanation:
Only the neighbor table and the topology table of EIGRP route information are held in RAM and maintained through the use of hello and update packets.

QUESTION NO: 336

Refer to the exhibit. Which address and mask combination represents a summary of the routes learned by EIGRP?

```
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 ActualTests
```

A. 192.168.25.0 255.255.255.252
B. 192.168.25.28 255.255.255.240
C. 192.168.25.16 255.255.255.240

D. 192.168.25.0 255.255.255.240
E. 192.168.25.28 255.255.255.252
F. 192.168.25.16 255.255.255.252

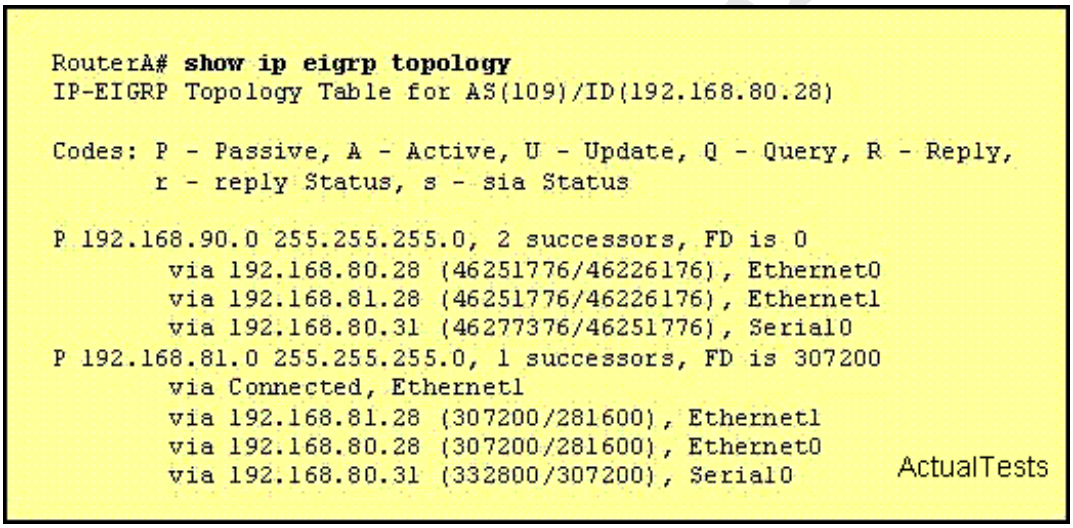
Answer: C

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.

QUESTION NO: 337

Refer to the exhibit. Why does RouterA show multiple unequal cost paths to network 192.168.81.0/24?

Exhibit:



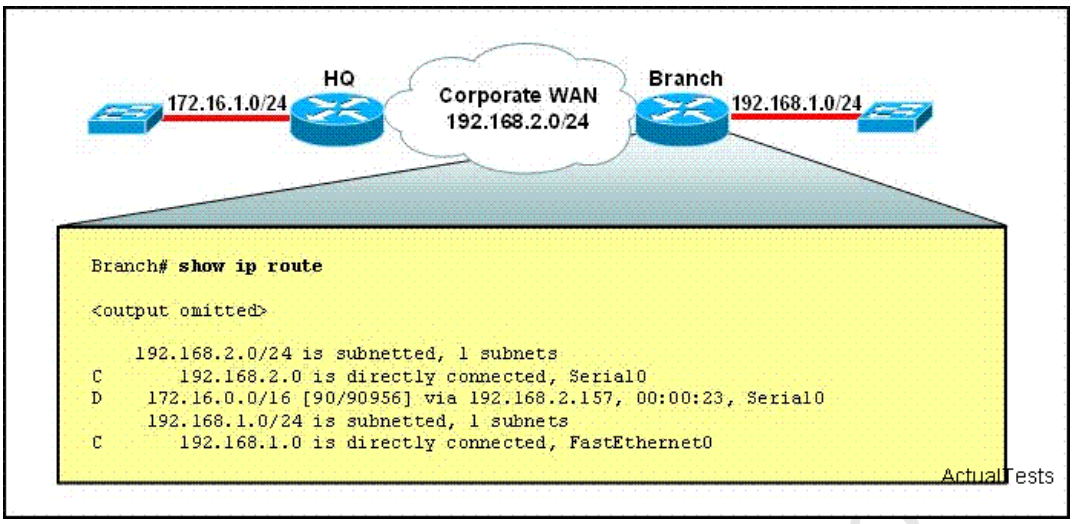
A. Multiple floating static routes were configured to network 192.168.81.0 via interface Serial0.
B. The EIGRP topology table displays all routes to a destination.
C. The EIGRP topology table shows only backup routes to a destination.
D. A variance was configured for EIGRP autonomous system 109.

Answer: B

Explanation:
EIGRP cannot display all routing information but refresh routing information based on the cost.

QUESTION NO: 338

Refer to the exhibit. The Branch router displays knowledge of a route to network 172.16.0.0/16. The actual network number at headquarters is 172.16.1.0/24. Why does the network number appear as it does in the routing table?



A. The routing protocol on the Branch router has been misconfigured.
B. The Branch router has a static route configured for the 172.16.0.0/16 network.
C. The Branch router is configured to summarize to classful boundaries.
D. The routing protocol on the HQ router is using automatic route summarization.
E. The routing protocol that is forwarding this route only sends classful updates.

Answer: D

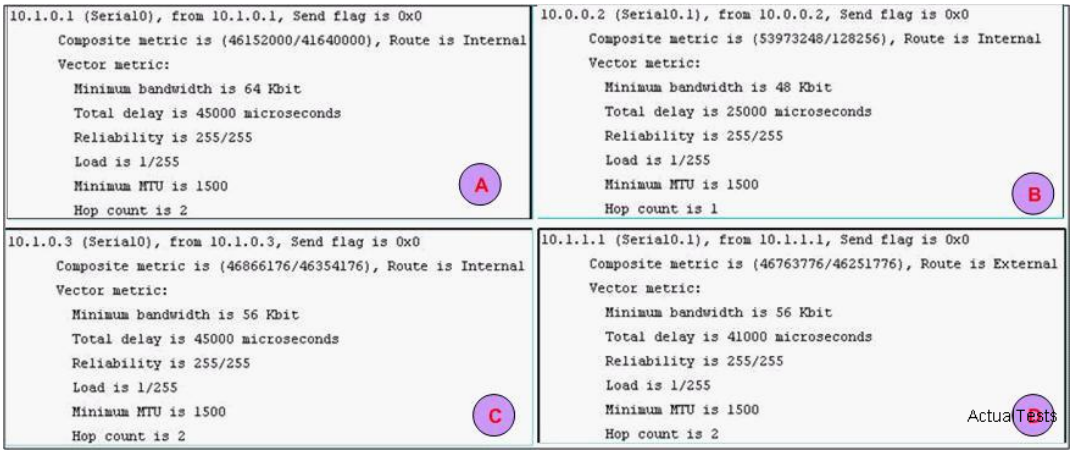
Explanation:
Automatic route summarization is enabled by default with the EIGRP routing protocol. In this example, automatic summarization will summarize the 172.16.1.0/24 network and advertise it as a 172.16.0.0/16.

From show ip route we know that the 172.16.0.0/16 learnt from 192.168.2.157 is a summary route.

QUESTION NO: 339

Refer to the exhibits. Given the output from the show ip eigrp topology command, which router is the feasible successor?

```
Router # show ip eigrp topology 10.0.0.5 255.255.255.255
IP-EIGRP topology entry for 10.0.0.5/32 State is Passive, Query
Origin flag is 1, 1 Successor(s), FD is 41152000
```



A. A
B. B
C. C
D. D

Answer: C

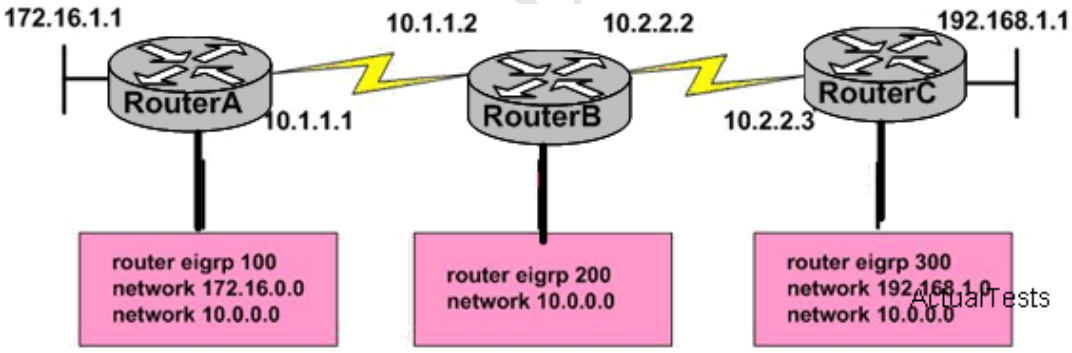
Explanation:
The AD of the feasible successor must be smaller than the FD of successor. From the output provided in the exhibit, we know that the FD of successor is 41152000.
In the option A, the AD is 41640000
In the option B , the AD is 128256
In the option C, the AD is 46354176
In the option D, the AD is 46251776.
Through comparison, we know that only the AD in option B is smaller than FD, so B can be used as feasible successor.

Successor: A successor for a particular destination is a next hop router that satisfies these two conditions:
it provides the least distance to that destination
it is guaranteed not to be a part of some routing loop
The first condition can be satisfied by comparing metrics from all neighboring routers that advertise that particular destination, increasing the metrics by the cost of the link to that respective neighbor, and selecting the neighbor that yields the least total distance. The second condition can be satisfied by testing a so-called Feasibility Condition for every neighbor advertising that destination. There can be multiple successors for a destination, depending on the actual topology. The successors for a destination are recorded in the topology table and afterwards they are used to populate the routing table as next-hops for that destination.
Feasible successor: A feasible successor for a particular destination is a next hop router that satisfies this condition:
it is guaranteed not to be a part of some routing loop
This condition is also verified by testing the Feasibility Condition.

Thus, every successor is also a feasible successor. However, in most references about EIGRP the term "feasible successor" is used to denote only those routers which provide a loop-free path but which are not successors (i.e. they do not provide the least distance). From this point of view, for a reachable destination there is always at least one successor, however, there might not be any feasible successors.
A feasible successor provides a working route to the same destination, although with a higher distance. At any time, a router can send a packet to a destination marked "Passive" through any of its successors or feasible successors without alerting them in the first place, and this packet will be delivered properly. Feasible successors are also recorded in the topology table.
AD : Advertised Distance (AD) is the distance to a particular destination as reported by a router to its neighbors. This distance is sometimes also called a Reported Distance and is equal to the current lowest total distance through a successor.
FD: A Feasible Distance (FD) is the lowest known distance from a router to a particular destination since the last time the route went from Active to Passive state. It can be expressed in other words as a historically lowest known distance to a particular destination. While a route remains in Passive state, the FD is updated only if the actual distance to the destination decreases, otherwise it stays at its present value. On the other hand, if a router needs to enter Active state for that destination, the FD will be updated with a new value after the router transitions back from Active to Passive state. This is the only case when the FD can be increased. The transition from Active to Passive state in effect marks the start of a new history for that route.

QUESTION NO: 340

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



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

Answer: B

QUESTION NO: 341

As a cisco technician, you need to know EIGRP protocol very well.

Which of the following is true about EIGRP successor routes? (Choose two.)

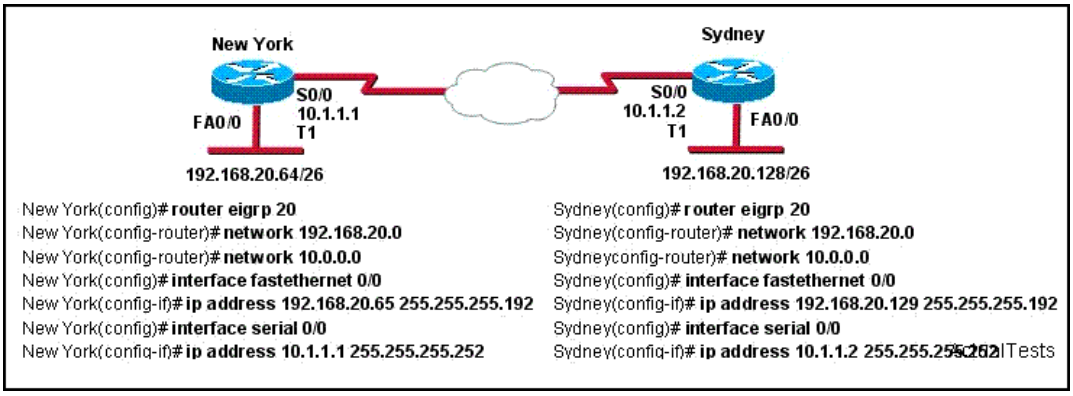
A. A successor route is used by EIGRP to forward traffic to a destination.
B. Successor routes are stored in the neighbor table following the discovery process.
C. A successor route may be backed up by a feasible successor route.
D. Successor routes are flagged as "active" in the routing table.

Answer: A,C

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

QUESTION NO: 342

Why has the network shown in the exhibit failed to converge?



A. The no auto-summary command needs to be applied to the routers.
B. The subnet masks for the network numbers have not been properly configured.
C. The network numbers have not been properly configured on the routers.
D. The autonomous system number has not been properly configured.
E. The bandwidth values have not been properly configured on the serial interfaces.

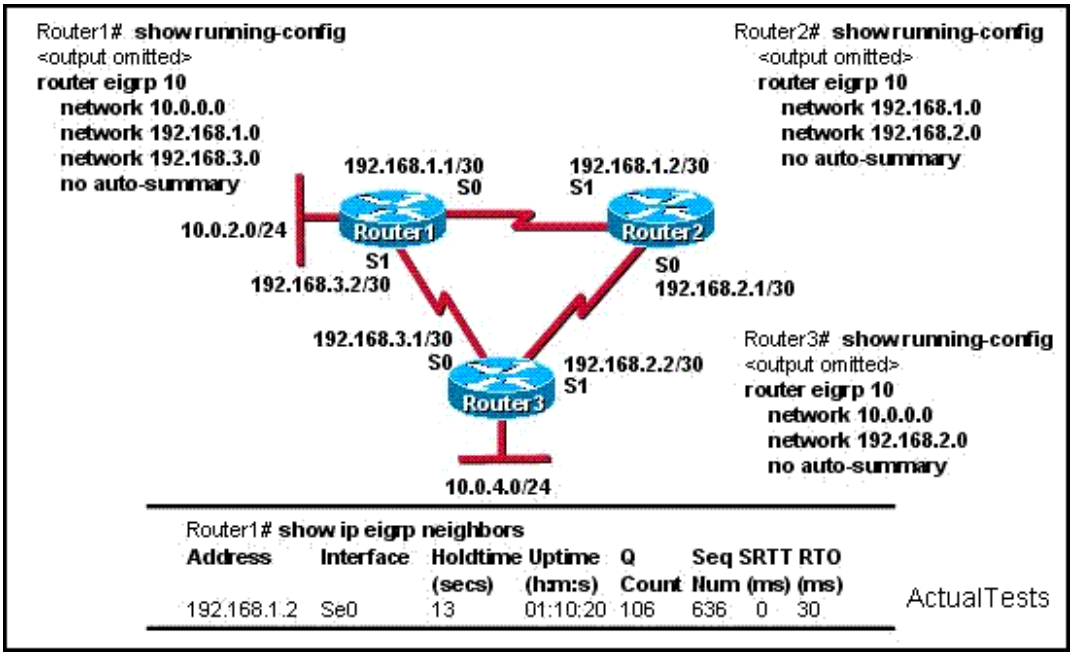
Answer: A

Explanation:
The two routers segments the network into several subnets. If auto-summary is not shut down, the disconnectivity between these subnets will occur.

More often than not, in order to solve the problem that Discontinuous subnets communicate with each other, it is needed to disable the auto-summary of route and use the manual summary to advertise routes. In the network structure shown above, assuming that auto-summary is not shut down, when the router advertises the route of 192.168.20.0/24, the route of /26 subnet will not be advertised , the result is that the network is unreachable.

QUESTION NO: 343

IP addresses and routing for the network are configured as shown in the exhibit. The network administrator issues the show ip eigrp neighbors command from Router1 and receives the output shown below the topology. Which statement is true?



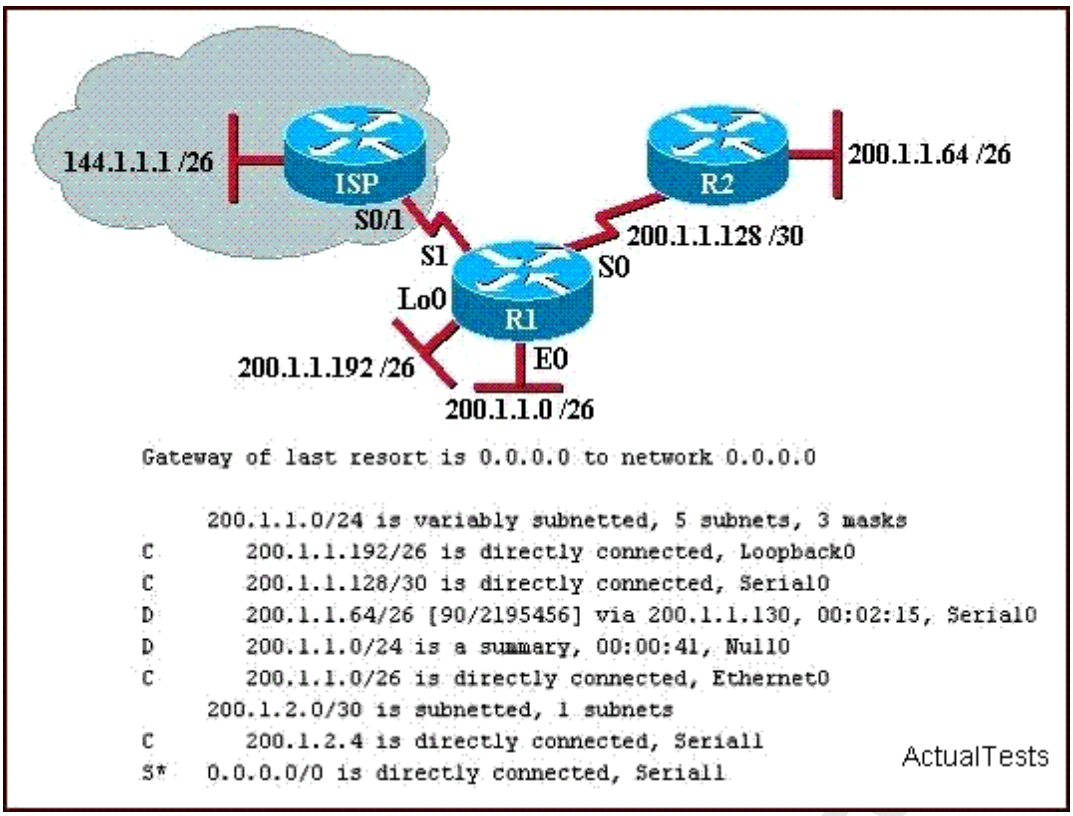
A. It is normal for Router1 to show one active neighbor at a time to prevent routing loops.
B. Routing is not completely configured on Router3.
C. The IP addresses are not configured properly on the Router1 and Router3 interfaces.
D. The no auto-summary command configured on the routers prevents Router1 and Router2 from forming a neighbor relationship.

Answer: B

Explanation:
The Router Router3 is connected to three different networks: 192.168.3.1/30, 192.168.2.2/30, and 10.0.4.0/24 but only 10.0.4.0 and 192.168.2.0 are being advertised via EIGRP. In Router3 the "network 192.168.3.0" command should be placed under the EIGRP 10 process.

QUESTION NO: 344

What can be determined from the router output shown in the graphic?



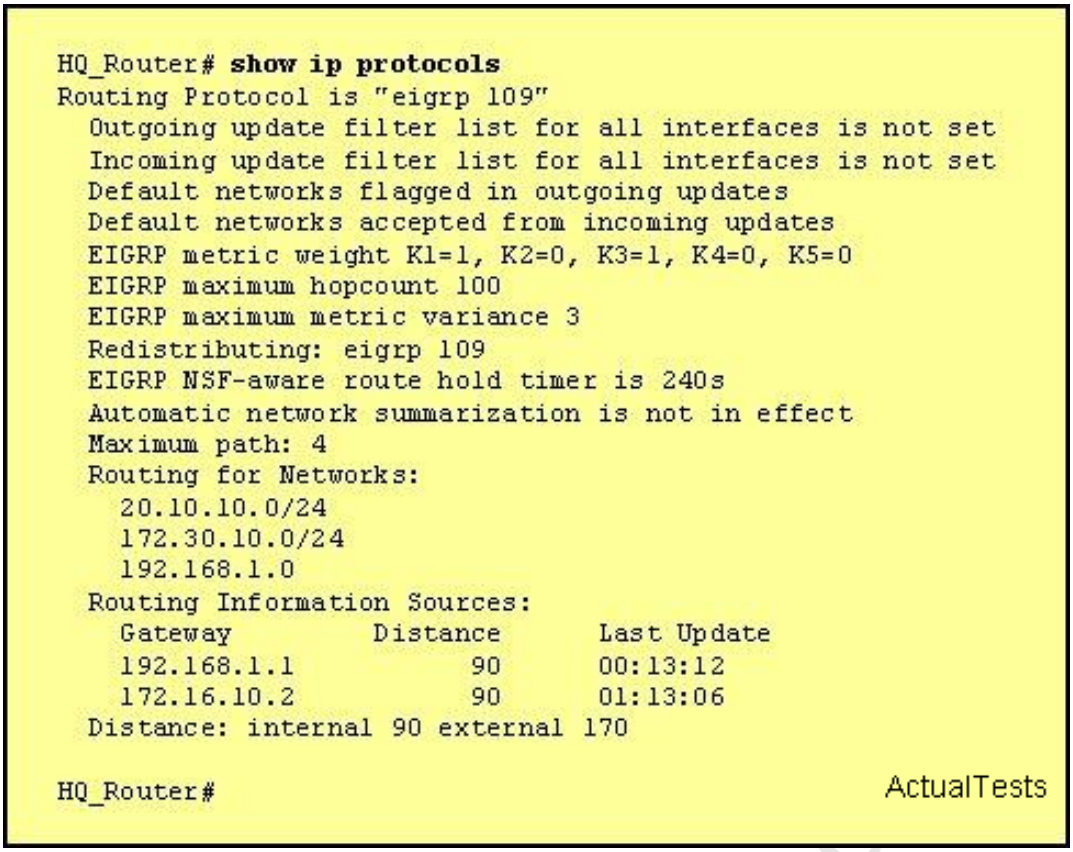
A. The output shows that there are three default routes.
B. The output came from a router that has four physical interfaces.
C. The output came from router R2.
D. EIGRP is in use in this network.
E. 200.1.1.64 is a default route.

Answer: D

Explanation:
In the routing table the "B" letter marks the route learned from EIGRP routing protocol. Based on the routing table above, there are 4 directly connected IP interfaces, 2 EIGRP learned routes (which means that EIGRP is in use on this network) and a static default route was also configured.

QUESTION NO: 345

Refer to the exhibit. How many paths can the EIGRP routing process use to forward packets from HQ_Router to a neighbor router?

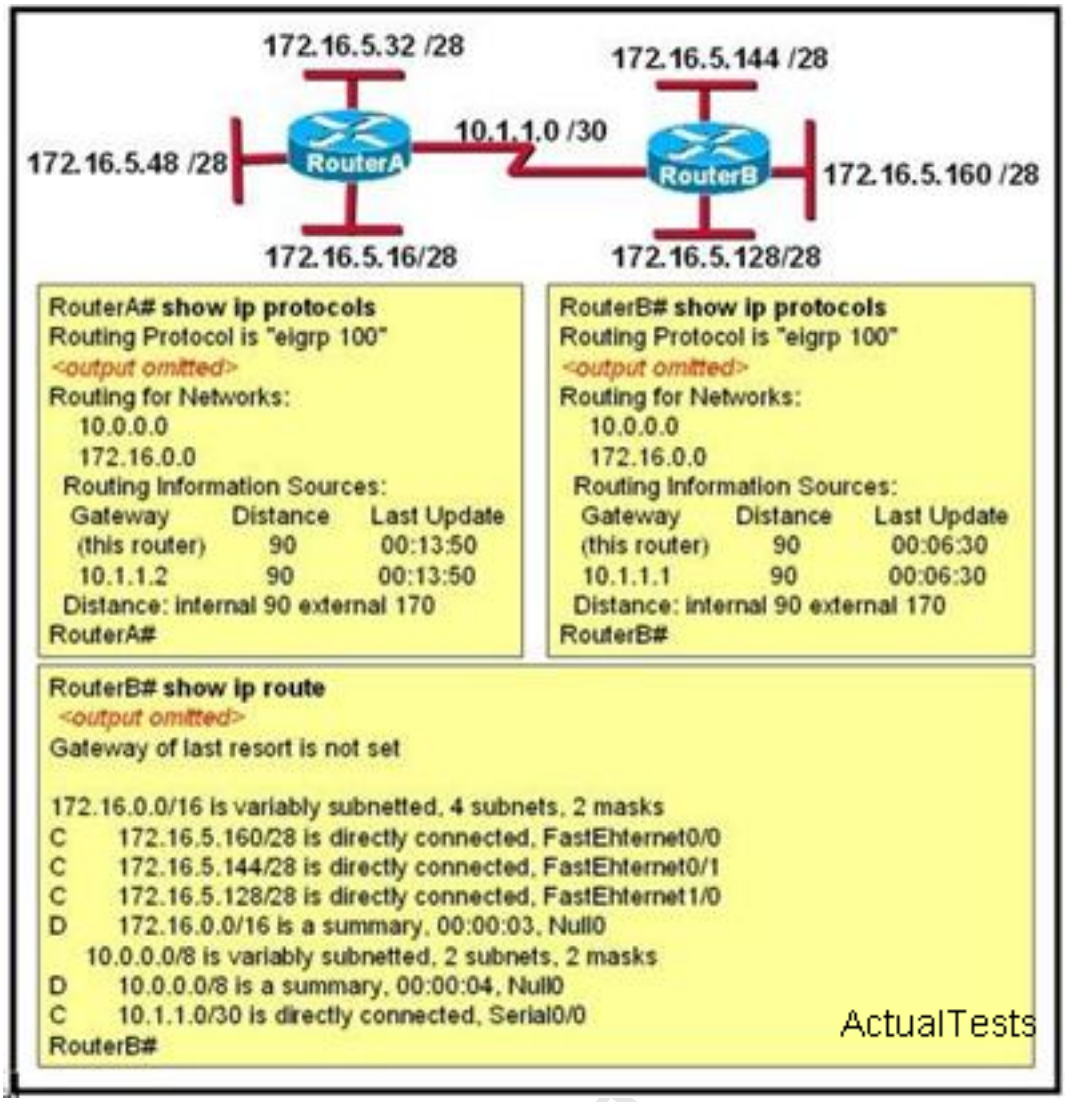


A. two equal-cost paths
B. two unequal-cost paths
C. three equal-cost paths
D. three unequal-cost paths
E. four equal-cost paths
F. four unequal--cost paths

Answer: F

QUESTION NO: 346

Refer to the exhibit. From RouterA, a network administrator is able to ping the serial interface of RouterB but unable to ping any of the subnets attached to RouterB. Based on the partial outputs in the exhibit, what could be the problem?



A. EIGRP does not support VLSM.
B. The EIGRP network statements are incorrectly configured.
C. The IP addressing on the serial interface of RouterA is incorrect.
D. The routing protocol has summarized on the classful boundary.
E. EIGRP has been configured with an invalid autonomous system number.

Answer: D

QUESTION NO: 347

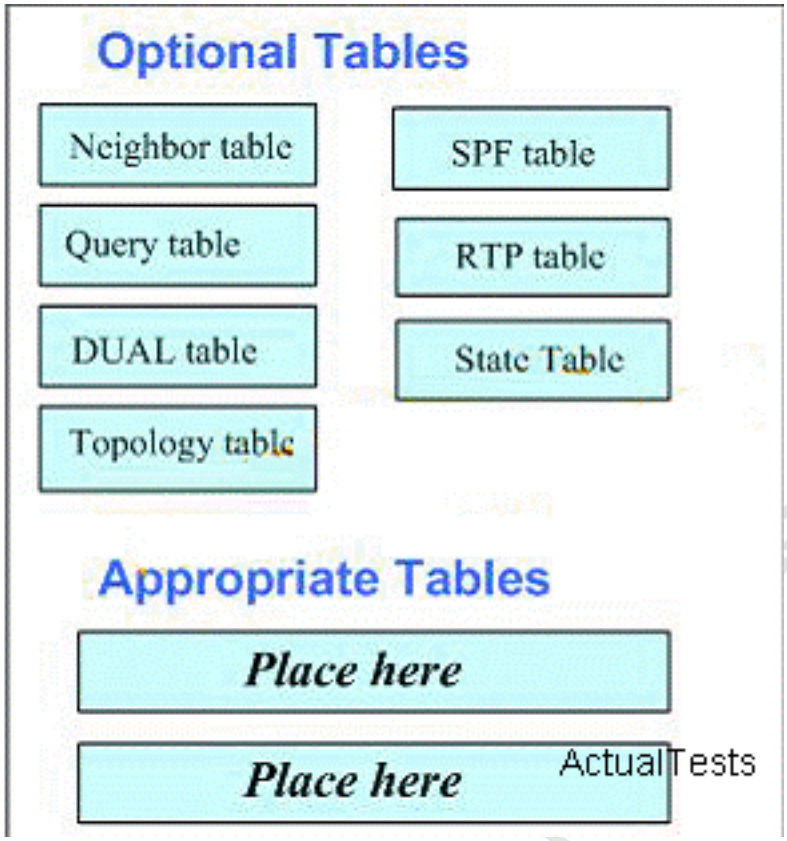
Which two statements are true regarding EIGRP? (Choose two.)

A. Passive routes are in the process of being calculated by DUAL.
B. EIGRP supports VLSM, route summarization, and routing update authentication.
C. EIGRP exchanges full routing table information with neighboring routers with every update.
D. If the feasible successor has a higher advertised distance than the successor route, it becomes the primary route.
E. A query process is used to discover a replacement for a failed route if a feasible successor is not identified from the current routing information.

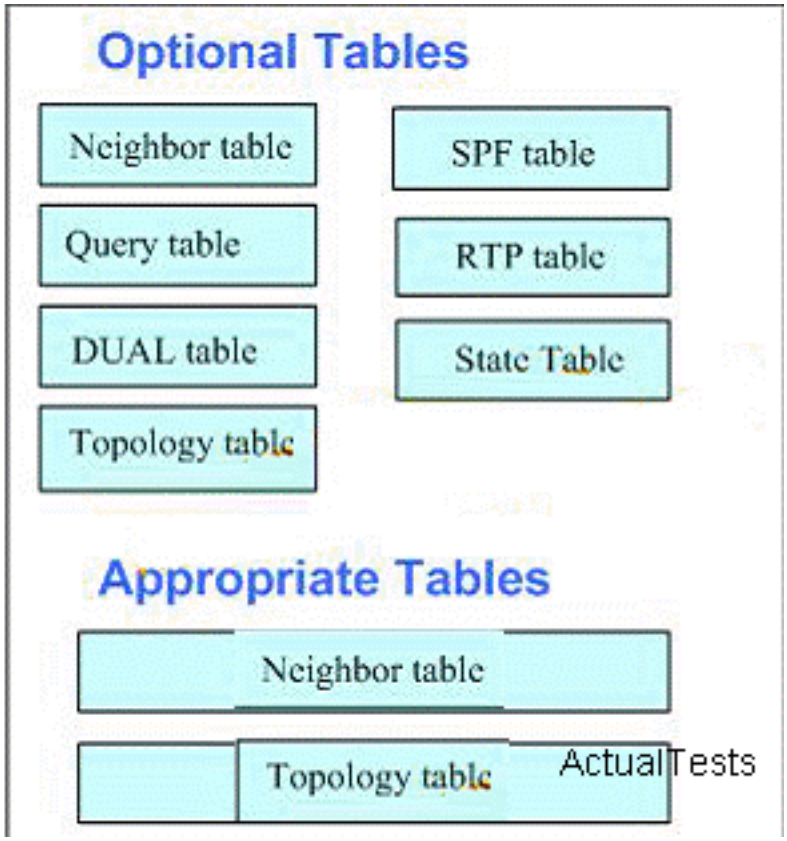
Answer: B,E

QUESTION NO: 348 DRAG DROP

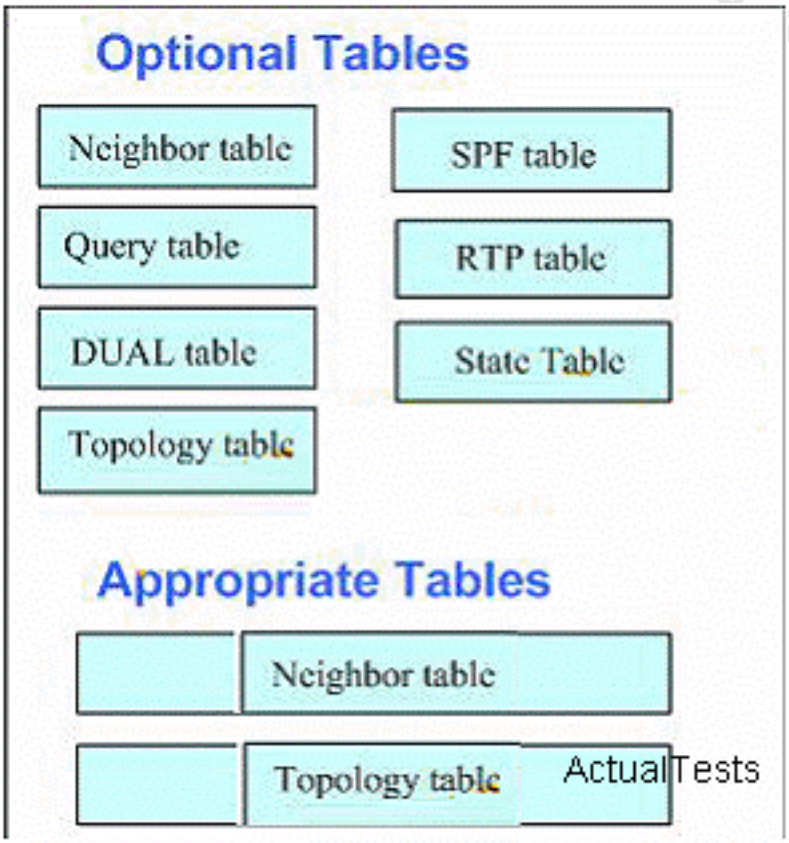
As a CCNA candidate, you need to know EIGRP very well. Which tables of EIGRP route information are held in RAM and maintained through the use of hello and update packets? Please choose two appropriate tables and drag the items to the proper locations.



Answer:



Explanation:



Only the neighbor table and the topology table of EIGRP route information are held in RAM and maintained through the use of hello and update packets.

Section 14: Verify network connectivity (including: using ping, traceroute, and telnet or SSH) (2 questions)

QUESTION NO: 349

What are two characteristics of Telnet? (Choose two.)

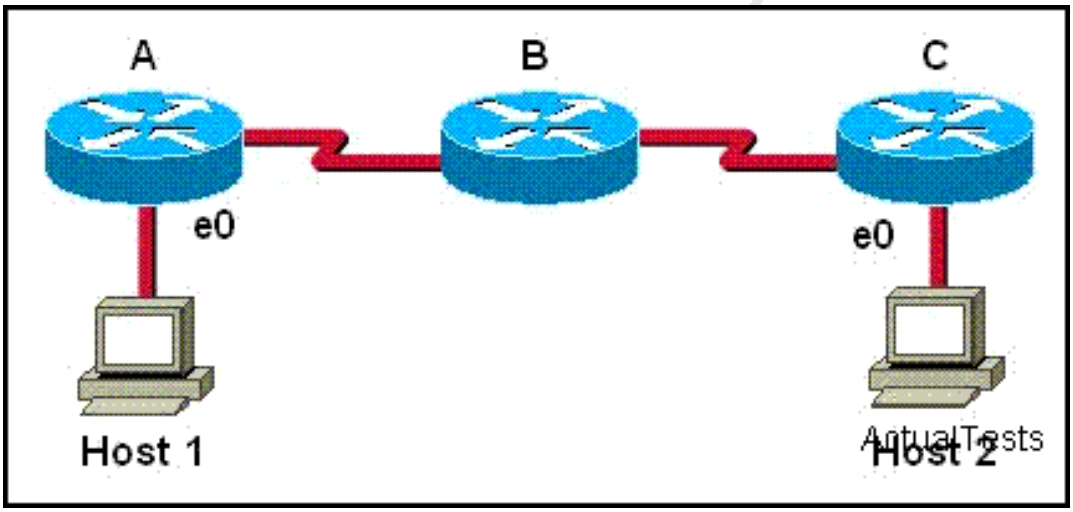
A. It requires that the destination device be configured to support Telnet connections.
B. It is no longer supported on Cisco network devices.
C. It sends data in clear text format.
D. It is more secure than SSH.

Answer: A,C

Explanation:
Telnet sends data in clear text. If a remote device wants to access the destination device through Telnet, the destination device must be configured to support Telnet connections.

QUESTION NO: 350

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

Answer: A,E

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.

Section 15: Troubleshoot routing issues (3 questions)

QUESTION NO: 351

Refer to the exhibit. What can be determined about routes that are learned from the router at IP address 190.171.23.12?

```
HQ_Router# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 18 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    Ethernet0             2     2
    Ethernet1             2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    190.171.0.0
    190.172.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    190.171.23.10         120      00:00:22
    190.171.23.12         120      00:03:30
    190.172.32.10         120      00:00:16
  Distance: (default is 120)
                                                    ActualTests
HQ_Router#
```

A. HQ_Router last received an update from 190.171.23.12 at3:30 am.
B. If HQ_Router does not receive an update from 190.171.23.12 in 30 seconds, all routes from that source will be flagged with a hold-down timer.
C. If HQ_Router does not receive an update from 190.171.23.12 in 30 seconds, all routes from that source will be removed from the routing table.
D. 190.171.23.12 is expected to send an update to HQ_Router for network 190.172.0.0 in 3 minutes and 30 seconds.

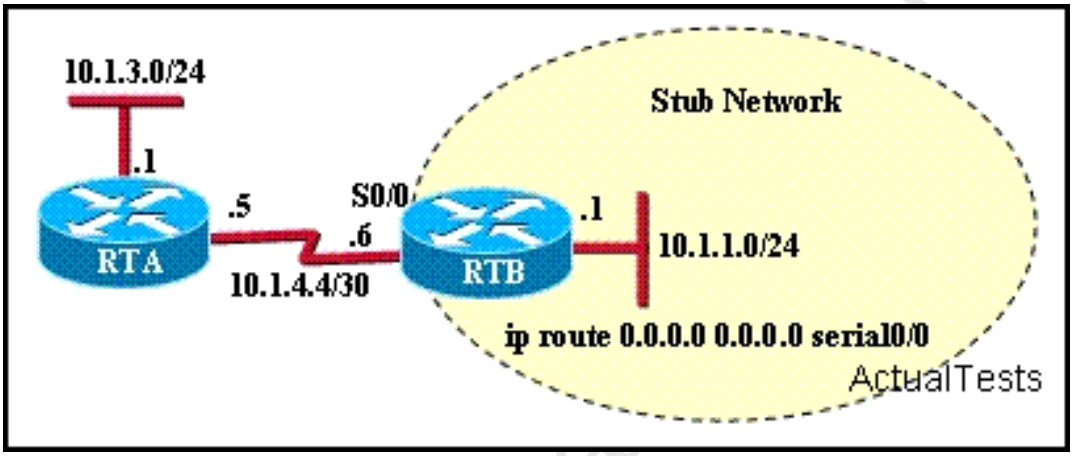
Answer: C

Explanation:
Routing information sources:
Gateway Distance Last Update
190.171.23.12 120 00:03:30
The RIP protocol broadcasts updates every 30 seconds, but the route 190.171.23.12 is not

updated for three minutes and thirty seconds. We can infer that the route is a faulty route. The following shows how RIP handles faulty routes:
sending updates every 30 seconds,
Invalid after 180 seconds,
hold down 180
flushed after 240
The route 190.171.23.12 is not updated for three minutes and thirty seconds, that is, 210 seconds. According to flushed timer=240, we can infer that the route will be removed in 30 seconds.

QUESTION NO: 352

Refer to the exhibit. Subnet 10.1.3.0/24 is unknown to router RTB. Which router command will prevent router RTB from dropping a packet destined for the 10.1.3.0/24 network if a default route is configured?



A. ip classless
B. network 10.1.1.0
C. network 10.1.1.0 0.0.0.255 area 0
D. ip default-network

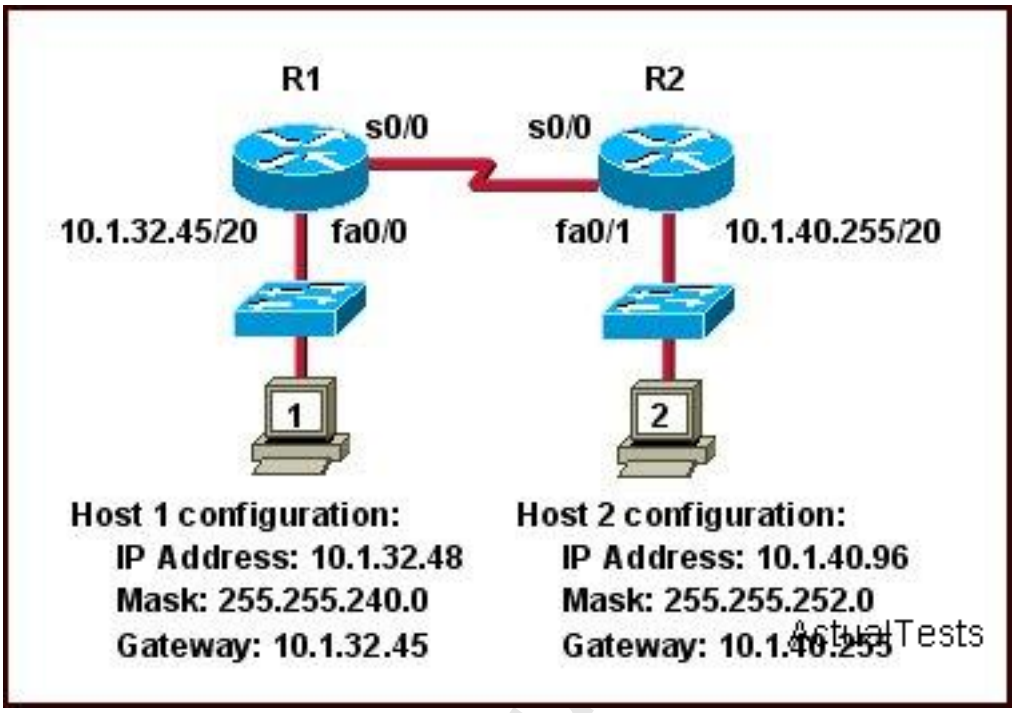
Answer: A

Explanation:
When data packets are sent to network segment 10.1.3.0/24 through RTB, because the routing table of RTB does not contain the route of 10.1.3.0/24, if configuring the command ip classless, RTB will let packets cross the default route and forward packets to RTA to reach the destination network segment; if not configuring the command ip classlees, RTB will find that the destination address is 10.0.0.0, the address of class A, the network segments directly connected to RTB belong to the class A address. So ,it will search for information related to the main class and the subnet in the routing table, if it finds the matching one , it will forward packets,if not ,it will discard packets. It is obvious that there are two subnets in the routing table: 10.1.1.0/24 and 10.1.4.4/30, the network segment 10.1.3.0/24 that the packets want to reach does not exist, so it will discard the packets.

At times the router might receive packets destined for a subnet of a network that has no network default route. To have the Cisco IOS software forward such packets to the best supernet route possible, use the ip classless global configuration command. To disable this feature, use the no form of this command.

QUESTION NO: 353

Refer to the graphic. Host 1 cannot receive packets from Host 2. Assuming that RIP v1 is the routing protocol in use, what is wrong with the IP configuration information shown? (Choose two.)



A. The fa0/1 interface of router R2 has been assigned a broadcast address.
B. The fa0/1 network on router R2 overlaps with the LAN attached to R1.
C. Host 2 has been assigned the incorrect subnet mask.
D. Host 1 has been configured with the 255.255.248.0 subnet mask.
E. Host 2 on router R2 is on a different subnet than its gateway.

Answer: B,C

Explanation:
Section 16: Verify router hardware and software operation using SHOW & DEBUG commands. (5 questions)

QUESTION NO: 354

You work as a network technician in a Company. Please study the exhibit carefully.

```
00:34:43:  RIP:  recevied v1 update from 192.168.11.2 on Serial0/0
00:34:43:          192.168.12.0  in  1 hops
00:34:43:  RIP:  update contains 1 routers
00:34:50:  Serial0/0: HDLC myseq 179, mineseen 179*, yourseen 180, line up
00:35:00:  Serial0/0: HDLC myseq 180, mineseen 180*, yourseen 181, line up
00:35:00:  IP: s= 192.168.11.1 (local), d= 192.168.11.2 (Serial0/0), len 40, rcvd 3
00:35:00:  IP: s= 192.168.11.2 (Serial0/0), d= 192.168.11.1 (Serial0/0), len 40, rcvd 3
00:35:00:  tcp2: I ESTAB 192.168.11.2: 11] 03 192.168.11.1: 23 seq 4063973782
         ACK  4061200175  WIN  4049                                  ActualTests
```

The router console screen is rapidly displaying line after line of output similar to what is shown in the exhibit. The help desk has called to say that users are reporting a slowdown in the network. What will solve this problem while not interrupting network operation?

A. Press the CTRL+C keys.
B. Save the configuration and reboot the router.
C. Enter the no debug all command.
D. Use the show processes command.

Answer: C

Explanation:
The output shown in this example is a result of one or more debug commands that have been used to troubleshoot an issue. Using debug commands might slow down traffic on busy networks. To see the current debug command settings, enter the show debug command. To stop the debug output, enter the no debug command. To stop all debug messages from being displayed, enter the no debug all command.

QUESTION NO: 355

Which of the following are true regarding the command output shown in the display? (Choose two.)

```
RtrA#debug ip rip
RIP protocol debugging is on
RtrA#
1d05h: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (172.16.1.1)
1d05h: RIP: build update entries
1d05h:  network 10.0.0.0 metric 1
1d05h:  network 192.168.1.0 metric 2
1d05h: RIP: sending v1 update to 255.255.255.255 via Serial0/0 (10.0.8.1)
1d05h: RIP: build update entries
1d05h:  network 172.16.0.0 metric 1
RtrA#
1d05h: RIP: received v1 update from 10.0.15.2 on Serial0/0
1d05h:      192.168.1.0 in 1 hops
1d05h:      192.168.168.0 in 16 hops (inaccessible)          ActualTests
```

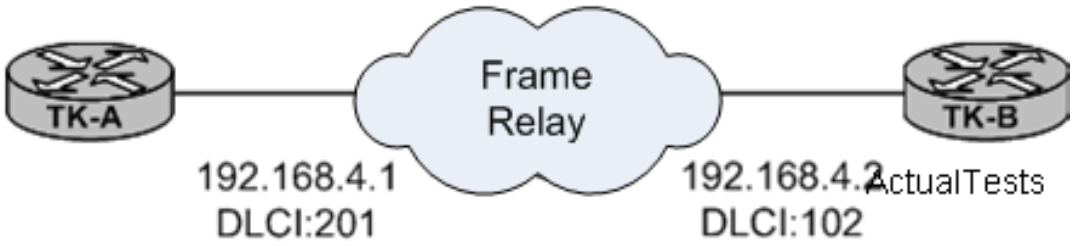
A. There are at least two routers participating in the RIP process.
B. A ping to 10.0.15.2 will be successful.
C. RtrA has three interfaces participating in the RIP process.
D. A ping to 192.168.168.2 will be successful.

Answer: A,B

Explanation:
The Serial0 / 0 interface of the router RTRA receives RIP update from the address of 10.0.15.2, it is obvious that the destination network of 10.0.15.2 is reachable. At the same time RTRA will send RIP update from the interface Fa0 / 0 and the interface S0 / 0 of its own, it is known that there are two routers at least running RIP process in the network.

QUESTION NO: 356

Refer to the network shown below. A ping from 192.168.4.1 to 192.168.4.2 was unsuccessful. Which three commands will provide the most useful troubleshooting information? (Choose three)



A. show frame-relay map
B. show protocols
C. show interfaces
D. show frame-relay pvc

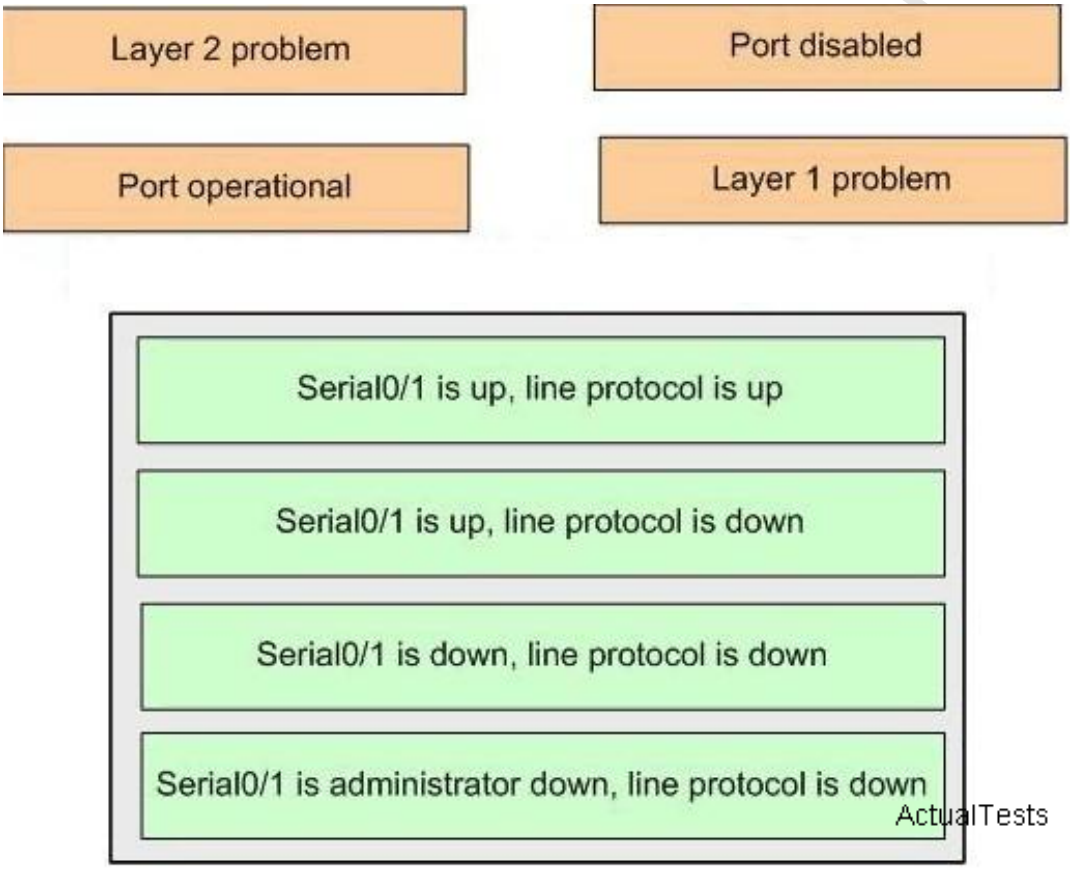
Answer: A,C,D

Explanation:
When troubleshooting connections between two directly connected routers over a frame relay network, the first step would be to issue the "show interfaces" command to ensure that the interfaces and line protocol is up for each. If they are indeed up, then the next step would be to troubleshoot the frame relay connection itself and looking at the status of the PVC by using the "show frame-relay map" and "show frame-relay pvc" commands.
Commonly Used Frame Relay Commands :
This section describes two Cisco IOS commands that are especially useful when configuring Frame Relay.
show frame-relay pvc
This command shows the status of the permanent virtual circuit (PVC), packets in and out, dropped packets if there is congestion on the line via forward explicit congestion notification

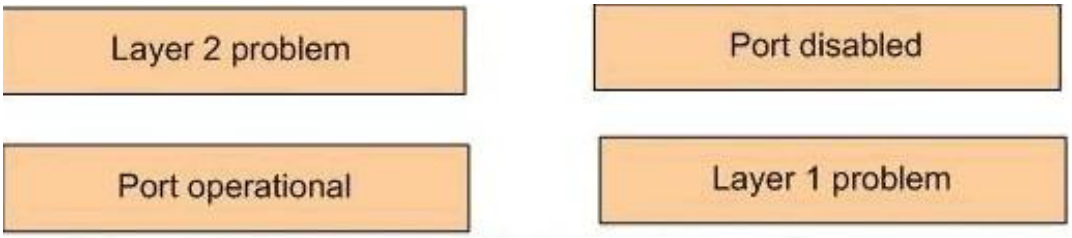
(FECN) and backward explicit congestion notification (BECN), and so on. For a detailed description of the fields used with the show frame-relay pvc command, click here.
show frame-relay map
Use this command to determine if frame-relay inverse-arp resolved a remote IP address to a local DLCI. This command is not enabled for point-to-point subinterfaces. It is useful for multipoint interfaces and subinterfaces only.
Reference:
http://www.cisco.com/en/US/partner/tech/tk713/tk237/technologies_tech_note09186a008014f8a7.shtml#topic11

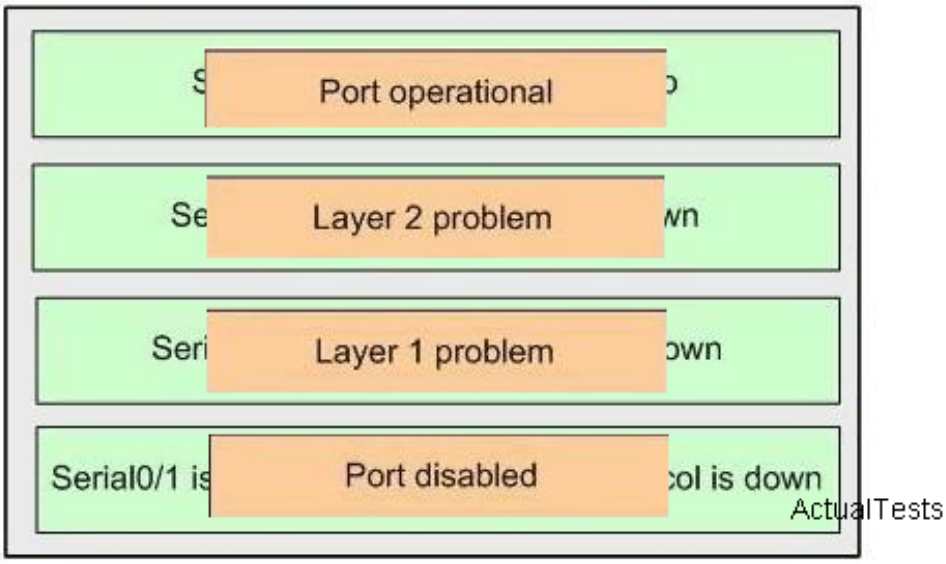
QUESTION NO: 357 DRAG DROP

The above describes some categories, while the below provides their corresponding router output lines. Drag the above items to the proper locations.

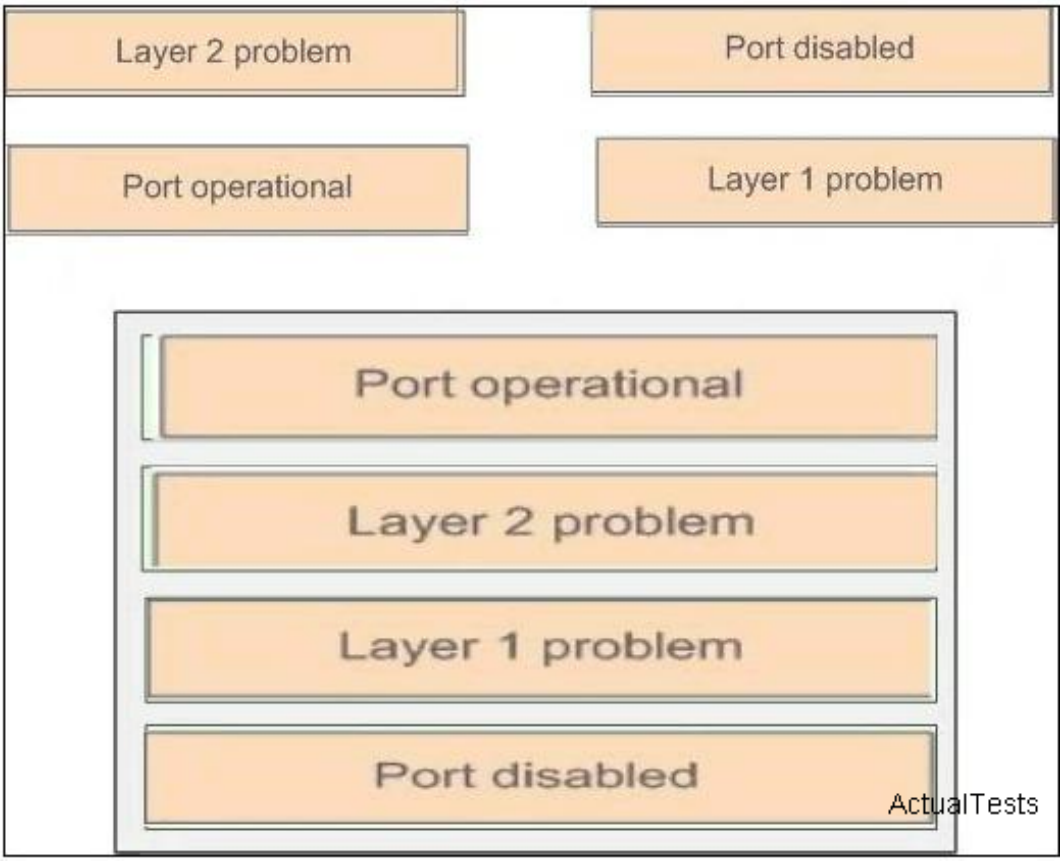


Answer:





Explanation:



QUESTION NO: 358

Which command displays CPU utilization?

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

Answer: B

Explanation:
Section 17: Implement basic router security (4 questions)

QUESTION NO: 359

You just entered the following command:

Router (config)# line console 0

A. Create a password on the console terminal line.
B. Establish a terminal type 4 connection to a remote host.
C. Configure the terminal type.
D. Enter protocol parameters for a serial line.

Answer: A

QUESTION NO: 360

Which two passwords must be supplied in order to connect by Telnet to a properly secured Cisco switch and make changes to the device configuration? (Choose two.)

A. tty password
B. enable secret password
C. vty password
D. aux password
E. console password
F. username password

Answer: B,C

Explanation:
Telnet presents a potential security risk, so Telnet uses vty for connecting a remote Cisco switch. For access security, the vty password and enable password must be configured.

***

QUESTION NO: 361

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

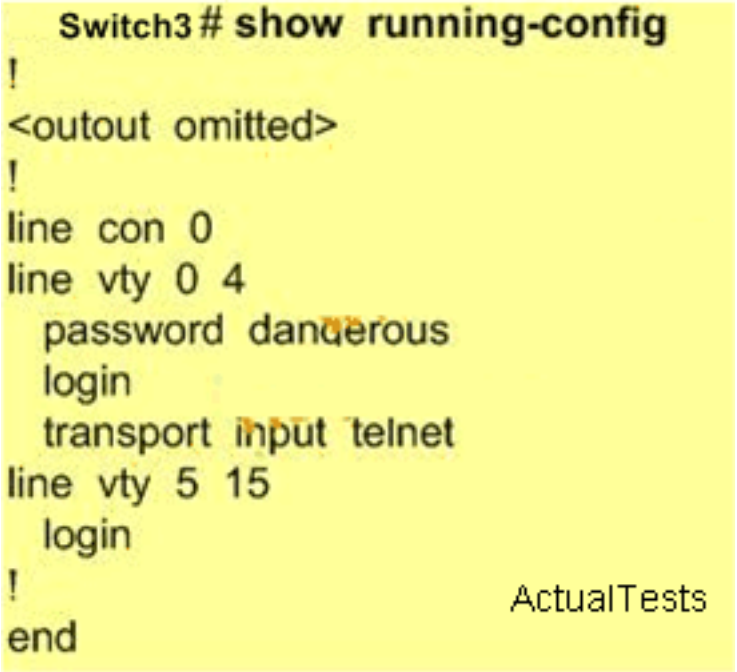
A. Only the enable password will be encrypted.
B. It will encrypt all current and future passwords.
C. It will encrypt the secret password and remove the enable secret password from the configuration.
D. Only the enable secret password will be encrypted.
E. Only passwords configured after the command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

Answer: B

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: 362

Refer to the exhibit. The lines of Switch3 are configured as shown. Which statement correctly describes the effect of this configuration?



A. The Telnet protocol is supported only on lines 0 through 4.

B. The SSH protocol is supported on lines 5 through 15.
C. The console line cannot be used until it is configured.
D. A password challenge protects all virtual terminal lines.

Answer: D

QUESTION NO: 363

A new hardware item is using an IEEE 802.11b a wireless LAN. What is the maximum data rate specified for this WLAN?

A. 10 mbps
B. 11 Mbps
C. 1000 Mbps
D. 16 Mbps
E. 100 Mbps

Answer: B

Explanation:
The maximum speed for 802.11b is 11 Mbps.
Incorrect Answers:
A: This is the maximum speed for legacy Ethernet networks.
C: This is the maximum speed supported by the other prevalent wireless standards, 802.11a and 802.11g.D, This is the maximum speed of Ethernet

QUESTION NO: 364

As a CCNA candidate, you will be expected to know Wireless networking standards very well. What is the maximum data rate specified for IEEE 802.11b WLANs?

A. 10 Mbps
B. 100 Mbps
C. 11 Mbps
D. 54 Mbps

Answer: C

Explanation:
IEEE 802.11b, which is also called 11 Mbps Wi-Fi, operates at a maximum speed of 11 Mbps and is thus slightly faster than 10BASE-T Ethernet. Most IEEE 802.11b hardware is designed to operate at four speeds, using three different data-encoding methods depending on the speed range. It operates at 11 Mbps using quatenery phase-shift keying/complimentary code keying

(QPSK/CCK); at 5.5 Mbps also using QPSK/CCK; at 2 Mbps using differential quaternary phase-shift keying (DQPSK); and at 1 Mbps using differential binary phase-shift keying (DBPSK). As distances change and signal strength increases or decreases, IEEE 802.11b hardware switches to the most suitable data-encoding method. Wireless networks running IEEE 802.11b hardware use the 2.4 GHz radio frequency band that many portable phones, wireless speakers, security devices, microwave ovens, and the Bluetooth short-range networking products use. Although the increasing use of these products is a potential source of interference, the short range of wireless networks (indoor ranges up to 300 feet and outdoor ranges up to 1,500 feet , varying by product) minimizes the practical risks. Many devices use a spread-spectrum method of connecting with other products to minimize potential interference. IEEE 802.11b networks can connect to wired Ethernet networks or be used as independent networks.

Incorrect Answers:

A: This is the maximum speed of Ethernet and Gig E connections.Section 2: Identify and describe the purpose of the components in a small wireless network. (Including: SSID, BSS, ESS) (3 questions)

D: This is the maximum speed supported by the other prevalent wireless standards, 802.11a and 802.11g.

QUESTION NO: 365

Which spread spectrum technology does the 802.11b standard define for operation?

A. DSSS and FHSS
B. IR
C. DSSS
D. IR, FHSS, and DSSS
E. FHSS

Answer: C

Explanation:

In telecommunications, direct-sequence spread spectrum (DSSS) is a modulation technique. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated. The name 'spread spectrum' comes from the fact that the carrier signals occur over the full bandwidth (spectrum) of a device's transmitting frequency.

QUESTION NO: 366

You and a co-worker have established wireless communication directly between your wireless laptops. What type of wireless topology has been created?

A. BSS
B. IBSS
C. SSID
D. ESS

Answer: B

Explanation:
The IBSS network architecture consists of two or more STAs(stations) communicating directly with each other using 802.11 wireless technology without an AP(Access Point). Most IBSSs are confined to a small number of STAs, and their primary purpose is to provide a short-lived communication session for a specific purpose.

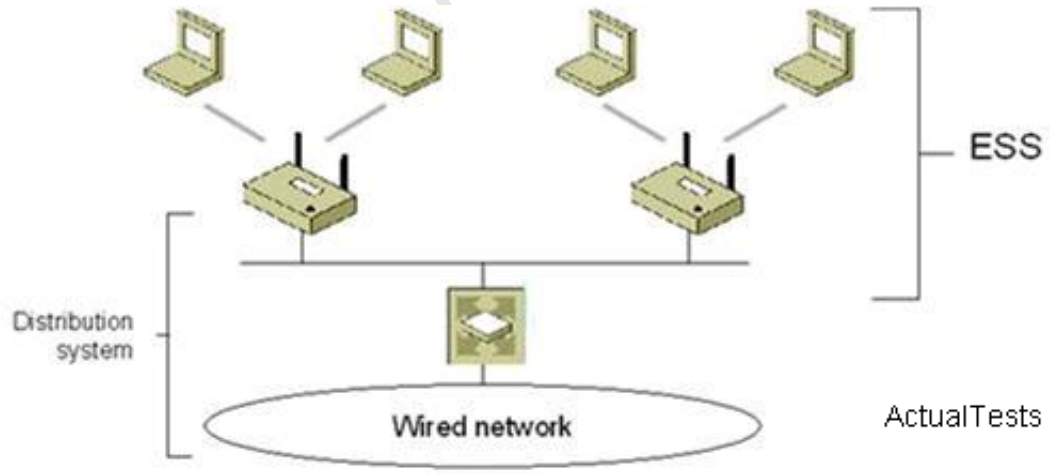
QUESTION NO: 367

Three access points have been installed and configured to cover a small office. What term defines the wireless topology?

A. BSS
B. IBSS
C. ESS
D. SSID

Answer: C

Explanation:
A single wireless AP supporting one or multiple wireless clients is known as a Basic Service Set (BSS). A set of two or more wireless APs connected to the same wired network is known as an Extended Service Set (ESS). An ESS is a single logical network segment (also known as a subnet), and is identified by its SSID
See the Figure:



Section 3: Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point (4 questions)

QUESTION NO: 368

You have finished physically installing an access point on the ceiling at your office. At a minimum, which parameter must be configured on the access point in order to allow a wireless client to operate on it?

A. SSID
B. AES
C. TKIP
D. PSK
E. WEP

Answer: A

Explanation:
SSID (Service Set Identifier) can also be written as ESSID, which is used to distinguish different networks. It has 32 characters at most, WLAN cards set up different SSID to enter different networks. SSID is usually broadcast by AP or wireless routers , you can view SSID of the present area through XP built-in scanning feature .Taking security into consideration, SSID can be not broadcast, meanwhile users need to set up SSID manually to enter the appropriate network. Simply speaking, SSID is the name of a local area network, only those computers that set up the same SSID value can communicate with each other.

QUESTION NO: 369

A single 802.11g access point has been configured and installed in the center of a square office. A few wireless users are experiencing slow performance and drops while most users are operating at peak efficiency. What are three likely causes of this problem? (Choose three.)

A. antenna type or direction
B. metal file cabinets
C. mismatched SSID
D. cordless phones

Answer: A,B,D

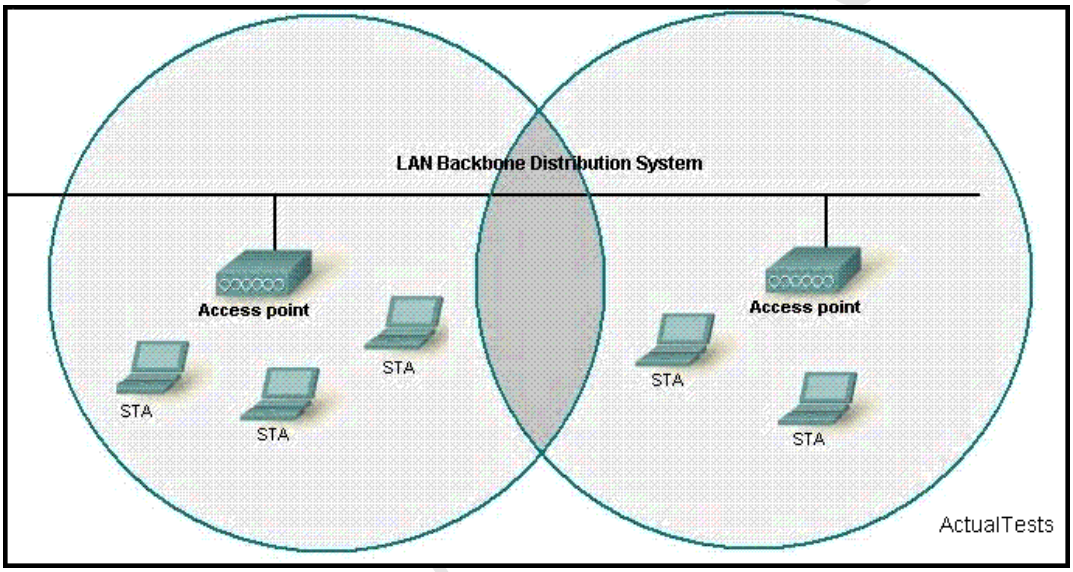
Explanation:
D: If you have cordless phones or other wireless electronics in your home or office, your computer might not be able to "hear" your router over the noise from the other wireless devices. To quiet the noise, avoid wireless electronics that use the 2.8GHz frequency. Instead, look for cordless phones that use the 5.8GHz or 900MHz frequencies.
A: The antennas supplied with your router are designed to be omni-directional, meaning they

broadcast in all directions around the router. If your router is near an outside wall, half of the wireless signals will be sent outside your office, and much of your router's power will be wasted.

Since most users operate at peak efficiency in our example, it could be that a few of the users are simply placed too far from the antenna, or the antenna is not placed in the center of the office.
B: Metal, walls, and floors will interfere with your router's wireless signals. The closer your router is to these obstructions, the more severe the interference, and the weaker your connection will be.

QUESTION NO: 370

Refer to the exhibit. What two facts can be determined from the WLAN diagram? (Choose two.)



A. The area of overlap of the two cells represents a basic service set (BSS).
B. The area of overlap must be less than 10% of the area to ensure connectivity.
C. The network diagram represents an extended service set (ESS).
D. Access points in each cell must be configured to use channel 1.
E. The two APs should be configured to operate on different channels.

Answer: C,E

QUESTION NO: 371

What are three basic parameters to configure on a wireless access point? (Choose three.)

A. authentication method
B. RTS/CTS
C. RF channel
D. SSID

Answer: A,C,D

Explanation:
SSID (Service Set Identifier) can also be written as ESSID, which is used to distinguish different networks. It has 32 characters at most, WLAN cards set up different SSID to enter different networks. SSID is usually broadcast by AP or wireless routers , you can view SSID of the present area through XP built-in scanning feature .Taking security into consideration, SSID can be not broadcast, meanwhile users need to set up SSID manually to enter the appropriate network. Simply speaking, SSID is the name of a local area network, only those computers that set up the same SSID value can communicate with each other.
RF is an acronym for Radio Frequency. It is the electromagnetic frequency that can be radiated to space, frequency range from 300 KHz to 30GHz. RTS/CTS protocol (Request To Send /Clear To Send) is protocol that requests to send / allows to send, which is equivalent to a handshake protocol, mainly used to deal with "hidden terminal" problems. " Hidden Stations ": base station A sends a message to base station B, base C sends message to B too because it fails to detect the station A. so both A and C send signals to B at the same time, conflict occurs, and the result is both messages are lost.

Section 4: Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2) (4 questions)

QUESTION NO: 372

Which two statements best describe the wireless security standard that is defined by WPA? (Choose two.)

A. It specifies the use of dynamic encryption keys that change each time a client establishes a connection.
B. It specifies use of a static encryption key that must be changed frequently to enhance security.
C. It includes authentication by PSK.
D. It requires that all access points and wireless devices use the same encryption key.
E. It requires use of an open authentication method.

Answer: A,C

Explanation:
WPA is a more powerful security technology for Wi-Fi networks than WEP. It provides strong data protection by using encryption as well as strong access controls and user authentication. WPA

utilizes 128-bit encryption keys and dynamic session keys to ensure your wireless network's privacy and enterprise security. There are two basic forms of WPA:
WPA Enterprise (requires a Radius server) WPA Personal (also known as WPA-PSK) Either can use TKIP or AES for encryption. Not all WPA hardware supports AES. WPA-PSK is basically an authentication mechanism in which users provide some form of credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN. Encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is in WPA-PSK, authentication is reduced to a simple common password, instead of user-specific credentials. The Pre-Shared Key (PSK) mode of WPA is considered vulnerable to the same risks as any other shared password system - dictionary attacks for example. Another issue may be key management difficulties such as removing a user once access has been granted where the key is shared among multiple users, not likely in a home environment.
Reference: http://www.dslreports.com/faq/wifisecurity/2.2_WPA

WPA is a standard-based interoperable solution designed to enhance the security of WLAN, which greatly improves the present and future level of data protection and access control of WLAN. WPA is evolved from the being developed IEEE802.11i standards and keeps compatible with its former. WPA can protect WLAN users data with proper deployment , and only the authorized network users can access the WLAN network.
WPA provides users with a temporary solution. The encryption of this standard adopts TKIP (Temporary Key Integrity Protocol). There are two authentication modes to choose :one mode uses 802.1 x protocol to authenticate, the other is known as PSK (Pre-Shared Key) Mode.

QUESTION NO: 373

According to capabilities of WPA security, which encryption type does WPA2 use?

A. AES-CCMP
B. PSK
C. PPK via IV
D. TKIP/MIC

Answer: A

Explanation:
(AES-Counter Mode CBC-MAC Protocol) is an encryption algorithm used in 802.11 i security protocol. It uses AES block encryption algorithm, but the key length is limited to 128. AES-CCMP combines two complex encryption technologies (counter mode and CBC-MAC) and applies them to Ethernet frame, thus provide a robust security protocol between moving clients and AP.

In 2004, the IEEE 802.11i task group responsible for Wi-Fi security for the WLAN provided a series of recommendations to fix known problems with Wireless Equivalent Privacy (WEP). Its recommendations included using encryption techniques known as Advanced Encryption Standard Counter-Mode Cipher Block Chaining (AES-CCMP) or AES for short.
AES is not the end of the story, as the industry had a problem when it moved from WEP to AES. What could be done, for example, about legacy devices that could not support the upgrade to AES? The IEEE 802.11i task group recommended using the Temporal Key Integrity Protocol (TKIP). As a patch, TKIP is not as secure as AES, but it protects against all currently known attacks.
The urgent need to fix WEP caused the Wi-Fi Alliance to develop security patch recommendations for Wi-Fi Protected Access (WPA) before the IEEE finalized standards. WPA was drawn from an early draft of the IEEE 802.11i standard, and there are significant differences between WPA and TKIP. What is similar is that neither the WPA patch for WEP nor the TKIP patch is as secure as AES.
The Wi-Fi Alliance later came out with a new security recommendation-WPA, version 2 (WPA2)-to make WPA consistent with IEEE 802.11i standards. One improvement to WPA2 was the recommendation to use AES-CCMP encryption mode . WPA2 has thus become synonymous with AES.
The table below summarizes the different encryption algorithms used for WLAN privacy.
Reference: http://www.convergedigest.com/bp-bbw/bp1.asp?ID=465&ctgy=Mesh

QUESTION NO: 374

What is one reason that WPA encryption is preferred over WEP?

A. The values of WPA keys can change dynamically while the system is used.
B. WPA key values remain the same until the client configuration is changed.
C. The access point and the client are manually configured with different WPA key values.
D. A WPA key is longer and requires more special characters than the WEP key.

Answer: A

Explanation:
WEP is security mechanism that encrypts grouping information between Access Point and Client in RC4 mode. Password is easily cracked. The encryption key that WEP uses includes the 40 bits (104 bits) general key that both receiver and sender predefined, and the 24 bits encryption key (IV key) that sender defined for each group. However, in order to tell communication object the IV key, IV key is embedded in the grouping information directly and sent out without encryption. If wiretapping, collecting some certain IV key grouping information and then analyze, even secret general key will be worked out.

WPA is a new mechanism that takes up basic WEP principle while solves its shortcomings. With WPA, even if you collect grouping information and analyze it, you will never work out its general key.

QUESTION NO: 375

Which two practices help secure the configuration utilities on wireless access points from unauthorized access? (Choose two.)

A. configuring traffic filtering
B. changing the mixed mode setting to single mode
C. configuring a new administrator password
D. assigning a private IP address to the AP
E. changing the default SSID value

Answer: C,E

Explanation:
To add new wireless network access point and to ensure that unauthorized access can not penetrate, you may set a new administrator password after the access of new AP;
Service Set Identifier technology: this technology can divide a wireless LAN into several subnets that need different Authentication, each subnet needs an independent authentication, users will enter the corresponding network only if they pass through the authentication, and unauthorized users are unable to access to the network. In other words, SSID is the name of your wireless network. It should be noted that the wireless router or AP from the same vender uses the same SSID. Once attackers who seek for illegal connection use of generic initialization string to connect the wireless network, they will easily set up an illegal connection, and bring threat to our wireless network. Therefore, it is suggested that you name your SSID a personalized name.

SSID is a common network name for the devices in a WLAN system that creates the wireless LAN. An SSID prevents access by any client device that doesn't have the SSID. The main security concern is that, by default, an access point broadcasts it's SSID in its beacon many times a second. And even if SSID broadcasting is turned off, a hacker can discover the SSID by monitoring the network and just waiting for a client response to the access point. To secure the Wireless Access Point (AP) from unauthorized access set the SSID manually and change the administrator password.
Section 5: Identify common issues with implementing wireless networks. (Including: Interface, missconfiguration) (4 questions)

QUESTION NO: 376

Which two devices can interfere with the operation of a wireless network because they operate on similar frequencies? (Choose two.)

A. toaster
B. IP phone
C. AM radio
D. cordless phone
E. microwave oven
F. copier

Answer: D,E

Explanation:
The microwave and cordless phone in the 2.4GHz spectrum band will interfere with the operation of a wireless network.

QUESTION NO: 377

Which additional configuration step is necessary in order to connect to an access point that has SSID broadcasting disabled?

A. Set the SSID value in the client software to public.
B. Configure open authentication on the AP and the client.
C. Set the SSID value on the client to the SSID configured on the AP.
D. Configure MAC address filtering to permit the client to connect to the AP.

Answer: C

QUESTION NO: 378

As the network administrator, you need to add a wireless access point to a new office, which additional configuration step is necessary in order to connect to an access point that has SSID broadcasting disabled?

A. Set the SSID value in the client software to public.
B. Configure open authentication on the AP and the client.
C. Configure MAC address filtering to permit the client to connect to the AP.
D. Set the SSID value on the client to the SSID configured on the AP.

Answer: D

Explanation:

SSID (Service Set Identifier) can also be written as ESSID, which is used to distinguish different networks and has 32 characters at most , WLAN cards set up different SSID to enter different networks. SSID is usually broadcast by AP, you can view SSID of the present area through XP built-in scanning feature .Taking security into consideration, SSID can be not broadcast, meanwhile users need to set up SSID manually to enter the appropriate network. In simple terms, SSID is the name of a local area network, only those computers that set up the same SSID values can communicate with each other.

QUESTION NO: 379

Which wireless LAN design ensures that a mobile wireless client will not lose connectivity when moving from one access point to another?

A. utilizing MAC address filtering to allow the client MAC address to authenticate with the surrounding APs
B. using adapters and access points manufactured by the same company
C. overlapping the wireless cell coverage by at least 10%
D. configuring all access points to use the same channel

Answer: C

Explanation:
To ensure that wireless users will not lose connectivity when moving from the initial access point to a new access point, we have to ensure that the two access point has at least 10 percent coverage.

QUESTION NO: 380

Which type of attack is characterized by a flood of packets that are requesting a TCP connection to a server?

A. brute force
B. denial of service
C. Trojan horse
D. reconnaissance

Answer: B

Explanation:
DDoS is short for Distributed Denial of Service. It can be interpreted that all actions leading to legitimate users being not able to access normal network services are regarded as denial of service attacks, in other words, the purpose of denial of service attack is very clear: that is to block legitimate users from accessing normal network services in order to achieve attacker??s ulterior

motives. There are differences between DDoS and DOS, although both of them are denial of service attack. The attack strategies adopted by DDoS focus on sending a large number of seemingly legitimate network packets to attacked hosts through many "zombie hosts" (hosts are attacked or can be used indirectly), resulting in network congestion or server resources exhausted and finally refusing to provide services. Once distributed denial of service attacks are implemented, attacking network packets will pour into attacked hosts and flood network packets of legitimate users, thus the legitimate users can't access network resources of servers properly. Denial of service attack is also called 'flood attack'. The most common DDoS attack methods are SYN Flood??ACK Flood??UDP Flood??ICMP Flood??TCP Flood??Connections Flood??Script Flood??Proxy Flood etc; while DOS emphasizes on using specific loopholes of hosts to make network stack fail, system crash and host crash, thus unable to provide normal network services, and finally deny services.

QUESTION NO: 381

What should be part of a comprehensive network security plan?

A. Minimize network overhead by deactivating automatic antivirus client updates.
B. Encourage users to use personal information in their passwords to minimize the likelihood of passwords being forgotten.
C. Delay deployment of software patches and updates until their effect on end-user equipment is well known and widely reported.
D. Physically secure network equipment from potential access by unauthorized individuals.
E. Allow users to develop their own approach to network security.

Answer: D

Explanation:
Computer systems and networks are vulnerable to physical attack; therefore, procedures should be implemented to ensure that systems and networks are physically secure. Physical access to a system or network provides the opportunity for an intruder to damage, steal, or corrupt computer equipment, software, and information. When computer systems are networked with other departments or agencies for the purpose of sharing information, it is critical that each party to the network take appropriate measures to ensure that its system will not be physically breached, thereby compromising the entire network. Physical security procedures may be the least expensive to implement but can also be the most costly if not implemented. The most expensive and sophisticated computer protection software can be overcome once an intruder obtains physical access to the network.

Section 2: Explain general methods to mitigate common security threats to network devices, hosts, and applications (1 question)

QUESTION NO: 382

What are two recommended ways of protecting network device configuration files from outside network security threats? (Choose two.)

A. Allow unrestricted access to the console or VTY ports.
B. Use a firewall to restrict access from the outside to the network devices.
C. Always use Telnet to access the device command line because its data is automatically encrypted.
D. Use SSH or another encrypted and authenticated transport to access device configurations.
E. Prevent the loss of passwords by disabling password encryption.

Answer: B,D

Explanation:
Whenever the trusted (inside) part of the network connects to an untrusted (outside, or internet) network, the use of a firewall should be implemented to ensure only legitimate traffic is allowed within the enterprise. SSH is a secure alternative to telnet that encrypts the traffic so that data carried within can not be "sniffed." It is always recommended to use SSH over telnet whenever possible.
Section 3: Describe the functions of common security appliances and applications (1 question)

QUESTION NO: 383

What are two security appliances that can be installed in a network? (Choose two.)

A. IDS
B. IOS
C. ATM
D. IOX
E. SDM
F. IPS

Answer: A,F

Explanation:
IDS is an abbreviation of "Intrusion Detection Systems", which means to detect the operation status of network and system according to some security policy, and find every kind of intrusion attempts, intrusion actions or intrusion results, to enhance the confidentiality, integrality and usability.
IPS(Intrusion Prevention System) is between firewall and network devices. When attacks detected, IPS would stop this malicious communication before the diffusion of this attack to other

areas.
Section 4: Describe security recommended practices including initial steps to secure network devices (1 question)

QUESTION NO: 384

What are three valid reasons to assign ports to VLANs on a switch? (Choose three.)

A. to make VTP easier to implement
B. to isolate broadcast traffic
C. to increase the size of the collision domain
D. to allow more devices to connect to the network
E. to logically group hosts according to function
F. to increase network security

Answer: B,E,F

QUESTION NO: 385

When are packets processed by an inbound access list?

A. after they are routed to an outbound interface
B. before and after they are routed to an outbound interface
C. before they are routed to an outbound interface
D. after they are routed to an outbound interface but before being placed in the outbound queue

Answer: C

Explanation:
For inbound ACL, before the router forwards groups to other interface, the router will compare group and interface ACL. ACL statement will process in top-down order, until a match item is found; the follow-up statement will no longer be handled. If no matching item is found in ACL, groups will be discarded (implicit refusal).

When a packet is received on an interface with an inbound access list configured, the packets are matched against the access list to determine if they should be permitted or denied. After this check, the packets are processed by the routing function. The access list check is always done first.
Incorrect Answers:
A: The packets are always processed by the inbound access list prior to being routed.
B: All packets are always checked against a specific access list only once. While packets traversing through a router may be checked against different access lists for each interface and in

each direction (inbound and outbound), each access list is always only consulted once.
D: The packets are always processed by the inbound access list prior to being routed.

QUESTION NO: 386

What three pieces of information can be used in an extended access list to filter traffic? (Choose three.)

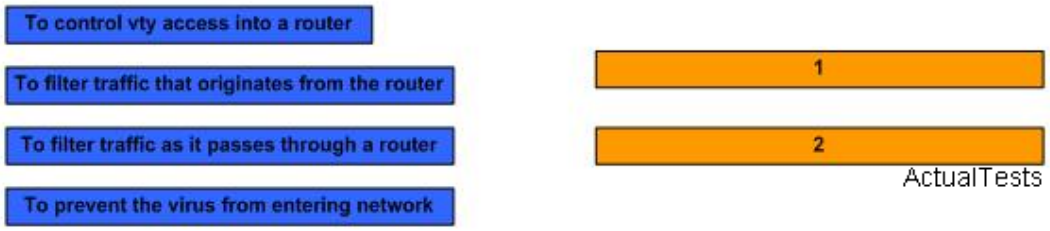
A. VLAN number
B. TCP or UDP port numbers
C. source switch port number
D. source IP address and destination IP address
E. protocol
F. source MAC address and destination MAC address

Answer: B,D,E

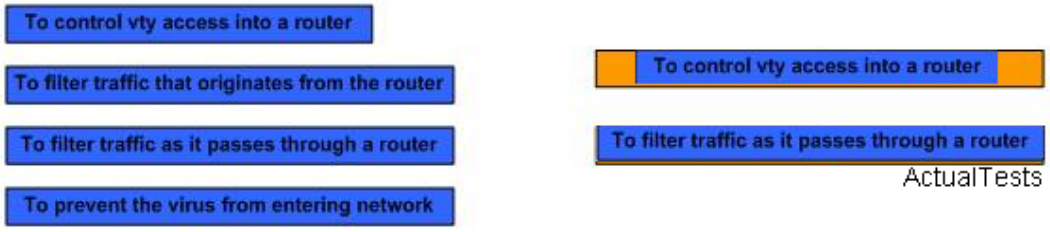
Explanation:
1. A standard access control list filters traffic based on source IP addresses.
2. An extended access control list filters traffic based on source IP addresses and destination IP addresses, protocols, TCP or UDP port numbers.

QUESTION NO: 387 DRAG DROP

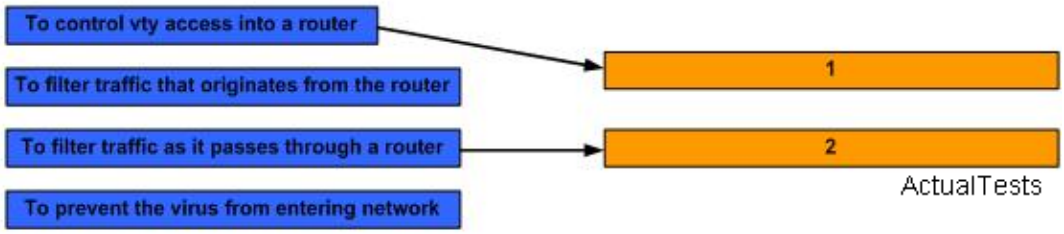
In order to enhance the security of the enterprise network, the network administrators use ACL(Access Control lists). What are two reasons that the network administrator would use access lists?



Answer:



Explanation:
The purposes for setting ACLs on a router are controlling vty access into a router and filtering traffic as it passes through a router.



Access Control List (ACL) can be used to affect traffic transmitted from one port to another. It acquired its name due to having filtering capability when traffic flows in and out of interface and it also can be used for other purposes, such as:

* Place restrictions on accessing router Telnet (VTY).
* Filter routing information.
* Distinguish precedence of WAN traffic by queuing technology.
* Trigger calls through the Dial-on-demand routing (DDR).
* Change administrative distance of routing

QUESTION NO: 388

What are two reasons that a network administrator would use access lists? (Choose two.)

A. to filter traffic that originates from the router
B. to replace passwords as a line of defense against security incursions
C. to control vty access into a router
D. to filter traffic as it passes through a router
E. to control broadcast traffic through a router

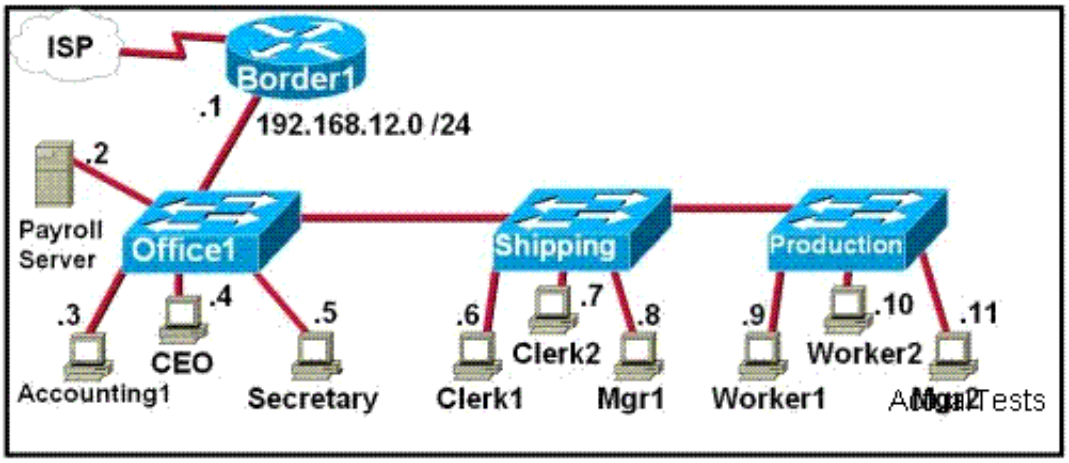
Answer: C,D

Explanation:
The purposes for setting ACLs on a router are controlling vty access into a router and filtering traffic as it passes through a router.
Section 2: Configure and apply ACLs based on network filtering requirements. (including: CLI/SDM) (10 question)

QUESTION NO: 389

Refer to the exhibit. The FMJ manufacturing company is concerned about unauthorized access to the Payroll Server. The Accounting1, CEO, Mgr1, and Mgr2 workstations should be the only computers with access to the Payroll Server. What two technologies should be implemented to

help prevent unauthorized access to the server? (Choose two.)



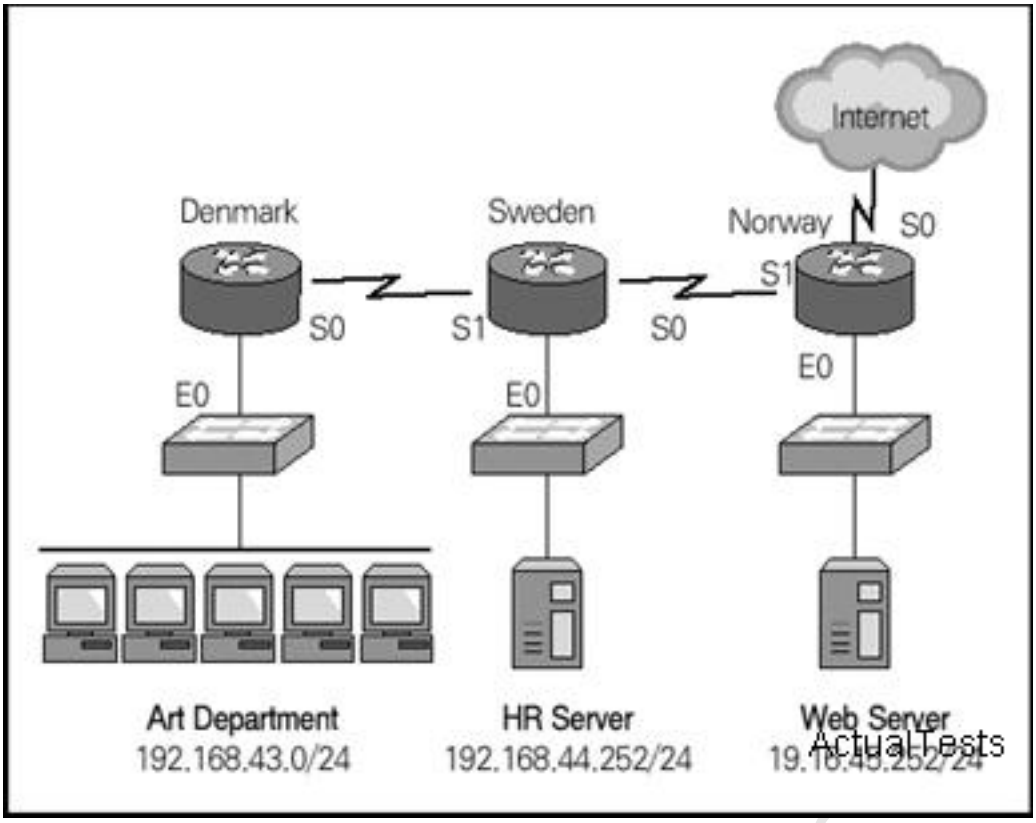
A. STP
B. access lists
C. VTP
D. VLANs
E. wireless LANs
F. encrypted router passwords

Answer: B,D

Explanation:
Group these workstations into the same VLAN and use access control lists to set the access authority of the VLAN.

QUESTION NO: 390

Based on this information, which of the following access list statements are necessary to allow FTP access to the HR server from the Internet while blocking all other traffic? (Select two.)



A. access-list 101 permit tcp 192.168.44.252 0.0.0.0 any eq 21
B. access-list 101 permit tcp any 192.168.44.252 0.0.0.0 eq 20
C. access-list 101 permit tcp 192.168.44.252 0.0.0.0 any eq 20
D. access-list 101 permit tcp any 192.168.44.252 0.0.0.0 eq 21

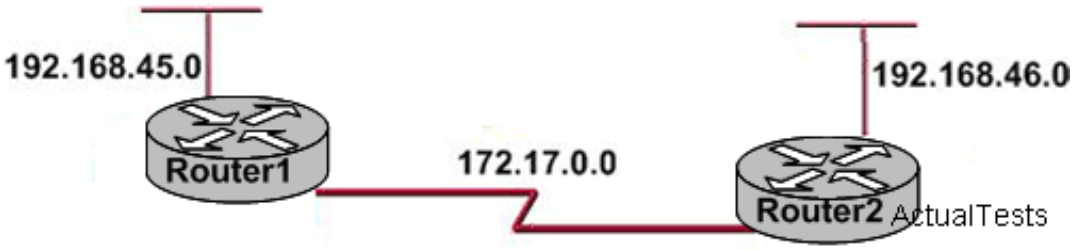
Answer: B,D

Explanation:
Access Control List (ACL) is the directive list used in router interface. These lists of instructions are to tell the router which data packets can be received, and which should be rejected. As for whether the packet will be received or rejected, it is determined by particular instructive conditions such as source address, destination address, port number, and so on.

FTP uses two ports: TCP port 20 and TCP port 21. you want to allow all hosts (ANY) to access the HR server (192.168.44.252 0.0.0.0) through ftp (eq 20 & eq 21) and the implicit deny any rule will block everything else.

QUESTION NO: 391

As the network administrator, you have been instructed to prevent all traffic originating on the Router 1 LAN from entering the router2. Which the following command would implement the access list on the interface of router2?



A. access-list 101 out
B. ip access-group 101 out
C. access-list101 in
D. ip access-group101 in

Answer: D

QUESTION NO: 392

The following access list below was applied outbound on the E0 interface connected to the 192.169.1.8/29 LAN:

access-list 135 deny tcp 192.169.1.8 0.0.0.7 eq 20 any
access-list 135 deny tcp 192.169.1.8 0.0.0.7 eq 21 any

How will the above access lists affect traffic?

A. FTP traffic from 192.169.1.9 to any host will be denied.
B. All traffic exiting E0 will be denied.
C. All FTP traffic to network 192.169.1.9/29 will be denied.
D. No traffic, except for FTP traffic will be allowed to exit E0.
E. FTP traffic from 192.169.1.22 will be denied.

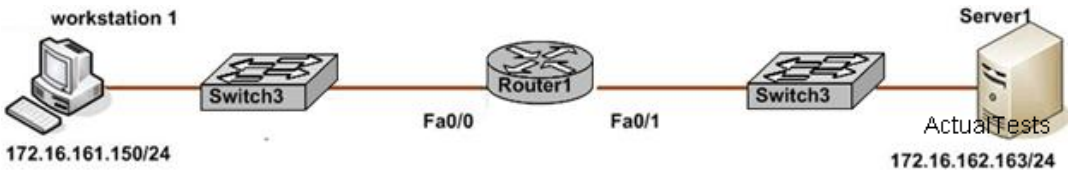
Answer: B

Explanation:
When an access list is created, an implicit deny all entry is created at the end. Therefore, each access list created needs to have at least one permit statement, otherwise it will have the effect of prohibiting all traffic. If the intent in this example was to block only certain hosts from being able to FTP, then the following line should have been included at the end of the access list:

Router(config)#access-list 135 permit ip any any

QUESTION NO: 393

Refer to the graphic. It has been decided that workstation1 should be denied access to Server1. Which of the following commands are required to prevent only workstation1 from accessing Server1 while allowing all other traffic to flow normally? (Choose two.)



A. ROUTER1(config)# interface fa0/0
ROUTER1(config-if)# ip access-group 101 out
B. ROUTER1(config)# access-list 101 deny ip 172.16.161.150 0.0.0.255 172.16.162.163 0.0.0.0
ROUTER1(config)# access-list 101 permit ip any any
C. ROUTER1(config)# interface fa0/0
ROUTER1(config-if)# ip access-group 101 in
D. ROUTER1(config)# access-list 101 deny ip host 172.16.161.150 host 172.16.162.163
ROUTER1(config)# access-list 101 permit ip any any

Answer: C,D

Explanation:
Taking security into consideration, you will implement access control on router ROUTER1. When the traffic coming from workstation1 to Server1 crosses the router ROUTER1, it will be refused, but all other traffic than this can cross ROUTER1 normally. Therefore, in the configuration of access list, it is needed to deny datagrams from the specified source to the specified destination and allow all other datagrams to cross.
1.The standard Access Control List should be placed near to the source.
2.Extended Access Control List should be placed near to the destination.

There are two solutions to issue this problem:
1.Apply access list to interface fa0/0 in the inbound direction.
ROUTER1(config)# access-list 101 deny ip host 172.16.161.150 host 172.16.162.163
ROUTER1(config)# access-list 101 permit ip any any
ROUTER1(config)# interface fa0/0
ROUTER1(config-if)# ip access-group 101 in
ROUTER1(config-if)# exit
2.Apply access list to interface fa0/1 in the outbound direction.
ROUTER1(config)# access-list 101 deny ip host 172.16.161.150 host 172.16.162.163
ROUTER1(config)# access-list 101 permit ip any any
ROUTER1(config)# interface fa0/1
ROUTER1(config-if)# ip access-group 101 out
ROUTER1(config-if)# exit

Both methods will be used in the actual work. But the company will advise you to use the first

method on the basis of savings routing resources. However, in the examination environment, please complete the steps of answering questions according to options provided. We remind you that the examination environment and the actual environment are not exactly the same.

To block communication between Workstation A and Server 1, we have to configure Extended Access List.

To define an extended IP access list, use the extended version of the access-list command in global configuration mode. To remove the access lists, use the no form of this command.

access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol source source-wildcard destination destination-wildcard

Source Address will be of the Workstation A i.e. 172.16.161.150 and destination address will be of the Server 1 i.e. 172.16.162.163.

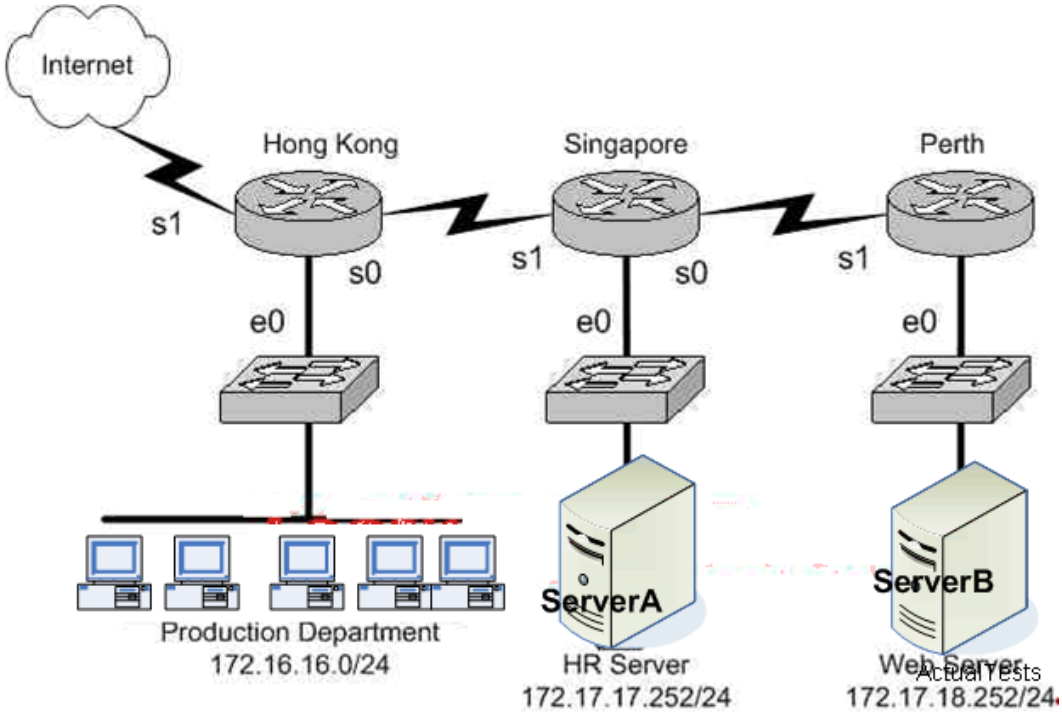
The access list will be placed on the FA0/0 of Router Router1.

QUESTION NO: 394

Refer to the graphic. Assuming the following goals:

1) allow Telnet from the Internet to the HR server
2) allow HTTP access from the Internet to the web server
3) all other traffic from the Internet should be blocked

Which of the following access list statements are necessary to accomplish these goals? (Select two.)



A. access-list 101 permit tcp any 172.17.17.252 0.0.0.0 eq 23
B. access-list 101 permit tcp any 172.17.18.252 0.0.0.0 eq 80
C. access-list 101 deny tcp any 172.17.18.252 0.0.0.0 eq 80
D. access-list 1 permit tcp any 172.17.17.252 0.0.0.0 eq 23

Answer: A,B

Explanation:
Extended ACL has the ability of filtering based on source and destination addresses, with which you can prevent the sending station from visiting some specific receiving station and at the same time, allow access to other resources. Extended ACL can also filter in accordance with protocol (such as port number). Extended ACL number scope is: 100-199 and 2000-2699.

Because of the implicit deny rule at the end of every access list, only two choices need to be made, as the final requirement is automatic.
A. This is correct as we need to allow the access list to allow port 80 connections (port 80 = HTTP) from anywhere, to the web server's IP address.
F. This will fulfill the first requirement, as it allows port 23 (Telnet) traffic from anywhere.
Incorrect Answers:
D: The answer asks you to create an access list, a single one. The answer choices require you to choose two answers. For two statements to be on the same list, you need them to have the same number. So answer choice B can be ruled out by process of elimination. In addition to this, access list 1 is an illegal number, since we need an extended access list to use source and destination information, and extended access lists are in the 100-199 range.

QUESTION NO: 395

A network administrator wants to add a line to an access list that will block only Telnet access by the hosts on subnet 192.168.1.128/28 to the server at 192.168.1.5. What command should be issued to accomplish this task?

A. access-list 1 deny tcp 192.168.1.128 0.0.0.15 host 192.168.1.5 eq 23
access-list 1 permit ip any any
B. access-list 101 deny tcp 192.168.1.128 0.0.0.240 192.168.1.5 0.0.0.0 eq 23
access-list 101 permit ip any any
C. access-list 1 deny tcp 192.168.1.128 0.0.0.255 192.168.1.5 0.0.0.0 eq 21
access-list 1 permit ip any any
D. access-list 101 deny tcp 192.168.1.128 0.0.0.15 192.168.1.5 0.0.0.0 eq 23
access-list 101 permit ip any any

Answer: D

Explanation:
Only choice specifies the correct TCT port and wildcard mask, and uses a valid access list number.
Incorrect Answers:
A: Access list 1 is used for these choices, which is a standard access list. In this example, an extended access list is required. Choice C also specifies port 21, which is used by FTP not Telnet.
B: These choices use an incorrect wildcard mask of 0.0.0.240. It should be 0.0.0.15 for a /28 subnet.
C: Access list 1 is used for these choices, which is a standard access list. In this example, an extended access list is required. Choice C also specifies port 21, which is used by FTP not Telnet.

QUESTION NO: 396

You are securing a network and want to apply an ACL (access control list) to an interface of a router. Which one of the following commands would you use?

A. apply access-list 101 out
B. ip access-group 101 out
C. access-class 101 out
D. permit access-list 101 out

Answer: B

Explanation:
Access Control List (ACL) is the instruction list that is applied to the router interface . These instruction lists tell routers which data packets can be received and which data packets should be denied. Whether the data packets will be received or denied can be determined by such desired

conditions as the source address, the destination address, port numbers and so on.

The steps to establish the Access Control List (ACL) are as follows:

Step 1: Set parameters for this access list test statement (which can be one of several statements).
Router(config)#access-list access-list-number {permit | deny} {test conditions}
Step 2: Enable an interface to use the specified access list.
Router(config-if)#{protocol} access-group access-list-number {in | out}
Standard IP lists (1-99)
Extended IP lists (100-199)

QUESTION NO: 397

Which IP address and wildcard mask would you use in your ACL to block all the hosts in the subnet 192.168.16.43/28?

A. 192.168.16.43 0.0.0.212
B. 192.168.16.32 0.0.0.15
C. 192.168.16.32 0.0.0.16
D. 192.168.16.0 0.0.0.31

Answer: B

Explanation:
Since there are 28 bits in the subnet mask, we can find the inverse mask by reversing the 1's and 0's.

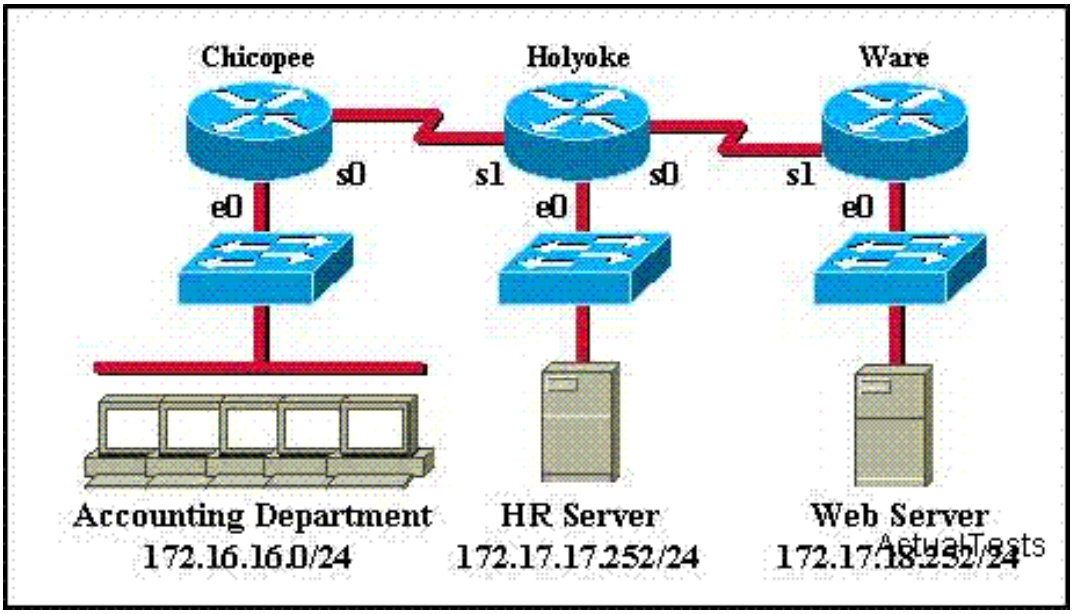
/28 = 11111111.11111111.11111111.11110000
/28 Inverse = 00000000.00000000.00000000.00001111 = 192.168.16.32/15

The address 192.168.16.32 and the wildcard mask 0.0.0.15 is the correct answer as shown. This will match all addresses in the 192.168.16.32-192.168.16.47 range.

QUESTION NO: 398

An access list has been designed to prevent HTTP traffic from the Accounting Department from reaching the HR server attached to the Holyoke router. Which of the following access lists will accomplish this task when grouped with the e0 interface on the Chicopee router?

Exhibit:



A. permit ip any any
deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 eq 80
B. permit ip any any
deny tcp 172.17.17.252 0.0.0.0 172.16.16.0 0.0.0.255 eq 80
C. deny tcp 172.17.17.252 0.0.0.0 172.16.16.0 0.0.0.255 eq 80
permit ip any any
D. deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 eq 80
permit ip any any

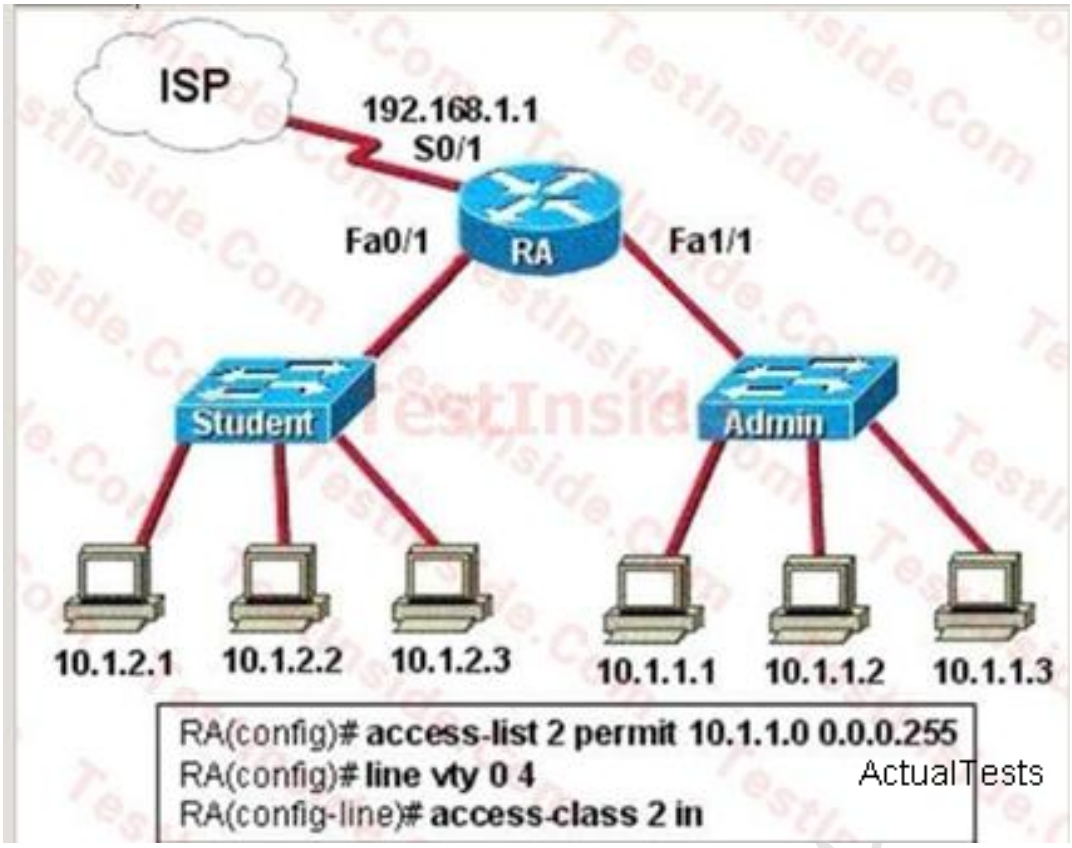
Answer: D

Explanation:
The HTTP service establishes connection through the TCP protocol. To prevent HTTP traffic from the Accounting Department from reaching the HR server attached to the Holyoke router, reject all the TCP requests from the Accounting department to the 80 port and reject all the TCP connection requests from the HR server to the Accounting department.

Section 3: Configure and apply an ACLs to limit telnet and SSH access to the router using (including: SDM/CLI) (4 question)

QUESTION NO: 399

The network topology exhibit is shown below:



Why would the network administrator configure RA in this manner?

A. To give students access to the internet
B. To prevent students from accessing the command prompt of RA
C. To prevent administrators from accessing the console of RA
D. To give administrators access to the internet
E. To prevent students from accessing the internet
F. To prevent students from accessing the Admin network

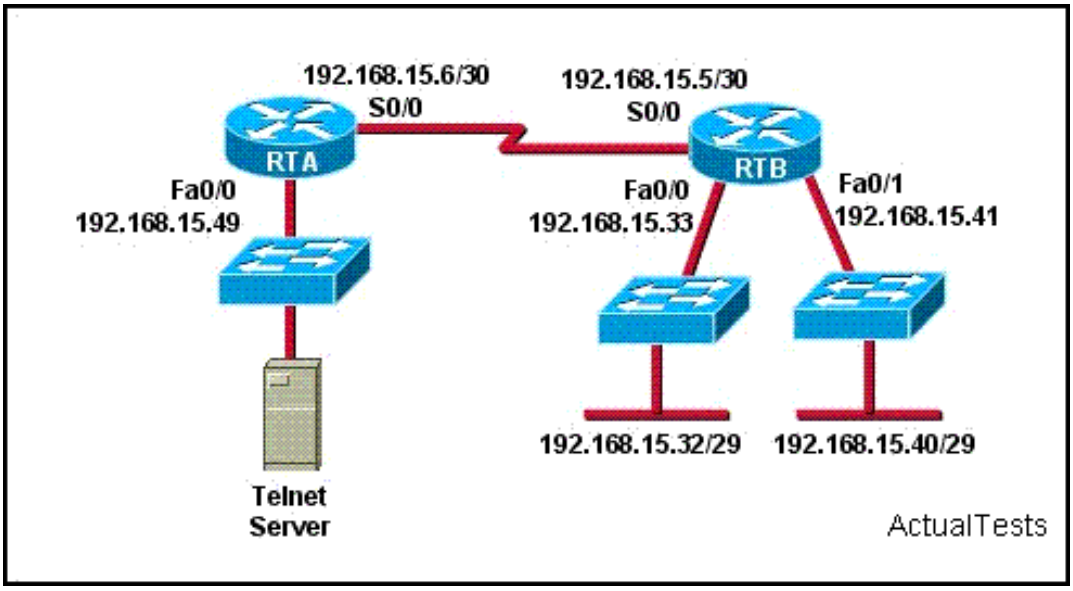
Answer: B

Explanation:
An ACL is configured on RA to allow users on the 10.1.1.0/24 network to access VTY line of RA and to prevent the access of other users.

QUESTION NO: 400

Refer to the exhibit. The access list has been configured on the S0/0 interface of router RTB in the outbound direction. Which two packets, if routed to the interface, will be denied? (Choose two.)

access-list 101 deny tcp 192.168.15.32 0.0.0.15 any eq telnet
access-list 101 permit ip any any



A. source ip address:, 192.168.15.36 destination port: 23
B. source ip address:, 192.168.15.41 destination port: 21
C. source ip address:, 192.168.15.49 destination port: 23
D. source ip address: 192.168.15.46; destination port: 23
E. source ip address: 192.168.15.5; destination port: 21
F. source ip address:, 192.168.15.37 destination port: 21

Answer: A,D

Explanation:
From the access control list, we know that the denied network segment is 192.168.15.32 0.0.0.15, that is, 192.168.15.32/28 ---192.168.15.32~192.168.15.47. Telnet requests from a host in this network segment will be denied.

QUESTION NO: 401

Recently, unauthorized users have used Telnet to gain access to the company router. As the network administrator, you want to configure and apply an access list to allow Telnet access to the router, but only from your computer. Please consider the problem carefully, which group of commands would be the best choice to allow only the IP address 172.16.3.3 to have Telnet access to the router?

A. access-list 101 permit tcp any host 172.16.3.3 eq telnet
interface s0/0
ip access-group 101 in
B. access-list 3 permit host 172.16.3.3
line vty 0 4
ip access-group 3 in
C. access-list 3 permit host 172.16.3.3
line vty 0 4

access-class 3 in
D. access-list 101 permit tcp any host 172.16.3.3 eq telnet
access-list 101 permit ip any any
interface s0/0
ip access-group 101 in

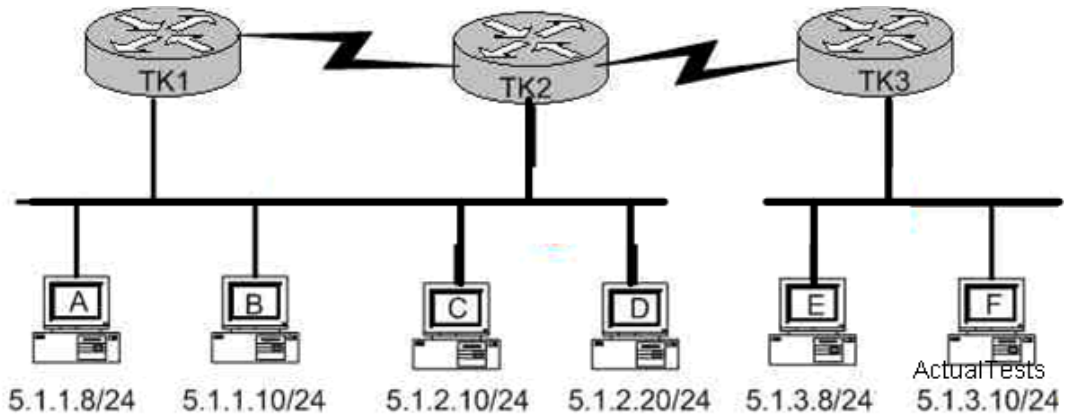
Answer: C

Explanation:
To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list, use the access-class command in line configuration mode.
Example:
The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router:
access-list 12 permit 192.89.55.0 0.0.0.255
line 1 5
access-class 12 in
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800873c8.html#wp1017389

QUESTION NO: 402

Exhibit:
access-list 101 deny tcp 5.1.1.10 0.0.0.0 5.1.3.0 0.0.0.255 eq telnet
access-list 101 permit ip any any

The access control list shown in the graphic has been applied to the Ethernet interface of router TK1 using the ip access-group 101 in command. Which of the following Telnet sessions will be blocked by this ACL? (Choose two.)



A. from host B to host 5.1.3.8
B. from host A to host 5.1.1.10
C. from host A to host 5.1.3.10
D. from host B to host 5.1.2.10

Answer: A,C

Explanation:
All the telnet sessions from the single host (host B) to any device in the 5.1.3.0/24 network will be denied, while all other traffic will be permitted as specified by the second line in access list 101.

"Access-list 101 deny tcp 5.1.1.8 0.0.0.3 5.1.3.0 0.0.0.255 eq telnet" means: deny all telnet dialog from the network segment 5.1.1.8 - 5.1.1.10/24 to network segment 5.1.3.0/24
From the chart above, the refused dialogs are:

from host 5.1.1.8/24 to host 5.1.3.8;
from host 5.1.1.8/24 to host 5.1.3.10;
from host 5.1.1.10/24 to host 5.1.3.8;
from host 5.1.1.10/24 to host 5.1.3.10.

Section 4: Verify and monitor ACLs in a network environment (7 question)

QUESTION NO: 403

An inbound access list has been configured on a serial interface to deny packet entry for TCP and UDP ports 21, 23 and 25. What types of packets will be permitted by this ACL? (Choose three.)

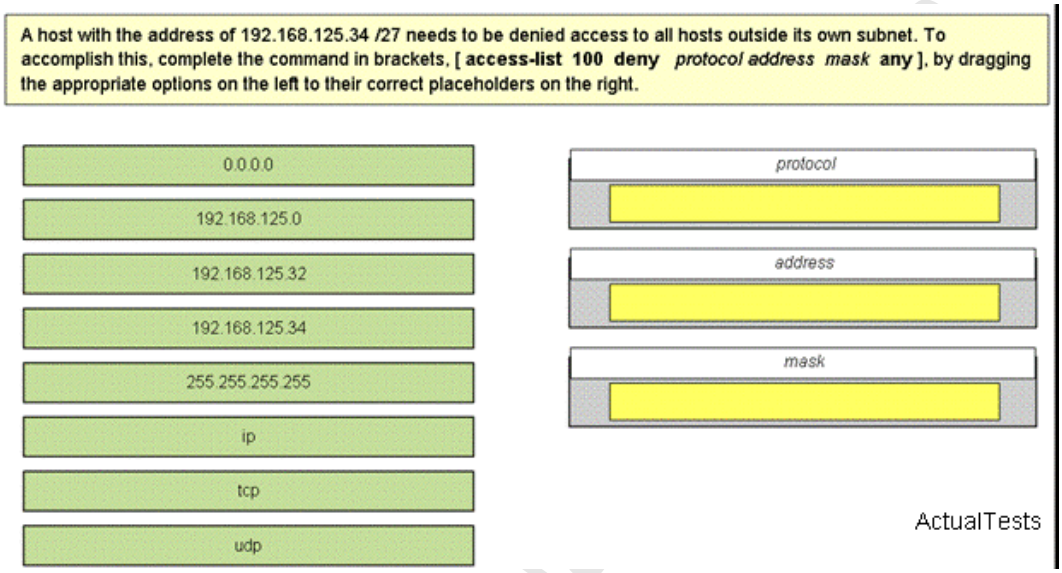
A. HTTP
B. FTP
C. POP3
D. Telnet
E. SMTP
F. DNS

Answer: A,C,F

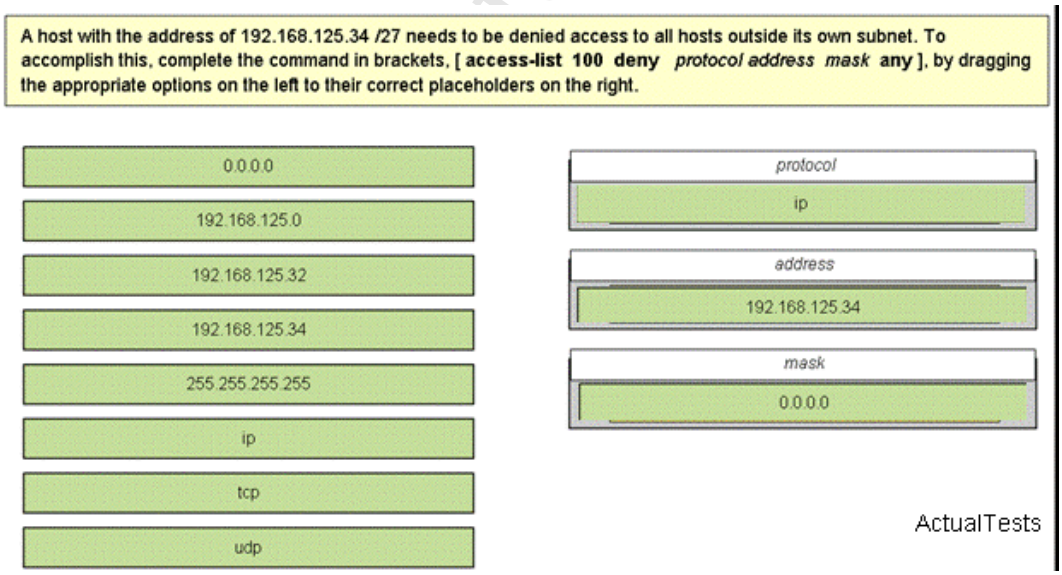
Explanation:
The most often used port numbers of TCP/UDP are as follows:
The port numbers of TCP:
20 FTP data
21 FTP control
23 Telnet
25 SMTP

53 DNS
80 WWW
100 POP3
The port numbers of UDP
53 DNS
69 TFTP
161 SNMP
Note: DNS uses TCP to perform Zone Transfers and UDP to query name .
The ACL created on the router denied the traffic from the ports 21,23,25, thus allowing these three types of traffic such as DNS, POP3, HTTP to cross .

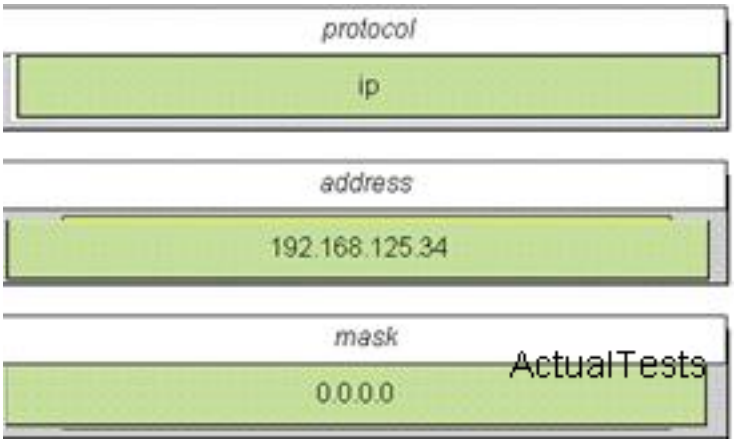
QUESTION NO: 404 DRAG DROP



Answer:

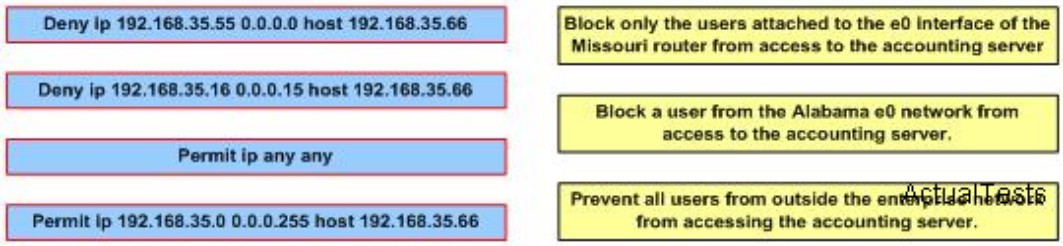


Explanation:

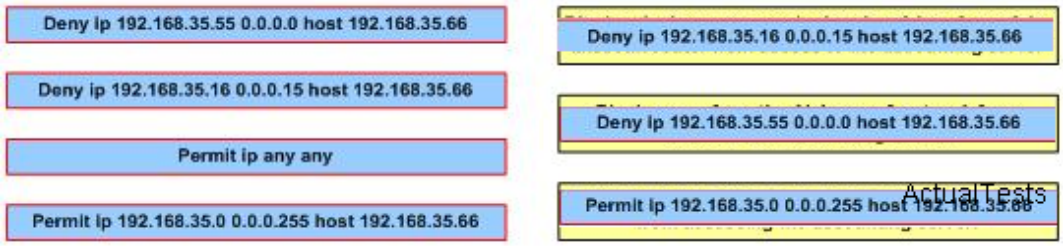


QUESTION NO: 405 DRAG DROP

Answer added from Engine.The Missouri branch office router is connected through its s0 interface to the Alabama Headquarters router s1 interface.The Alabama router has two LANs. Missouri user obtain internet access through the Headquarters router. The network interfaces in the topology are addressed as follows:
Missouri: e0-192.168.35.33/28;
Alabama: e0-192.168.35.49/28
e1-192.168.35.65/28
s1-192.168.35.34/28
The accounting server has the address of 192.168.35.66/28.Match the access list conditions on the left with the goals on the right.(Not all options on the left are used.)



Answer:



Explanation:

QUESTION NO: 406

On your newly installed router, you apply the access list illustrated below to interface Ethernet 0 on a router.
The interface is connected to the 192.168.1.8/29 LAN.
access-list 123 deny tcp 192.168.166.18 0.0.0.7 eq 20 any
access-list 123 deny tcp 192.168.166.18 0.0.0.7 eq 21 any

How will the above access lists affect traffic?

A. All traffic will be allowed to exit E0 except FTP traffic.
B. FTP traffic from 192.168.166.19 to any host will be denied.
C. All traffic exiting E0 will be denied.
D. All FTP traffic to network 192.168.166.18/29 from any host will be denied.

Answer: C

Explanation:
Access Control List (ACL) is the directive list used in router interface. These instructive lists are to tell the router which data packets can be received, and which should be rejected. As for whether the packet will be received or rejected, it is determined by particular instructive conditions such as source address, destination address, port number, and agreement.

By default every access list contains an implicit deny statement at the end. Because of this, only an access list that contains at least one permit statement will be useful. In this example there is no permit statement, so it will deny all traffic exiting E0 Interface.
Incorrect Answers:
A: It will deny everything, including FTP and telnet traffic.
B: It will deny all traffic in addition to the condition mentioned in these answers, because there is no permit statement at the end.
D: It will deny all traffic in addition to the condition mentioned in these answers, because there is no permit statement at the end.

QUESTION NO: 407

Which of the following statements regarding the use of multiple access lists are valid when configuring a single interface on a Cisco router?

A. One access list may be configured per direction for each Layer 3 protocol configured on an interface.
B. Application of up to three access lists per protocol to a single interface.
C. The maximum number allowed varies due to RAM availability in the router.
D. No more than two access lists per interface.

Answer: A

Explanation:
For each interface, one access list for each protocol (IP, IPX, etc) can be applied in the inbound direction, and one for the outbound direction.
Incorrect Answers:
D: It is true that no more than two access lists can be applied per interface (inbound and outbound). However, this applies per layer 3 protocol, so it is possible to configure more than 2 access lists per interface.

QUESTION NO: 408

An access list was written with the four statements shown in the graphic. Which single access list statement will combine all four of these statements into a single statement that will have exactly the same effect?

```
access-list 10 permit 172.29.16.0 0.0.0.255
access-list 10 permit 172.29.17.0 0.0.0.255
access-list 10 permit 172.29.18.0 0.0.0.255
access-list 10 permit 172.29.19.0 0.0.0.255
```

A. access-list 11 permit 172.29.161.0 0.0.1.255
B. access-list 11 permit 172.29.161.0 0.0.0.255
C. access-list 10 permit 172.29.16.0 0.0.3.255
D. access-list 11 permit 172.29.161.0 0.0.15.255

Answer: C

Explanation:
172.29.16.0 0.0.3.255 is an aggregate address for those 4 networks. If you would write all these addresses in binary form and will mark the equal part, than you will see that it is 172.29.16.0 0.0.3.255 is the correct wildcard mask as it will aggregate these four contiguous ACL statements.

QUESTION NO: 409

Which command shows if an access list is assigned to an interface?

A. show ip interface [interface] access-lists
B. show ip access-lists interface [interface]
C. show ip interface [interface]
D. show ip access-lists [interface]

Answer: C

Explanation:
Section 5: Troubleshoot ACL issues (2 question)

QUESTION NO: 410

What is the effect of the following access list condition?

access-list 101 permit ip 10.25.30.0 0.0.0.255 any

A. permit all packets matching the host bits in the source address to all destinations
B. permit all packets from the third subnet of the network address to all destinations
C. permit all packets matching the last octet of the destination address and accept all source addresses
D. permit all packets to destinations matching the first three octets in the destination address
E. permit all packets matching the first three octets of the source address to all destinations

Answer: E

Explanation:
Standard IP Access Control Lists: a Standard IP Access Control List will match the source address or part of the source address within IP packet; it may refuse or allow the matched packet. The Access Control List with No. range from 1 to 99 is the Standard IP Access Control List. Extended IP Access Control List: Extended IP Access Control List has more matching options than Standard IP Access Control Lists, including protocol type, source address, destination address, source end, destination end, connections establishing and IP priority, and so on. The access control list with No. range from 100 to 199 is Extended IP Access Control Lists. Named IP Access Control Lists: Named IP Access Control List is so called because list name is used instead of list number upon the definition of IP Access Control Lists.

QUESTION NO: 411

For security reasons, the network administrator needs to prevent pings into the corporate networks from hosts outside the internetwork. Which protocol should be blocked with access control lists?

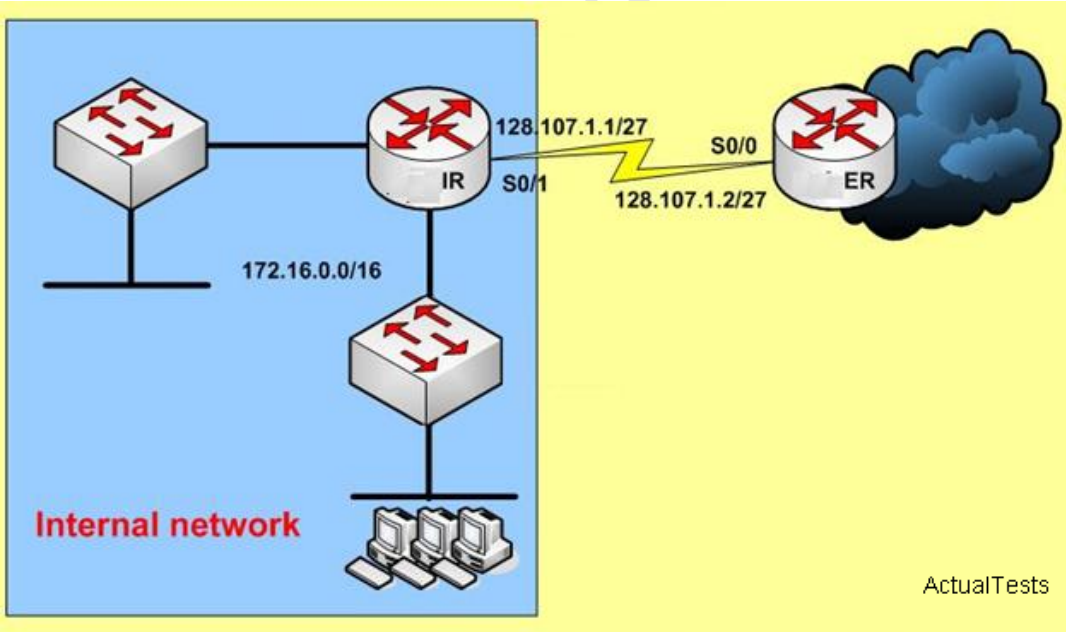
A. ICMP
B. UDP
C. TCP
D. IP

Answer: A

Explanation:
Ping packets use the ICMP protocol; therefore, the ICMP protocol should be blocked with access control lists.
Section 6: Explain the basic operation of NAT (4 question)

QUESTION NO: 412

Study the exhibit carefully. NAT has been used for converting all the IP addresses on the internal network to the single address 128.107.1.1 as traffic is routed toward the Internet. Which of these statements accurately describes what will happen when the IP traffic returns from the Internet destined for hosts on the internal network?

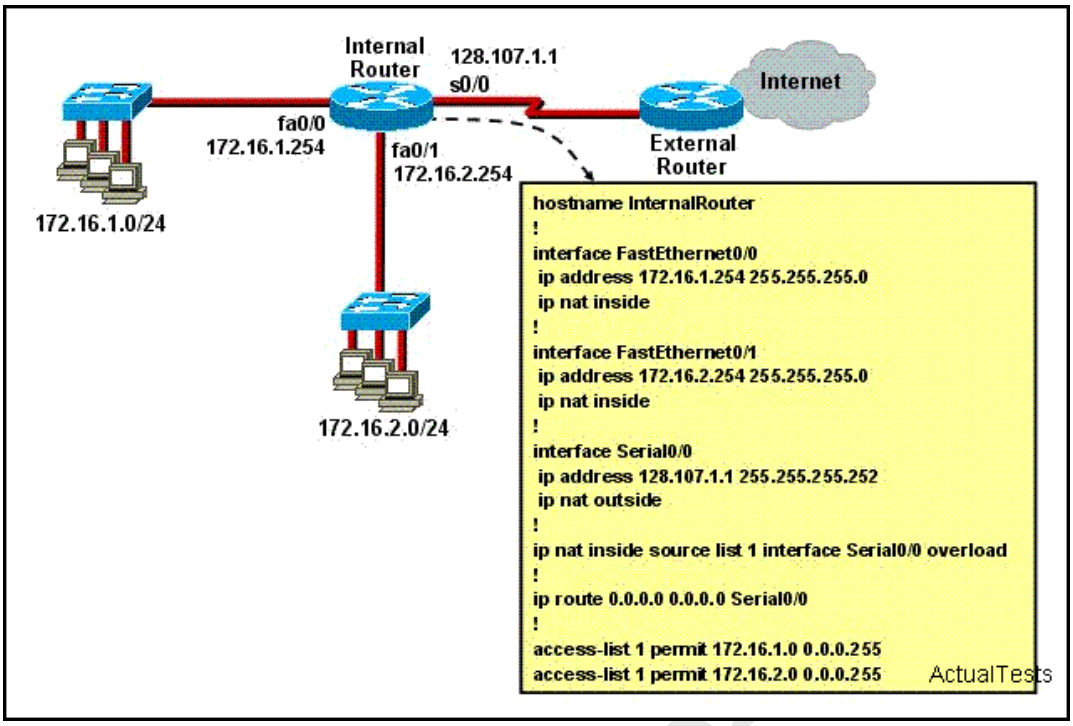


A. IR will convert the source IP addresses of all packets before forwarding them onto the internal network.
B. ER will translate the destination IP addresses of all packets before forwarding them to IR.
C. ER will require a route to 172.16.0.0/16 in its routing table to properly direct the traffic.
D. ER can use the directly connected interface on the 128.107.1.0/27 network to route return traffic to its originators.

Answer: D

QUESTION NO: 413

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. ExternalRouter must be configured with static routes to networks 172.16.1.0/24 and 172.16.2.0/24.
C. The number 1 referred to in the ip nat inside source command references access-list number 1.
D. Because of the addressing on interface FastEthernet0/1, the Serial0/0 interface address will not support the NAT configuration as shown.

Answer: C

Explanation:
Command ip nat inside source list needs to configure a standard IP access control list to designate internal source address used for transmission --- transmit any address listed by permit, not transmit any address listed by deny or implicitly denied address.

The ip nat inside source list 1 pool interface command tells the router to translate
IP addresses that match access-list 1 to an IP address of Serail0/0 inteface.
The access list in this case is not being used to permit or deny traffic as we would use it for security reasons to filter traffic. It is being used in this case to select or designate what we often call interesting traffic. When interesting traffic has been matched with the access list, it is pulled into the NAT process to be translated.

QUESTION NO: 414

In any NAT (network address translation) configuration, what is the Inside Global IP address?

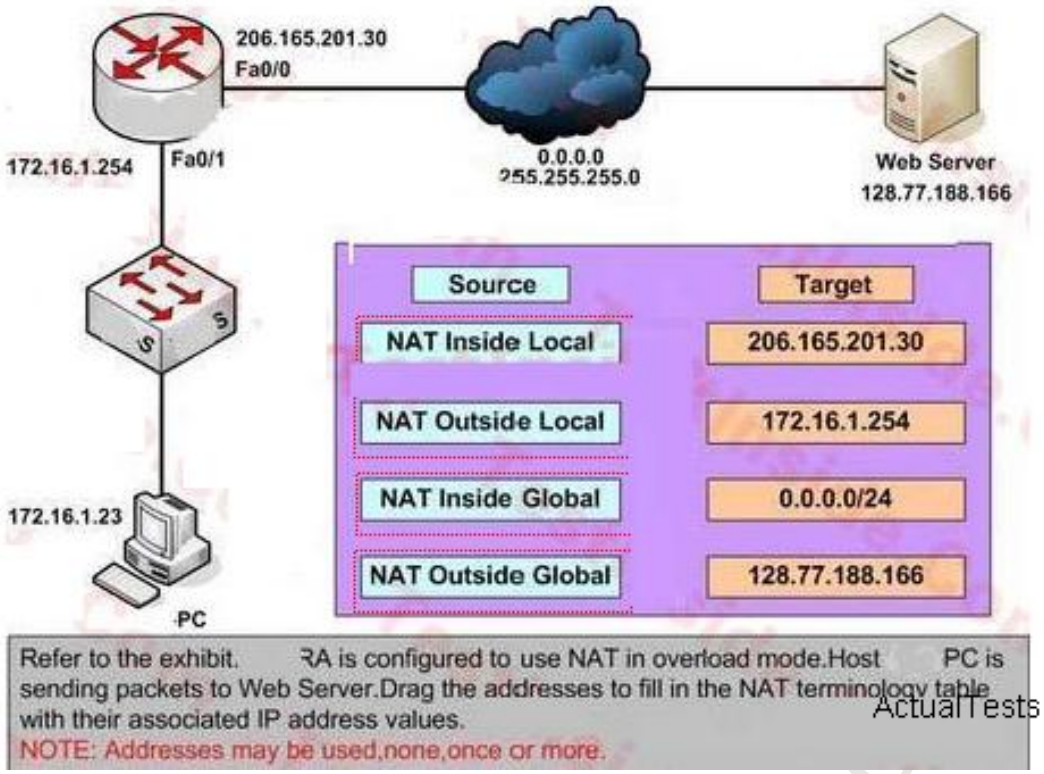
A. a registered address that represents an inside host to an outside network
B. a globally unique, private IP address assigned to a host on the inside network
C. the summarized address for all of the internal subnetted addresses
D. the MAC address of the router used by inside hosts to connect to the Internet

Answer: A

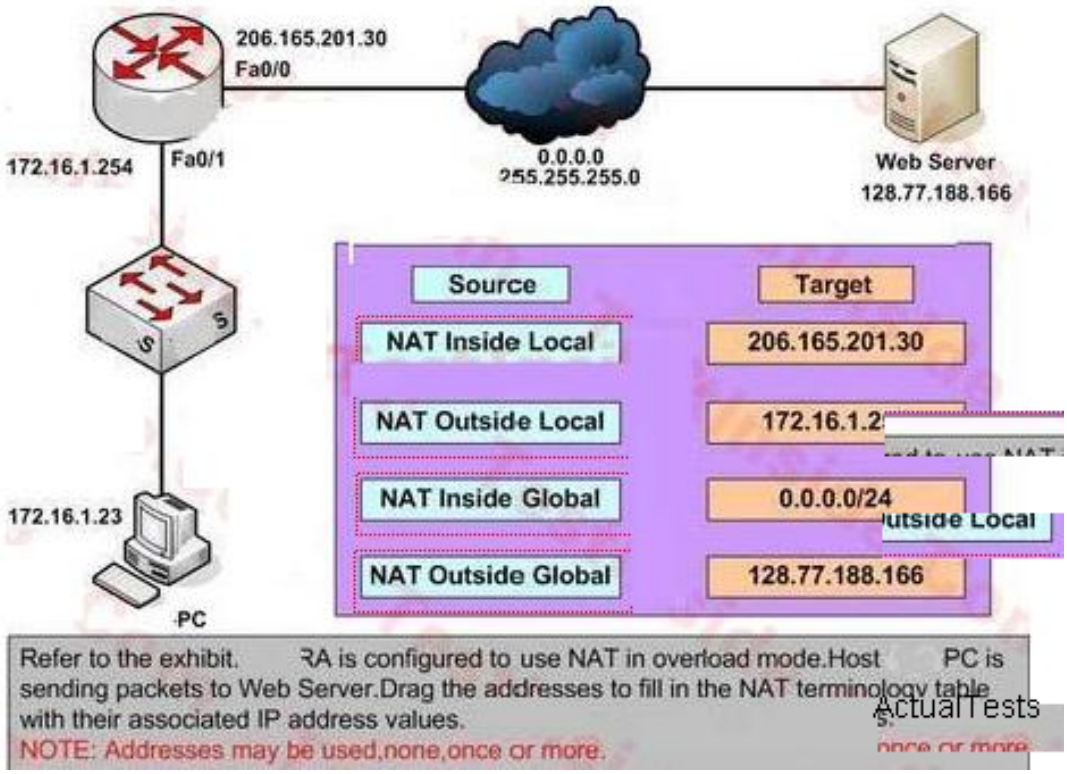
Explanation:
With NAT, Cisco defines 4 different types of addresses as follows:
* Inside local address - The IP address assigned to a host on the inside network. This is the address configured as a parameter of the computer's OS or received via dynamic address allocation protocols such as DHCP. The address is likely not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.
* Inside global address - A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.
* Outside local address - The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.
* Outside global address - The IP address assigned to a host on the outside network by the host's owner. The address is allocated from a globally routable address or network space.
The above definitions still leave a lot to be interpreted. For this example, this document redefines these terms by first defining "local address" and "global address." Keep in mind that the terms "inside" and "outside" are NAT definitions. Interfaces on a NAT router are defined as "inside" or "outside" with the NAT configuration commands, ip nat inside and ip nat outside . Networks to which these interfaces connect can then be thought of as "inside" networks or "outside" networks, respectively.
* Local address - A local address is any address that appears on the "inside" portion of the network.
* Global address - A global address is any address that appears on the "outside" portion of the network.

QUESTION NO: 415 DRAG DROP

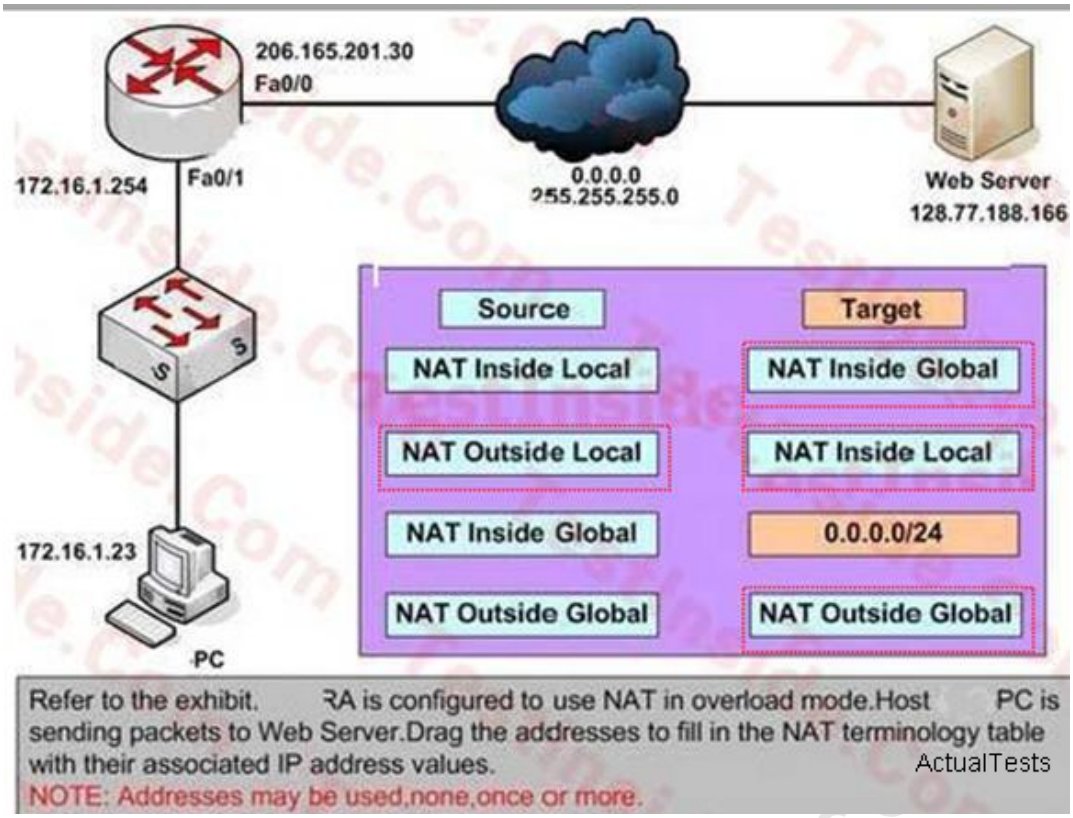
Exhibit:



Answer:



Explanation:



NAT addresses can be divided into two categories: inside network and outside network which are defined based on the NAT functions. The device that has NAT functions connects the inside and the outside network like a bridge, the NIC connected to the inside network is called "inside" , the NIC connected to the outside network is called "outside", that is to say, the inside addresses are used by the inside network devices, while the outside addresses are used by the outside network devices.

Addresses can also be divided into local and global addresses. Local address refers to the address that can be seen and used by the inside network devices; while global address refers to the address that can be seen and used by the outside network devices.

These four addresses are:
Inside local address is the IP address used by the inside network devices, which is often a private address.

Inside global address is a public address provided by ISP. It is often used when the inside network devices communicate with the outside network devices.

Outside local address is the address used by the outside network device as it appears to the inside network device. It is not necessarily a public network address.

Outside global address is the real address used by the outside network devices.

IP packets sent from the inside network devices regard "inside local address" as the source address and "outside local address" as the destination address. When the packets reach the

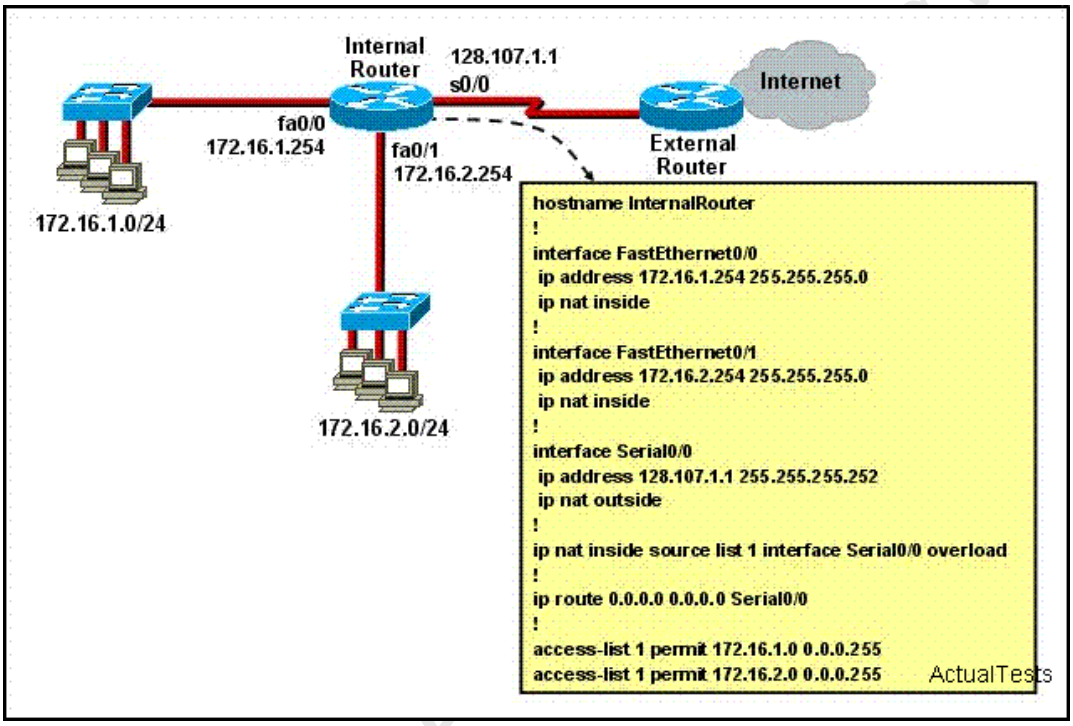
"inside" interface of the NAT equipment, the addresses will be translated into "inside global address" and "outside global address" , the packets will be out from the "outside" interface .

In the same way, IP packets sent from the outside network devices regard "outside global address" as the source address and "inside global address" as the destination address. When the packets reach the "outside" interface of the NAT equipment, the addresses will be translated into "outside local address" and "inside local address", the packets will be out from the "inside" interface.

Section 7: Configure NAT for given network requirements using (including: CLI/SDM) (2 question)

QUESTION NO: 416

Refer to the exhibit. What is the purpose of the configuration that is shown?



A. to translate addresses of hosts on the fa0/0 and fa0/1 networks to a single public IP address for Internet access

B. to allow IP hosts on the Internet to initiate TCP/IP connections to hosts on fa0/0 and fa0/1

C. to provide security on fa0/0 and fa0/1 through the application of an access list

D. to translate the internal address of each host on fa0/0 and fa0/1 to a unique external IP address for Internet acces

Answer: A

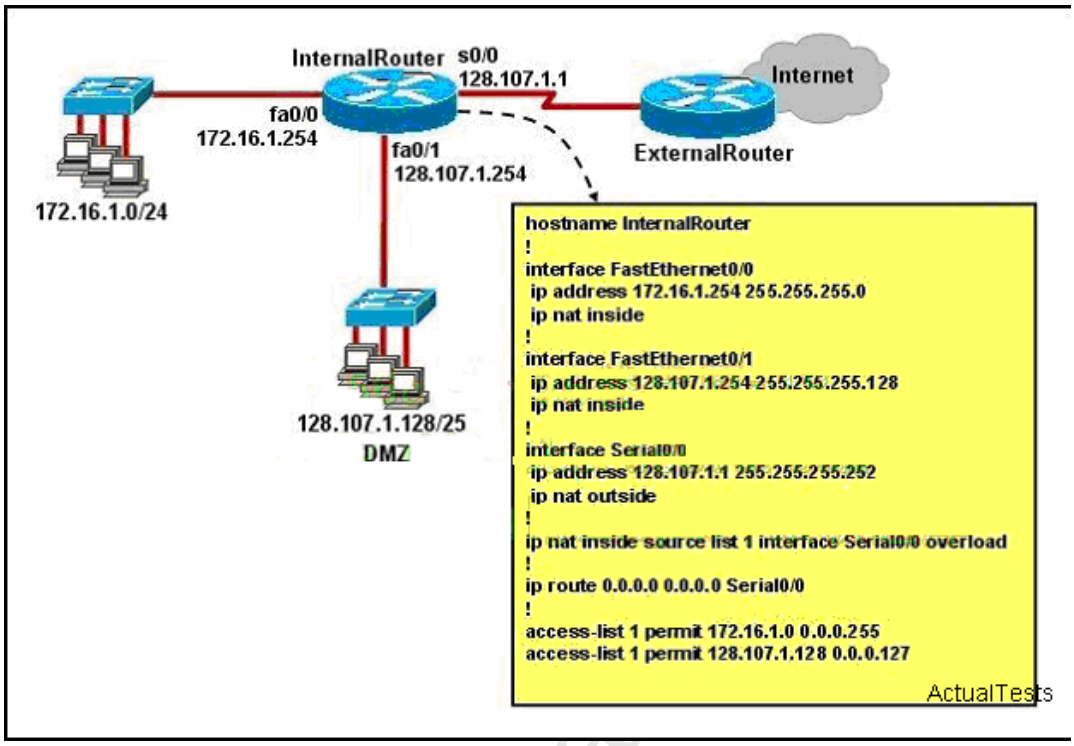
Explanation:

The internal network, which is connected by the internal router, uses private IP addresses. These IP addresses cannot be routed in a public network, so NAT is used. Two ACLs are defined on the internal router to allow the fa0/0 and fa0/1 networks to invoke the NAT pool for address translation.

All devices with an IP address in the 172.16.1.0/24 and 172.16.20./24 subnets will be translated to the single IP address of the S0/0 interface, which is 28.107.1.1. This configuration is an example of many-to-1 NAT or NAT overload

QUESTION NO: 417

Refer to the exhibit. A junior network engineer has prepared the exhibited configuration file. What two statements are true of the planned configuration for interface fa0/1? (Choose two.)



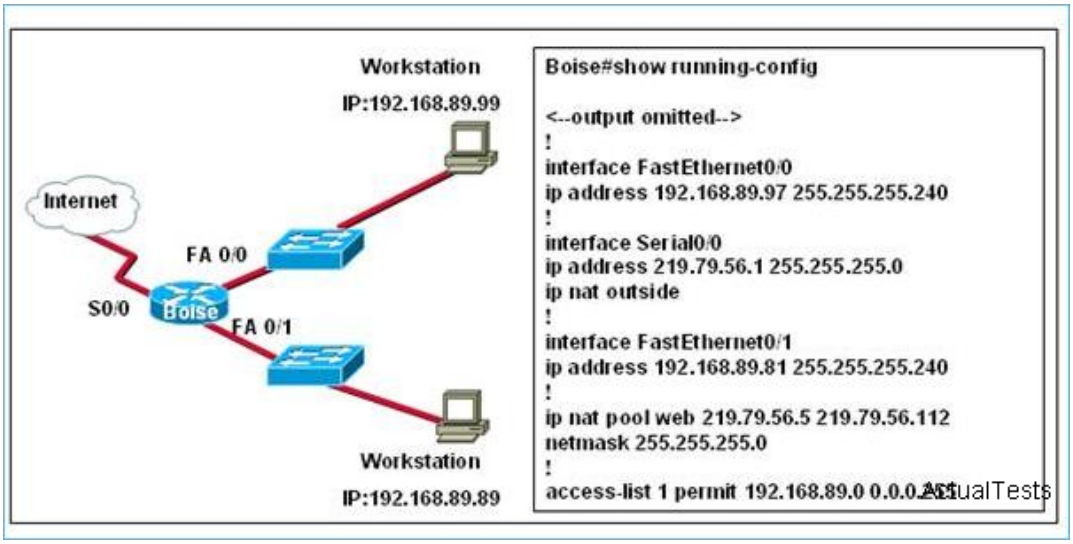
A. The two FastEthernet interfaces will require NAT configured on two outside serial interfaces.
B. Address translation on fa0/1 is not required for DMZ Devices to access the Internet.
C. The fa0/1 IP address overlaps with the space used by s0/0.
D. The fa0/1 IP address is invalid for the IP subnet on which it resides.
E. Internet hosts may not initiate connections to DMZ Devices through the configuration that is shown.

Answer: B,E

Explanation:
Section 8: Troubleshoot NAT issues (9 question)

QUESTION NO: 418

Refer to the exhibit. Which statements describe why the workstation with the IP address 192.168.89.99 cannot access the Internet? (Choose two.)

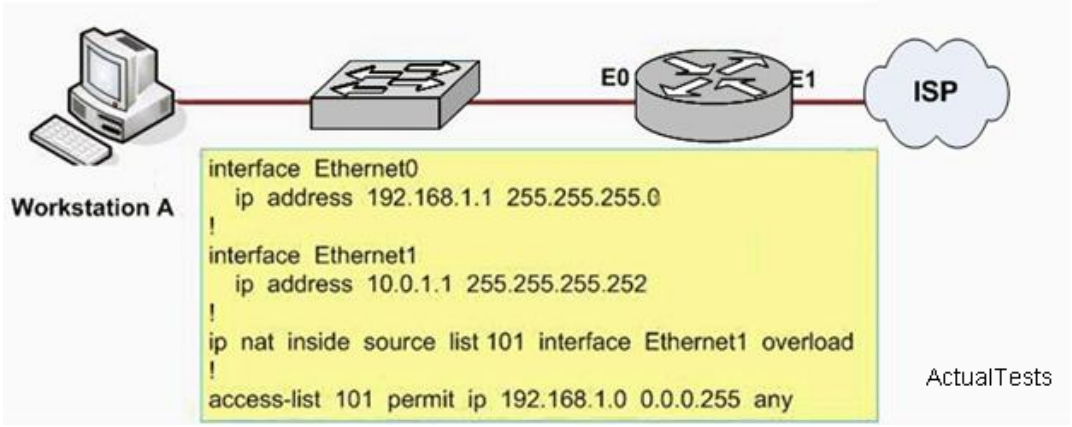


A. The NAT pool is not properly configured to use routable outside addresses.
B. The NAT outside interface is not configured properly.
C. The router is not properly configured to use the access control list for NAT.
D. The NAT inside interfaces are not configured properly.

Answer: C,D

QUESTION NO: 419

Refer to the exhibit. Given the partial configuration shown in the exhibit, why do internal workstations on the 192.168.1.0 network fail to access the Internet?



A. A NAT pool has not been defined.
B. NAT has not been applied to the inside and outside interfaces.
C. The access list has not been applied to the proper interface to allow traffic out of the internal network.
D. The wrong interface is overloaded.

Answer: B

Explanation:

Two basic configurations are needed when configuring NAT in CISCO IOS: 1, the definition of address translation types (global configuration mode command); 2, the definition of devices location (interface sub-configuration mode command). Inside and outside parameters designate the transmission direction. Designate inside on interface that is connected to internal network, and designate outside on interface that is connected to external network. The configuration in the figure above does not apply NAT to interface, so address can not be translated.

QUESTION NO: 420

What is the function of the Cisco IOS command ip nat inside source static 10.1.1.5 172.35.16.5?

A. It maps one inside source address to a range of outside global addresses.
B. It creates a global address pool for all outside NAT transactions.
C. It establishes a dynamic address pool for an inside static address.
D. It creates a one-to-one mapping between an inside local address and an inside global address.
E. It creates dynamic source translations for all inside local PAT transactions.

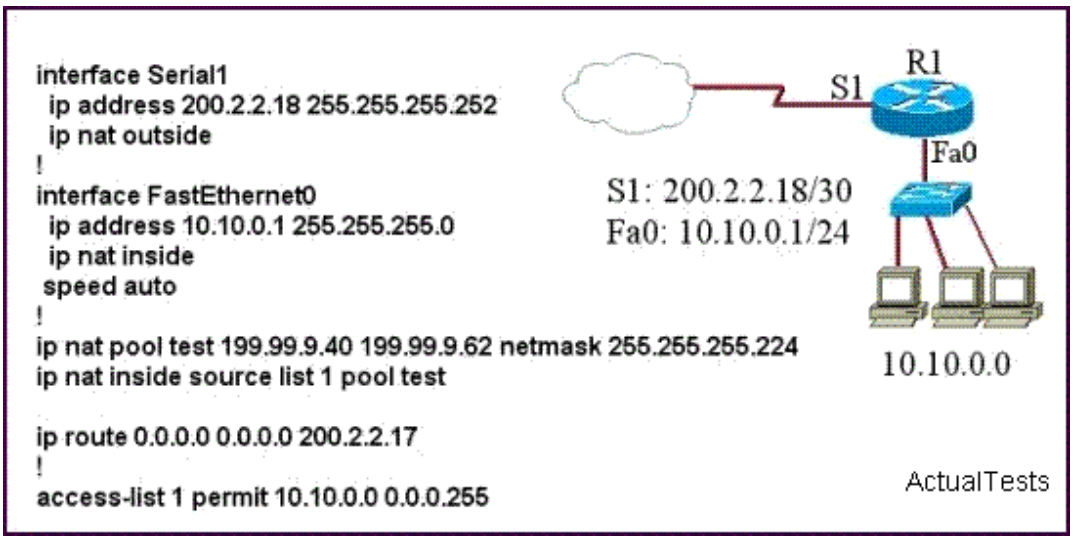
Answer: D

Explanation:
It creates a one-to-one static IP mapping between an inside local address and an inside global address.

In this example, the inside IP address of 10.1.1.5 is being translated to the 172.35.16.5 public IP address. This static 1-1 mapping is typically done for Internet facing servers, such as web servers, FTP servers, or email servers so that users from the outside can access the inside server using the outside (public) IP address.

QUESTION NO: 421

Refer to the topology and router configuration shown in the graphic. A host on the LAN is accessing an FTP server across the Internet. Which of the following addresses could appear as a source address for the packets forwarded by the router to the destination server?



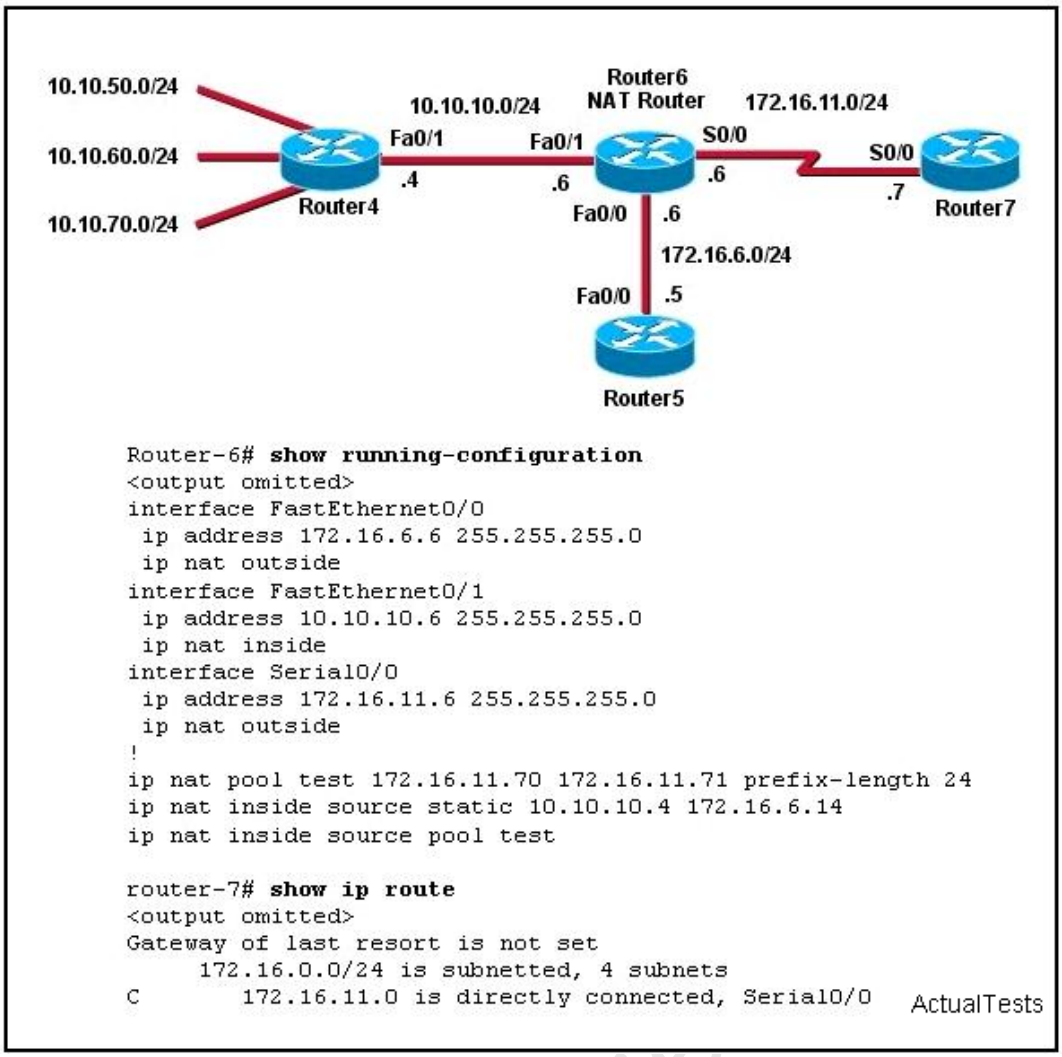
A. 10.10.0.1
B. 200.2.2.17
C. 200.2.2.18
D. 10.10.0.2
E. 199.99.9.33
F. 199.99.9.57

Answer: F

Explanation:
Using NAT we can translate the Source or Destination Address. In our example all source address from the 10.10.00 0.0.0.255 network will be translated to an IP address form the 199.99.9.40-62 pool, making 199.99.9.57 correct.

QUESTION NO: 422

Refer to the exhibit. Router4 can ping Router5 (172.16.6.5), but not Router7 (172.16.11.7). There are no routing protocols running in any of the routers, and Router4 has Router6 as its default gateway. What can be done to address this problem?




```
Router-6# show running-configuration
<output omitted>
interface FastEthernet0/0
 ip address 172.16.6.6 255.255.255.0
 ip nat outside
interface FastEthernet0/1
 ip address 10.10.10.6 255.255.255.0
 ip nat inside
interface Serial0/0
 ip address 172.16.11.6 255.255.255.0
 ip nat outside
!
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24
ip nat inside source static 10.10.10.4 172.16.6.14
ip nat inside source pool test

router-7# show ip route
<output omitted>
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.11.0 is directly connected, Serial0/0
```

ActualTests

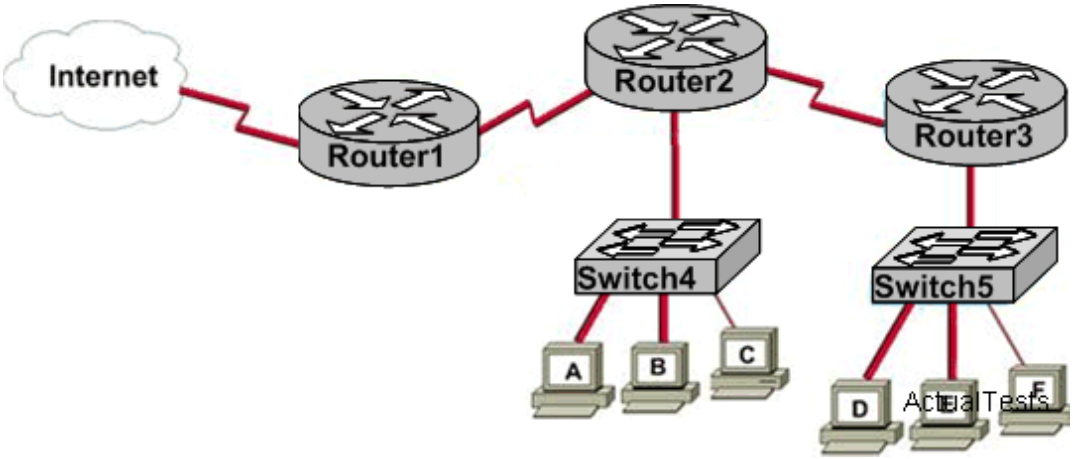
A. Change the inside and outside NAT commands.
B. Add a static route in Router7 back to Router4.
C. Convert to static NAT.
D. Convert to dynamic NAT.

Answer: B

Explanation:
In this example NAT is translating the 10.10.10.4 (Router4 IP) statically to 172.16.6.14. However, we can see that Router7 does not have any route to the 172.16.6.0/24 network so there is no way for Router7 to return the ping traffic back to Router4. Configuring a static route to the 172.16.6.0 network will fix this problem.
Note: The reason that pings to Router5 work is because it knows how to get back to the 172.16.6.0/24 network, since this network resides on its directly connected interface.

QUESTION NO: 423

The network is shown below:



The network administrator would like to implement NAT in the network segment shown in the graphic to allow inside hosts to use a private addressing scheme. In this network segment, where should NAT be configured?

A. router3
B. router1
C. all routers
D. router2

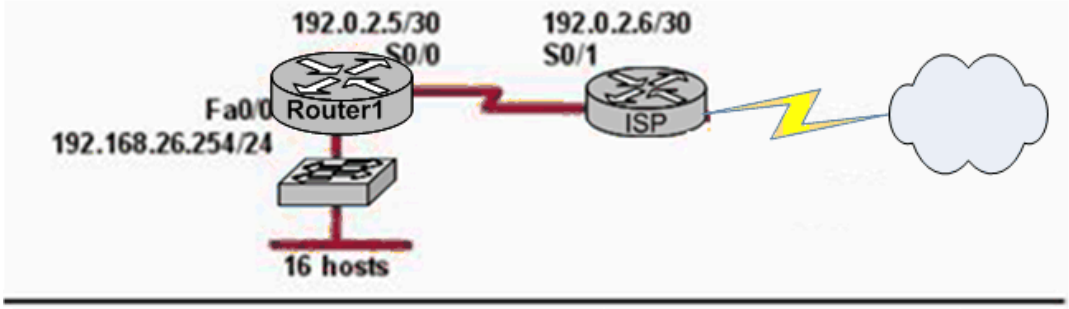
Answer: B

Explanation:
NAT is usually placed on the edge of the enterprise network. It can convert all private IP addresses to public addresses to allow the internal network to communicate with hosts in the Internet.

NAT should always be configured on the b order device. It can be a either a b order router or a PIX firewall connecting to the Internet.

QUESTION NO: 424

Based on the network diagram and configuration shown in the exhibit. The network at the Company has just been configured for NAT as shown. Initial tests indicate that everything is functioning as intended. However, it is found that a number of hosts cannot access the Internet. Why?




```
Router1(config)# ip nat pool SOS 192.0.2.161 192.0.2.165 netmask 255.255.255.224
Router1(config)# access-list 1 permit 192.168.26.0 0.0.0.255
Router1(config)# ip nat inside source list 1 pool SOS
Router1(config)# interface fastethernet 0/0
Router1(config-if)# ip nat inside
Router1(config)# interface serial 0/0
Router1(config-if)# ip nat outside
```

ActualTests

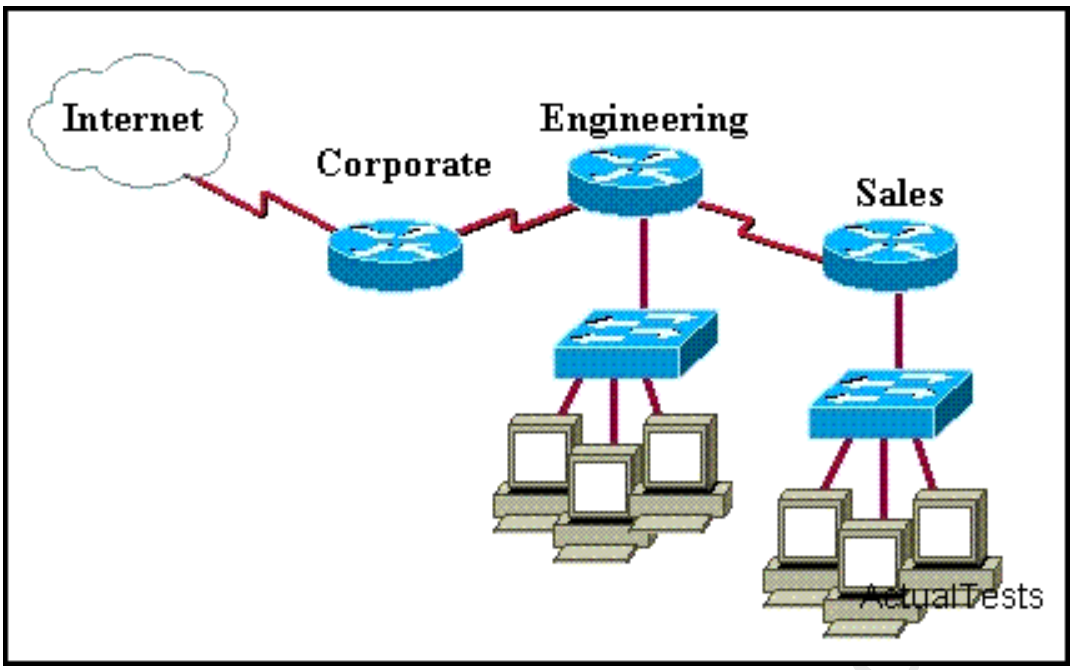
A. There are not enough IP addresses available in the NAT address pool.
B. The S0/1 interface of the ISP router is in the wrong subnet.
C. The wrong interface has been configured with the ip nat inside command.
D. The access list is not correct.

Answer: A

Explanation:
According to the configuration shown above, the NAT pool only specifies 5 IP addresses (192.0.2.161-165) while there are 16 hosts on the network that need to be translated. This explains why everything functions well for the first hosts, but not for the rest. To fix this issue, more IP addresses need to be specified in the NAT pool named SOS, or alternatively the "overload" keyword could be used to specify many to one address translation, or PAT.
Several internal addresses can be NATed to only one or a few external addresses by using a feature called Port Address Translation (PAT) which is also referred to as "overload", a subset of NAT functionality.
PAT uses unique source port numbers on the Inside Global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number could theoretically be as high as 65,536 per IP address. PAT will attempt to preserve the original source port, if this source port is already allocated PAT will attempt to find the first available port number starting from the beginning ofthe appropriate port group 0-5111, 512-1023 or 1024-65535. If there is still no port available from the appropriate group and more than one IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. This continues until it runs out of available ports and IP addresses.
Alternatively, we could have configured port address translation, or NAT overload, to provide Internet access to the given number of hosts.

QUESTION NO: 425

A network administrator would like to implement NAT in the network shown in the graphic to allow inside hosts to use a private addressing scheme. Where should NAT be configured?



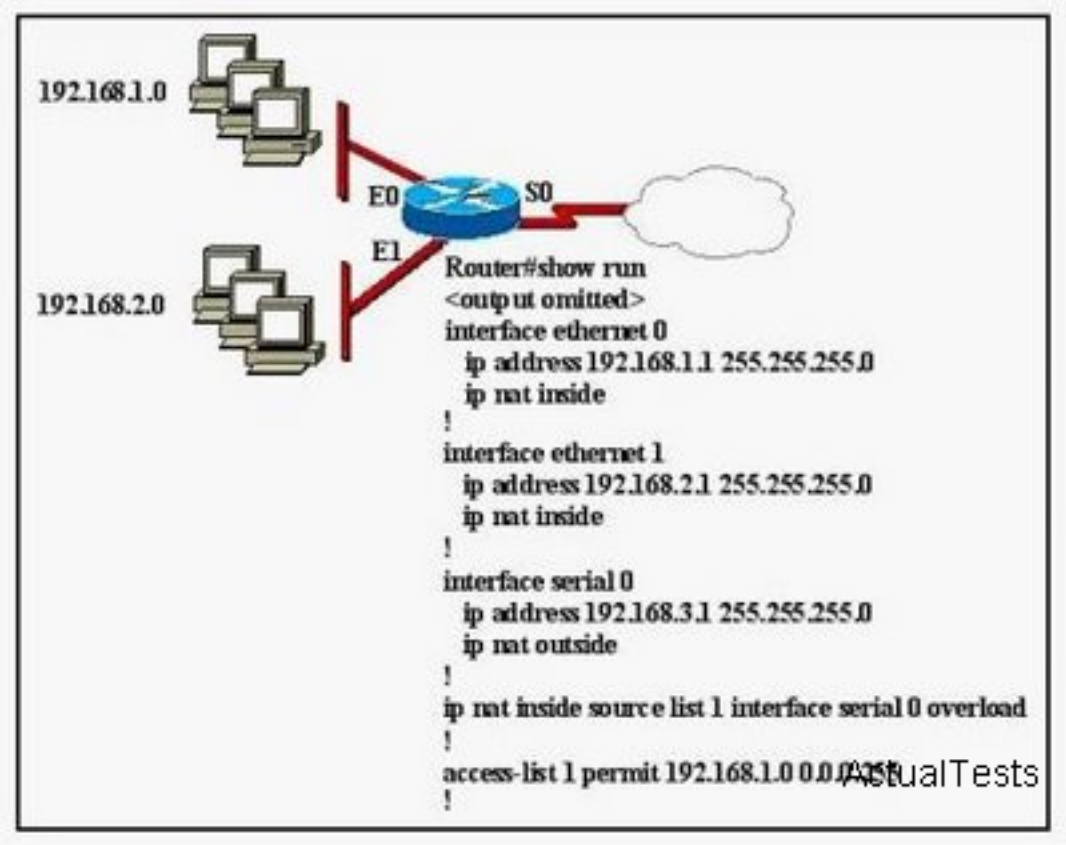
A. all routers
B. all routers and switches
C. Sales router
D. Corporate router
E. Engineering router

Answer: D

Explanation:
NAT is usually placed on the edge of the enterprise network. It can convert all private IP addresses to public addresses to allow the internal network to communicate with hosts in the Internet.

QUESTION NO: 426

The network administrator has configured NAT as shown in the graphic. Some clients can access the Internet while others cannot. What should the network administrator do to resolve this problem?



A. Configure an IP NAT pool.
B. Properly configure the ACL.
C. Apply the ACL to the S0 interface.
D. Configure another interface with the ip nat outside command.

Answer: B

Explanation:
The NAT translation will only translate 192.168.1.0 /24 because of the access-list 1 statement permit matches only 192.168.1.0 network . Therefore other networks were ignored by NAT. To correct this problem change the access-list statement with correct wild card mask access-list 1 permit 192.168.1.0 0.0.255.255

QUESTION NO: 427

Which three types of layer 2 encapsulation are used by the WAN and differ from the LAN? (Choose three)

A. Token bus
B. PPP
C. CSMA/CD
D. Frame Relay
E. Ethernet

F. HDLC

Answer: B,D,F

Explanation:
HDLC, Frame Relay, and PPP are the most common encapsulation types set for serial interfaces in a Cisco router. HDLC is often used in point to point circuits with Cisco routers on each end. HDLC is Cisco proprietary and offers an alternative to PPP.

QUESTION NO: 428

What can a network administrator utilize by using PPP Layer 2 encapsulation? (Choose three.)

A. quality of service
B. multilink support
C. authentication
D. sliding windows
E. compression
F. VLAN support

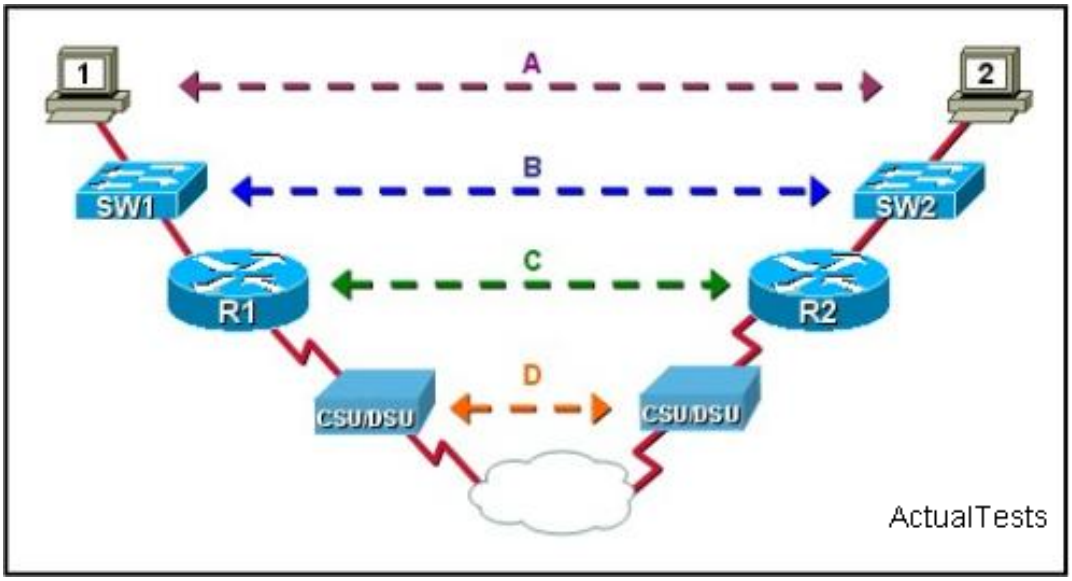
Answer: B,C,E

Explanation:
Compared to HDLC ,PPP has more features. Similar to HDLC, PPP defines a type of frame and how to communicate between PPP devices including the multiplexed networks and the data link layer protocols cross the same link. However, PPP has more characteristics as follows:
Perform the dynamic configuration of the link.
Allow for authentication.
Compress packet header.
Test the quality of the link.
Complete detecting and troubleshooting.
Allow for combining many PPP physical links into a single logical link.

PPP has 3 main components.
1. frame format
2.LCP(Link Control Protocol)
3.NCP(Network Control Protocol)

QUESTION NO: 429

Refer to the exhibit.



In the communication between host 1 and host 2 over the point-to-point WAN, which protocol or technology is represented dashed line A?

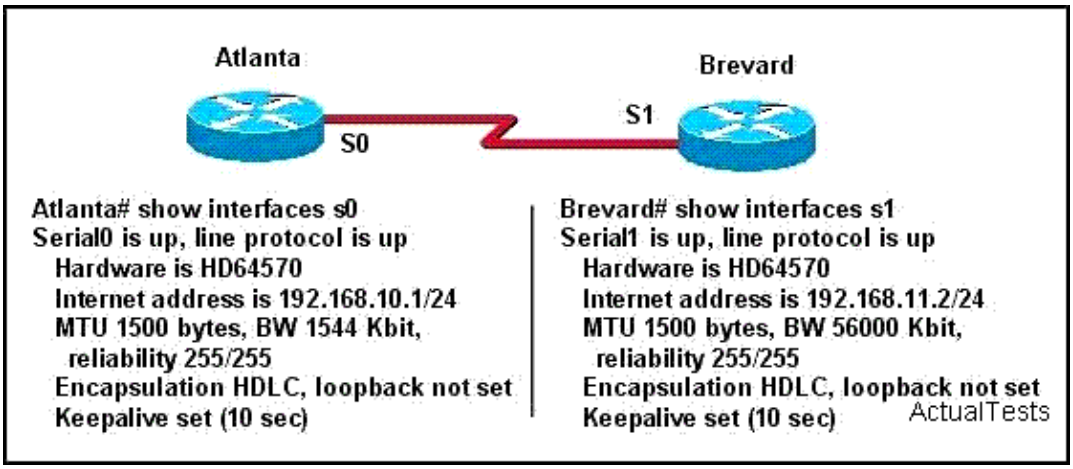
A. IP
B. T1
C. PPP
D. IEEE 802.3

Answer: A

Explanation:
Section 2: Configure and verify a basic WAN serial connection (8 question)

QUESTION NO: 430

Two routers named Atlanta and Brevard are connected by their serial interfaces as shown in the exhibit, but there is no data connectivity between them. The Atlanta router is known to have a correct configuration. Given the partial configurations shown in the exhibit, what is the problem on the Brevard router that is causing the lack of connectivity?



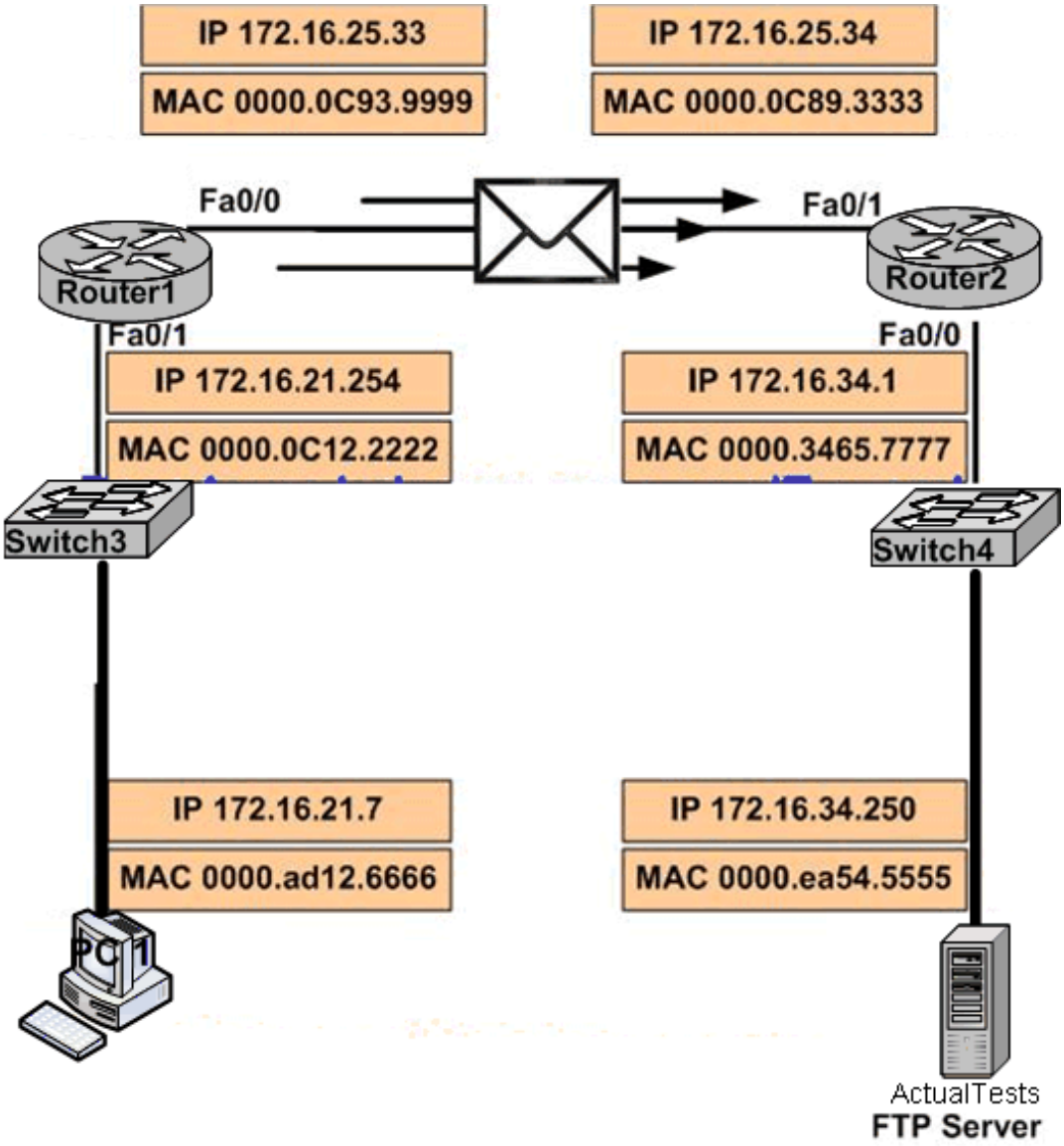
A. The serial line encapsulations are incompatible.
B. The subnet mask is incorrect.
C. The bandwidth setting is incompatible with the connected interface.
D. The maximum transmission unit (MTU) size is too large.
E. The IP address is incorrect.
F. A loopback is not set.

Answer: E

Explanation:
The IP address of the S0 interface of Atlanta is 192.168.10.0/24, and the IP address of the S1 interface of Breavard is 192.168.11.0/24. Change the IP address of the S1 interface to 192.168.10.0/24, the same as that of the S0 interface.

QUESTION NO: 431

As the network administrator, you are configuring Router1 to connect to a non-Cisco network. Which two commands would be applied to the S0/0 WAN interface, but not to the Fa0/0 LAN interface? (Choose two.)



A. ip address
B. no shutdown
C. authentication pap
D. encapsulation ppp

Answer: C,D

Explanation:
Because of the open standards of PPP, it is often used for serial WAN connection. It can work asynchronously and synchronously. Because pap is the most unsafe one in PPP certification protocol, PAP will experience shook hands processes twice during certification stage. At that stage, sending station will send in plain text the user name (the host name) and password to the receiving station. It is not suitable for LAN between Fa0/0.

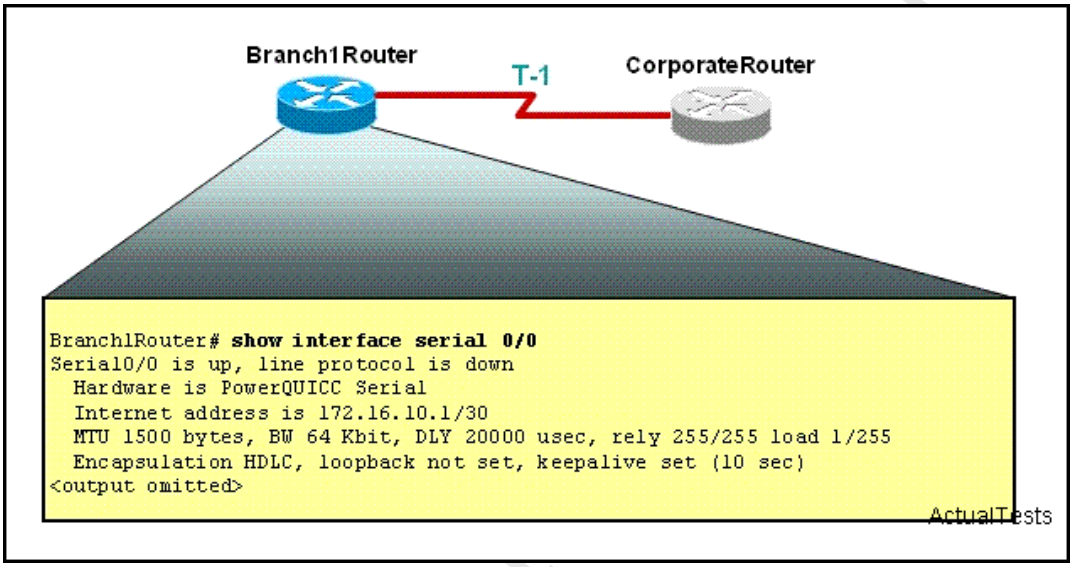
Since we are connecting to a non Cisco device, we must use PPP on the serial interface. PAP authentication is an optional parameter that can also used on this interface.
Incorrect Answers:

A: Although are indeed configurable on the serial interface, they are also configured on the LAN interface and we are being asked to choose the options that apply to the serial interface only.
B: Although are indeed configurable on the serial interface, they are also configured on the LAN interface and we are being asked to choose the options that apply to the serial interface only.

QUESTION NO: 432

Refer to the exhibit. The corporate office and branch location have been attached through two non-Cisco routers over a highly reliable WAN connection for over a year. A new Cisco router has been installed to replace the hardware at the branch location. Since the installation, IP communication cannot be verified across the link.

Given the output on Branch1Router, what would be a logical first step to take to resolve this problem?



A. Change the encapsulation on Branch1Router to match CorporateRouter.
B. Verify successful DCE communication between the two sites.
C. Ensure an exact match between the bandwidth setting on CorporateRouter and Branch1Router.
D. Verify Layer 1 communication on the Branch1Router Serial 0/0 interface.
E. Change the encapsulation on CorporateRouter to HDLC.
F. Change the bandwidth setting on Branch1Router to match the actual line speed.

Answer: A

Explanation:
Based on the information provided in the exhibit, we know that Serial0/0 is up, line protocol is down. There are three common states:
1. serial0/0 up, line protocol is up The interface is up and the line protocol is up.

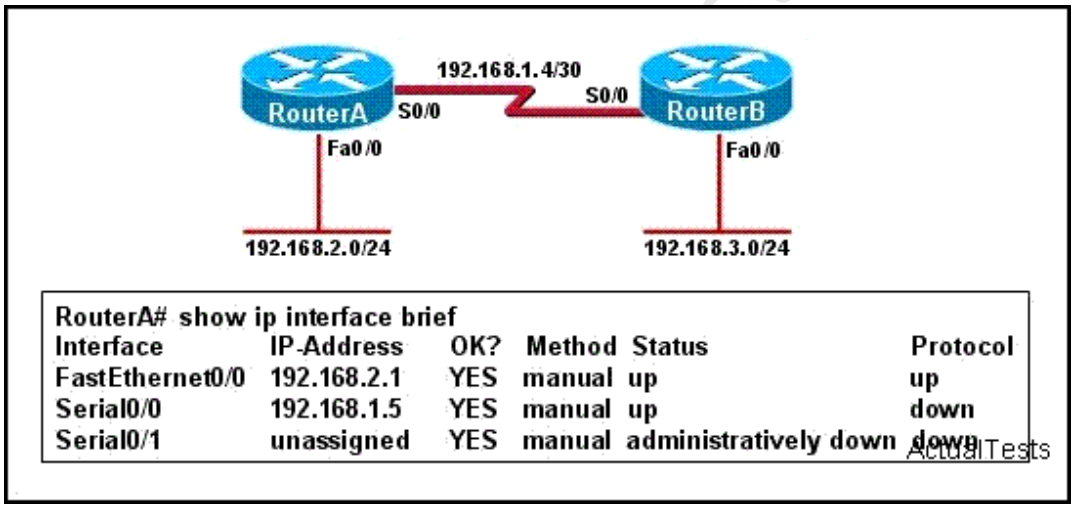
2. serial0/0 down, line protocol is down The interface is down , there is something wrong with the physical layer.

3. serial0/0 up, line protocol is down The interface is up, the encapsulation format is not matched.

The High Level Data Link Control protocol (HDLC) is the default encapsulation used on the synchronous serial interfaces of a Cisco router.
Because of the proprietary nature of vendor HDLC implementations, you should only use HDLC framing on point-to-point links when the router at each end of a link is from the same vendor. In cases where you want to connect equipment from different vendors over a leased line, the Point-to-Point Protocol (PPP) should be used. Always remember that the router on both sides of a point-to-point link must be using the same data framing method in order to communicate.
Reference: http://www.2000trainers.com/cisco-ccna-11/ccna-hdlc/

QUESTION NO: 433

Refer to the exhibit. 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. Interface S0/0 on RouterB is administratively down.
B. Interface S0/0 on RouterA is configured with an incorrect subnet mask.
C. Interface S0/0 on RouterA is not receiving a clock signal from the CSU/DSU.
D. The IP address that is configured on S0/0 of RouterB is not in the correct subnet.
E. The encapsulation that is configured on S0/0 of RouterB does not match the encapsulation that is configured on S0/0 of RouterA.
F. The cable that is connected to S0/0 on RouterA is faulty.

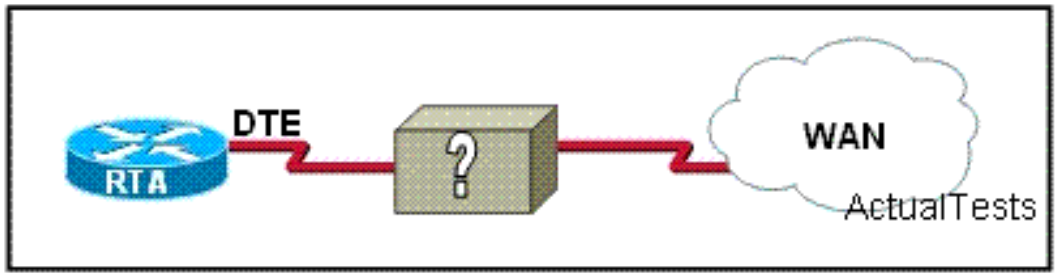
Answer: C,E

Explanation:

Based on the information provided in the exhibit, we know that Serial0/0 is up, line protocol is down, under normal circumstances there are three states:
1. serial0/0 up, line protocol is up The interface is up and the line protocol is up
2. serial0/0 down, line protocol is down The interface is down and there is something wrong with the physical layer.
3. serial0/0 up, line protocol is down The interface is up, but the encapsulation format is not matching ,clock rate issues

QUESTION NO: 434

Refer to the exhibit. The network administrator must complete the connection between the RTA of the XYZ Company and the service provider. To accomplish this task, which two devices could be installed at the customer site to provide a connection through the local loop to the central office of the provider? (Choose two.)



A. multiplexer
B. ATM switch
C. WAN switch
D. PVC
E. CSU/DSU
F. modem

Answer: E,F

Explanation:
only CSU/DSU and modem can achieve the connection of router to WAN.

DTE is an abbreviation for Data Terminal Equipment , and refers to an end instrument that converts user information into signals for transmission, or reconverts the received signals into user information. A DTE device communicates with the Data Circuit-terminating Equipment (DCE), such as a modem or CSU/DSU.
A DTE is the functional unit of a data station that serves as a data source or a data sink and provides for the data communication control function to be performed in accordance with link protocol.
The data terminal equipment (DTE) may be a single piece of equipment or an interconnected subsystem of multiple pieces of equipment that perform all the required functions necessary to

permit users to communicate. A user interacts with the DTE (e.g. through a Human-Machine Interface), or the DTE may be the user.
Usually, the DTE device is the terminal (or a computer emulating a terminal), and the DCE is a modem.
A CSU/DSU (Channel Service Unit/Data Service Unit) is a hardware device about the size of an external modem that converts a digital data frame from the communications technology used on a local area network (LAN) into a frame appropriate to a wide-area network (WAN) and vice versa. The DSU provides an interface to the data terminal equipment (DTE) using a standard (EIA/CCITT) interface. It also provides testing capabilities.

QUESTION NO: 435

While logged into a router you manually shut down the serial 0 interface using the "shutdown" interface configuration command. You then issue the "show interface serial 0" command in exec mode. What could you expect the status of the serial 0 interface to be?

A. Serial 0 is down, line protocol is down
B. Serial 0 is administratively down, line protocol is down
C. Serial 0 is down, line protocol is up
D. Serial 0 is up, line protocol is up

Answer: B

Explanation:
when administrator shut down interface manually, the interface information prompts in show interface status is administratively shut down, i.e. administratively down.

To bring down an interface for administrative reasons and, as a side effect, remove the connected router from the routing table, you can use the shutdown interface subcommand. To enable the interface back up, issue the "no shutdown" configuration command.
Incorrect Answers:
A: This is the status of a fully operational interface.
C: These two interface conditions should never be seen.
D: These are the results of line problems or configuration errors.

QUESTION NO: 436

Refer to the exhibit. What is the reason that the interface status is "administratively down, line protocol down"?

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

A. The interface has been configured with the shutdown command.
B. The wrong type of cable is connected to the interface.
C. The interface is not receiving any keepalives.
D. There is no encapsulation type configured.
E. There is a mismatch in encapsulation types.
F. The interface needs to be configured as a DTE device.

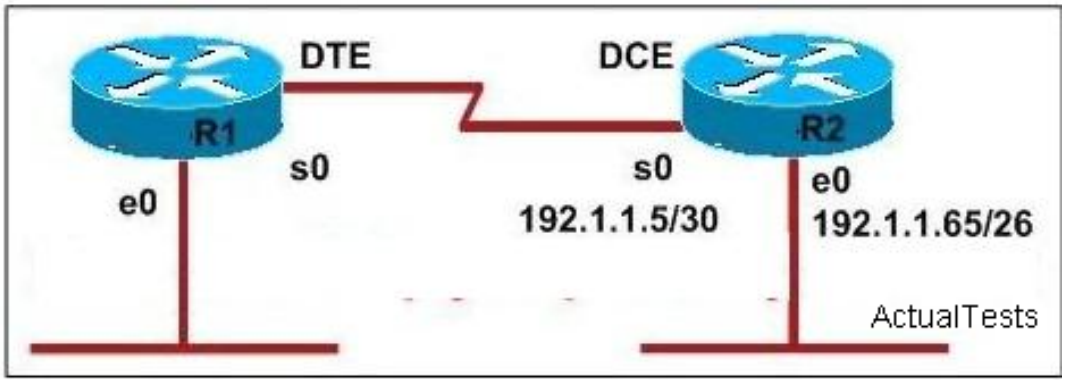
Answer: A

Explanation:
To be an effective troubleshooter, you have to know how things look when all is well, not just when something is broken! When an interface is functioning correctly, this is what we see at the top of the show interface output. I'll use Serial0 for all examples in this section.
Example1: Normal operational status:
Router1#show int serial0 Serial0 is up, line protocol is up

Example2: Interface is administratively down:
TK1#show int serial0 Serial0 is administratively down, line protocol is down
Administratively down means the interface is indeed shut down using the "shutdown" interface command. Open the interface with no shutdown.
TK1(config)#int serial0 Router1(config-if)#no shutdown
Always wait a minute or so to come up after enabling a serial interface.
TK1#show interface serial0 Serial0 is up, line protocol is up

QUESTION NO: 437

Refer to the following graphic, the enterprise network address is 192.1.1.0/24 and the routing protocol being used is RIP. Which set of commands can be used on R1 to build LAN-to-LAN communication between R1 and R2? (Choose three.)



A. R1(config)# interface ethernet 0
R1(config-if)# ip address 192.1.1.129 255.255.255.192
R1(config-if)# no shutdown
B. R1(config)# interface ethernet 0
R1(config-if)# ip address 192.1.1.97 255.255.255.192
R1(config-if)# no shutdown
C. R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.1.1.0
D. R1(config)# interface serial 0
R1(config-if)# ip address 192.1.1.6 255.255.255.252
R1(config-if)# no shutdown

Answer: A,C,D

Explanation:
Section 3: Configure and verify Frame Relay on Cisco routers (18 question)

QUESTION NO: 438

Refer to the exhibit. What is the meaning of the term dynamic as displayed in the output of the show frame-relay map command shown?

```
R1# show frame-relay map
Serial0/0 (up): ip 172.16.3.1 dlci 100 (0x64, 0x1840), dynamic
        broadcast,, status defined, active
```


A. The mapping between DLCI 100 and the end station IP address 172.16.3.1 was learned through Inverse ARP.
B. The Serial0/0 interface is passing traffic.
C. The DLCI 100 will be dynamically changed as required to adapt to changes in the Frame Relay cloud.
D. The DLCI 100 was dynamically allocated by the router.
E. The Serial0/0 interface acquired the IP address of 172.16.3.1 from a DHCP server.

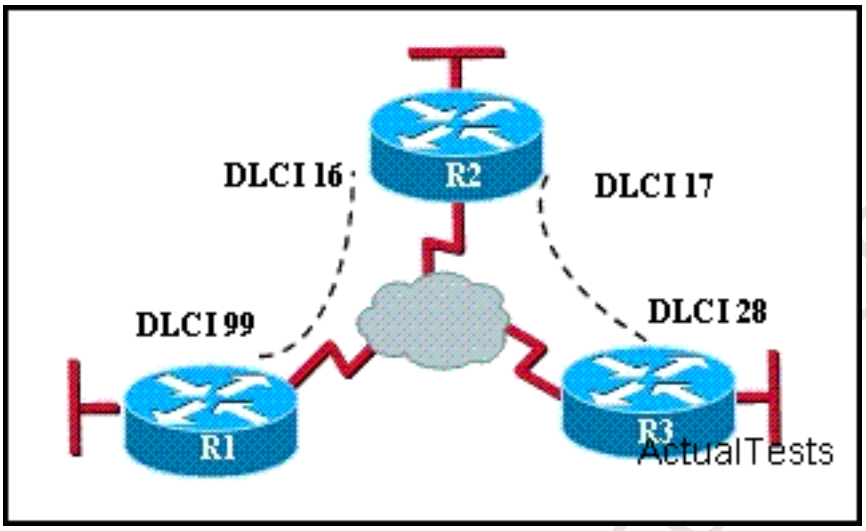
Answer: A

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: 439

Refer to the exhibit. Which statement describes DLCI 17?



A. DLCI 17 is the Layer 2 address used by R2 to describe a PVC to R3.
B. DLCI 17 describes a PVC on R2. It cannot be used on R3 or R1.
C. DLCI 17 describes the dial-up circuit from R2 and R3 to the service provider.
D. DLCI 17 describes the ISDN circuit between R2 and R3.

Answer: A

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: 440

An administrator is configuring a router that will act as the hub in a Frame Relay hub-and-spoke topology. What is the advantage of using point-to-point subinterfaces instead of a multipoint interface on this router?

A. It avoids split-horizon issues with distance vector routing protocols.

B. Only a single physical interface is needed with point-to-point subinterfaces, whereas a multipoint interface logically combines multiple physical interfaces.
C. Only one IP network address needs to be used to communicate with all the spoke devices.
D. Point-to-point subinterfaces offer greater security compared to a multipoint interface configuration.
E. IP addresses can be conserved if VLSM is not being used for subnetting.

Answer: E

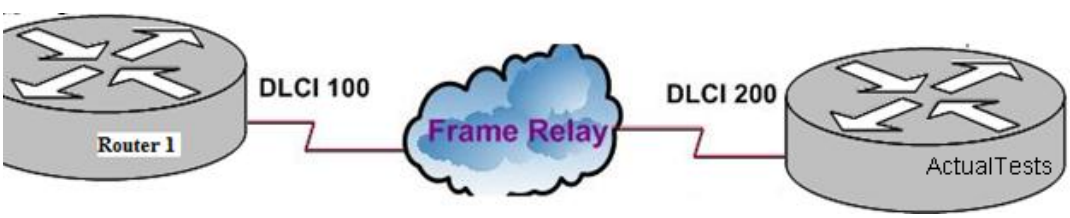
Explanation:
Frame Relay supports two types of interfaces: point-to-point and multipoint. The one you choose determines whether you need to use the configuration commands that ensure IP address to data-link connection identifier (DLCI) mappings. After configuring the PVC itself, you must tell the router which PVC to use in order to reach a specific destination. Let's look at these options: Point-to-point subinterface - With point-to-point subinterfaces, each pair of routers has its own subnet. If you put the PVC on a point-to-point subinterface, the router assumes that there is only one point-to-point PVC configured on the subinterface. Therefore, any IP packets with a destination IP address in the same subnet are forwarded on this VC. This is the simplest way to configure the mapping and is therefore the recommended method. Use the frame-relay interface-dlci command to assign a DLCI to a specified Frame Relay subinterface. Multipoint networks - Multipoint networks have three or more routers in the same subnet. If you put the PVC in a point-to-multipoint subinterface or in the main interface (which is multipoint by default), you need to either configure a static mapping or enable inverse Address Resolution Protocol (ARP) for dynamic mapping.

QUESTION NO: 441

Exhibit:
Rpiter# show running-config

<some output text omitted>

interface serial0/0
bandwidth 64
ip address 172.16.100.2 255.255.0.0
encapsulation frame-relay
frame-relay map ip 172.16.100.1 100 broadcast



As a technician, you found the router1 is unable to reach the second router. Both routers are running IOS version 12.0. Based on this information, what is the most likely cause of the problem?

A. incorrect IP address
B. incorrect bandwidth configuration
C. incorrect map statement
D. incorrect LMI configuration

Answer: C

Explanation:
The local DLCI from Router1 to Frame-relay cloud is 100, the local DLCI from the second router to FR cloud is 200. FR mapping from router1 to the second router is as follows:
frame-relay map ip 172.16.100.1 100 broadcast

DLCI's are locally significant. The local DLCI needs to be specified in the "frame-relay map" configuration statement to reach the neighboring frame-relay router. In this case DLCI 100 is used to reach 172.16.100.1, so the correct configuration statement should be "frame-relay map ip 172.16.100.1 100 broadcast."

QUESTION NO: 442

Which of the following Frame-Relay encapsulation commands would you use, if you had to connect your Cisco router to a non-Cisco router?

A. Router(config-if)# Encapsulation frame-relay aal5snap
B. Router(config-if)# Encapsulation frame-relay isl
C. Router(config-if)# Encapsulation frame-relay ietf
D. Router(config-if)# Encapsulation frame-relay dot1q

Answer: C

Explanation:
In general, the IETF Frame Relay encapsulation should be used when connecting a Cisco router to non-Cisco equipment across a Frame Relay network. The IETF Frame Relay encapsulation allows interoperability between equipment from multiple vendors. Both Cisco and IETF encapsulations for Frame Relay can be configured on a per-virtual-circuit (VC) basis. This gives greater flexibility when configuring Frame Relay in a multi-vendor environment. A user can specify the Frame Relay encapsulation types to be used on different virtual circuits configured under the same physical interface.
Incorrect Answers:

A: AAL 5 SNAP is an ATM encapsulation and is not related to frame relay.
B: 802.1Q and ISL are trunking encapsulation types and have nothing to do with frame relay.
D: 802.1Q and ISL are trunking encapsulation types and have nothing to do with frame relay.

QUESTION NO: 443

A network administrator is configuring a router that will act as the hub in a Frame Relay hub-and-spoke topology. What is the advantage of using point-to-point subinterfaces instead of a multipoint interface on this router?

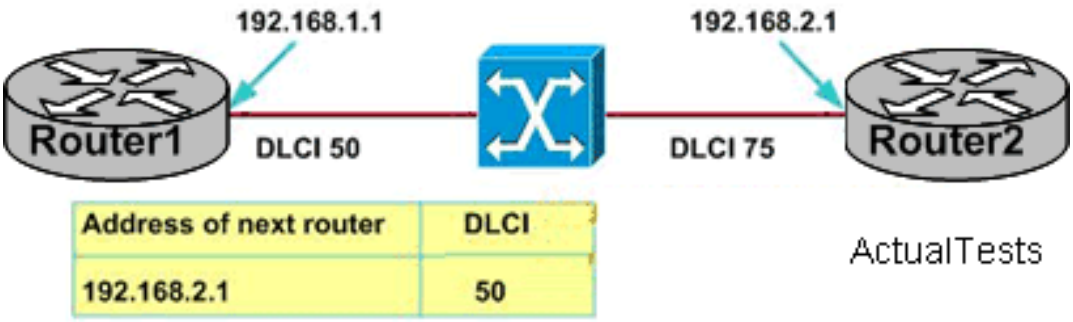
A. Point-to-point subinterfaces offer greater security compared to a multipoint interface configuration.
B. Only one IP network address needs to be used to communicate with all the spoke devices.
C. It avoids split-horizon issues with distance vector routing protocols.
D. Only a single physical interface is needed with point-to-point subinterfaces, whereas a multipoint interface logically combines multiple physical interfaces.

Answer: C

Explanation:
Using split horizon in frame relay network will result in the situation that route fails to reach the destination router. There are usually two ways to solve split horizon of frame relay networks:
1. Close split horizon manually on "Hub" router; the premise to use this method is that the network will not cause loop;
2. Divide some sub-division in the logic interface on "Hub" router, so that each interface belongs to different network.

QUESTION NO: 444

What Frame Relay mechanism is used to build the map illustrated in the accompanying graphic?



A. inverse multiplexing
B. LMI mapping
C. ARP

D. Inverse ARP

Answer: D

Explanation:
The locally significant DLCI must be mapped to the destination router's IP address. There are two options for this, Inverse ARP and static mapping.
In both of the following examples, the single physical Serial interface on Router 1 is configured with two logical connections through the frame relay cloud, one to Router 2 and one to Router 3. Inverse ARP runs by default once Frame Relay is enabled, and starts working as soon as you open the interface. By running show frame-relay map after enabling Frame Relay, two dynamic mappings are shown on this router. If a dynamic mapping is shown, Inverse ARP performed it.
R1#show frame map
Serial0 (up): ip 200.1.1.2 dlci 122(0x7A,0x1CA0), dynamic,
broadcast,, status defined, active
Serial0 (up): ip 200.1.1.3 dlci 123(0x7B,0x1CB0), dynamic,
broadcast,, status defined, active
Static mappings require the use of a frame map statement. To use static mappings, turn Inverse ARP off with the no frame-relay inverse-arp statement, and configure a frame map statement for each remote destination that maps the local DLCI to the remote IP address. Frame Relay requires the broadcast keyword to send broadcasts to the remote device.
R1#conf t
R1(config)#interface serial0
R1(config-if)#no frame-relay inverse-arp
R1(config-if)#frame map ip 200.1.1.2 122 broadcast
R1(config-if)#frame map ip 200.1.1.3 123 broadcast

QUESTION NO: 445

How should a router that is being used in a Frame Relay network be configured to avoid split horizon issues from preventing routing updates?

A. Configure a separate sub-interface for each PVC with a unique DLCI and subnet assigned to the sub-interface.
B. Configure each Frame Relay circuit as a point-to-point line to support multicast and broadcast traffic.
C. Configure a single sub-interface to establish multiple PVC connections to multiple remote router interfaces.
D. Configure many sub-interfaces on the same subnet.

Answer: A

Explanation:

Point-To-Point Subinterfaces:

The concept of subinterfaces was originally created in order to better handle issues caused by split-horizon over Non-Broadcast Multiple Access (NBMA) networks (e.g. frame relay, X.25) and distance-vector based routing protocols (e.g. IPX RIP/SAP, AppleTalk). Split-horizon dictates that a routing update received on an interface cannot be retransmitted out onto the same interface. This rule holds even if the routing update was received on one frame relay PVC and destined to retransmit out onto another frame relay PVC. Referring to figure 2, this would mean that sites B and C can exchange routing information with site A, but would not be able to exchange routing information with each other. Split-horizon does not allow Site A to send routing updates received from Site B on to Site C and vice versa.

Note: For TCP/IP, Cisco routers can disable split-horizon limitations on all frame relay interfaces and multipoint subinterfaces and do this by default. However, split-horizon cannot be disabled for other protocols like IPX and AppleTalk. These other protocols must use subinterfaces if dynamic routing is desired.

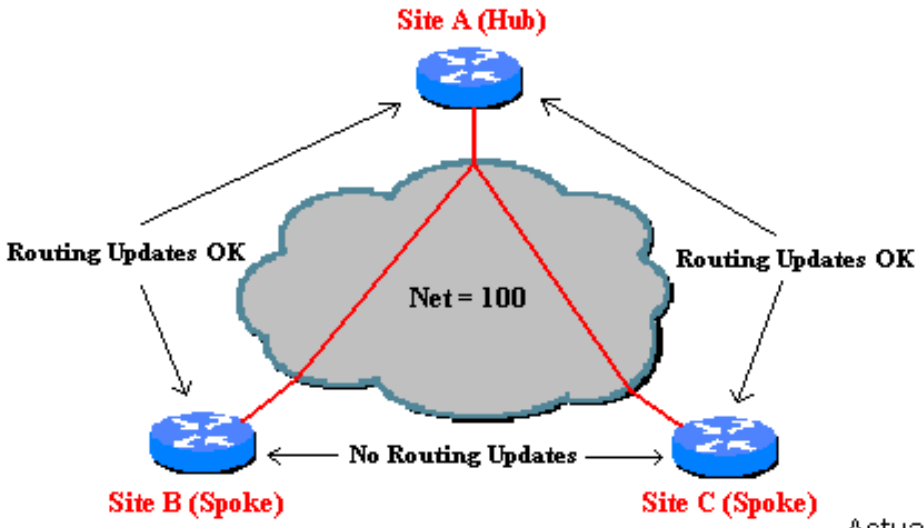


Figure 2: Split-horizon does not allow remote sites to send routing updates to each other.

By dividing the partially-meshed frame relay network into a number of virtual, point-to-point networks using subinterfaces, the split-horizon problem can be overcome. Each new point-to-point subnetwork is assigned its own network number. To the routed protocol, each subnetwork now appears to be located on separate interfaces (Figure 3). Routing updates received from Site B on one logical point-to-point subinterface can be forwarded to site C on a separate logical interface without violating split horizon.

QUESTION NO: 446

A Cisco router that was providing Frame Relay connectivity at a remote site was replaced with a different vendor's frame relay router. Connectivity is now down between the central and remote site. What is the most likely cause of the problem?

A. mismatched LMI types
B. incorrect DLCI
C. mismatched encapsulation types
D. incorrect IP address mapping

Answer: C

Explanation:
The frame relay connectivity problem is usually caused by mismatched encapsulation types.

QUESTION NO: 447

Which function does the Frame Relay DLCI provide with respect to router RouterA?

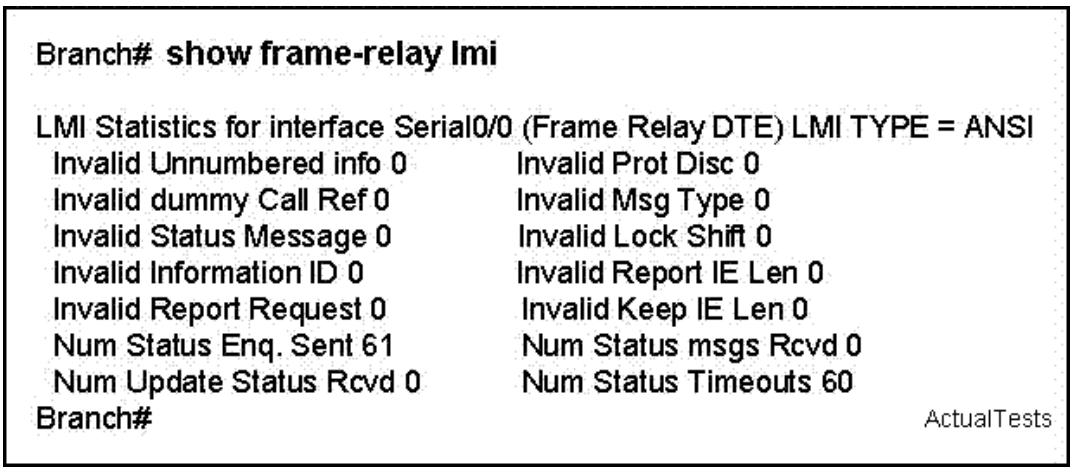
A. defines the signaling standard between router RouterA and the frame switch
B. identifies the circuit between router RouterB and the frame switch
C. identifies the encapsulation used between router RouterA and router RouterB
D. identifies the circuit between router RouterA and the frame switch

Answer: D

Explanation:
RouterA sends frames with DLCI, and they reach the local switch. The local switch sees the DLCI field and forwards the frame through the Frame Relay network until it reaches the switch connected to RouterB. The RouterB's local switch forwards the frame out of the access link to RouterB. DLCI information is considered to be locally significant, meaning that the DLCI is used between the end router and the carrier's local frame relay switch.
Reference: CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 386
Incorrect Answers:
A: DLCI is used only as a circuit identifier (DLCI=Data Link Circuit Identifier), and not used for signaling.
C: The encapsulation options are not defined with DLCIs.

QUESTION NO: 448

Refer to the exhibit. Which two statements are true based the output of the show frame-relay lmi command issued on the Branch router? (Choose two.)



A. LMI messages are being sent on DLCI 1023.
B. The LMI exchange between the router and Frame Relay switch is functioning properly.
C. LMI messages are being sent on DLCI 0.
D. The Frame Relay switch is not responding to LMI requests from the router.
E. The router is providing a clock signal on Serial0/0 on the circuit to the Frame Relay switch.
F. Interface Serial0/0 is not configured to encapsulate Frame Relay.

Answer: C,D

Explanation:
Local Management Interface (LMI) messages manage the local access link between the router and the Frame Relay switch. A Frame Relay DTE can send an LMI Status Enquiry message to the switch; the switch then replies with an LMI Status message to inform the router about the DLCIs of the defined VCs, as well as the status of each VC. By default, the LMI messages flow every 10 seconds. Every sixth message carries a full Status message, which includes more complete status information about each VC. As we can see, the router has sent 61 messages, but received back none. We also know that DLCI 0 is used as this is the LMI DLCI used in ANSI. If the LMI type had been Cisco, the DLCI used is 1023.
Reference:
http://www.cisco.com/en/US/tech/tk713/tk237/technologies_tech_note09186a0080094183.shtml

QUESTION NO: 449

In a Frame Relay environment, what is the function of the DE bit?

A. the activation of the LMI protocol
B. the identification of frames that are transmitted above the CIR
C. the identification of what routing updates to block
D. the identification of the virtual circuit

Answer: B

QUESTION NO: 450

When a router is connected to a Frame Relay WAN link using a serial DTE interface, how is the interface clock rate determined?

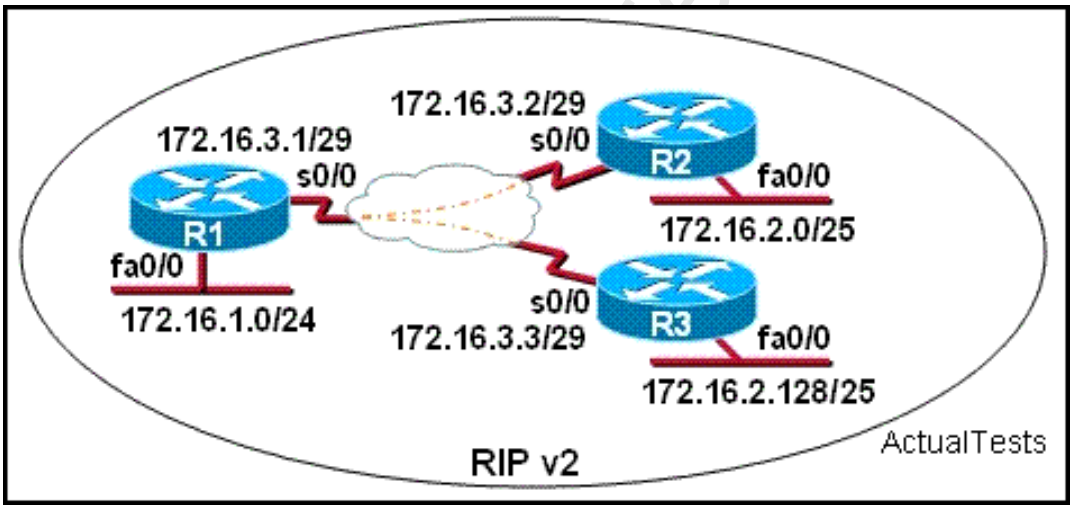
A. It is supplied by the far end router.
B. It is determined by the clock rate command.
C. It is supplied by the CSU/DSU.
D. It is supplied by the Layer 1 bit stream timing.

Answer: C

Explanation:
A frame relay WAN needs a clock rate, which can be supplied by the CSU/DSU.

QUESTION NO: 451

Refer to the exhibit. S0/0 on R1 is configured as a multipoint interface to communicate with R2 and R3 in this hub-and-spoke Frame Relay topology. While testing this configuration, a technician notes that pings are successful from hosts on the 172.16.1.0/24 network to hosts on both the 172.16.2.0/25 and 172.16.2.128/25 networks. However, pings between hosts on the 172.16.2.0/25 and 172.16.2.128/25 networks are not successful. What could explain this connectivity problem?



A. The RIP v2 dynamic routing protocol cannot be used across a Frame Relay network.
B. The ip subnet-zero command has been issued on the R1 router.
C. Split horizon is preventing R2 from learning about the R3 networks and R3 from learning about the R2 networks.
D. The 172.16.3.0/29 network used on the Frame Relay links is creating a discontiguous network between the R2 and R3 router subnetworks.
E. The 172.16.2.0/25 and 172.16.2.128/25 networks are overlapping networks that can be seen by R1, but not between R2 and R3.

Answer: C

Explanation:
Under normal circumstances, the router that is connected to the broadcast IP network and uses the distance vector routing protocol will use split horizon mechanism to avoid routing loop.
Split horizon is a technology to avoid routing loop and speed up the routing convergence. The router may receive the routing information sent by itself which is useless, split horizon will not advertise the routing update information back received from the terminal , while it will advertise those routes that will not be cleared because of the endless counting .It can be simply interpreted that the route learnt by a router from one interface will not be sent through the same interface .
For the non-broadcast network (such as Frame Relay and High Speed Switched Data Services), the effect of split horizon is not ideal. So, we can use the following commands to disable or enable split horizon.
ip split-horizon to enable split horizon
no ip split-horizon to disable split horizon

The problem in this situation is related to split horizon , which reduces incorrect routing information and routing overhead in a distance-vector network by enforcing the rule that information cannot be sent back in the direction from which it was received. In other words, the routing protocol differentiates which interface a network route was learned on, and once it determines this, it won't advertise the route back out of that same interface.
in a spoke and hub Frame Relay topology, the Frame Relay interface for the hub router must have split-horizon processing disabled. Otherwise, the spoke routers never receive each other's routes.

QUESTION NO: 452

A default Frame Relay WAN is classified as what type of physical network?

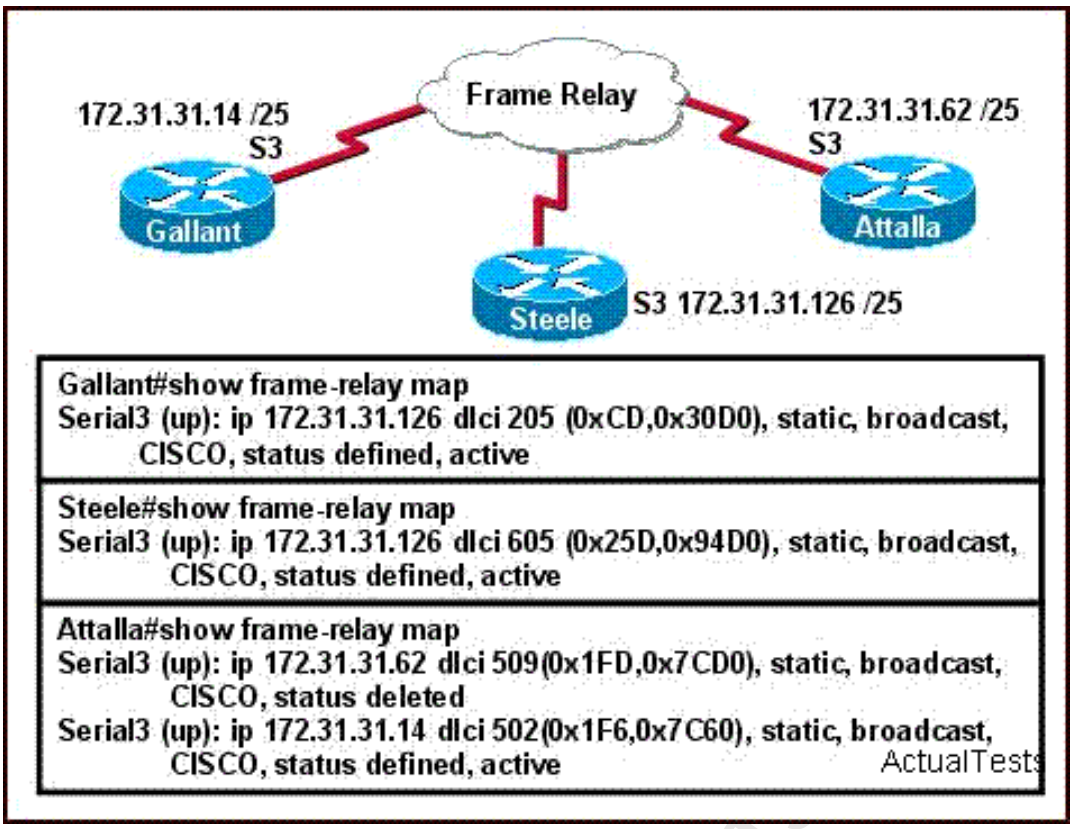
A. broadcast multi-access
B. broadcast point-to-multipoint
C. nonbroadcast multi-access
D. nonbroadcast multipoint
E. point-to-point

Answer: C

Explanation:
A default Frame Relay WAN is classified as Nonbroadcast multi-access (NBMA).

QUESTION NO: 453

The Frame Relay network in the diagram is not functioning properly. What is the cause of the problem?



A. The Gallant router has the wrong LMI type configured.
B. The IP address on the serial interface of the Attalla router is configured incorrectly.
C. The frame-relay map statement in the Attalla router for the PVC to Steele is not correct.
D. The S3 interface of the Steele router has been configured with the frame-relay encapsulation ietf command.
E. Inverse ARP is providing the wrong PVC information to the Gallant router.

Answer: C

Explanation:
On serial 3 of Attalla we can see that there are 2 PVC's defined, but only one of them is working and is shown as active. The frame relay map that was used to specify DLCI 509 was incorrect. Incorrect DLCI assignments that are configured in routers normally show up as "deleted" in the frame relay maps.

QUESTION NO: 454

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. 102 is the remote DLCI that will receive the information.

B. The broadcast option allows packets, such as RIP updates, to be forwarded across the PVC.
C. The IP address 10.121.16.8 is the local router port used to forward data.
D. This command should be executed from the global configuration mode.
E. This command is required for all Frame Relay configurations.

Answer: B

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: 455

What are two characteristics of Frame Relay point-to-point subinterfaces? (Choose two.)

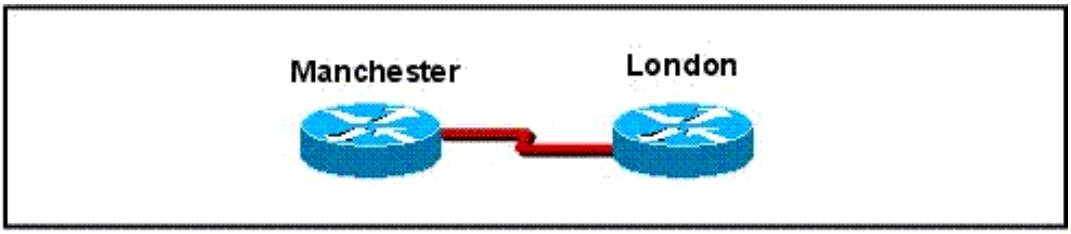
A. They create split-horizon issues.
B. They require a unique subnet within a routing domain.
C. They emulate leased lines.
D. They are ideal for full-mesh topologies.
E. They require the use of NBMA options when using OSPF.

Answer: B,C

Explanation:
Section 4: Troubleshoot WAN implementation issues (1 question)

QUESTION NO: 456

Refer to the exhibit. 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.)




```
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>                                    ActualTests
```

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

Answer: B,C,D

Explanation:
1. Use the show cdp entry * command on Device Manchester to find that the IP address of Device London is 10.1.1.2. Therefore, the IP address of the interface of Device Manchester is 10.1.1.1.

2. The results shown by running the show cdp entry command show that the platform of Device London is cisco 2610.
3. Interface: serial0/0 indicates that Device Manchester is connected with Device London through S0/0.
Section 5: Describe VPN technology (including: importance, benefits, role, impact, components) (0 question)
Section 6: Configure and verify a PPP connection between Cisco routers (5 question)

QUESTION NO: 457

Which PPP authentication methods will you use when configuring PPP on an interface of a Cisco router? (Choose two)

A. PAP
B. SSL

C. CHAP
D. SLIP

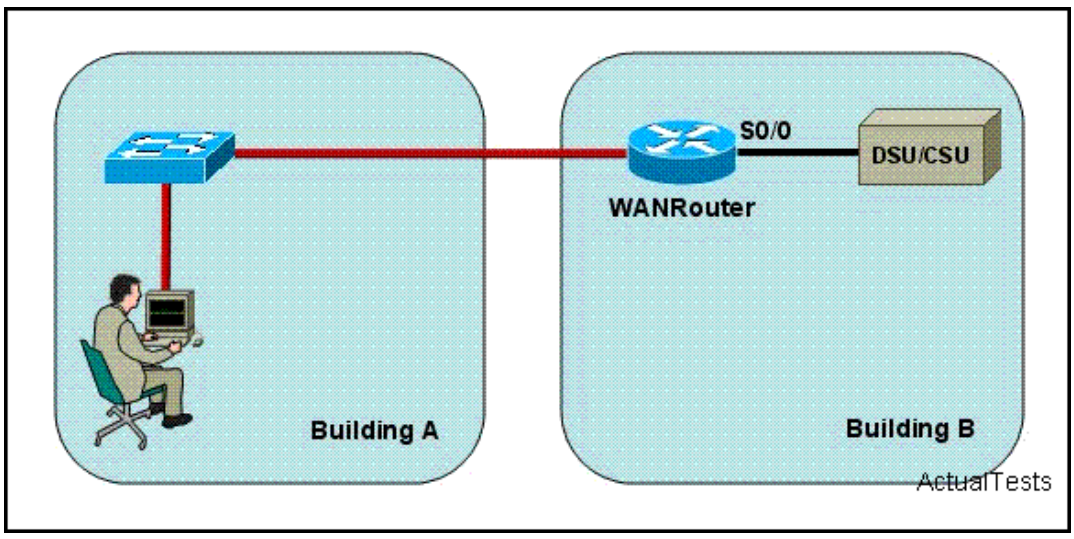
Answer: A,C

Explanation:
Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authenticate the endpoints on either end of a point-to-point serial link. Chap is the preferred method today because the identifying codes flowing over the link are created using a MD5 one-way hash, which is more secure that the clear-text passwords sent by PAP.
Reference:
CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 314

PPP has two ways to authenticate : one is PAP, the other is CHAP. PAP is less secure than CHAP. PAP transmits the password in the form of plaintext, while the transmission process of CHAP does not contain password, using hash to replace password. The PAP authentication can be achieved by two-way handshake ,while the CHAP authentication can be achieved by three-way handshake. The PAP authentication is that the dialed sends the request and the dial reply, while the CHAP authentication is that the dial send request and the dialed sends back a data packet which contains the random hash value sent by the dial, after confirming the database has no error, the dial will send a successfully connected packet to connect.

QUESTION NO: 458

Refer to the exhibit. The network administrator is in a campus building distant from Building B. WANRouter is hosting a newly installed WAN link on interface S0/0. The new link is not functioning and the administrator needs to determine if the correct cable has been attached to the S0/0 interface. How can the administrator accurately verify the correct cable type on S0/0 in the most efficient manner?



A. Telnet to WANRouter and execute the command show running-configuration
B. Telnet to WANRouter and execute the command show interfaces S0/0
C. Physically examine the cable between WANRouter S0/0 and the DCE.
D. Telnet to WANRouter and execute the command show processes S0/0
E. Telnet to WANRouter and execute the command show controller S0/0
F. Establish a console session on WANRouter and execute the command show interfaces S0/0

Answer: E

Explanation:
When the administrator is far away from the malfunction equipment, telnet may be used to log in the remote equipment to check. When the specific failure port is identified, execute show interface following with the specific port number.

QUESTION NO: 459

You are about to configure PPP on the interface of a Cisco router. Which authentication methods could you use? (Choose two)

A. CHAP
B. VNP
C. LAPB
D. PAP

Answer: A,D

Explanation:
PPP supports both Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authenticate the endpoints on either end of a point-to-point serial link. Chap is the preferred method today because the identifying codes flowing over the link are created using a MD5 one-way hash, which is more secure that the clear-text passwords sent by PAP.
Reference:
CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 314

QUESTION NO: 460

As a CCNA candidate, you need to know PPP very well. Which of the statements are true regarding key characteristics of PPP? (Choose three.)

A. encapsulates several routed protocols
B. can be used over analog circuits
C. provides error correction
D. supports IP only
E. maps Layer 2 to Layer 3 address

Answer: A,B,C

Explanation:
The Point-to-Point Protocol (PPP) originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network layer address negotiation and data-compression negotiation. PPP supports these functions by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities. In addition to IP, PPP supports other protocols, including Novell's Internetwork Packet Exchange (IPX) and DECnet.
http://www.cisco.com/en/US/docs/internetworking/technology/handbook/PPP.html

QUESTION NO: 461

An ISDN link can be encapsulated using either PPP or HDLC. What are the advantages of using PPP? (Choose two)

A. PPP can be routed across public facilities, while HDLC is not routable in circuit-switched networks.
B. PPP is consistently implemented among different equipment vendors.
C. PPP will run faster and more efficiently than HDLC on circuit-switched ISDN links.
D. PPP authentication will prevent unauthorized callers from establishing an ISDN circuit.

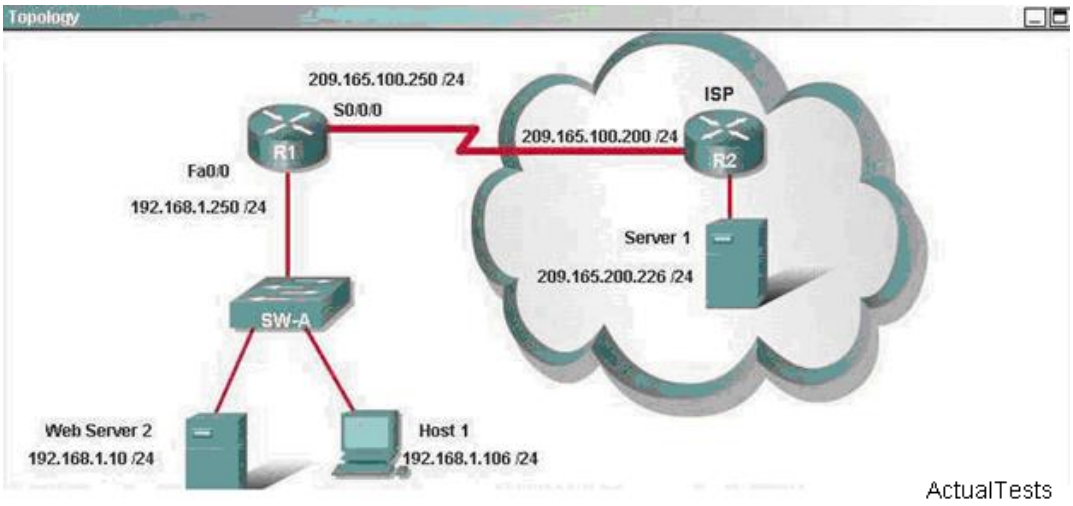
Answer: B,D

Explanation:
PPP is now the most popular data link encapsulation protocol. It provides improved compatibility, network providers are enabled to cooperate together; while HDLC is Cisco private, which has limitations. Meanwhile, PPP supports also Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). It bears better security.

PPP has numerous advantages over HDLC. Unlike HDLC which is Cisco proprietary, PPP was designed for multi-protocol interoperability. Secondly, PPP supports authentication, using either PAP or CHAP. Finally, PPP supports error correction and the use of bonded multilink circuits.

QUESTION NO: 462

If the router R1 has a packet with a destination address 192.168.1.255, what describes the operation of the network?



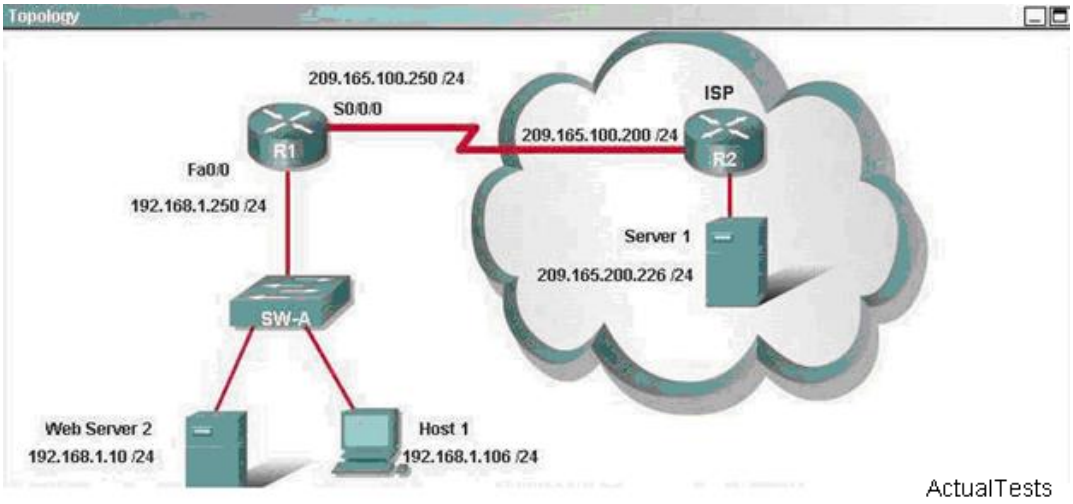
A. R1 will encapsulate the packet in a frame with a destination MAC address of FF-FF-FF-FF-FF-FF
B. R1 will forward the packet out all interface.
C. R1 will drop this packet because this it is not a valid IP address.
D. As R1 forwards the frame containing this packet, SW-A will add 192.168.1.255 to its MAC table.

Answer: C

Explanation:
The IP address 192.168.1.255 of data packet is a broadcast address, the router will not forward broadcast address, instead it will drop this packet.
Network address: 192.168.1.0 subnet mask: 255.255.255.0
Valid address scope of hosts: 192.168.1.1 C 192.168.1.254
Broadcast address: 192.168.1.255

QUESTION NO: 463

The router address 192.168.1.250 is the default gateway for both the Web Server 2 and Host 1. What is the correct subnet mask for this network?



A. 255.255.255.250
B. 255.255.255.128
C. 255.255.255.252
D. 255.255.255.0

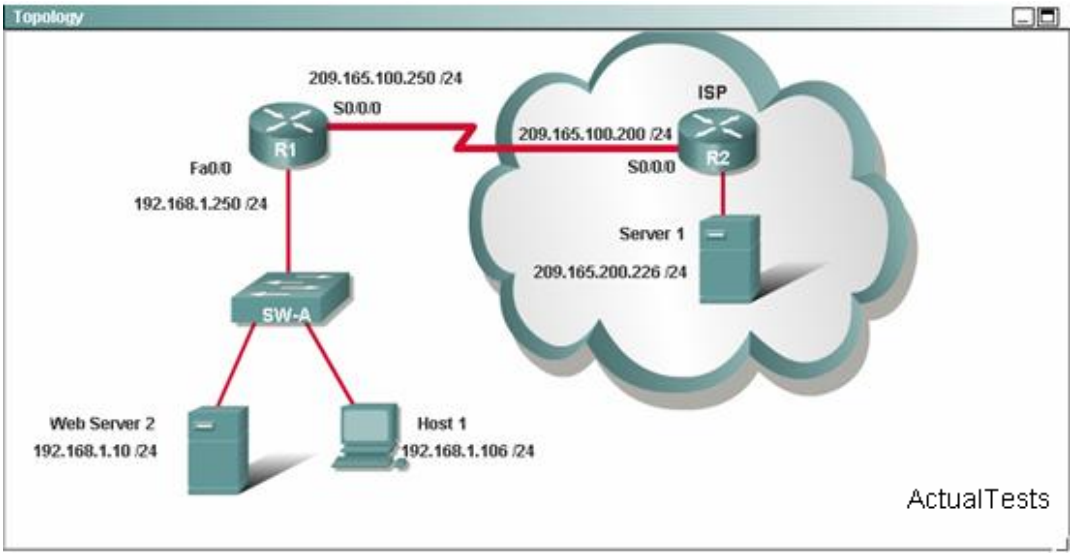
Answer: D

Explanation:
1. Based on the information provided in the exhibit, we know that the IP address of the interface Fa0/0 is 192.168.1.250/24, that is to say the subnet mask is 255.255.255.0??
2. When configuring the correct IP address and not wasting IP address, the network of 192.168.1.0 needs to contain the following three IP addresses of interfaces:
R1(fa 0/0) : 192.168.1.250
Host1: 192.168.1.106/24
Web server 2: 192.168.1.10/24
The correct mask is 255.255.255.0.

QUESTION NO: 464

Host 1 has just started up and requests a web page from web server 2. Which two statements describe steps in the process Host 1 uses to send the request to web server 2 (choose two)?

Exhibit:

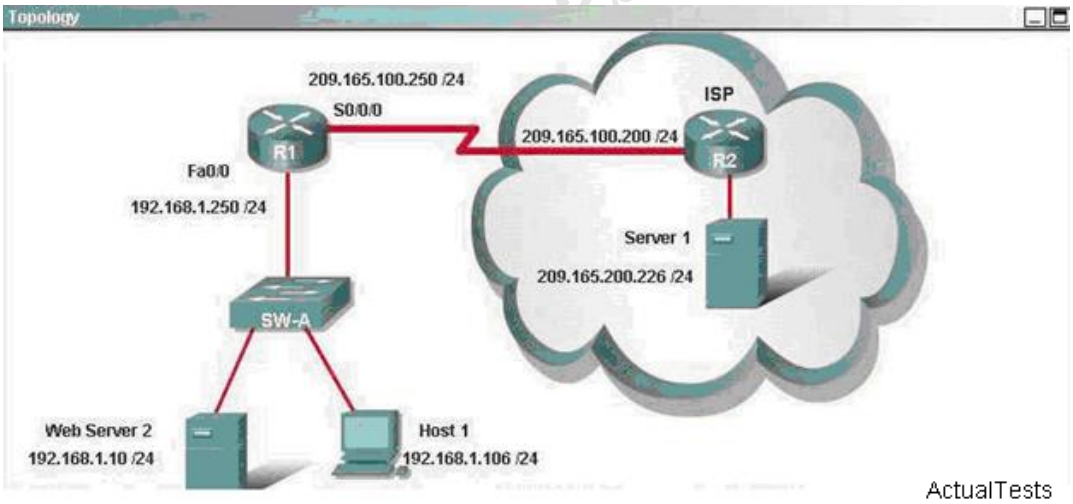


A. Host 1 looks in its ARP cache for the MAC address of router R1
B. Host 1 addresses the frames to the MAC address of router R1
C. Host 1 sends a broadcast ARP request to obtain the MAC address of webserver2.
D. Host 1 sends the packets to router R1 to be forwarded to web server 2
E. Host 1 addresses the frames to the MAC address of web server 2

Answer: C,E

QUESTION NO: 465

Users on the 192.168.1.0/24 network must access files located on the Server1.What route could be configured on router R1 for file requests to reach the server?



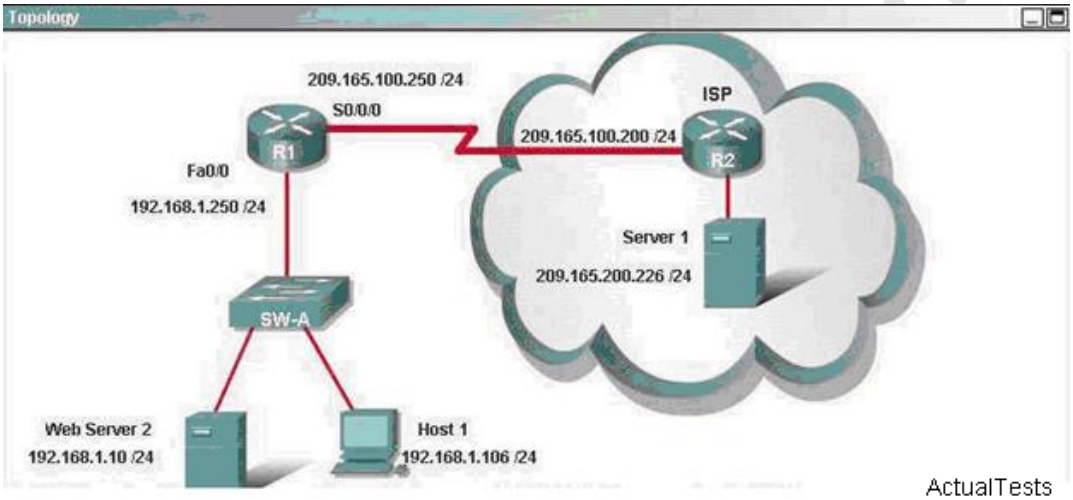
A. ip route 0.0.0.0 0.0.0.0 209.165.200.226
B. ip route 0.0.0.0 0.0.0.0 s0/0/0
C. ip route 192.168.1.0 255.255.255.0 209.165.100.250
D. ip route 209.165.200.0 255.255.255.0 192.168.1.250

Answer: B

Explanation:
In order to allow the network of 192.168.1.0/24 to access Serverl1, we need to establish a default route. The format of this default route is as follows:
ip route prefix mask {ip-address interface-type interface-number [ip-address]} [distance] [name] [permanent track number] [tag tag]
Based on the request of this subject, we need to configure the correct route as follows:
ip route 0.0.0.0 0.0.0.0 s0/0/0

QUESTION NO: 466

What must be configured on the network in order for users on the Internet to view web pages located on Web Server 2?



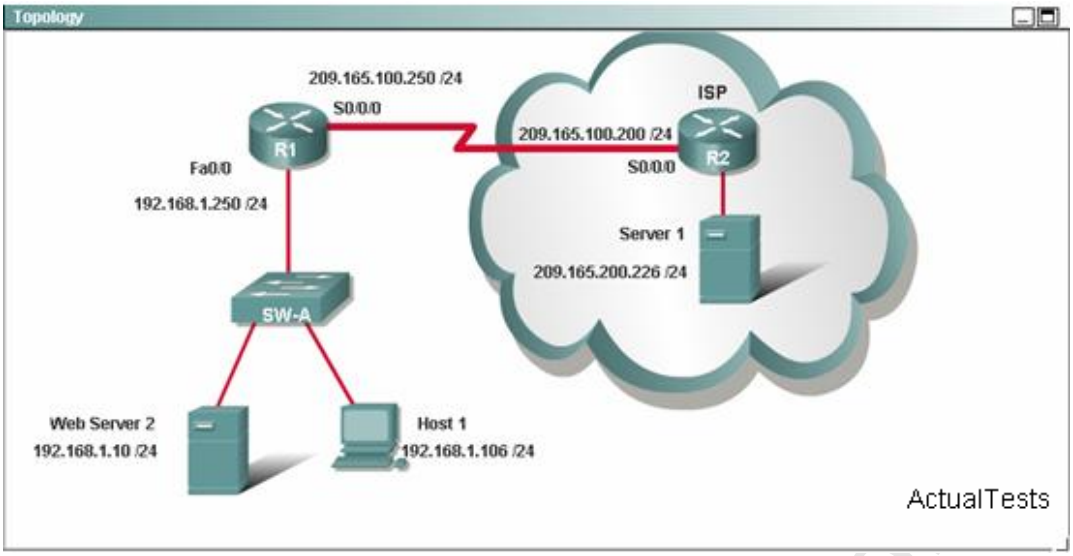
A. On router R1, configure a default static route to the 192.168.1.0 network.
B. On router R1, configure NAT to translate an address on the 209.165.100.0/24 network to 192.168.1.10
C. On router R1 ,configure DNS to resolve the URL assigned to Web Server 2 to the 192.168.1.10 address
D. On router R2, configure DHCP to assign a registered IP address on the 209.165.100.0/24 network to Web Server 2.

Answer: B

Explanation:
In order to allow internet users to access Web Server 2, we need to configure NAT address translation on router R1.

QUESTION NO: 467

R1 forwards a packet from Host 1 to remote Server 1. Which statement describes the use of a MAC as the frame carrying this packet leaves the s0/0/0 interface of R1?



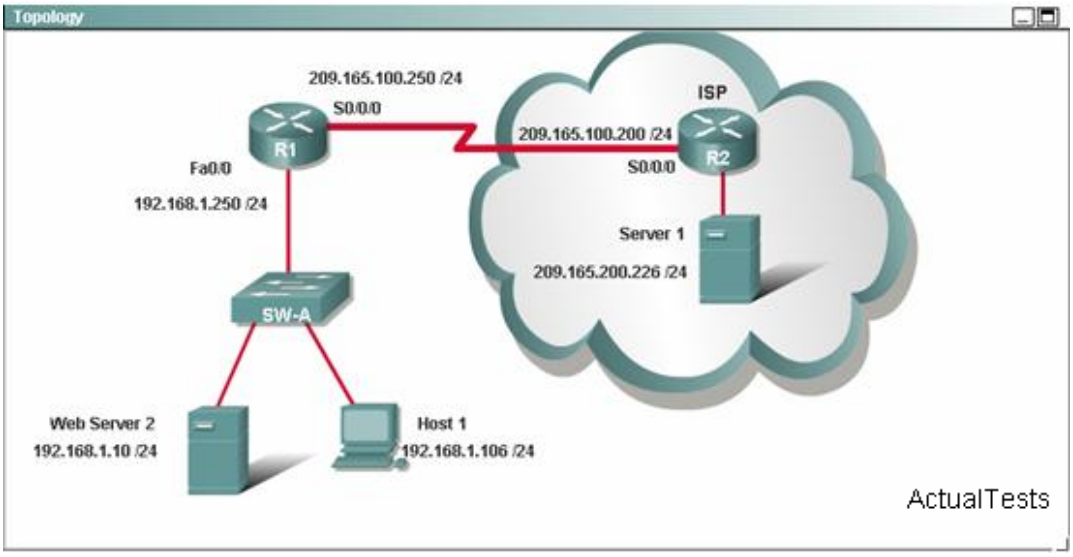
A. The frame does not have MAC addresses.
B. The destination MAC address in the frame is the MAC address of the s0/0/0 interface of R2
C. The source MAC address in the frame is the MAC address of the s0/0/0 interface of R1.
D. The destination MAC address in the frame is the MAC address of the NIC of server 1.
E. The source MAC address in the frame is the MAC address of the NIC of Host 1.

Answer: A

Explanation:
The frame relay network does not have hardware addresses.

QUESTION NO: 468

Host 1 receives a file from remote server 1. Which MAC address appears as the source address in the header of the frames received by Host 1?

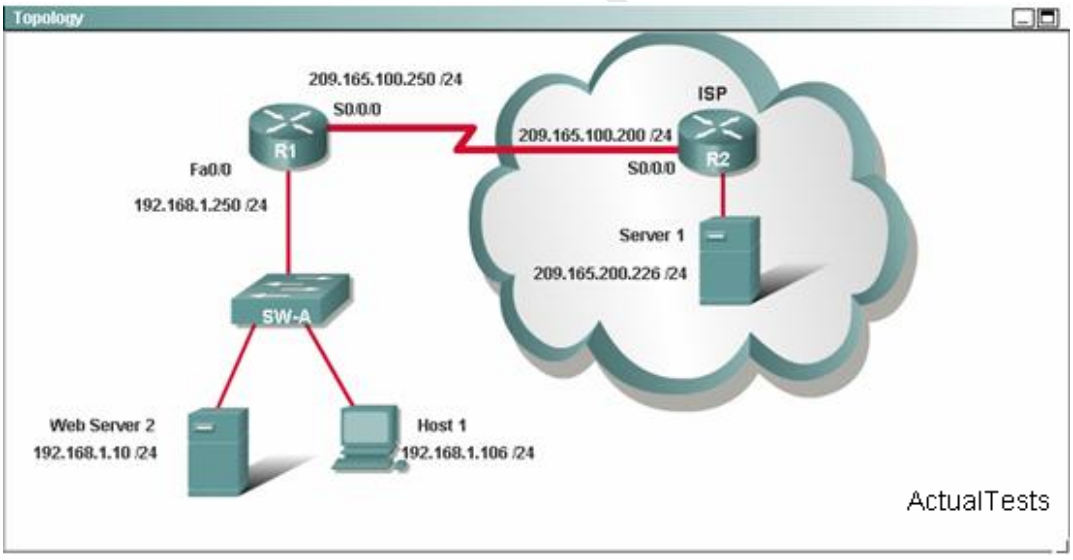


A. The MAC address of the s0/0/0 interface of the router R2
B. The MAC address of the Fa0/0 interface of router R1
C. The MAC address of the NIC in Host 1 .
D. The MAC address of the NIC in server 1.

Answer: B

QUESTION NO: 469

Host 1 sends an ICMP echo request to remote sever1. Which destination address does Host 1 place in the Layer2 header of the frame containing the ping packet?



A. The IP address of F0/0 interface of router R1.
B. The IP address of the s0/0/0 interface of router R2
C. The MAC address of the Fa0/0 interface of router R1.
D. The MAC address of the s0/0/0 interface of router R2
E. The MAC address of NIC in sever 1.

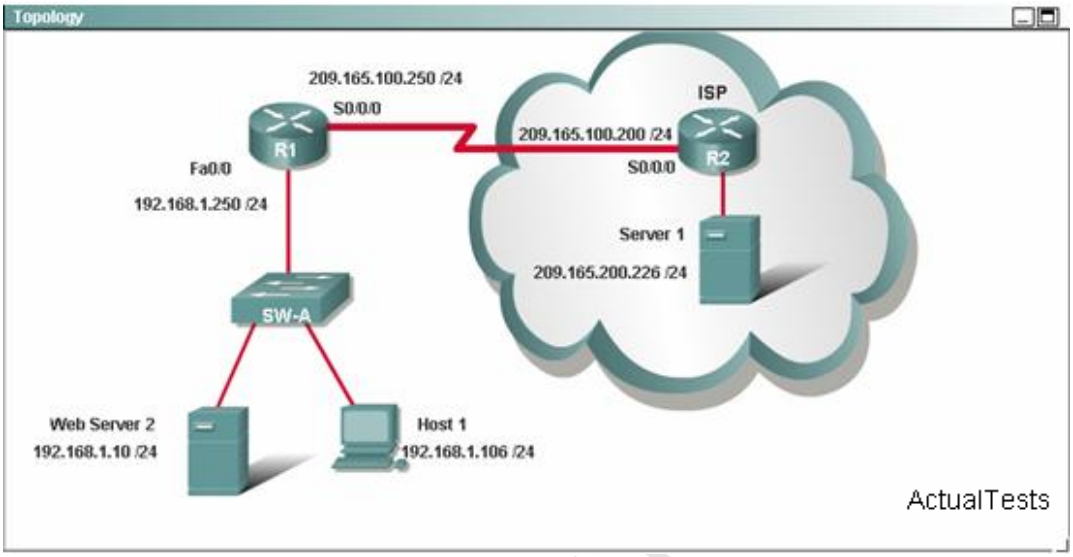
F. The IP address of sever 1.

Answer: C

Explanation:
Host1 learned the frame relay network through R1. Host1 can reach server1 by using the Ping command of the ICMP protocol.

QUESTION NO: 470

Please study the exhibit shown above carefully:



Host 1 sends a request for a file to remote server Server1. Which destination address does host 1 place in the layer 3 header of the packet containing the request?

A. The IP address of Server Server1
B. The MAC address of the s0/0/0 interface of router R2
C. The IP address of the Fa0/0 interface of router R1
D. The Mac address of the NIC in Sever Server1

Answer: A

Explanation:
In the packet that HOST 1 sent and request response, layer 3 destination address is Server Server1

QUESTION NO: 471

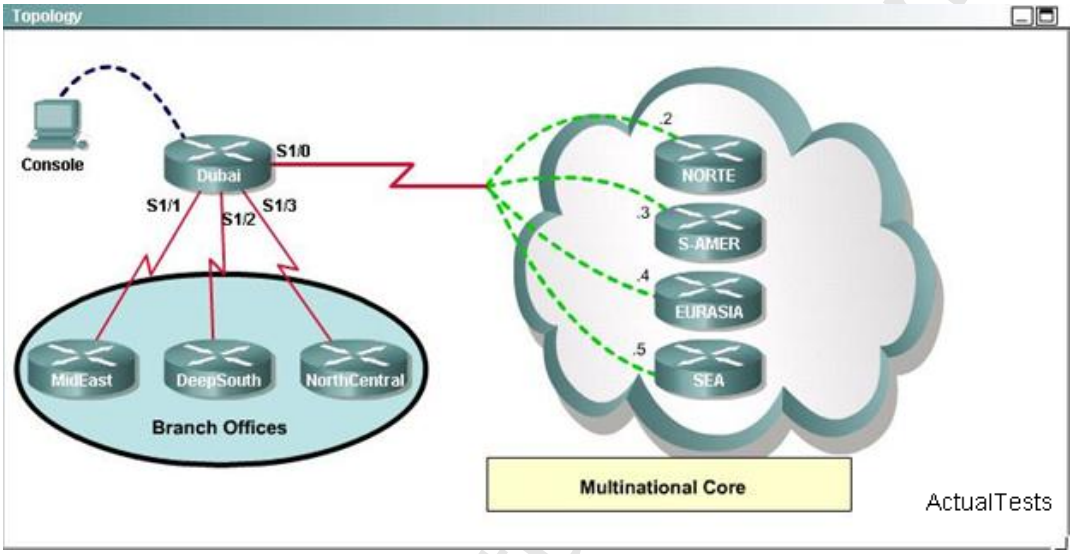
Jill has opened two Internet Explorer windows on her local PC. She uses them to simultaneously access the local web server at the time to browse WWW documents on the intranet. What mechanism makes the data to end up in the correct Internet Explorer window?

A. The TCP port numbers are used to direct the data to the correct application window.
B. The IP Source addresses of the packets will be used to direct the data to the correct browser window.
C. The OSI application layer tracks the conversations and directs them to the correct browser.
D. The browser track the data by the URL.

Answer: A

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.

QUESTION NO: 472



```
Dubai#sh frame-relay map
Serial1/0 (up): ip 172.30.0.2 dlci 704 (0x7B,0x1CB0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.3 dlci 196 (0xEA,0x38A0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.4 dlci 702 (0x159,0x5490), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.5 dlci 344 (0x1C8,0x7080), dynamic,
                broadcast,, status defined, active
Dubai#
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial1/0
 ip address 172.30.0.1 255.255.255.240
 encapsulation frame-relay
 no fair-queue
!
interface Serial1/1
 ip address 192.168.0.1 255.255.255.252
!
interface Serial1/2
 ip address 192.168.0.5 255.255.255.252
 encapsulation ppp
!
interface Serial1/3
 ip address 192.168.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.0.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password Tlnet
 login
!
end
```

ActualTests

Please study the exhibit shown above carefully, and answer the following questions.

A static map to the S-AMER location is required. Which command should be used to create this map?

A. frame-relay map ip 172.30.0.3 702 broadcast
B. frame-relay map ip 172.30.0.3 196 broadcast
C. frame-relay map ip 172.30.0.3 344 broadcast
D. frame-relay map ip 172.30.0.3 704 broadcast

Answer: B

Explanation:
Based on the output of the command "show frame-relay map", we know that DLCI mapped to the router S-AMER is 196. (.3 In the above network topology, the complete layer3 IP address is172.30.0.3)
Frame-relay map: The mapping command "Frame-relay map" can statically create a mapping reaching the remote protocol address.
The format is :

frame-relay map protocol protocol-address dlci [broadcast][ietf | cisco]

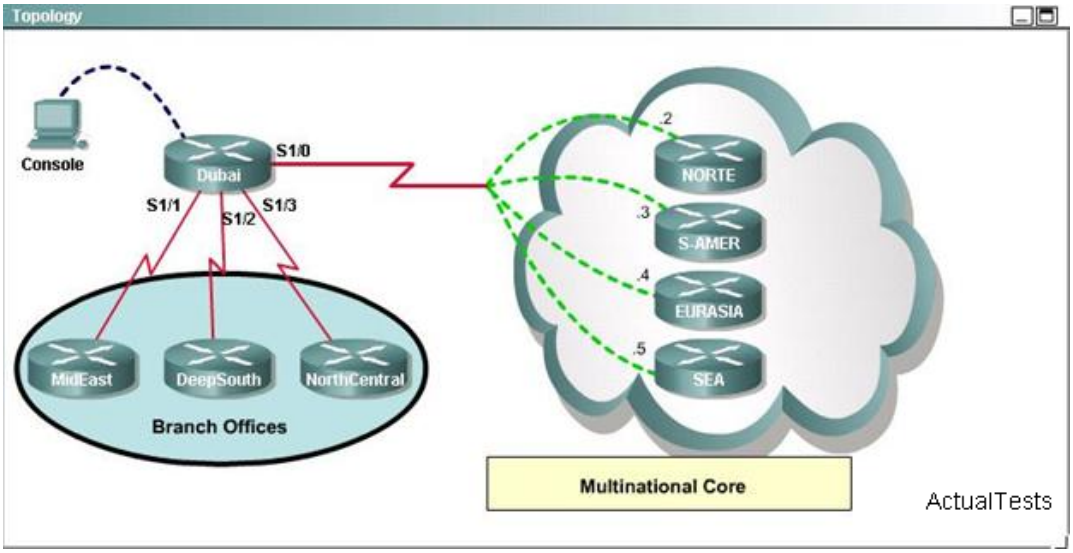
Configuring a static Frame Relay map is optional unless you are using subinterfaces. The Frame Relay map will map a Layer 3 address to a local DLCI. This step is optional because inverse-arp will automatically perform this map for you.
Syntax for frame-relay map is:

frame-relay map protocol address dlci [broadcast] [cisco | ietf]

The broadcast option allows packets, such as RIP updates to be forwarded across the PVC. If you are not using the broadcast option, you need to specify the neighbor to forward unicast packet using neighbor command.

neighbor a.b.c.d
Specify RIP neighbor. When a neighbor doesn't understand multicast, this command is used to specify neighbors. In some cases, not all routers will be able to understand multicasting, where packets are sent to a network or a group of addresses. In a situation where a neighbor cannot process multicast packets, it is necessary to establish a direct link between routers. The neighbor command allows the network administrator to specify a router as a RIP neighbor. The no neighbor a.b.c.d command will disable the RIP neighbor.

QUESTION NO: 473




```
Dubai#sh frame-relay map
Serial1/0 (up): ip 172.30.0.2 dlci 704 (0x7B,0x1CB0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.3 dlci 196 (0xEA,0x38A0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.4 dlci 702 (0x159,0x5490), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.5 dlci 344 (0x1C8,0x7080), dynamic,
                broadcast,, status defined, active
Dubai#
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial1/0
 ip address 172.30.0.1 255.255.255.240
 encapsulation frame-relay
 no fair-queue
!
interface Serial1/1
 ip address 192.168.0.1 255.255.255.252
!
interface Serial1/2
 ip address 192.168.0.5 255.255.255.252
 encapsulation ppp
!
interface Serial1/3
 ip address 192.168.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.0.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password Tlnet
 login
!
end
```

ActualTests

Please study the exhibit shown above carefully, and answer the following question.

Which connection user the default encapsulation for serial interfaces on Cisco routers?

A. The serial connection to theMidEast branch office.
B. The serial connection to the DeepSouth branch office.
C. The serial connection to the NorthCentral branch office.
D. The serial connection to the Multinational Core.

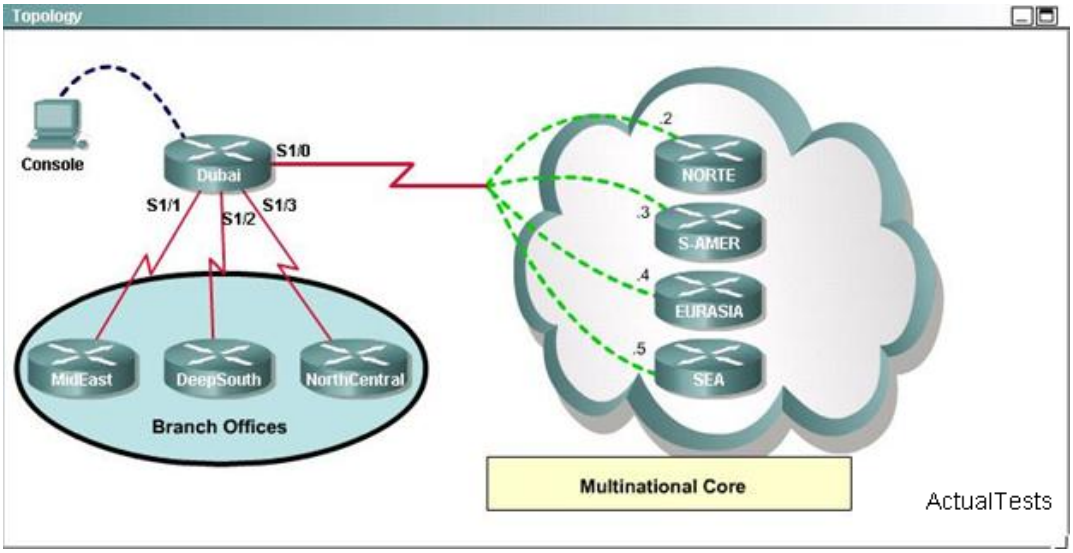
Answer: A

Explanation:
On the basis of the configuration on Dubai provided in the exhibit, we know that the encapsulation types of different interfaces are as follows:
Serial 1/0 : encapsulation frame-relay
Serial 1/2 and Serial 1/3 : both interfaces are encapsulated PPP
Serial 1/1: There is no related encapsulation information displayed, so its default encapsulation type is HDLC .
Based on the network topology provided in the exhibit, the interface Serial 1/1 is connected to the router Mideast of the branch office, so the encapsulation type of the router Mideast is by default.

The default encapsulation on a serial interface is HDLC. The original HDLC encapsulation was defined by the International Organization for Standards (ISO), those same folks who developed the OSI model. The ISO version of HDLC had one shortcoming, however; it had no options to support multiple Layer 3 routed protocols. As a result, most vendors have created their own form of HDLC. Cisco is no exception because it has its own proprietary form of HDLC to support various Layer 3 protocols such as IPX, IP, and AppleTalk.

The Serial connection to the Dub<i branch office using the default encapsulation type. You can change using:
* encapsulation <type> command on interface

QUESTION NO: 474




```
Dubai#sh frame-relay map
Serial1/0 (up): ip 172.30.0.2 dlci 704 (0x7B,0x1CB0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.3 dlci 196 (0xEA,0x38A0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.4 dlci 702 (0x159,0x5490), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.5 dlci 344 (0x1C8,0x7080), dynamic,
                broadcast,, status defined, active
Dubai#
```

```
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial1/0
 ip address 172.30.0.1 255.255.255.240
 encapsulation frame-relay
 no fair-queue
!
interface Serial1/1
 ip address 192.168.0.1 255.255.255.252
!
interface Serial1/2
 ip address 192.168.0.5 255.255.255.252
 encapsulation ppp
!
interface Serial1/3
 ip address 192.168.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.0.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password Tlnet
 login
!
end
```

ActualTests

Please study the exhibit shown above carefully, and answer the following questions.

What destination Layer2 address will be used in the frame header containing a packet for host 172.30.4.4?

A. 344
B. 704
C. 702
D. 196

Answer: C

Explanation:
Circuits are identified by data-link connection identifiers (DLCI). DLCIs are assigned by your provider and are used between your router and the Frame Relay provider. In other words, DLCIs are locally significant.

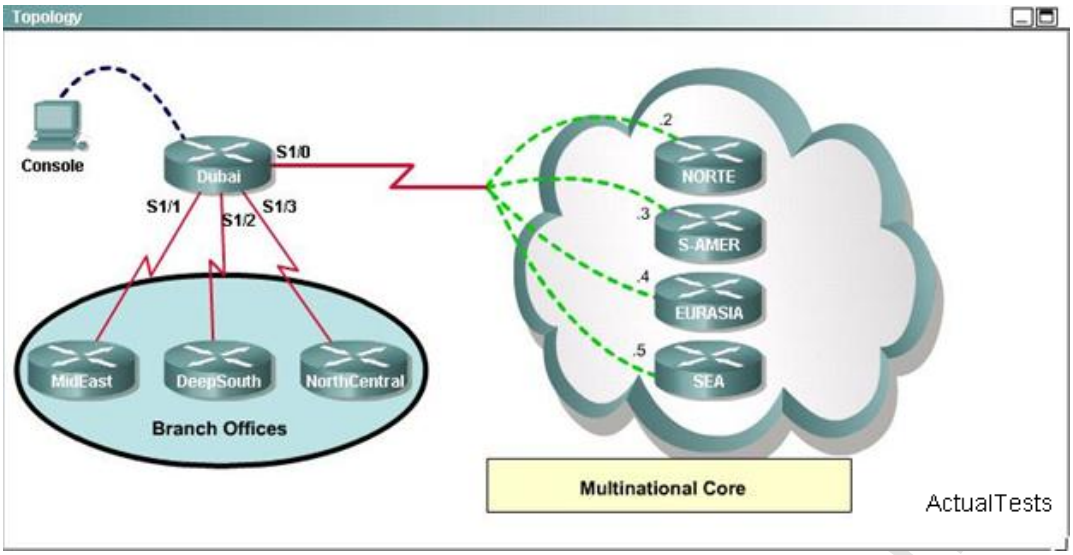
See the exhibit of show frame-relay map output, IP address 172.30.4.4 is mapped with 702 DLCI address, so layer 2 destination address (DLCI on frame-relay) will be 702.

You can map IP to DLCI with:
* frame-relay interface-dlci <dlci_num>
or
* frame-relay map ip <IP Address> <dlci>

In the Frame Relay network, the devices are connected with each other through DLCI. The address of the destination host presented in the subject is 172.30.0.4, on the basis of the output of the command "show frame-relay map" displayed in the exhibit , we know that the Layer3 IP address 172.30.0.4 corresponding DLCI is 702.

DLCI Addressing:The DLCI is an addressing mechanism used to identify a VC so that when multiple VCs use the same access link the Frame Relay switches know how to forward the frames to the correct remote sites.
Two important features of the DLCI are:
The Frame Relay headers, which have a single DLCI field, not both Source and Destination DLCI fields.
The local significance of the DLCI, which means that the addresses need to be unique only on the local access link. This is called local addressing.
Because there is only a single DLCI field in the Frame Relay header, Global addressing can be used, making DLCI addressing look like LAN addressing in concept. Global addressing is a way of choosing DLCI numbers when planning a Frame Relay network so that working with DLCIs is much easier.

QUESTION NO: 475



```
Dubai#sh frame-relay map
Serial1/0 (up): ip 172.30.0.2 dlci 704 (0x7B,0x1CB0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.3 dlci 196 (0xEA,0x38A0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.4 dlci 702 (0x159,0x5490), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.5 dlci 344 (0x1C8,0x7080), dynamic,
                broadcast,, status defined, active
Dubai#
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial1/0
 ip address 172.30.0.1 255.255.255.240
 encapsulation frame-relay
 no fair-queue
!
interface Serial1/1
 ip address 192.168.0.1 255.255.255.252
!
interface Serial1/2
 ip address 192.168.0.5 255.255.255.252
 encapsulation ppp
!
interface Serial1/3
 ip address 192.168.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.0.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password Tlnet
 login
!
end
```

ActualTests

Please study the exhibit shown above carefully, and answer the following question.

If required, what password should be configured on the DeepSouth router in the branch office to allow a connection to be established with the MidEast router?

A. Console
B. Enable
C. No password is required.
D. Secret
E. Telnet

Answer: C

Explanation:
No password is required because there is no authentication type is specified, it's just encapsulation type is changed. By default encapsulation type on serial interface is hdlc on Cisco router, that is Cisco proprietary code added hdlc . If you are going with different vendor router connection with cisco router on serial interface, you need to change hdlc encapsulation type to ppp.

QUESTION NO: 476

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

Success rate is 0 percent (0/5)

SwitchC>

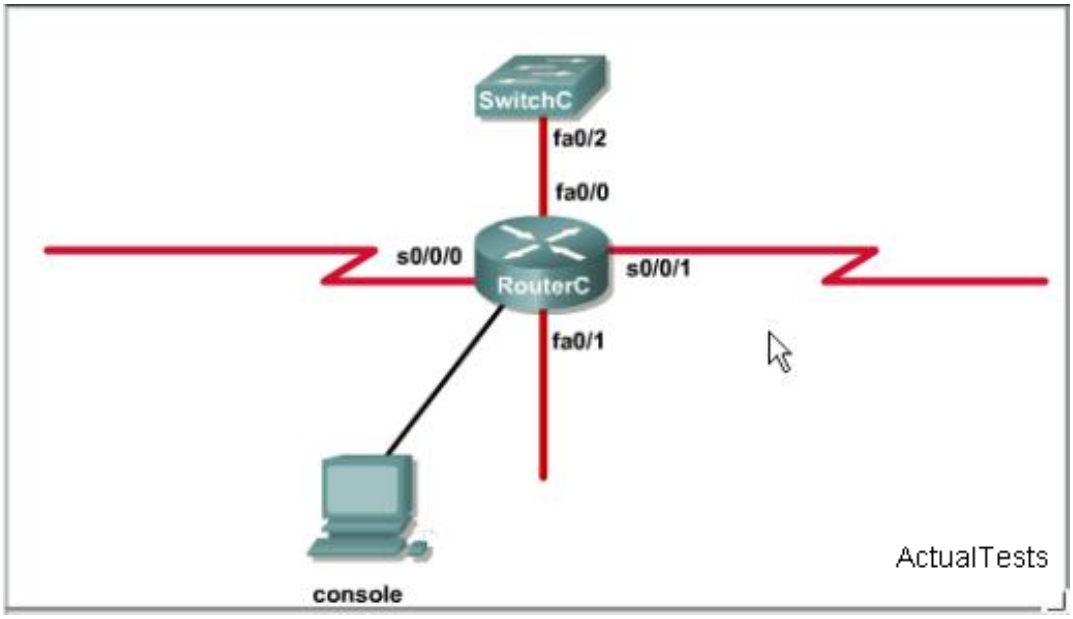
SwitchC> telnet 10.4.4.3

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.



RouterC

```
!
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
```

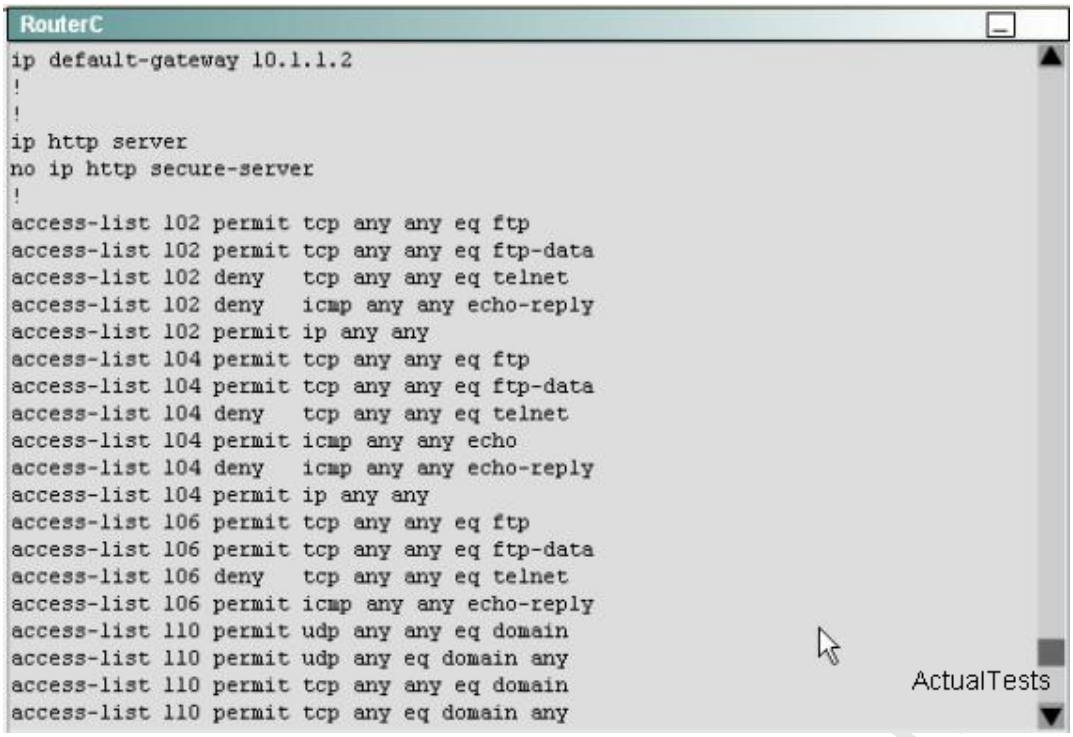
ActualTests

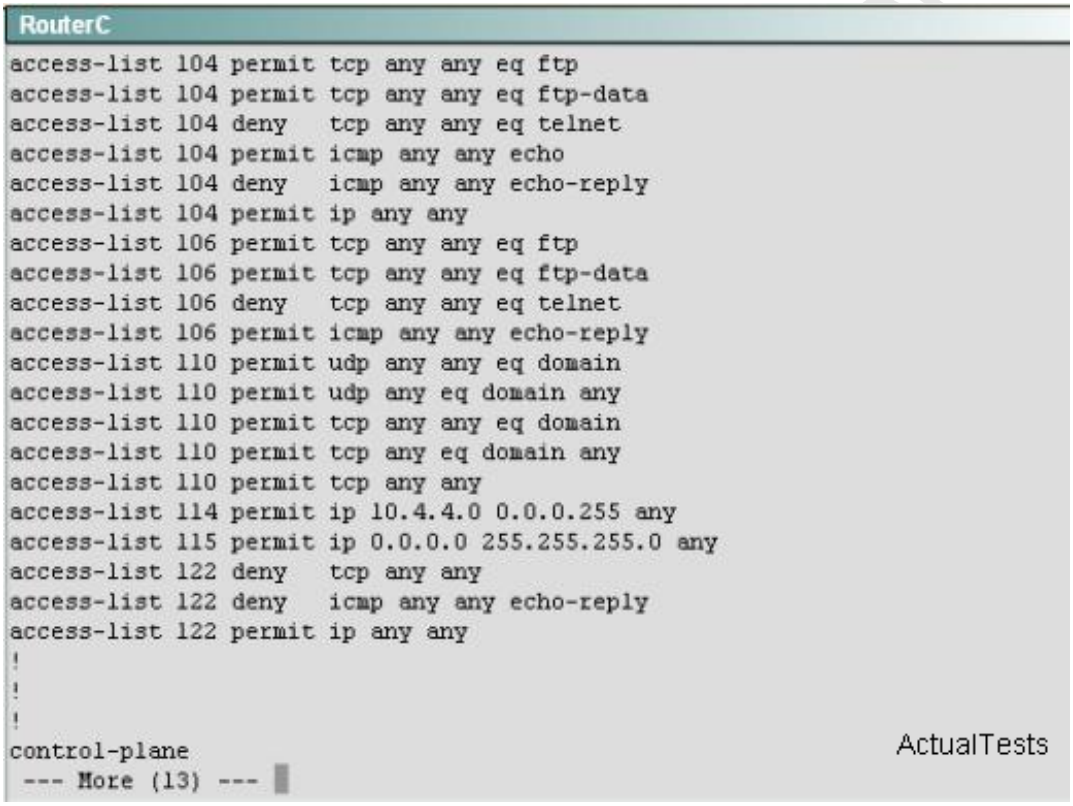
RouterC

```
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 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 Serial0/0/1
 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
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
 --- More (66) ---
```


RouterC

```
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.2.0
 no 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
```





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. Removeaccess-group 106 to 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 to from interface fa0/0 and add access-group 104 in.

Answer: E

QUESTION NO: 477

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

Success rate is 0 percent (0/5)

SwitchC>

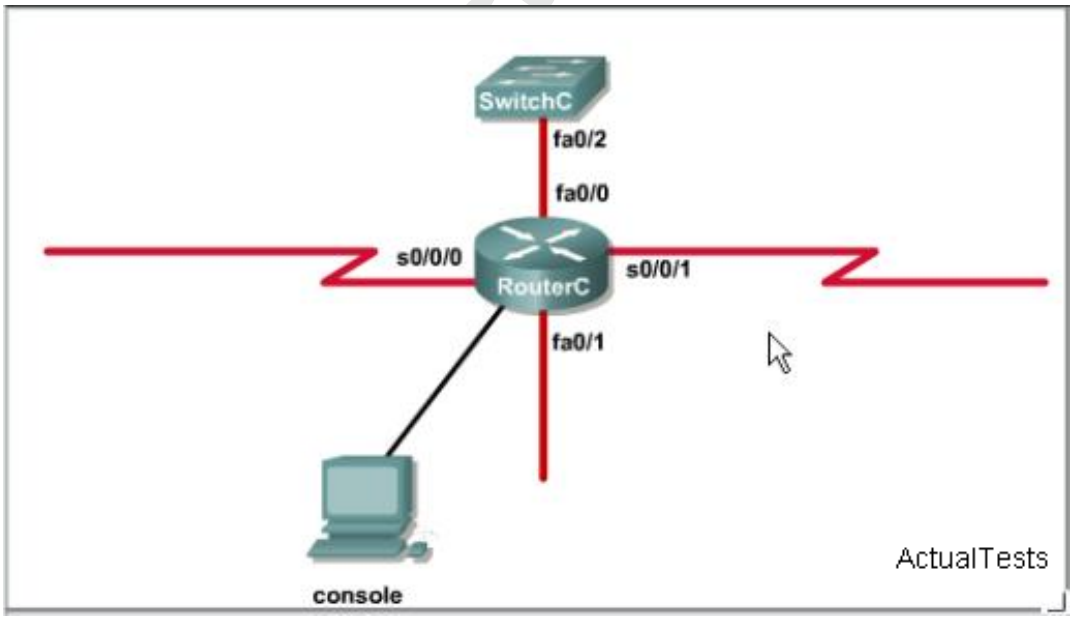
SwitchC> telnet 10.4.4.3

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.

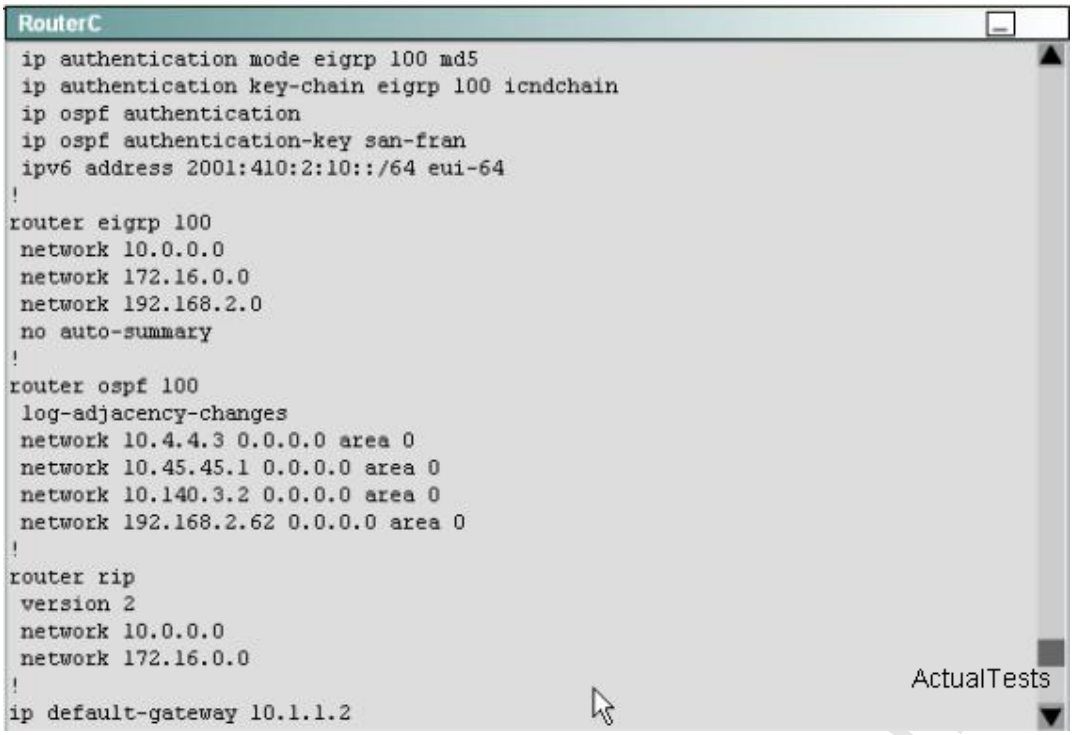


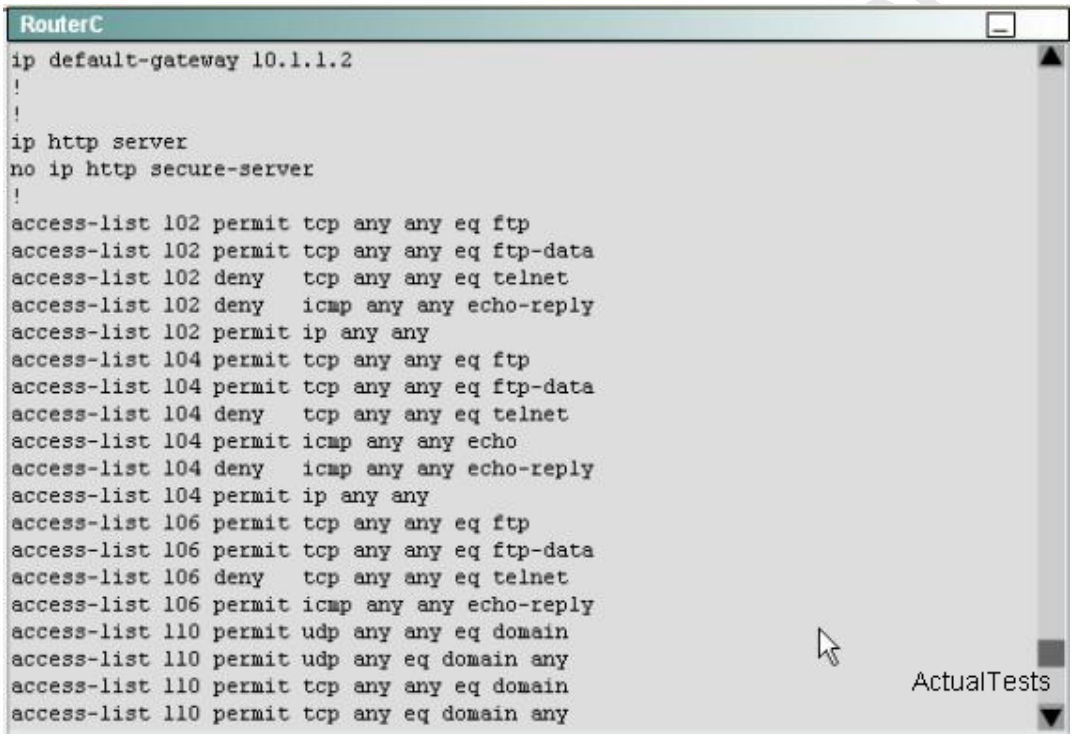
RouterC

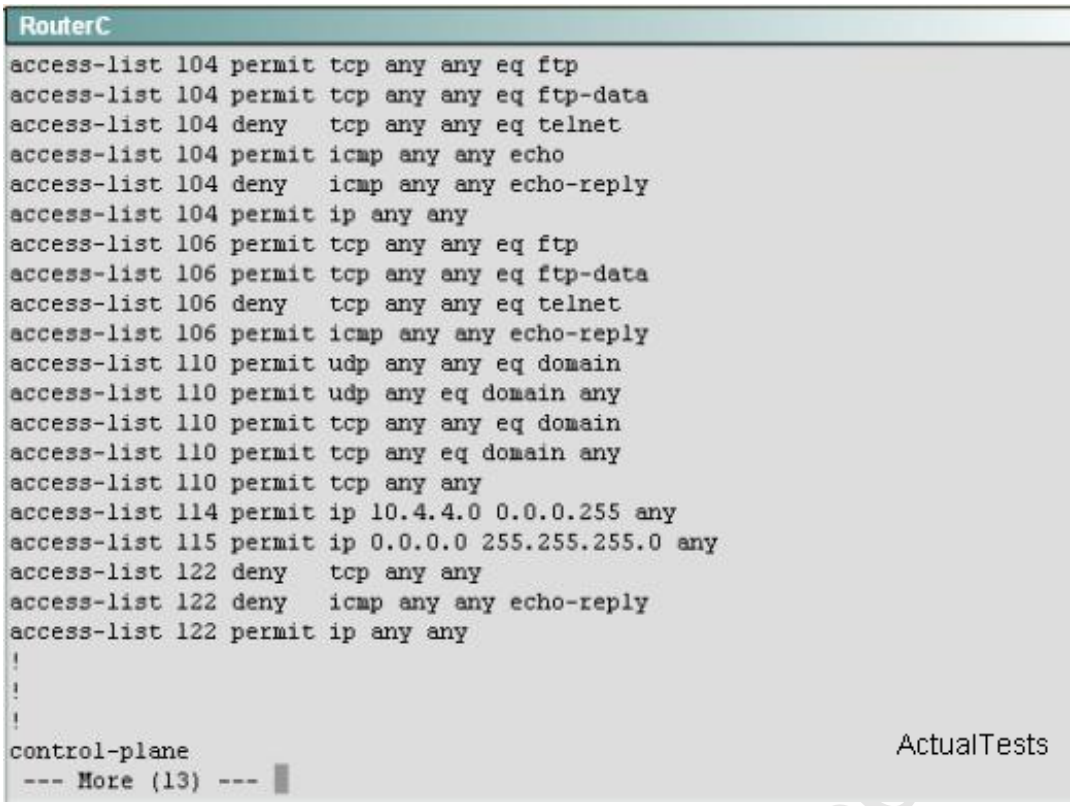
```
!
interface Loopback1
 ip address 172.16.4.1 255.255.255.0
!
interface Loopback2
 ip address 10.145.145.1 255.255.255.0
 ipv6 address 2001:410:2:3::/64 eui-64
!
interface FastEthernet0/0
 ip address 10.4.4.3 255.255.255.0
 ip access-group 106 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 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
```


RouterC

```
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 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 Serial0/0/1
 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
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
 --- More (66) ---
```


RouterC
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 icndchain
ip ospf authentication
ip ospf authentication-key san-fran
ipv6 address 2001:410:2:10::/64 eui-64
!
router eigrp 100
network 10.0.0.0
network 172.16.0.0
network 192.168.2.0
no 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
ActualTests


RouterC
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 eq 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
ActualTests



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 faO/0 interface.

Answer: B

QUESTION NO: 478

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

Success rate is 0 percent (0/5)

SwitchC>

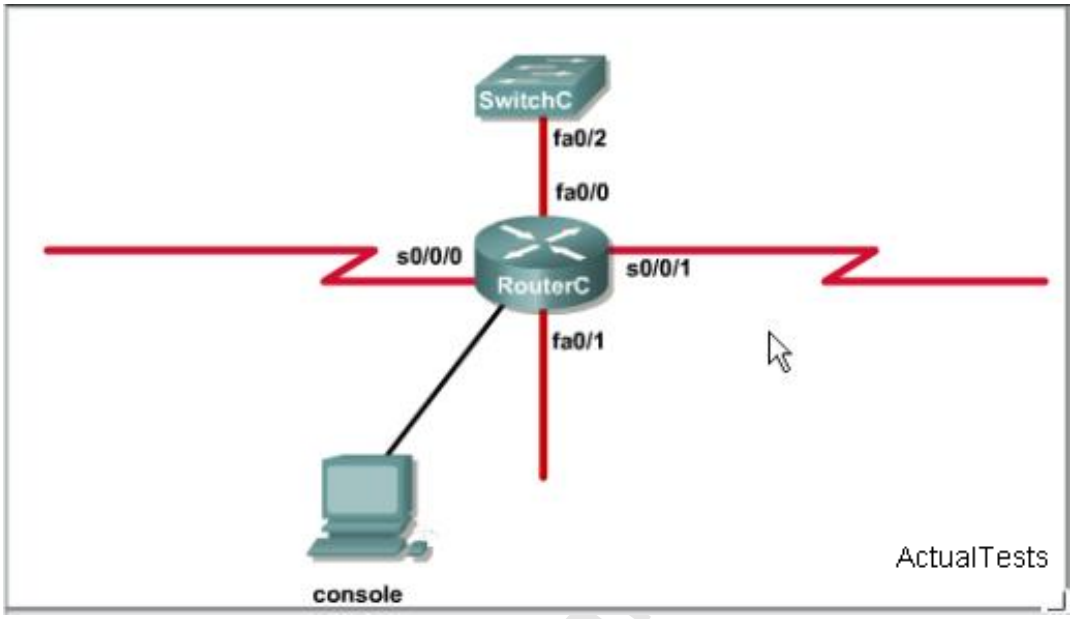
SwitchC> telnet 10.4.4.3

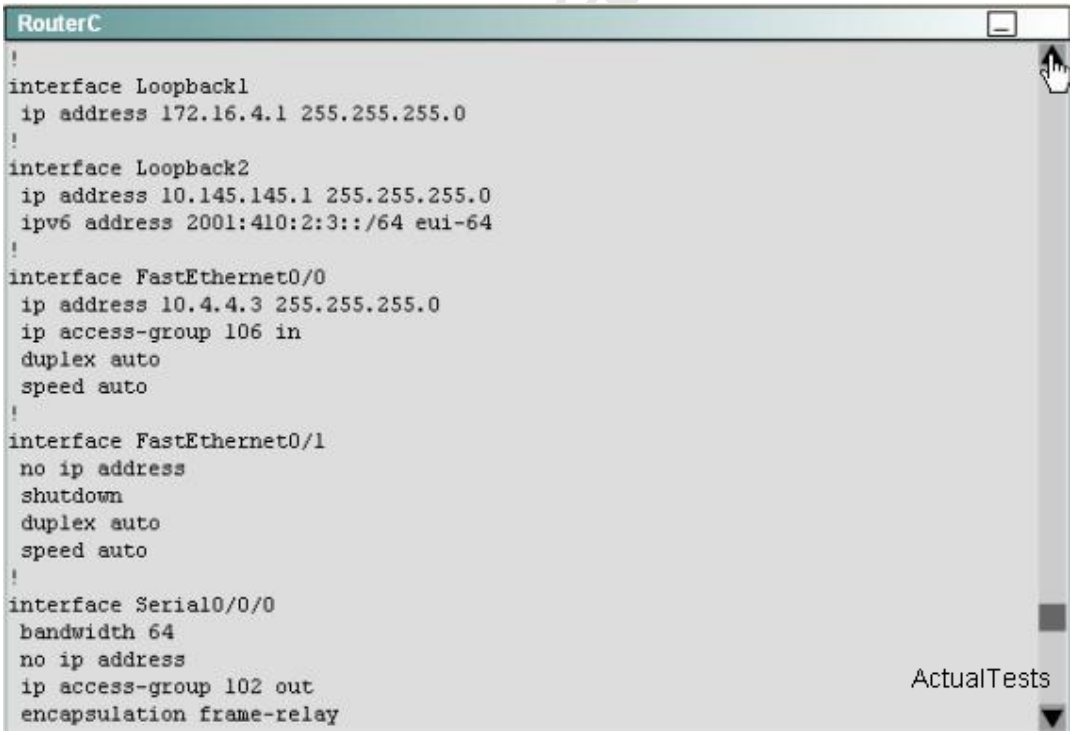
Trying 10.4.4.3...

% Destination unreachable; gateway or host down

SwitchC>

Click the console connected to RouterC and issue the appropriate commands to answer the questions.





RouterC

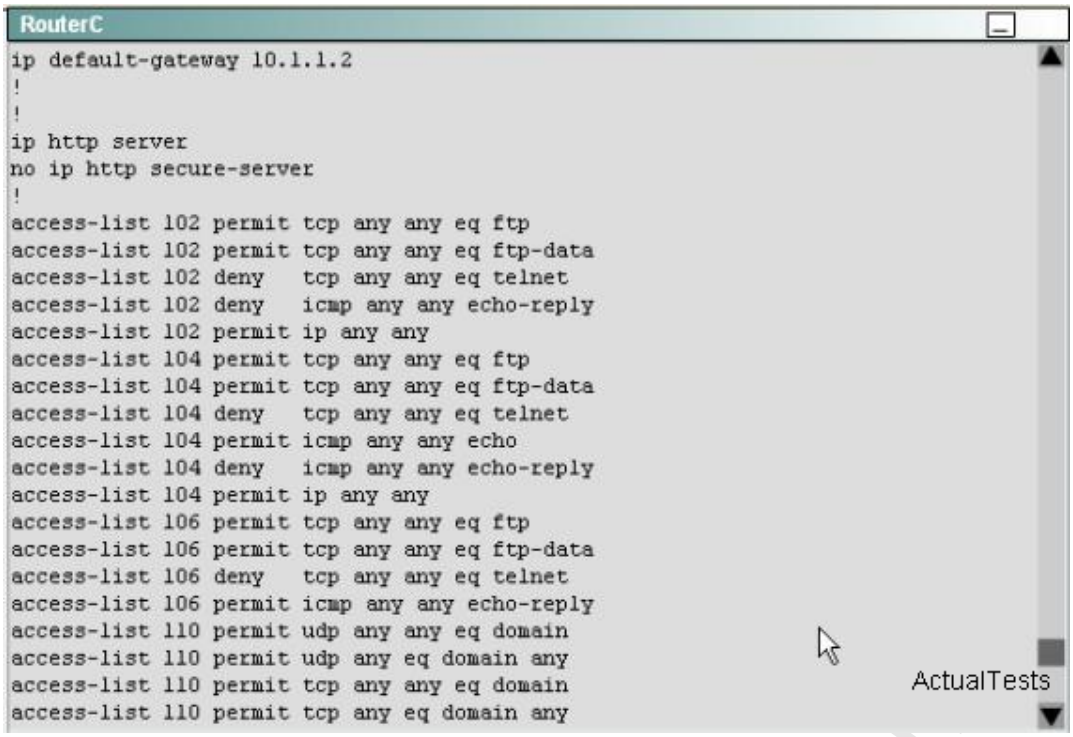
```
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.3.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serial0/0/1
 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
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
 --- More (66) ---
```

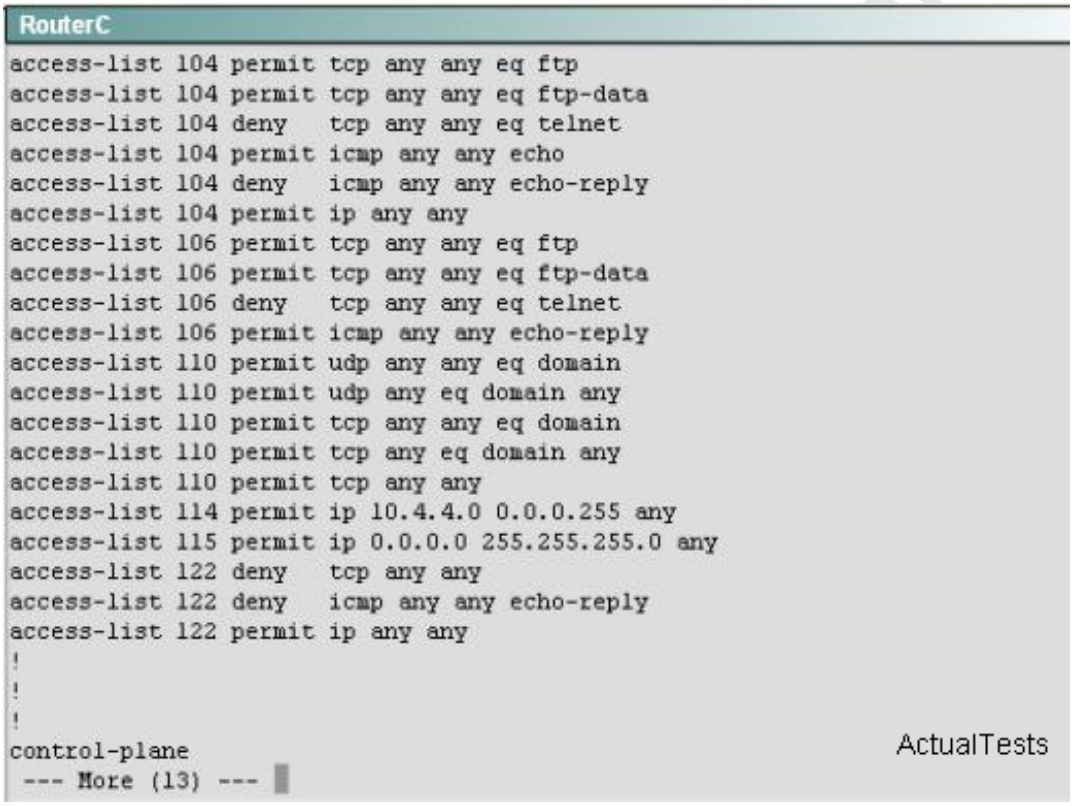
ActualTests

RouterC

```
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.2.0
 no 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
```

ActualTests





What would be the effect of issuing the command ip access-group 115 in on the s0/0/1 interface?

A. No host could connect to RouterC through s0/0/1.

B. Telnet and ping would work but routing updates would fail.

C. FTP, FTP-DATA, echo, and www would work but telnet would fail.

D. Only traffic from the 10.4.4.0 network would pass through the interface.

Answer: A

QUESTION NO: 479

For which type of connection should a straight-through cable be used?

A. switch to switch
B. switch to hub
C. switch to router
D. hub to hub
E. router to PC

Answer: C

QUESTION NO: 480

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

QUESTION NO: 481

By default, each port in a Cisco Catalyst switch is assigned to VLAN1. Which two recommendations are key to avoid unauthorized management access? (Choose two.)

A. Create an additional ACL to block the access to VLAN 1.
B. Move the management VLAN to something other than default.
C. Move all ports to another VLAN and deactivate the default VLAN.
D. Limit the access in the switch using port security configuration.
E. Use static VLAN in trunks and access ports to restrict connections.
F. Shutdown all unused ports in the Catalyst switch.

Answer: B,F

QUESTION NO: 482

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

QUESTION NO: 483

Which type of cable is used to connect the COM port of a host to the COM port of a router or switch?

A. crossover
B. straight-through
C. rolled
D. shielded twisted-pair

Answer: C

QUESTION NO: 484

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

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

Answer: B

QUESTION NO: 485

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

QUESTION NO: 486

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

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

Answer: D

QUESTION NO: 487

Which layer of the OSI reference model uses the hardware address of a device to ensure message delivery to the proper host on a LAN?

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

Answer: B

QUESTION NO: 488

Which layer of the OSI reference model uses flow control, sequencing, and acknowledgements to ensure that reliable networking occurs?

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

Answer: C

QUESTION NO: 489

What is the principle reason to use a private IP address on an internal network?

A. Subnet strategy for private companies.
B. Manage and scale the growth of the internal network.
C. Conserve public IP addresses so that we do not run out of them.
D. Allow access reserved to the devices.

Answer: C

QUESTION NO: 490

Which IP address can be assigned to an Internet interface?

A. 10.180.48.224
B. 9.255.255.10
C. 192.168.20.223
D. 172.16.200.18

Answer: B

QUESTION NO: 491

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 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 in a valid IP address.
D. Several automated methods will be necessary on the private network.
E. A conflict of IP addresses happens, because other public routers can use the same range.

Answer: A

QUESTION NO: 492

When is it necessary to use a public IP address on a routing interface?

A. Connect a router on a local network.
B. Connect a router to another router.
C. Allow distribution of routes between networks.
D. Translate a private IP address.

E. Connect a network to the Internet.

Answer: E

QUESTION NO: 493

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

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

Answer: C

QUESTION NO: 494

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

QUESTION NO: 495

Which term describes the process of encapsulating IPv6 packets inside IPv4 packets?

A. tunneling
B. hashing
C. routing
D. NAT

Answer: A

QUESTION NO: 496

Which statement about RIPng is true?

A. RIPng allows for routes with up to 30 hops.
B. RIPng is enabled on each interface separately.
C. RIPng uses broadcasts to exchange routes.
D. There can be only one RIPng process per router.

Answer: B

QUESTION NO: 497

Which statement about IPv6 is true?

A. Addresses are not hierarchical and are assigned at random.
B. Only one IPv6 address can exist on a given interface.
C. There are 2.7 billion addresses available.
D. Broadcasts have been eliminated and replaced with multicasts.

Answer: D

QUESTION NO: 498

A network admin wants to know every hop the packets take when he accesses cisco.com. Which command is the most appropriate to use?

A. path cisco.com
B. debug cisco.com
C. trace cisco.com
D. traceroute cisco.com

Answer: D

QUESTION NO: 499

QoS policies are applied on the switches of a LAN. Which type of command will show the effects of the policy in real time?

A. show command
B. debug command
C. configuration command
D. rommon command

Answer: B

QUESTION NO: 500

Which command will show the MAC addresses of stations connected to switch ports?

A. show mac-address
B. show arp
C. show table
D. show switchport

Answer: B

QUESTION NO: 501

What is the name of the VTP mode of operation that enables a switch to forward only VTP advertisements while still permitting the editing of local VLAN information?

A. server
B. client
C. tunnel
D. transparent

Answer: D

QUESTION NO: 502

Which port state is introduced by Rapid-PVST?

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

Answer: C

QUESTION NO: 503

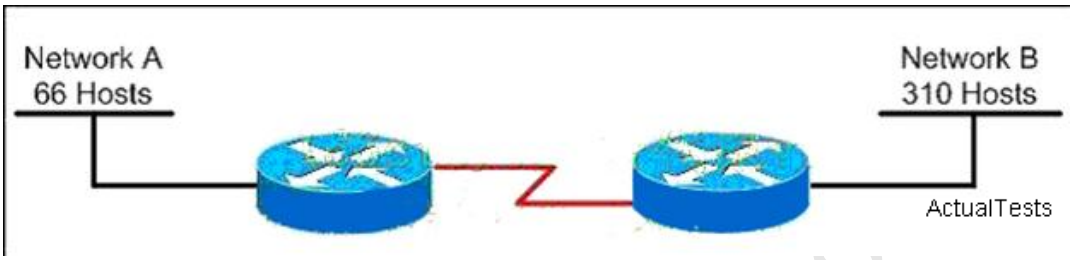
What speeds must be disabled in a mixed 802.11b/g WLAN to allow only 802.11g clients to connect?

A. 6, 9, 12, 18
B. 1, 2, 5.5, 6
C. 5.5, 6, 9, 11
D. 1, 2, 5.5, 11

Answer: D

QUESTION NO: 504

Refer to the exhibit. Which VLSM mask will allow for the appropriate number of host addresses for Network A?

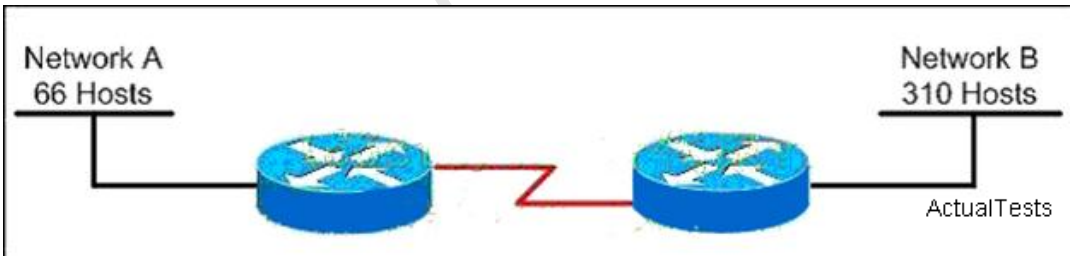


A. /25
B. /26
C. /27
D. /28

Answer: A

QUESTION NO: 505

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?

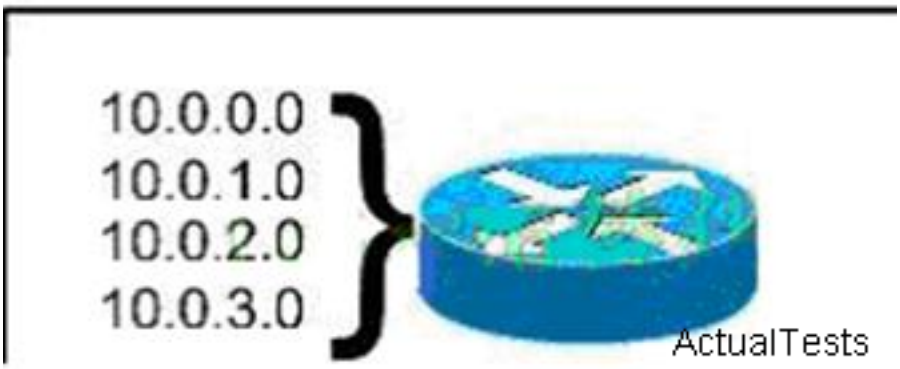


A. 255.255.255.0
B. 255.255.254.0
C. 255.255.252.0
D. 255.255.248.0

Answer: B

QUESTION NO: 506

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

QUESTION NO: 507

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

QUESTION NO: 508

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

QUESTION NO: 509

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

QUESTION NO: 510

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

QUESTION NO: 511

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

QUESTION NO: 512

On the network 131.1.123.0/27, what is the last IP address that can be assigned to a host?

A. 131.1.123.30
B. 131.1.123.31
C. 131.1.123.32
D. 131.1.123.33

Answer: A

QUESTION NO: 513

The ip subnet zero command is not configured on a router. What would be the IP address of Ethernet 0/0 using the first available address from the sixth subnet of the network 192.168.8.0/29?

A. 192.168.8.25
B. 192.168.8.41
C. 192.168.8.49
D. 192.168.8.113

Answer: C

QUESTION NO: 514

For the network 192.0.2.0/23, which option is a valid IP address that can be assigned to a host?

A. 192.0.2.0
B. 192.0.2.255
C. 192.0.3.255
D. 192.0.4.0

Answer: B

QUESTION NO: 515

How many addresses for hosts will the network 124.12.4.0/22 provide?

A. 510
B. 1022
C. 1024
D. 2048

Answer: B

QUESTION NO: 516

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

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

Answer: B

QUESTION NO: 517

Which VTP mode is capable of creating only local VLANs and does not synchronize with other switches in the VTP domain?

A. client
B. dynamic
C. server
D. static
E. transparent

Answer: E

QUESTION NO: 518

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

QUESTION NO: 519

Which two statements about the use of VLANs to segment a network are true? (Choose two.)

A. VLANs increase the size of collision domains.
B. VLANs allow logical grouping of users by function.
C. VLANs simplify switch administration.
D. VLANs enhance network security.

Answer: B,D

QUESTION NO: 520

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

QUESTION NO: 521

Which network protocol does DNS use?

A. FTP
B. TFTP
C. TCP
D. UDP
E. SCP

Answer: D

QUESTION NO: 522

When two hosts are trying to communicate across a network, how does the host originating the communication determine the hardware address of the host that it wants to "talk" to?

A. RARP request
B. Show Network Address request
C. Proxy ARP request
D. ARP request
E. Show Hardware Address request

Answer: D

QUESTION NO: 523

When a host transmits data across a network to another host, which process does the data go through?

A. standardization
B. conversion
C. encapsulation
D. synchronization

Answer: C

QUESTION NO: 524

An administrator attempts a traceroute but receives a "Destination Unreadable" message. Which protocol is responsible for that message?

A. RARP
B. RUDP
C. ICMP
D. SNMP

Answer: C

QUESTION NO: 525

When you are logged into a switch, which prompt indicates that you are in privileged mode?

A. %
B. @

C. >
D. $
E. #

Answer: E

QUESTION NO: 526

Which command shows system hardware and software version information?

A. show configuration
B. show environment
C. show inventory
D. show platform
E. show version

Answer: E

QUESTION NO: 527

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

QUESTION NO: 528

Workstation A has been assigned an IP address of 192.0.2.24/28. Workstation B has been assigned an IP address of 192.0.2.100/28. The two workstations are connected with a straight-through cable.
Attempts to ping between the hosts are unsuccessful. What two things can be done to allow communications between the hosts? (Choose two.)

A. Replace the straight-through cable with a crossover cable.

B. Change the subnet mask of the hosts to /25.
C. Change the subnet mask of the hosts to /26.
D. Change the address of Workstation A to 192.0.2.15.
E. Change the address of Workstation B to 192.0.2.111.

Answer: A,B

QUESTION NO: 529

Your ISP has given you the address 223.5.14.6/29 to assign to your router's interface. They have also given you the default gateway address of 223.5.14.7. After you have configured the address, the router is unable to ping any remote devices. What is preventing the router from pinging remote devices?

A. The default gateway is not an address on this subnet.
B. The default gateway is the broadcast address for this subnet.
C. The IP address is the broadcast address for this subnet.
D. The IP address is an invalid class D multicast address.

Answer: B

QUESTION NO: 530

Which command is used to copy the configuration from RAM into NVRAM?

A. copy running-config: startup-config
B. copy startup-config: running-config:
C. copy running config startup config
D. copy startup config running config
E. write terminal

Answer: A

QUESTION NO: 531

Which command is used to load a configuration from a TFTP server and merge the configuration into RAM?

A. copy running-config: TFTP:
B. copy TFTP: running-config
C. copy TFTP: startup-config

D. copy startup-config: TFTP:

Answer: B

QUESTION NO: 532

A system administrator types the command to change the hostname of a router. Where on the Cisco IFS is that change stored?

A. NVRAM
B. RAM
C. FLASH
D. ROM
E. PCMCIA

Answer: B

QUESTION NO: 533

Which command is used to configure a default route?

A. ip route 172.16.1.0 255.255.255.0 0.0.0.0
B. ip route 172.16.1.0 255.255.255.0 172.16.2.1
C. ip route 0.0.0.0 255.255.255.0 172.16.2.1
D. ip route 0.0.0.0 0.0.0.0 172.16.2.1

Answer: D

QUESTION NO: 534

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

QUESTION NO: 535

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

QUESTION NO: 536

Which command is used to debug a ping command?

A. debug icmp
B. debug ip icmp
C. debug tcp
D. debug packet

Answer: B

QUESTION NO: 537

When configuring a serial interface on a router, what is the default encapsulation?

A. atm-dxi
B. frame-relay
C. hdlc
D. lapb
E. ppp

Answer: C

QUESTION NO: 538

What must be set correctly when configuring a serial interface so that higher-level protocols calculate the best route?

A. bandwidth
B. delay

C. load
D. reliability

Answer: A

QUESTION NO: 539

A company implements video conferencing over IP on their Ethernet LAN. The users notice that the network slows down, and the video either stutters or fails completely. What is the most likely reason for this?

A. minimum cell rate (MCR)
B. quality of service (QoS)
C. modulation
D. packet switching exchange (PSE)
E. reliable transport protocol (RTP)

Answer: B

QUESTION NO: 540

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

QUESTION NO: 541

Data transfer is slow between the source and destination. The quality of service requested by the transport layer in the OSI reference model is not being maintained. To fix this issue, at which layer should the troubleshooting process begin?

A. presentation
B. session
C. transport

D. network
E. physical

Answer: D

QUESTION NO: 542

Which protocols are found in the network layer of the OSI reference model and are responsible for path determination and traffic switching?

A. LAN
B. routing
C. WAN
D. network

Answer: B

QUESTION NO: 543

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

QUESTION NO: 544

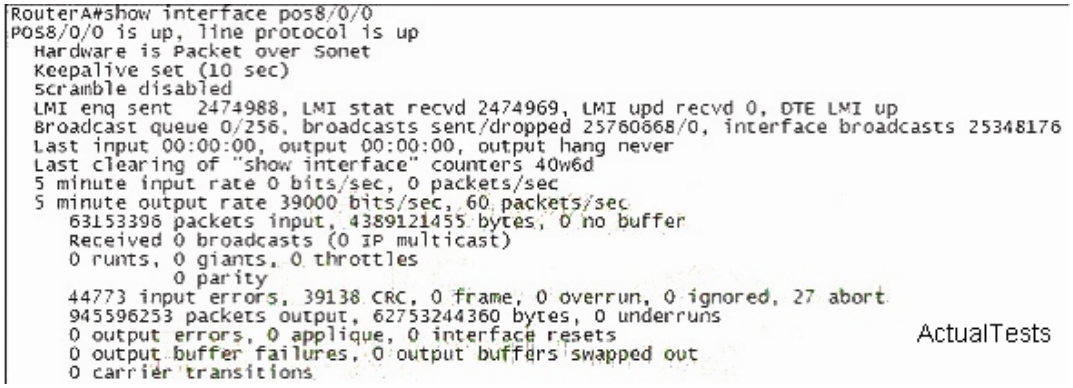
Which three options are valid WAN connectivity methods? (Choose three.)

A. PPP
B. WAP
C. HDLC
D. MPLS
E. L2TPv3
F. ATM

Answer: A,C,F

QUESTION NO: 545

Refer to the exhibit. Which WAN protocol is being used?



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

Answer: C

QUESTION NO: 546

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

QUESTION NO: 547

When troubleshooting a Frame Relay connection, what is the first step when performing a loopback test?

A. Set the encapsulation of the interface to HDLC.
B. Place the CSU/DSU in local-loop mode.

C. Enable local-loop mode on the DCE Frame Relay router.
D. Verify that the encapsulation is set to Frame Relay.

Answer: A

QUESTION NO: 548

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

QUESTION NO: 549

Refer to the exhibit. Addresses within the range 10.10.10.0/24 are not being translated to the 1.1.128.0/16 range. Which command shows if 10.10.10.0/24 are allowed inside addresses?

```
RouterA# show running-config
!
ip nat pool inside_green 1.1.128.1 1.1.255.254
ip nat inside source list 101 pool inside green
!
```

ActualTests

A. debug ip nat
B. show access-list
C. show ip nat translation
D. show ip nat statistics

Answer: B

QUESTION NO: 550

A wireless client cannot connect to an 802.11b/g BSS with a b/g wireless card. The client section of the access point does not list any active WLAN clients. What is a possible reason for this?

A. The incorrect channel is configured on the client.
B. The client's IP address is on the wrong subnet.
C. The client has an incorrect pre-shared key.
D. The SSID is configured incorrectly on the client.

Answer: D

QUESTION NO: 551

Which two features did WPAv1 add to address the inherent weaknesses found in WEP? (Choose two.)

A. a stronger encryption algorithm
B. key mixing using temporal keys
C. shared key authentication
D. a shorter initialization vector
E. per frame sequence counters

Answer: B,E

QUESTION NO: 552

Which two wireless encryption methods are based on the RC4 encryption algorithm? (Choose two.)

A. WEP
B. CCKM
C. AES
D. TKIP
E. CCMP

Answer: A,D

QUESTION NO: 553

What are two characteristics of RIPv2? (Choose two.)

A. classful routing protocol
B. variable-length subnet masks
C. broadcast addressing
D. manual route summarization

E. uses SPF algorithm to compute path

Answer: B,D

QUESTION NO: 554

Which two Ethernet fiber-optic modes support distances of greater than 550 meters?

A. 1000BASE-CX
B. 100BASE-FX
C. 1000BASE-LX
D. 1000BASE-SX
E. 1000BASE-ZX

Answer: C,E

QUESTION NO: 555

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

QUESTION NO: 556

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

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

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

Answer: C

QUESTION NO: 557

Refer to the exhibit. Which rule does the DHCP server use when there is an IP address conflict?

```
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
```


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 byPing is removed from the pool.
E. The IP will be shown, even after the conflict is resolved.

Answer: A

QUESTION NO: 558

Refer to the exhibit. You are connected to the router as user Mike. Which command allows you to see output from the OSPF debug command?

```
Router#show users
    Line       User       Host(s)              Idle       Location
*322 vty 0     Mike       idle                 00:00:00   laptop

  Interface    User               Mode         Idle     Peer Address

Router#debug ip ospf events
OSPF events debugging is on                                  ActualTests
Router#
```

A. terminal monitor
B. show debugging
C. show sessions
D. show ip ospf interface

Answer: A

QUESTION NO: 559

Refer to the exhibit. If number 2 is selected from the setup script, what happens when the user runs setup from a privileged prompt?

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:                                    ActualTests
```

A. Setup is additive and any changes will be added to the config script.
B. Setup effectively starts the configuration over as if the router was booted for the first time.
C. Setup will not run if an enable secret password exists on the router.
D. Setup will not run, because it is only viable when no configuration exists on the router.

Answer: A

QUESTION NO: 560

Refer to the exhibit. Which (config-router) command will allow the network represented on the interface to be advertised by RIP?

```
router rip
 version 2
 no auto-summary
!
interface ethernet0
 ip address 10.12.0.1 255.255.255.0
```

A. redistribute ethernet0
B. network ethernet0
C. redistribute 10.12.0.0
D. network 10.12.0.0

Answer: D

QUESTION NO: 561

Refer to the exhibit. What information can be gathered from the output?

```
RouterA#debug ip rip
RIP protocol debugging is on

00:34:32: RIP: sending v2 flash update to 224.0.0.9 via FastEthernet0/0 (172.16.1.1)
00:34:32: RIP: build flash update entries
00:34:32:       10.10.1.0/24 via 0.0.0.0, metric 1, tag 0
00:34:32: RIP: sending v2 flash update to 224.0.0.9 via Loopback0 (10.10.1.1)
00:34:32: RIP: build flash update entries
00:34:32:       10.0.0.0/8 via 0.0.0.0, metric 2, tag 0
00:34:32:       172.16.1.0/24 via 0.0.0.0, metric 1, tag 0
00:34:32: RIP: ignored v2 packet from 10.10.1.1 (sourced from one of our addresses)
00:34:33: RIP: received v2 update from 172.16.1.2 on FastEthernet0/0
00:34:33:      10.0.0.0/8 via 0.0.0.0 in 1 hops
00:34:44: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0 (172.16.1.1)
00:34:44: RIP: build update entries
00:34:44:       10.10.1.0/24 via 0.0.0.0, metric 1, tag 0
                                                        ActualTests
```

A. One router is running RIPv1.
B. RIP neighbor is 224.0.0.9.
C. The network contains a loop.
D. Network 10.10.1.0 is reachable.

Answer: D

QUESTION NO: 562

Refer to the exhibit. What type of connection would be supported by the cable diagram shown?

Pin Number	Color	Function	Pin	Color	Function
1	White/Green	TX+	1	White/Green	TX+
2	Green	TX-	2	Green	TX-
3	White/Orange	RX+	3	White/Orange	RX+
6	Orange	RX-	6	Orange	RX-

A. PC to router
B. PC to switch

C. server to router
D. router to router

Answer: B

QUESTION NO: 563

Refer to the exhibit. What type of connection would be supported by the cable diagram shown?

Pin Number	Color	Function	Pin	Color	Function
1	White/Green	TX+	3	Orange	RX+
2	Green	TX-	6	White/Orange	RX-
3	White/Orange	RX+	1	Green	TX+
6	Orange	RX-	2	White/Green	TX-

A. PC to router
B. PC to switch
C. server to switch
D. switch to router

Answer: A

QUESTION NO: 564

Refer to the exhibit. What can be determined about the router from the console output?

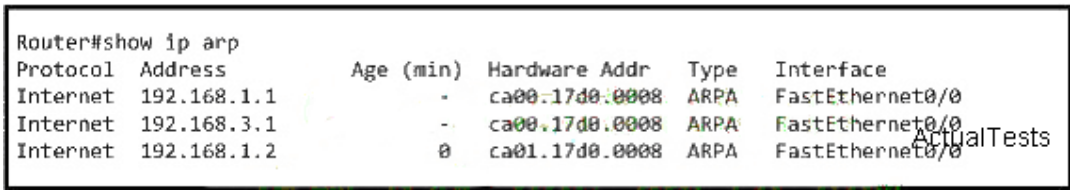
```
1 FastEthernet/IEEE 802.3 interface(s)
125K bytes of non-volatile configuration memory.

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]:
```

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

QUESTION NO: 565

Refer to the exhibit. What can be determined from the output?

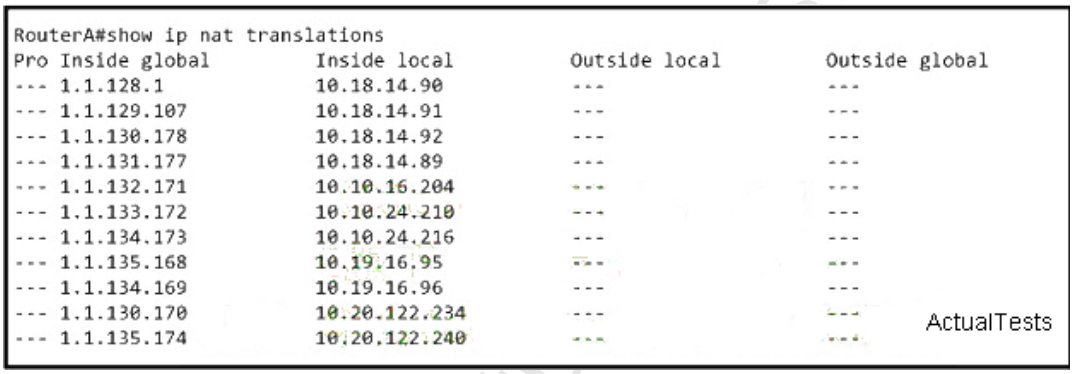


A. 192.168.1.2 is local to the router.
B. 192.168.3.1 is local to the router.
C. 192.168.1.2 will age out in less than 1 minute.
D. 192.168.3.1 has aged out and is marked for deletion.

Answer: B

QUESTION NO: 566

Refer to the exhibit. Which command would allow the translations to be created on the router?

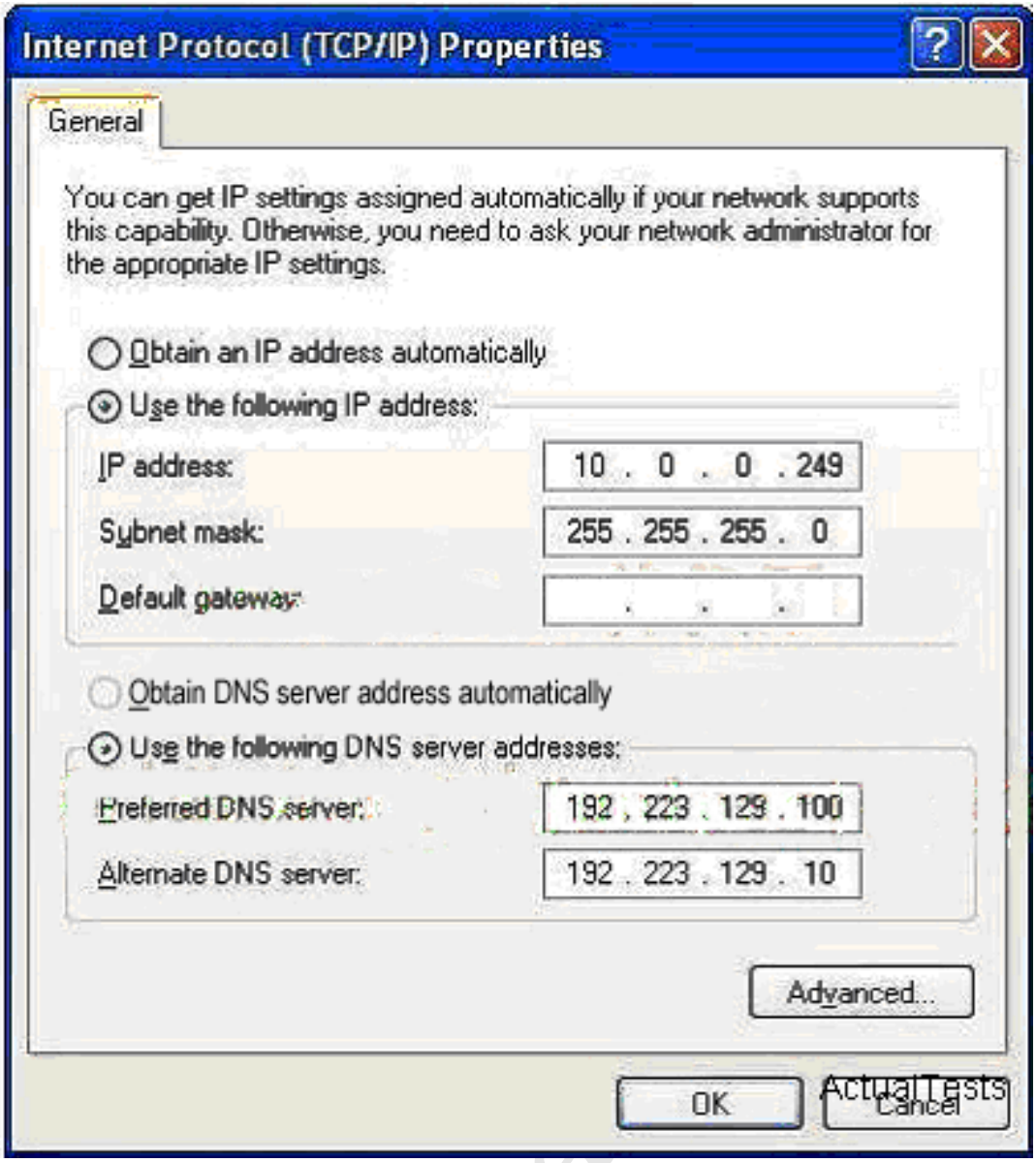


A. ip nat pool mynats 1.1.128.1 1.1.135.254 prefix-length 19
B. ip nat outside mynats 1.1.128.1 1.1.135.254 prefix-length 19
C. ip nat pool mynats 1.1.128.1 1.1.135.254 prefix-length 18
D. ip nat outside mynats 1.1.128.1 1.1.135.254 prefix-length 18

Answer: A

QUESTION NO: 567

Refer to the exhibit. Which value will be configured for Default Gateway of the Local Area Connection?

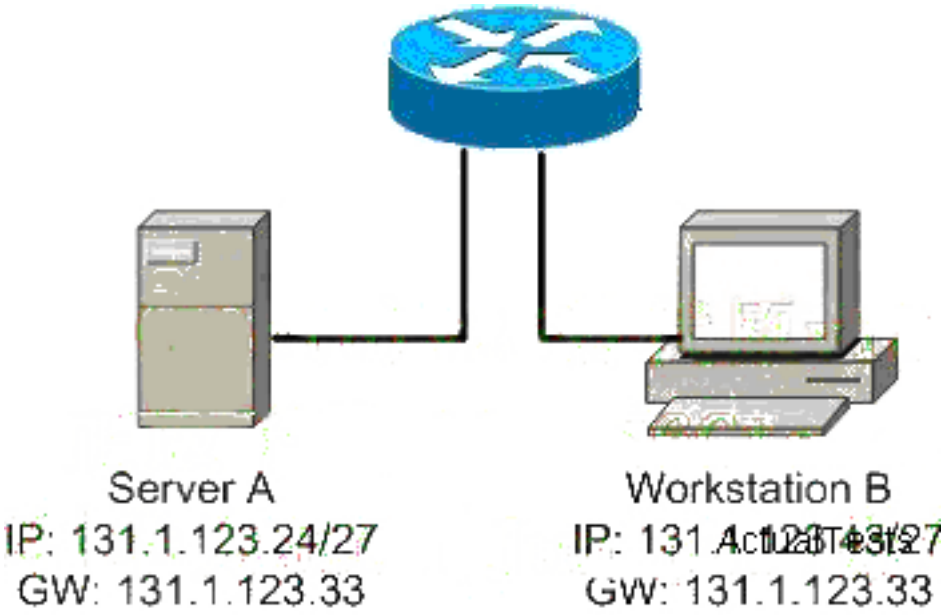


A. 10.0.0.0
B. 10.0.0.254
C. 192.223.129.0
D. 192.223.129.254

Answer: B

QUESTION NO: 568

Refer to the exhibit. The user at Workstation B reports that Server A cannot be reached. What is preventing Workstation B from reaching Server A?



A. The IP address for Server A is a broadcast address.
B. The IP address for Workstation B is a subnet address.
C. The gateway for Workstation B is not on the same subnet.
D. The gateway for Server A is not on the same subnet.

Answer: D

QUESTION NO: 569

Refer to the exhibit. What does the (*) represent in the output?

```
02:16:29: NAT: s=10.10.0.2->1.2.4.2, d=1.2.4.1 [51607]
02:16:29: NAT: s=1.2.4.1, d=1.2.4.2->10.10.0.2 [55227]
02:16:29: NAT*: s=10.10.0.2->1.2.4.2, d=1.2.4.1 [51608]
02:16:29: NAT*: s=10.10.0.2->1.2.4.2, d=1.2.4.1 [51609]
```

ActualTests

A. Packet is destined for a local interface to the router.
B. Packet was translated, but no response was received from the distant device.
C. Packet was not translated, because no additional ports are available.
D. Packet was translated and fast switched to the destination.

Answer: D

QUESTION NO: 570

Refer to the exhibit. What command sequence will enable PAT from the inside to outside network?

```
ip nat pool isp-net 1.2.4.10 1.2.4.240 netmask 255.255.255.0
!
interface ethernet 1
  description ISP Connection
  ip address 1.2.4.2 255.255.255.0
  ip nat outside
!
Interface ethernet 0
  description Ethernet to Firewall eth0
  ip address 10.10.0.1 255.255.255.0
  ip nat inside
!                                                    ActualTests
access-list 1 permit 10.0.0.0 0.255.255.255
```

A. (config) ip nat pool isp-net 1.2.4.2 netmask 255.255.255.0 overload
B. (config-if) ip nat outside overload
C. (config) ip nat inside source list 1 interface ethernet1 overload
D. (config-if) ip nat inside overload

Answer: C

QUESTION NO: 571

Refer to the exhibit. What will happen to HTTP traffic coming from the Internet that is destined for 172.16.12.10 if the traffic is processed by this ACL?

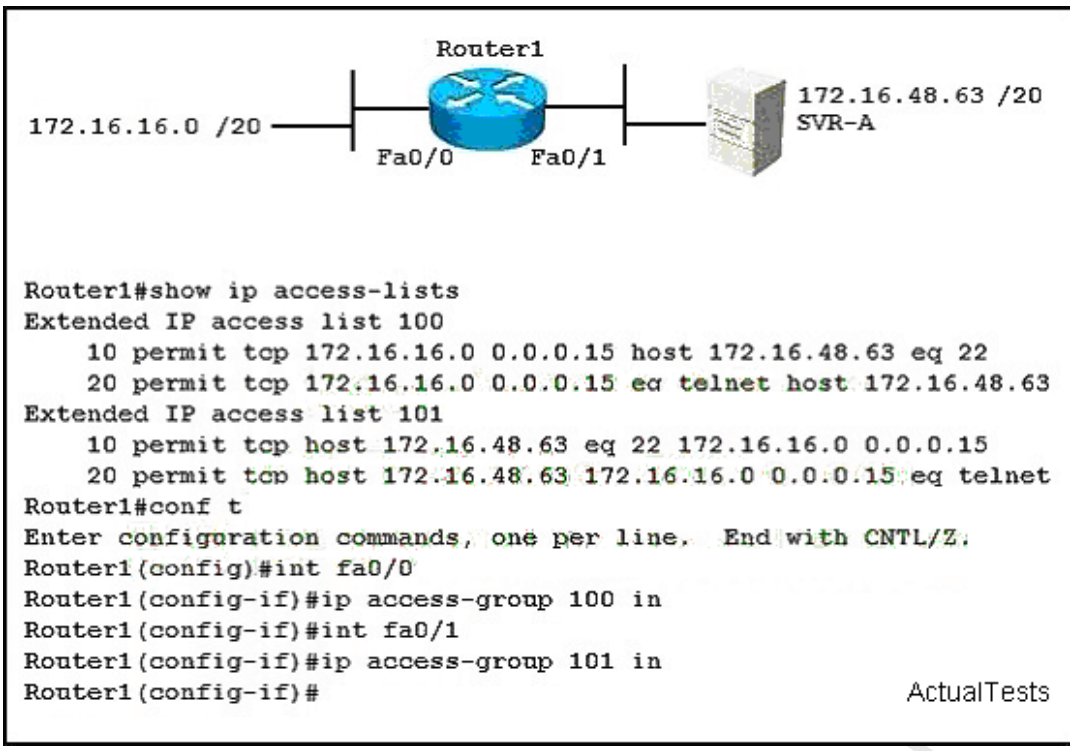
```
router#show access-lists
Extended IP access list 110
    10 deny tcp 172.16.0.0 0.0.255.255 any eq telnet
    20 deny tcp 172.16.0.0 0.0.255.255 any eq smtp
    30 deny tcp 172.16.0.0 0.0.255.255 any eq http
    40 permit tcp 172.16.0.0 0.0.255.255 any  ActualTests
```

A. Traffic will be dropped per line 30 of the ACL.
B. Traffic will be accepted per line 40 of the ACL.
C. Traffic will be dropped, because of the implicit deny all at the end of the ACL.
D. Traffic will be accepted, because the source address is not covered by the ACL.

Answer: C

QUESTION NO: 572

Refer to the exhibit. Which statement describes the effect that the Router1 configuration has on devices in the 172.16.16.0 subnet when they try to connect to SVR-A using Telnet or SSH?



A. Devices will not be able to use Telnet or SSH.

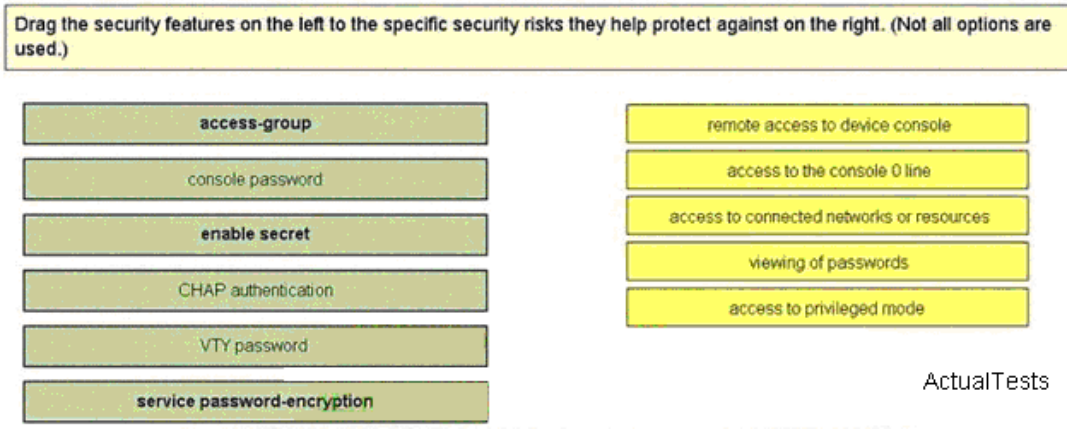
B. Devices will be able to use SSH, but not Telnet.

C. Devices will be able to use Telnet, but not SSH.

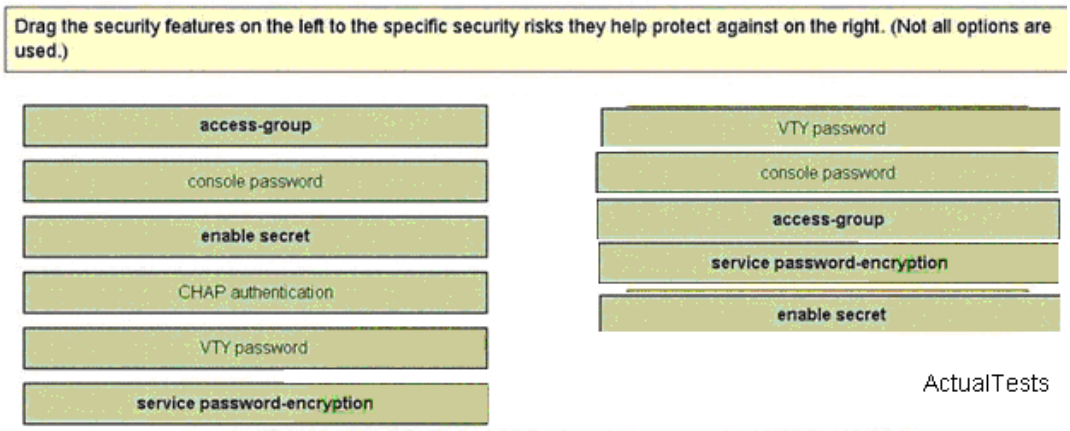
D. Devices will be able to use Telnet and SSH.

Answer: B

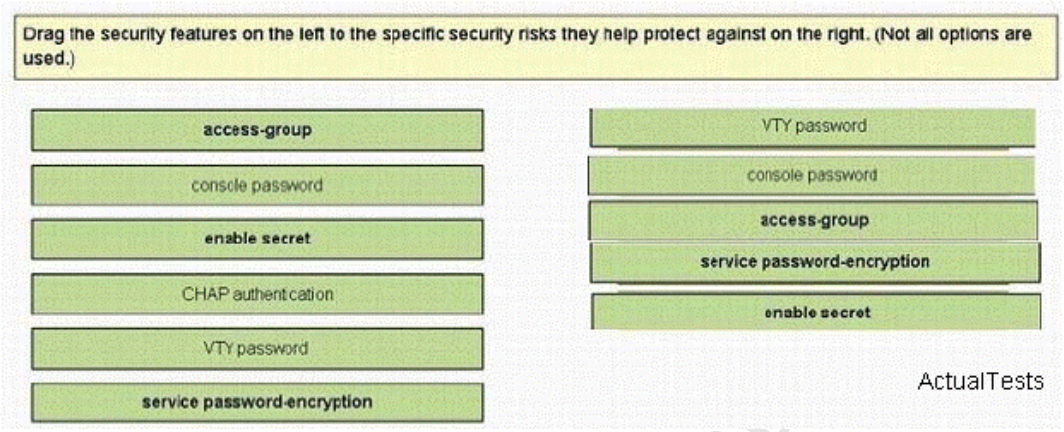
QUESTION NO: 573 DRAG DROP



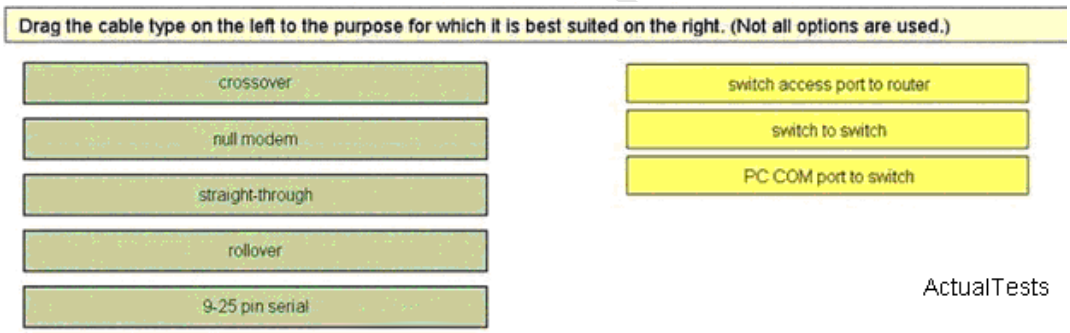
Answer:



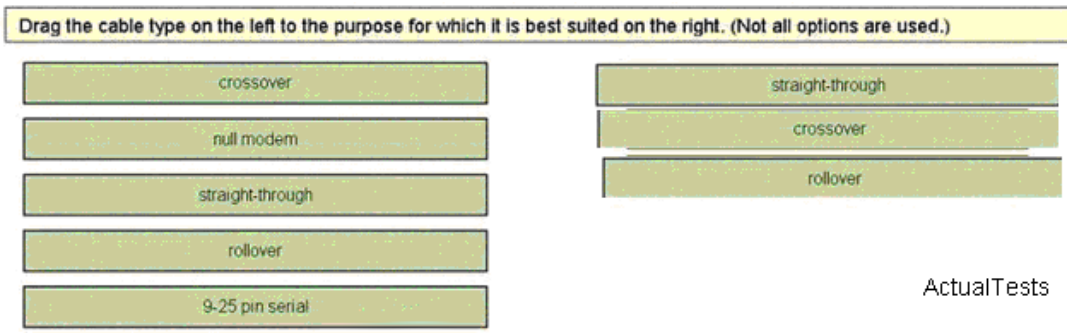
Explanation:



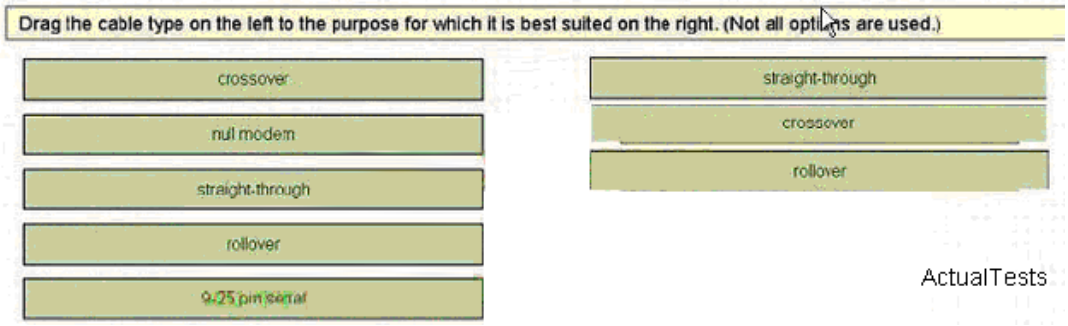
QUESTION NO: 574 DRAG DROP



Answer:



Explanation:



QUESTION NO: 575

Refer to the exhibit. * Missing*
Based on the output from RouterA, what metric will RouterB install in its routing table to reach network 192.168.3.0 if EIGRP is the only routing process in use in the network?

A. 2681856
B. 2172416
C. 28160
D. 2169856

Answer: B

QUESTION NO: 576

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

A. It designates VLAN 999 for untagged traffic.
B. It blocks VLAN 1 traffic from passing on the trunk.
C. It creates a VLAN 99 interface.
D. It designates VLAN 1 as the default for all unknown tagged traffic.

Answer: A

Explanation:
Native VLAN is the VLAN that you configure on the Catalyst interface before you configure the trunking on that interface. By default, all interfaces are in VLAN 1. Therefore, VLAN 1 is the native VLAN that you can change. On an 802.1Q trunk, all VLAN packets except the native VLAN are tagged. You must configure the native VLAN in the same way on each side of the trunk. Then, the router or switch can recognize to which VLAN a frame belongs when the router or switch receives a frame with no tag.

To configure the native VLAN use the following command. Cat2950(config-if)# switchport trunk

native vlan 10

QUESTION NO: 577

Which of the following are valid VLAN Trunk Protocols over Fast Ethernet? [Select 2].

A. Inter-Switch Link
B. 802.10
C. LANE
D. 802.1Q

Answer: A,D

QUESTION NO: 578

Which of the following is not a valid VTP mode?

A. Server
B. Client
C. Transparent
D. Hybrid

Answer: D

QUESTION NO: 579

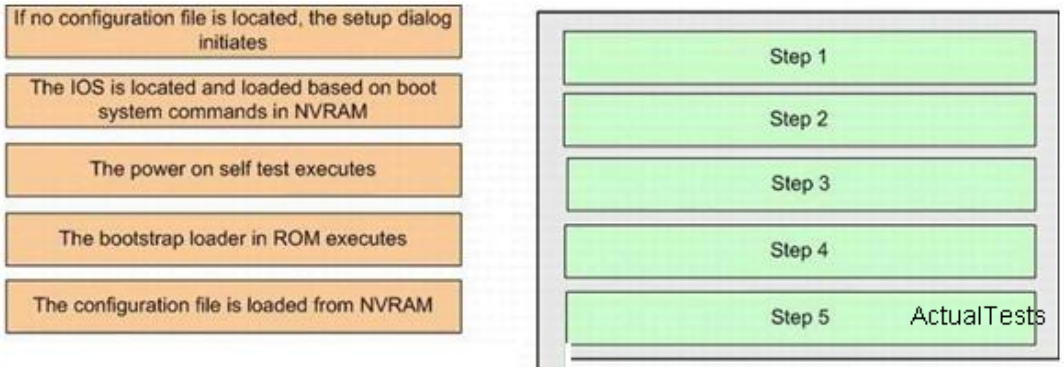
Given a subnet mask of 255.255.255.224, which of the following addresses can be assigned to network hosts? (Choose three.)

A. 15.234.118.63
B. 92.11.178.93
C. 134.178.18.56
D. 192.168.16.87
E. 201.45.116.159
F. 217.63.12.192

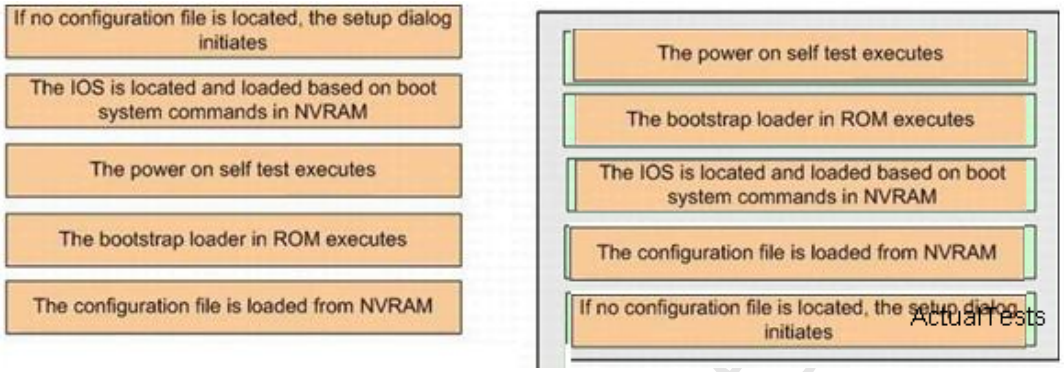
Answer: B,C,D

QUESTION NO: 580 DRAG DROP

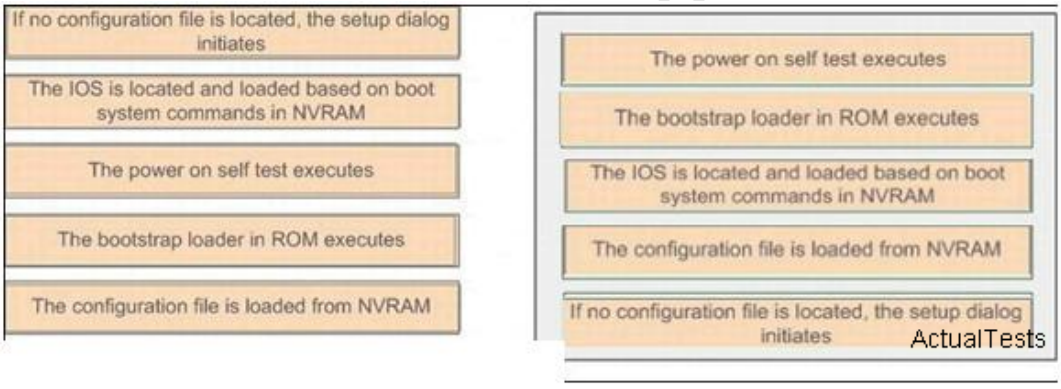
The left describes boot sequence, while the right describes the orders. Drag the items on the left to the proper locations.



Answer:

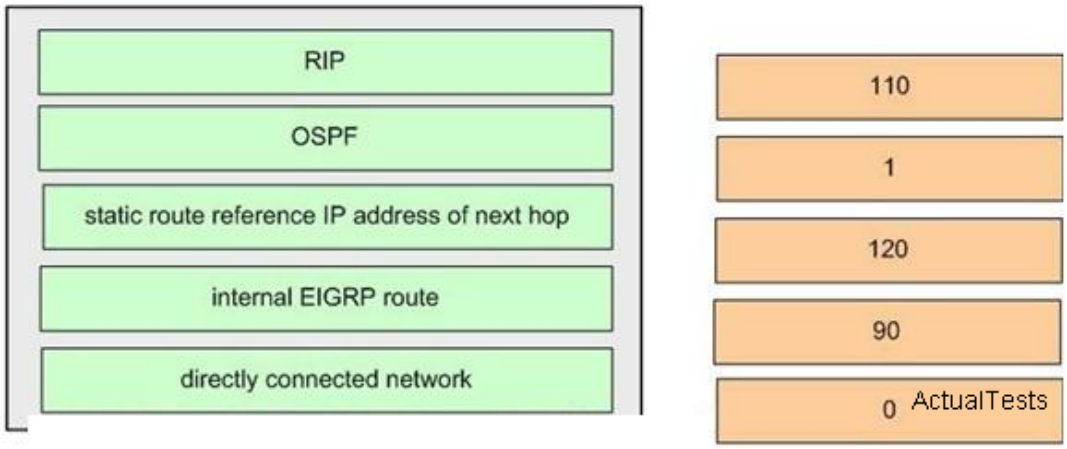


Explanation:



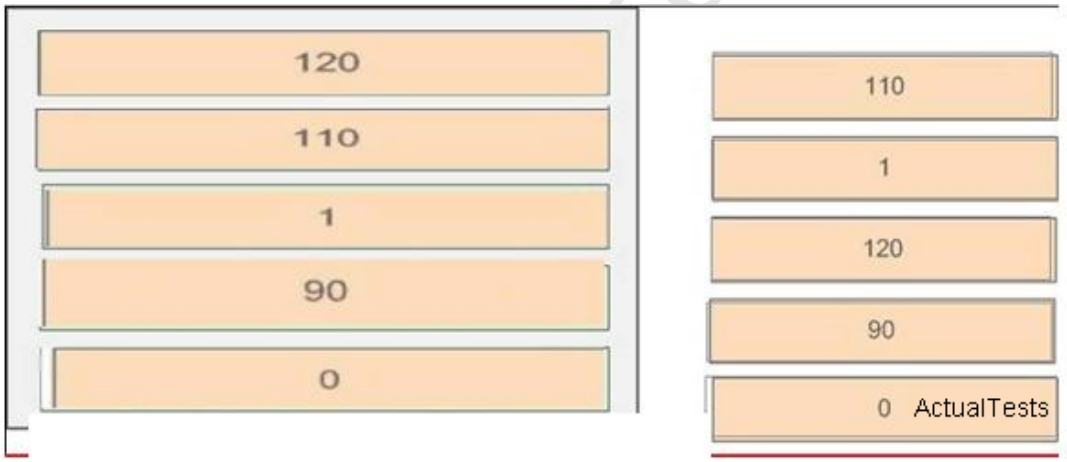
QUESTION NO: 581 DRAG DROP

The left provides some routing protocols, while the right gives several Cisco default administrator distances. Drag the items on the right to the proper locations.



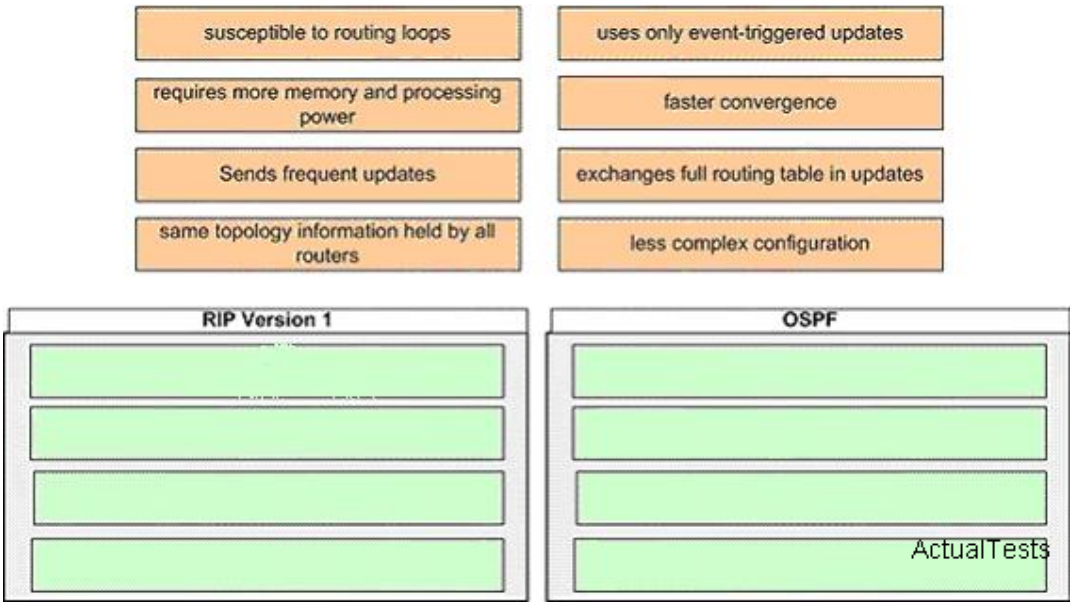
Answer:

Explanation:

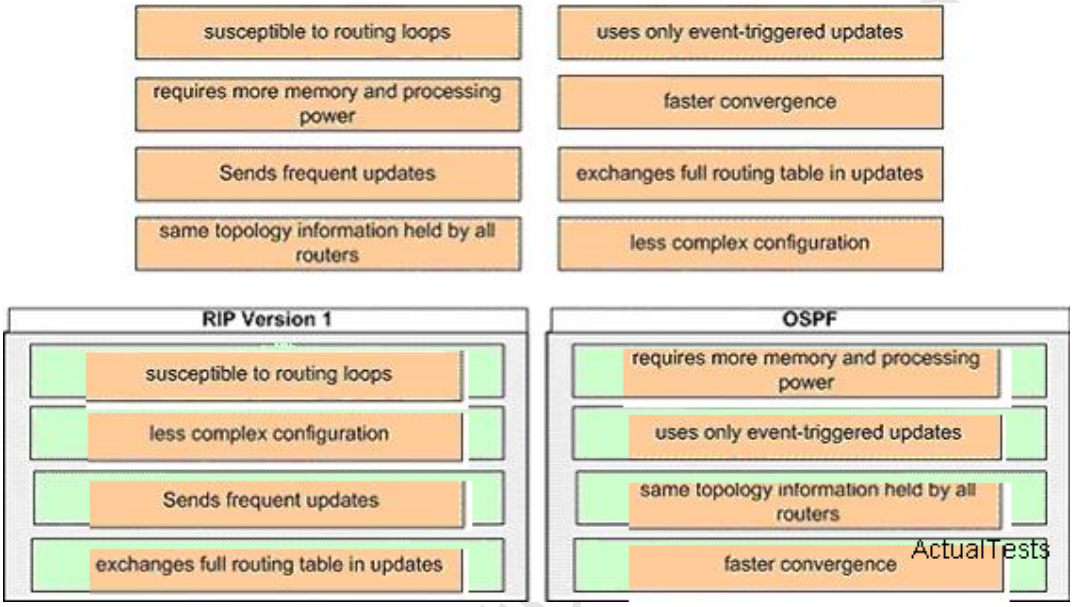


QUESTION NO: 582 DRAG DROP

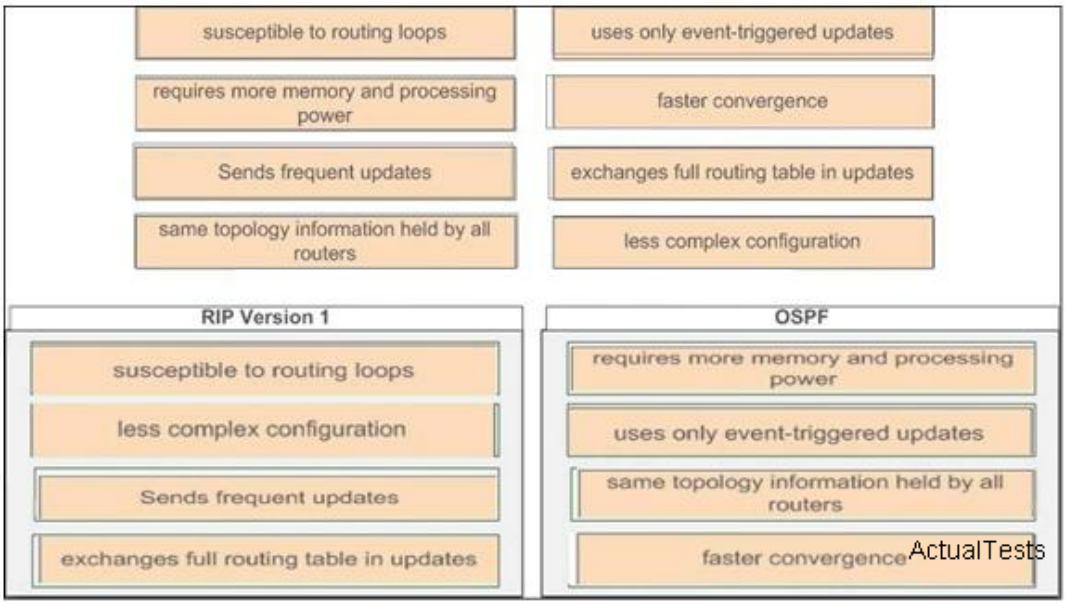
The above describes some features, while the below describes some routing protocols. Drag the above items to the proper locations.



Answer:

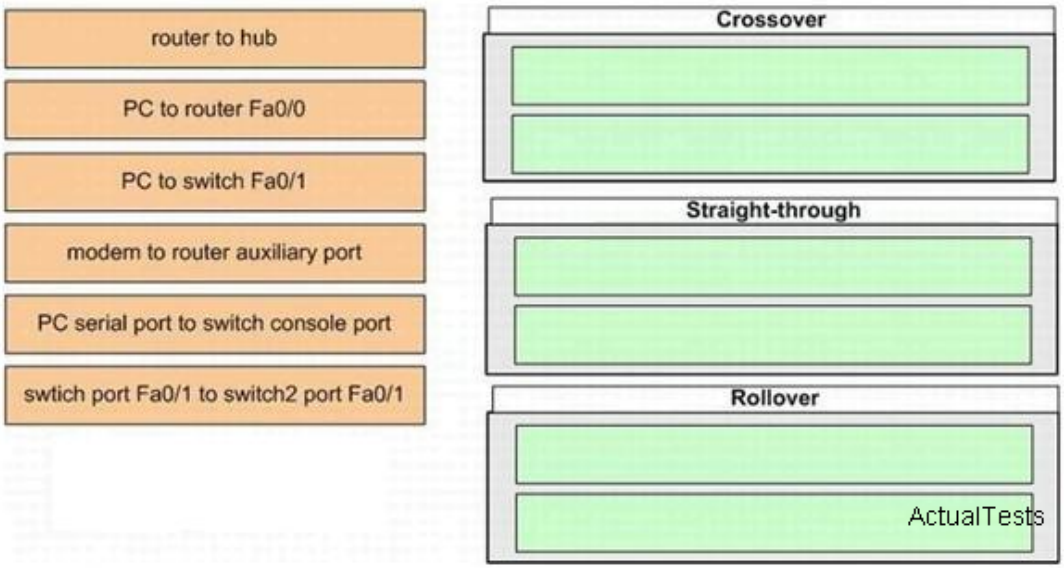


Explanation:

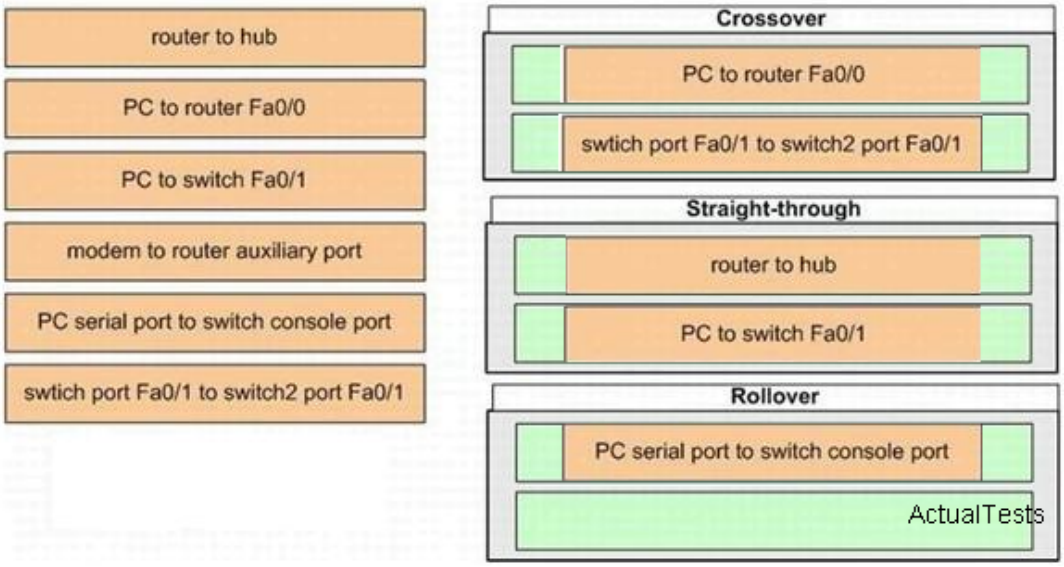


QUESTION NO: 583 DRAG DROP

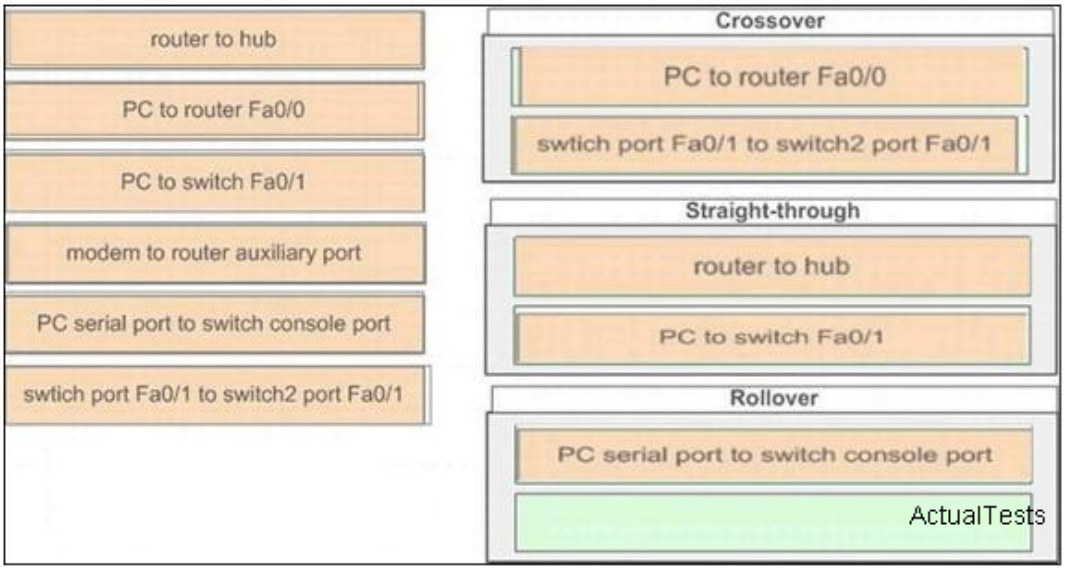
The left describes some types of connections, while the right describes some types of cables. Drag the items on the left to the proper locations.



Answer:

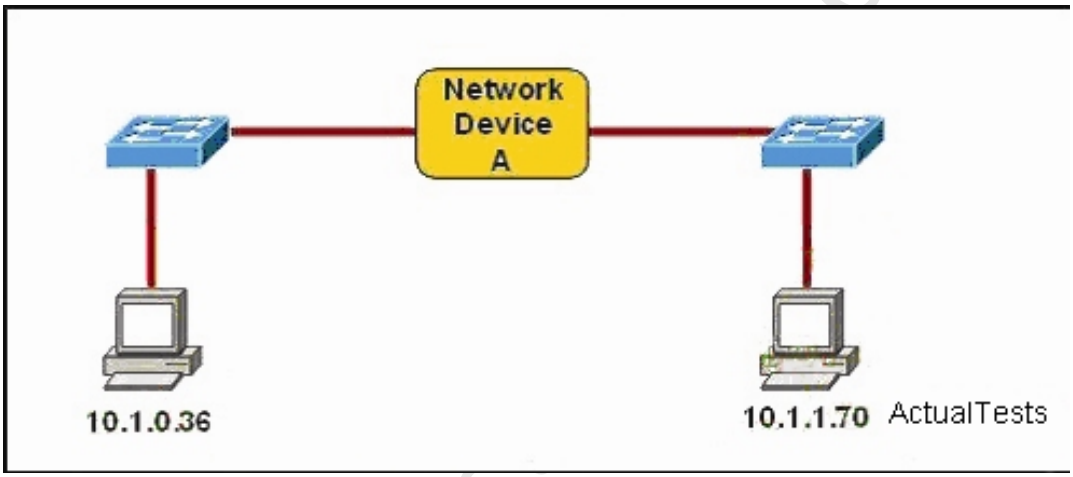


Explanation:



QUESTION NO: 584

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

QUESTION NO: 585

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

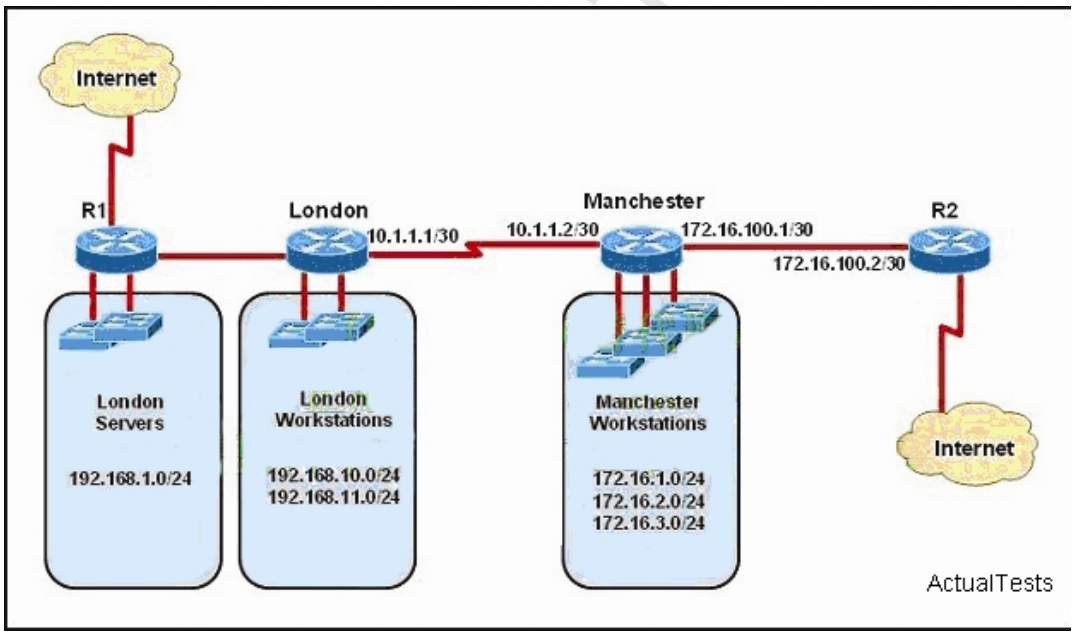
```
Switch# show spanning-tree interface fastethernet 0/10
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 19        128.2    P2p
VLAN0002         Altn BLK 19        128.2    P2p
VLAN0003       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

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

QUESTION NO: 586

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 onLondon to advertise all routes to Manchester.
B. Configure a dynamic routing protocol onLondon to advertise summarized routes to Manchester.
C. Configure a dynamic routing protocol onManchester to advertise a default route to the London router.

D. Configure a static default route onLondon with a next hop of 10.1.1.1.
E. Configure a static route onLondon 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 toLondon.

Answer: E

QUESTION NO: 587

A host is attempting to send data to another host on a different network. What is the first action that the sending host will take?

A. Drop the data.
B. Send the data frames to the default gateway.
C. Create an ARP request to get a MAC address for the receiving host.
D. Send a TCP SYN and wait for the SYN ACK with the IP address of the receiving host.

Answer: C

QUESTION NO: 588

Refer to the exhibit. Which statement is true?

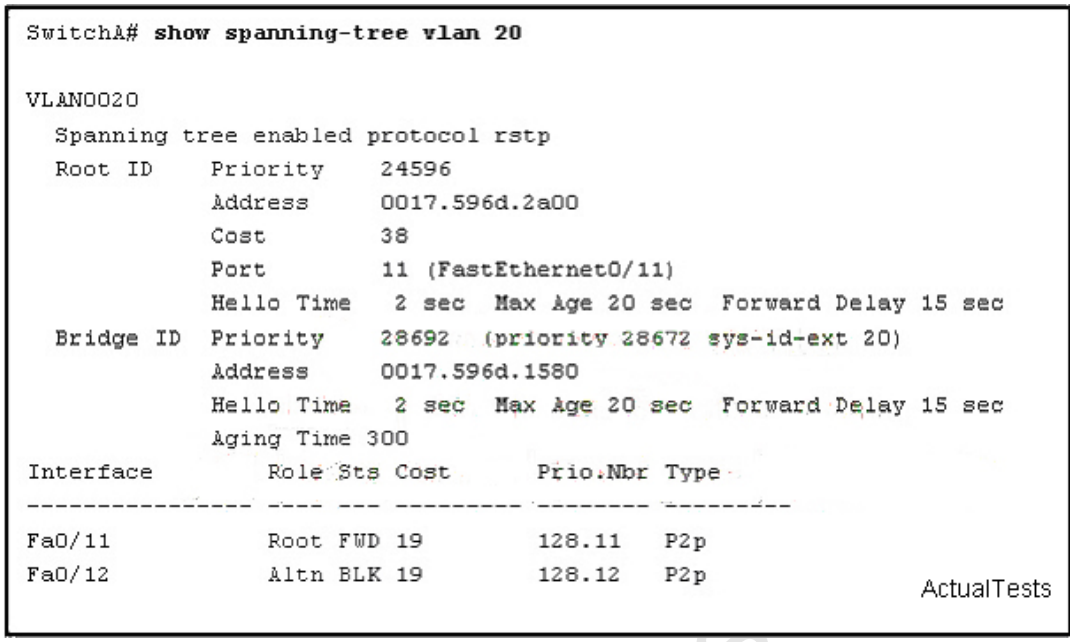
```
SwitchA# show spanning-tree vlan 20

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
                                                    ActualTests
```

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

QUESTION NO: 589

Refer to the exhibit. A system administrator installed a new switch using a script to configure it. IP connectivity was tested using pings to SwitchB. Later attempts to access NewSwitch using Telnet from SwitchA failed. Which statement is true?



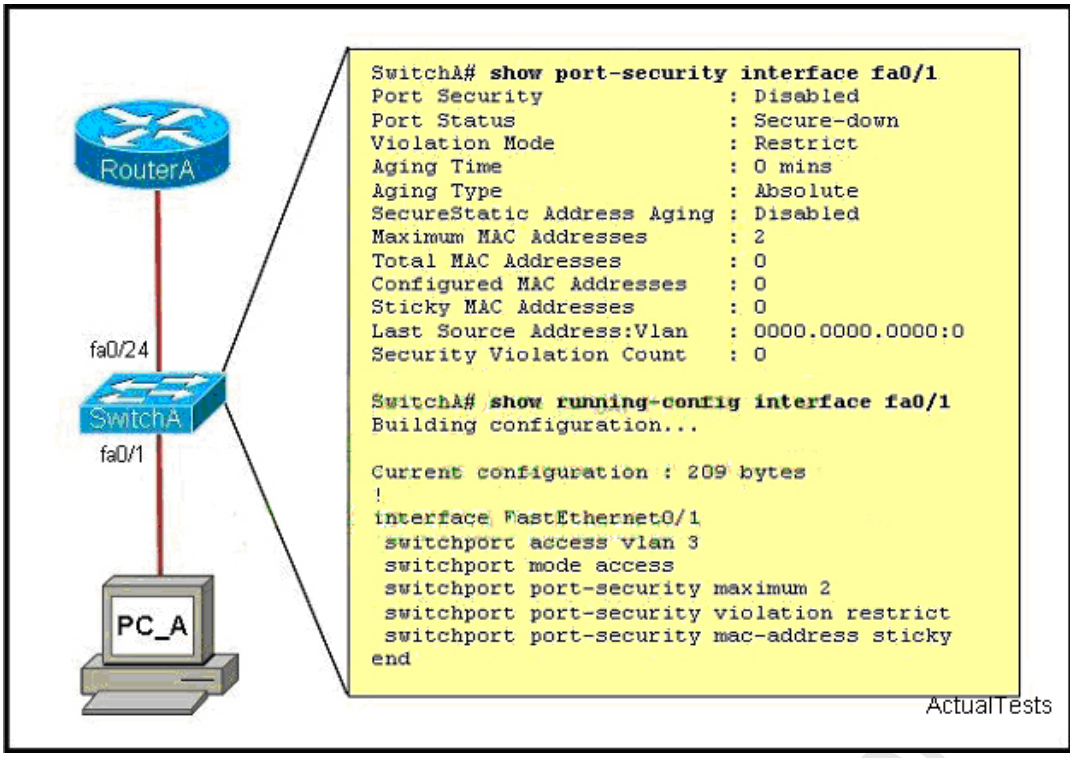
A. Executing password recovery is required.
B. The virtual terminal lines are misconfigured.
C. Use Telnet to connect to RouterA and then to NewSwitch to correct the error.
D. Power cycle of NewSwitch will return it to a default configuration.

Answer: C

QUESTION NO: 590

Refer to the exhibit. 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.)

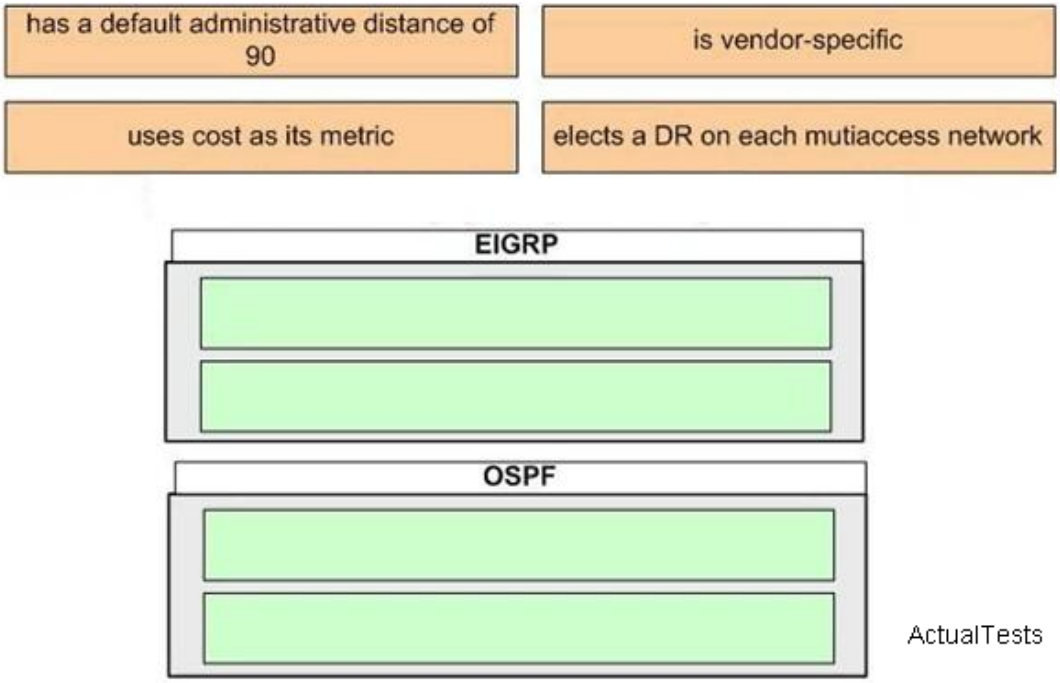


A. Port security needs to be globally enabled.
B. Port security needs to be enabled on the interface.
C. Port security needs to be configured to shut down the interface in the event of a violation.
D. Port security needs to be configured to allow only one learned MAC address.
E. Port security interface 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.

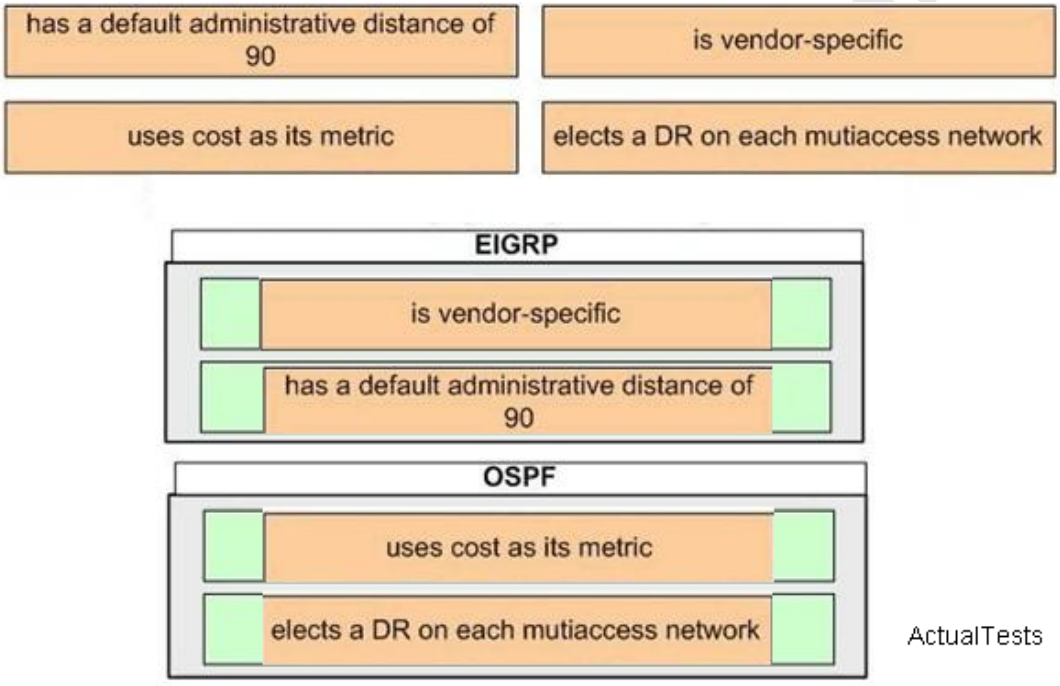
Answer: B,D

QUESTION NO: 591 DRAG DROP

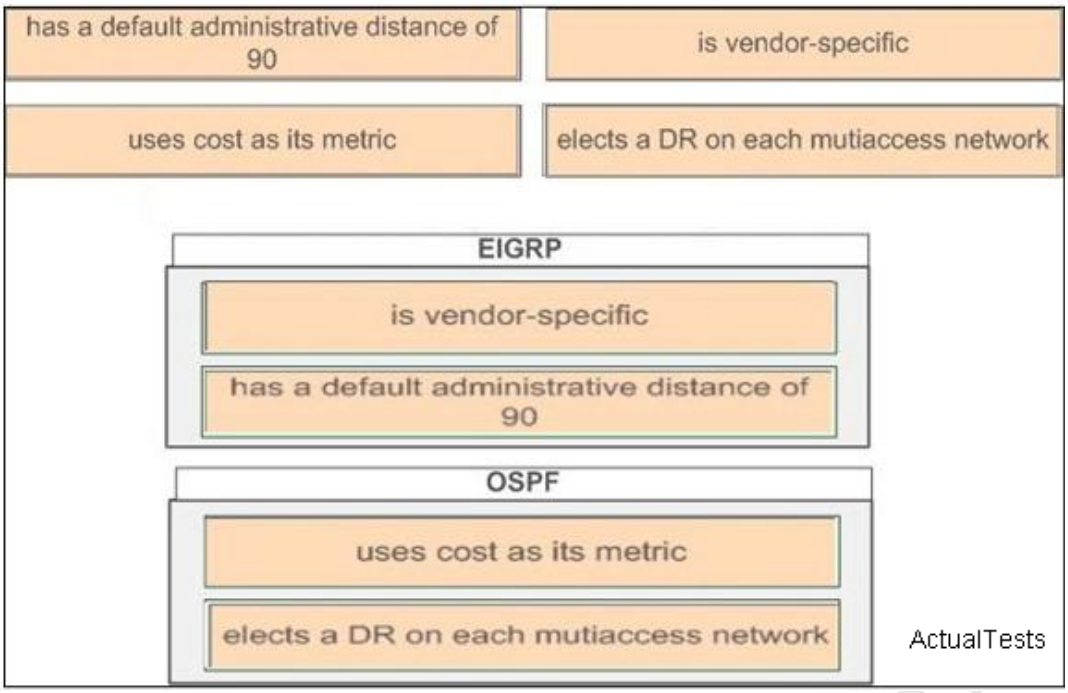
The above provides some descriptions, while the below provides some routing protocols. Drag the above items to the proper locations.



Answer:

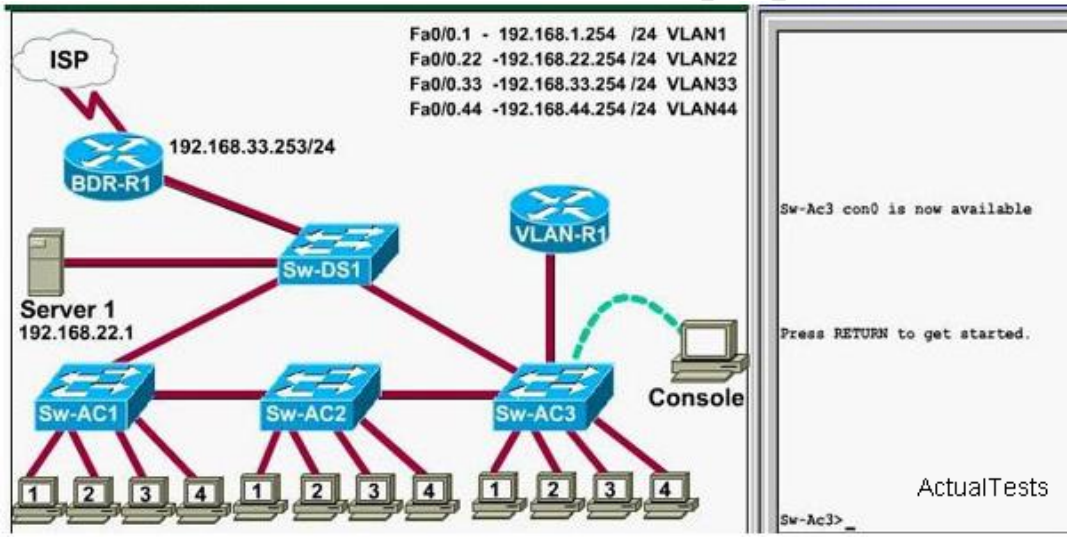


Explanation:



QUESTION NO: 592

This task requires you to use the CLI of Sw-AC3 to answer following question.



What interface did Sw-AC3 associate with source MAC address 0010.5a0c.ffba ?

A. Fa0/1
B. Fa0/3
C. Fa0/6
D. Fa0/8
E. Fa0/9
F. Fa0/12

Answer: D

Explanation:

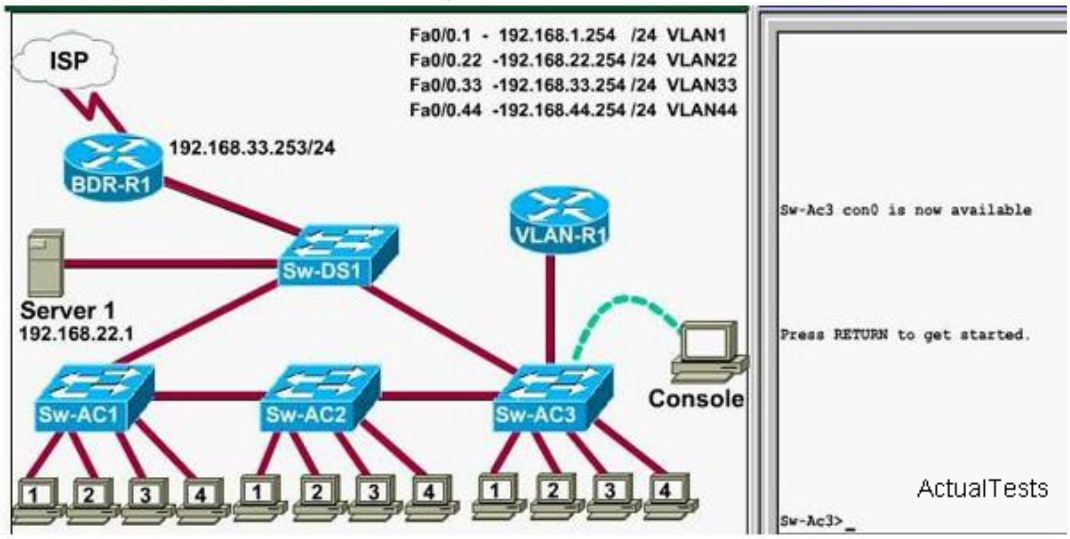
to find out which interface associated with a given MAC address, use the show mac-address-table command. It shows the learned MAC addresses and their associated interfaces. After entering this command, you will see a MAC address table like this:

```
Sw-Ac3#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.2485.8900    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0009.e8b2.c28c    DYNAMIC     Fa0/12
   1    000a.b7e9.8360    DYNAMIC     Fa0/3
   1    000f.2485.8b49    DYNAMIC     Fa0/9
  22    0009.e8b2.c28c    DYNAMIC     Fa0/12
  22    000a.b7e9.8360    DYNAMIC     Fa0/3
  22    0010.5a0c.ffba    DYNAMIC     Fa0/8
  33    0009.e8b2.c28c    DYNAMIC     Fa0/12
  33    000a.b7e9.8360    DYNAMIC     Fa0/3
  33    000c.ce8d.8860    DYNAMIC     Fa0/12
  33    0010.5a0c.fd86    DYNAMIC     Fa0/6
  33    0010.5a0c.feae    DYNAMIC     Fa0/12
  33    0010.5a0c.ff9f    DYNAMIC     Fa0/1
  44    0009.e8b2.c28c    DYNAMIC     Fa0/12
--More--
```


From this table we can figure out that the MAC address 0010.5a0c.ffba is associated with interface Fa0/8

QUESTION NO: 593

This task requires you to use the CLI of Sw-AC3 to answer following question.



What ports on Sw-AC3 are operating has trunks (choose three)?

A. Fa0/1
B. Fa0/3
C. Fa0/4
D. Fa0/6
E. Fa0/9
F. Fa0/12

Answer: B,E,F

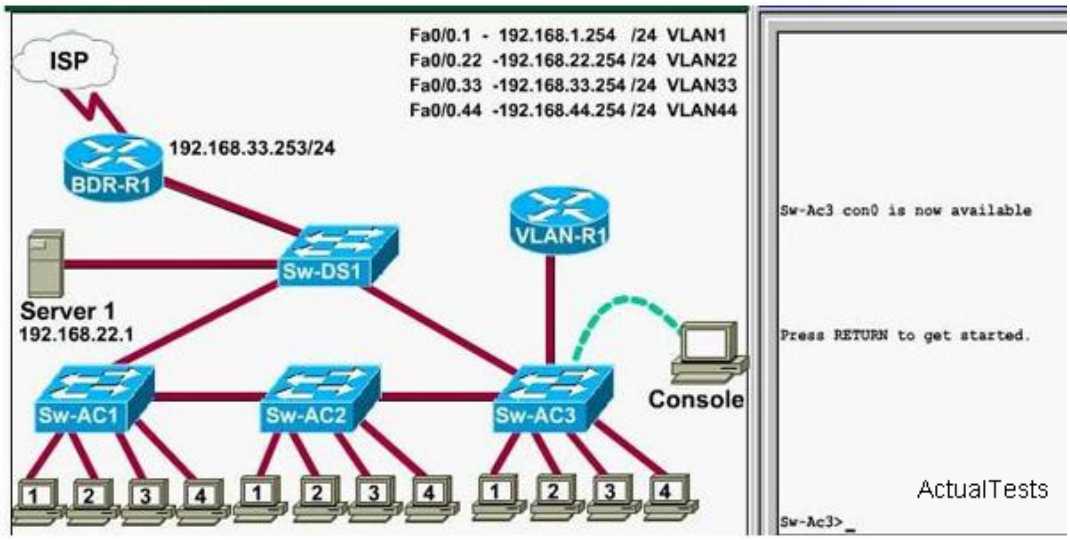
Explanation:
Use the show interface trunk command to determine the trunking status of a link and VLAN status. This command lists port, its mode, encapsulation and whether it is trunking. The image below shows how it works:

```
Sw-Ac3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1
Fa0/9       desirable    802.1q         trunking      1
Fa0/12      desirable    802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/9       1-4094
Fa0/12      1-4094

Port        Vlans allowed and active in management domain
Fa0/9       1
Fa0/12      1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/9       1
Fa0/12      1
Sw-Ac3#
```

ActualTests

QUESTION NO: 594

This task requires you to use the CLI of Sw-AC3 to answer following question.



What kind of router is VLAN-R1?

A. 1720
B. 1841
C. 2611
D. 2620

Answer: C

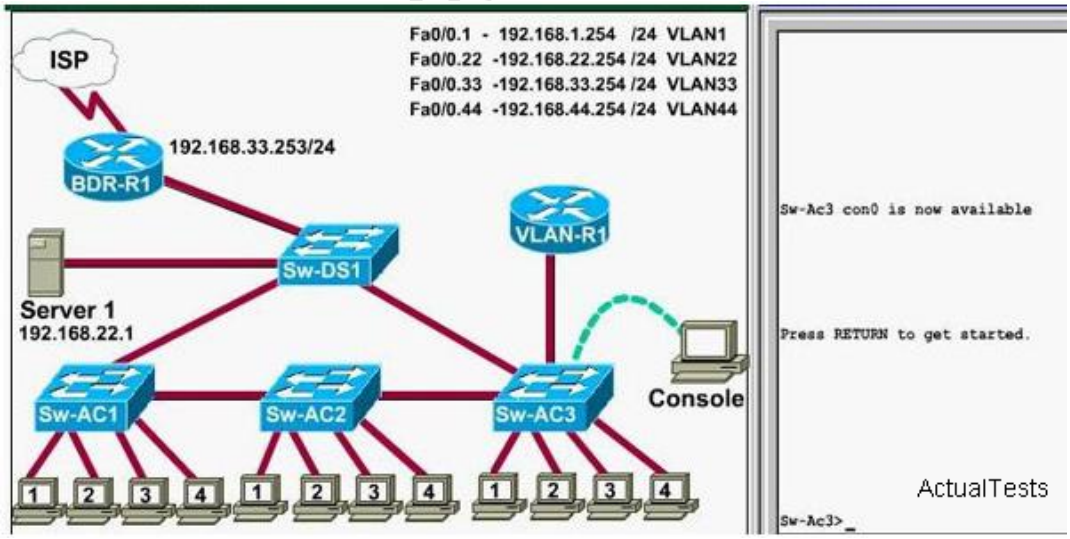
Explanation:
VLAN-R1 is the router directly connected to Sw-Ac3 switch, so we can use the show cdp neighbors command to see:
1. Neighbor Device ID : The name of the neighbor device; 2. Local Interface : The interface to which this neighbor is heard 3. Capability: Capability of this neighboring device - R for router, S for switch, H for Host etc. 4. Platform: Which type of device the neighbor is 5. Port ID: The interface of the remote neighbor you receive CDP information 6. Holdtime: Decremental hold time in seconds
Sample output of show cdp neighbors command:

```
Sw-Ac3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform     Port ID
Sw-DS1           Fas 0/12          130           S I   WS-C2950G-   Fas 0/12
Sw-AC2           Fas 0/9           176           S I   WS-C2950T-   Fas 0/9
VLAN-R1          Fas 0/3           152           R     2620         Fas 0/0.1
```

One thing I want to notice you is "Local Intrfce" in the image above refers to the local interface on the device you are running the "show cdp neighbors" command

QUESTION NO: 595 CORRECT TEXT

This task requires you to use the CLI of Sw-AC3 to answer following question.

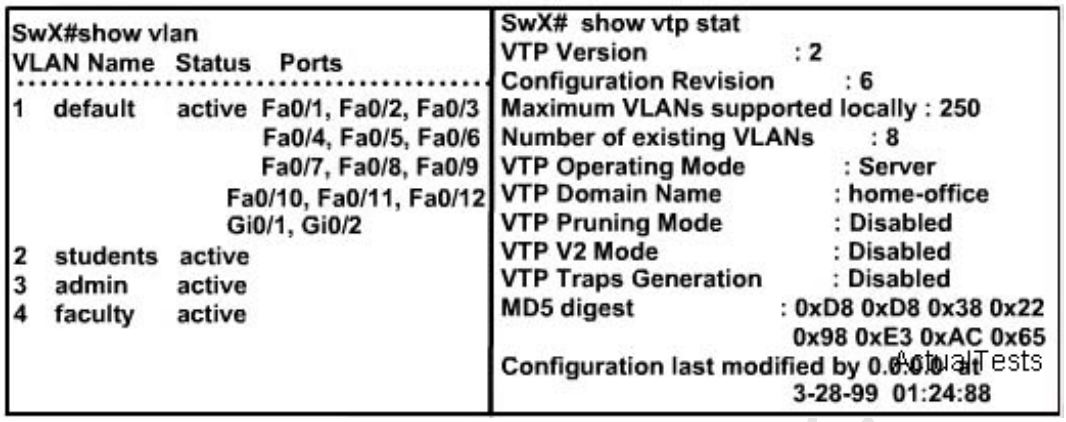


From which switch did Sw-Ac3 receive VLAN information ?

Answer: Sw-AC2

QUESTION NO: 596

Refer to the exibit, SwX was taken out of the production network for maintenance. It will be reconnected to the Fa 0/16 port of Sw-Ac3. What happens to the network when it is reconnected and a trunk exists between the two switches?



```
SwX#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
                   Gi0/1, Gi0/2
2   students   active
3   admin      active
4   faculty    active
```

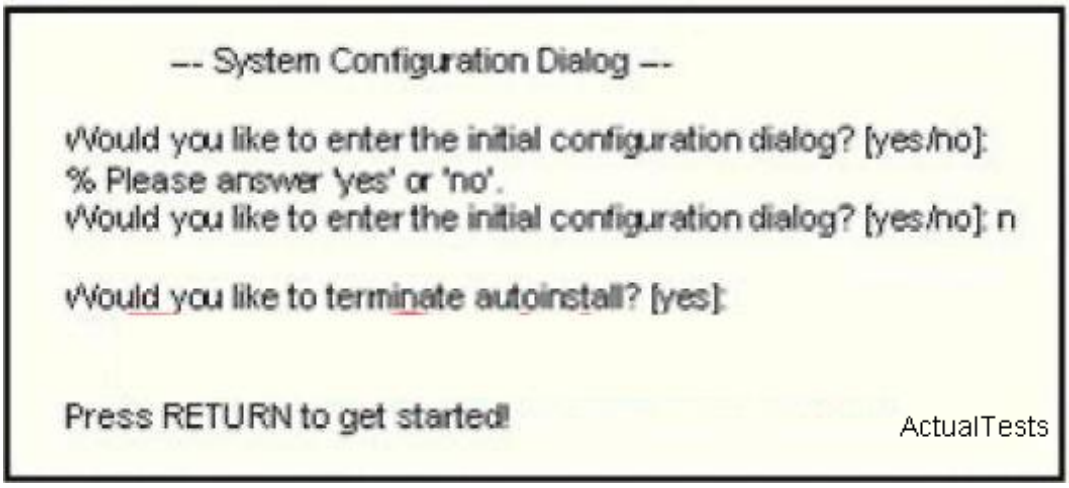
```
SwX#  show vtp stat
VTP Version                : 2
Configuration Revision     : 6
Maximum VLANs supported locally : 250
Number of existing VLANs   : 8
VTP Operating Mode         : Server
VTP Domain Name            : home-office
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xD8 0xD8 0x38 0x22
                             0x98 0xE3 0xAC 0x65
Configuration last modified by 0.0.0.0 at
                             3-28-99  01:24:88
```

A. All VLANs except the default VLAN win be removed from all switches
B. All existing switches will have the students, admin, faculty, Servers, Management, Production, and no-where VLANs
C. The VLANs Servers, Management, Production and no-where will replace the VLANs on SwX
D. The VLANs Servers, Management, Production and no-where will be removed from existing switches

Answer: D

QUESTION NO: 597

Refer to the exhibit. A network administrator configures a new router and enters the copy starup-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 0*2100.
C. The boot system flash command is missing from the configuration.
D. The configuration register is set to 0*2102.
E. The router is configured with the boot system startup command.

Answer: A

QUESTION NO: 598

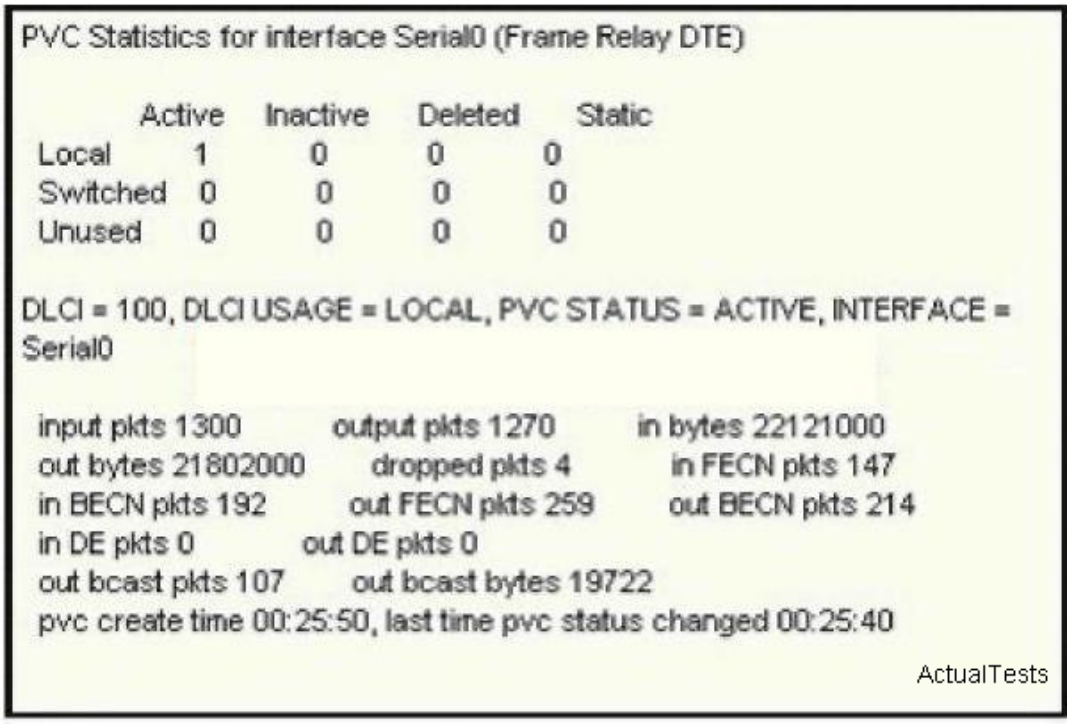
A network administrator needs to allow only one Telnet connection to a router. For anyone viewing the configuration and issuing the show run command, the password for Telnet access should be encrypted. Which set of commands will accomplish this task?

A. service password-encryption
access-listl permit 192.168.1.0.0.0.255
login
password cisco
access-class 1
B. enable password secret
Line vty 0
login
password cisco
C. service password-encryption
Line vty 0
login
password cisco
D. service password-encryption
Line vty0 4
login
password cisco

Answer: C

QUESTION NO: 599

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. Based on the partial output of the Router# show frame relay pvc command shown in the graphic, which output value indicates to the loacal router that traffic sent to the corporate site is experiencing congestion?



A. DLCI=100
B. last time PVC status changed00:25:40
C. in BECN packets 192
D. in FECN packets 147
F. in DF packets 0

Answer: C

QUESTION NO: 600

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

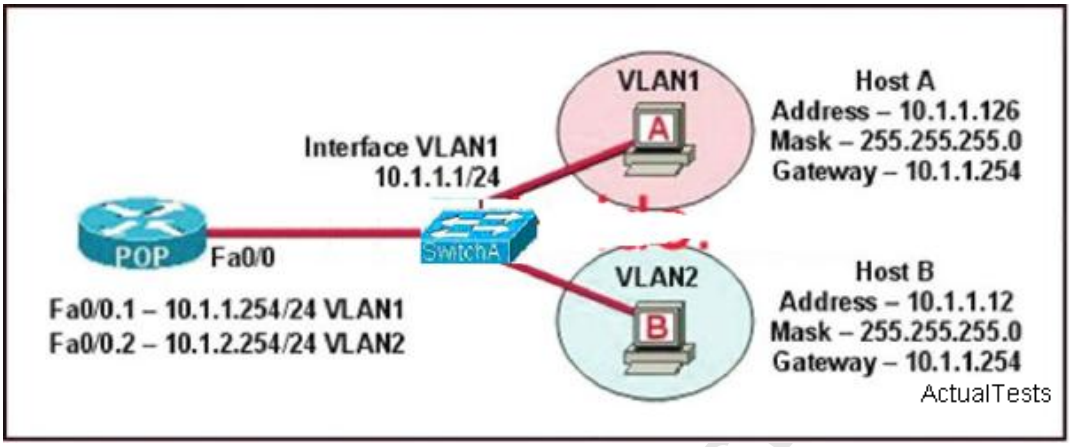
A. Addresses are allocated after a negotiation between the server and the host to determine the length of the agreement.
B. Addresses are permanently assigned so that the hosts uses the same address at all times.

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

QUESTION NO: 601

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

QUESTION NO: 602

What should be done prior to backing up an IOS image to a TFTP server? (Choose three.)

A. Make sure that the server can be reached across the network.
B. Check that authentication for TFTP access to the server is set.
C. Assure that the network server has adequate space for the IOS image.
D. Verify file naming and path requirements.
E. Make sure that the server can store binary files.
F. Adjust the TCP window size to speed up the transfer.

Answer: A,C,D

QUESTION NO: 603

Which of the following data network would you implement if you wanted a wireless network that had a relatively high data rate, but was limited to very short distances?

A. Broadband personal comm. Service (PCS)
B. Broadband circuit
C. Infrared
D. Spread spectrum

Answer: C

QUESTION NO: 604

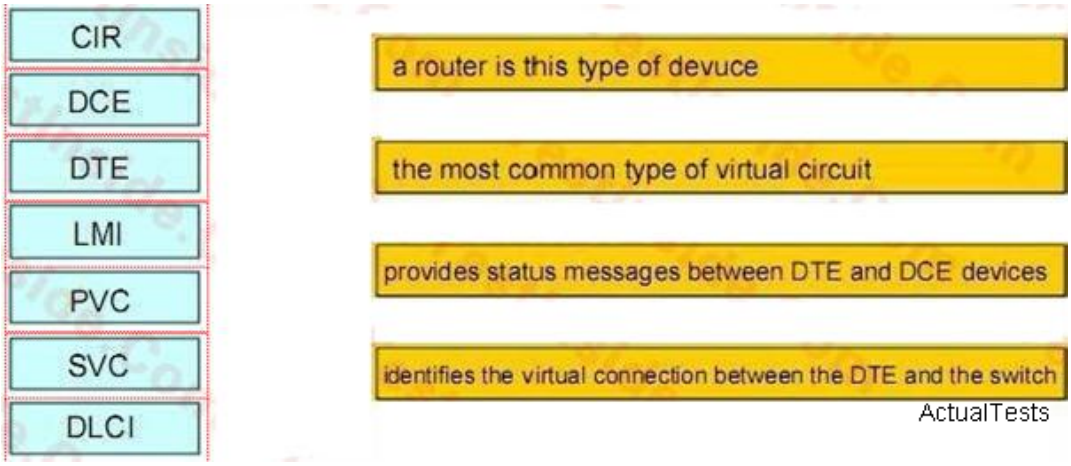
The corporate head office has a teleconferencing system that uses VOIP (voice over IP) technology. This system uses UDP as the transport for the data transmissions. If these UDP datagrams arrive at their destination out of sequence, what will happen?

A. UDP will send an ICMP Information Request to the source host.
B. UDP will pass the information in the datagrams up to the next OSI layer in the order that they arrive.
C. UDP will drop the datagrams.
D. UDP will use the sequence numbers in the datagram headers to reassemble the data in the correct order.

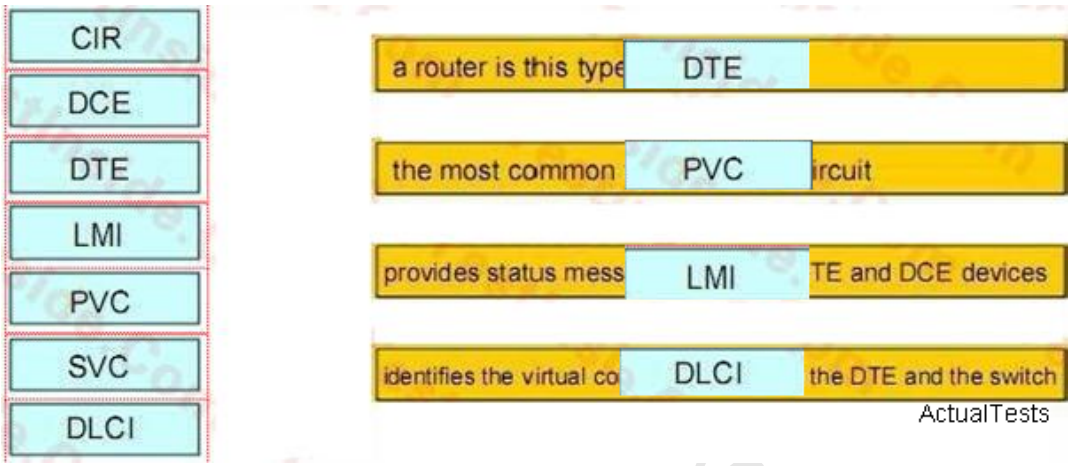
Answer: B

QUESTION NO: 605 DRAG DROP

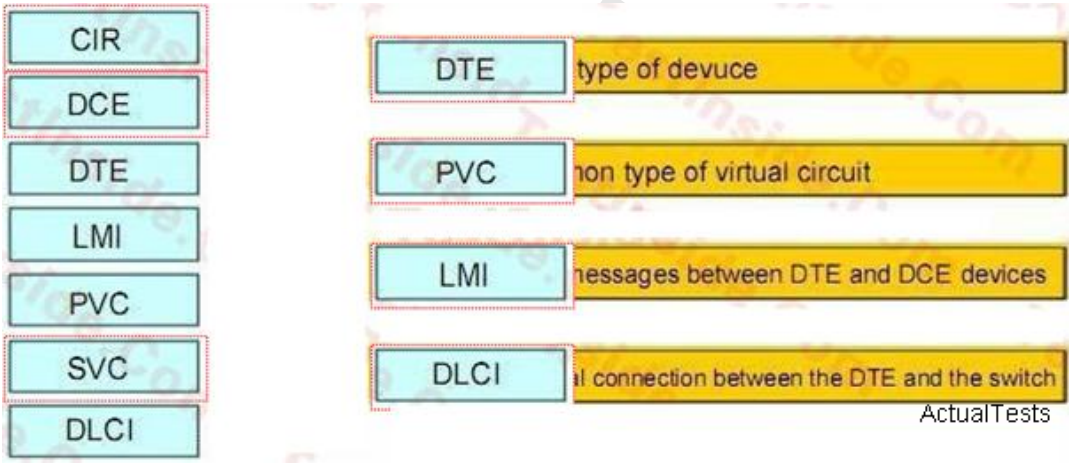
Drag the Frame Relay acronym on the left to match its definition on the right.(Not all acronyms are used.)



Answer:



Explanation:



QUESTION NO: 606

How does using the service password-encryption command on a router provide additional security?

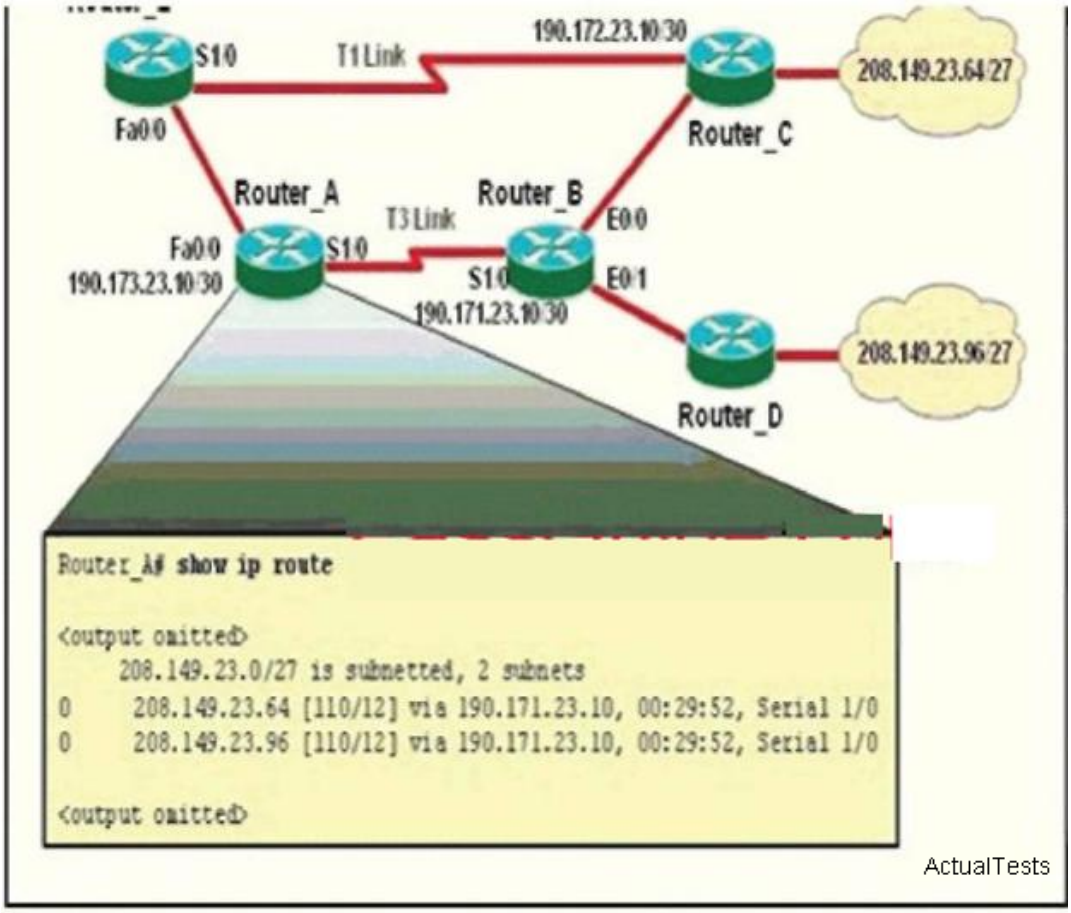
A. by encrypting all passwords passing through the router
B. by encrypting passwords in the plain text configuration file

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

QUESTION NO: 607

Refer to the exhibit. The network is converged. After link-state advertisements are received from Router_A, what information will Router_E contain in its routing table for the subnets 208.149.23.64 and 208.149.23.96?

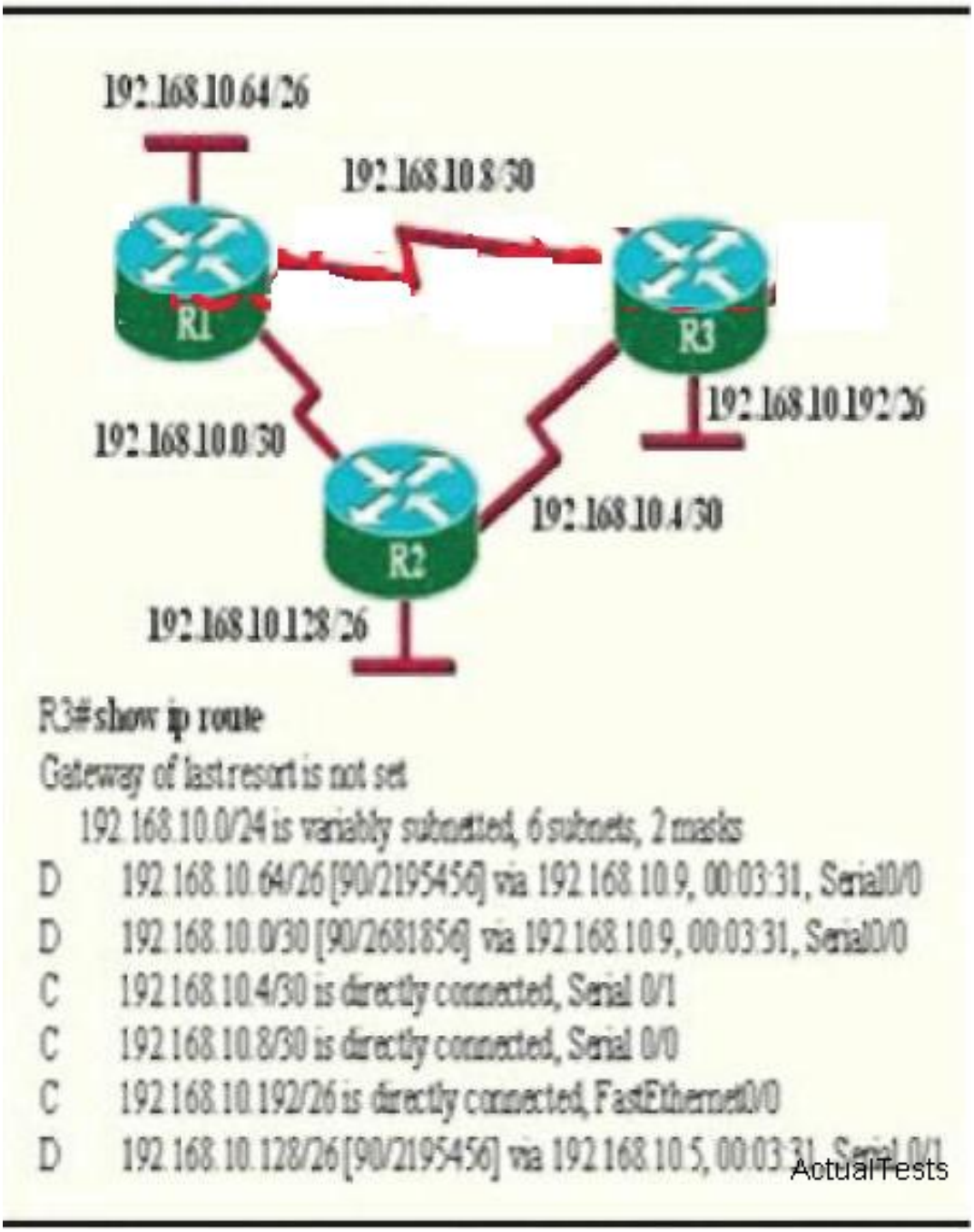


A. 208.149.23.64(110/13] via 190.173.23.10,00:00:07, FastEthemet0/0
208.149.23.96(110/13] via 190.173.23.10,00:00:16, FastEthemet0/0
B. 208.149.23.64(110/1] via 190.172.23.10,00:00:07, Serial1/0
208.149.23.96(110/3] via 190.173.23.10,00:00:16, FastEthemetO/0
C. 208.149.23.64(110/13] via 190.173.23.10,00:00:07, Serial1/0
208.149.23.96(110/13] via 190.173.23.10,00:00:16, Serial1/0
208.149.23.96(110/13] via 190.173.23.10,00:00:16, FastEthemetO/0
D. 208.149.23.64(110/3] via 190.172.23.10,00:00:07, Serial1/0
208.149.23.96(110/3] via 190.173.23.10,00:00:16, Serial1/0

Answer: A

QUESTION NO: 608

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

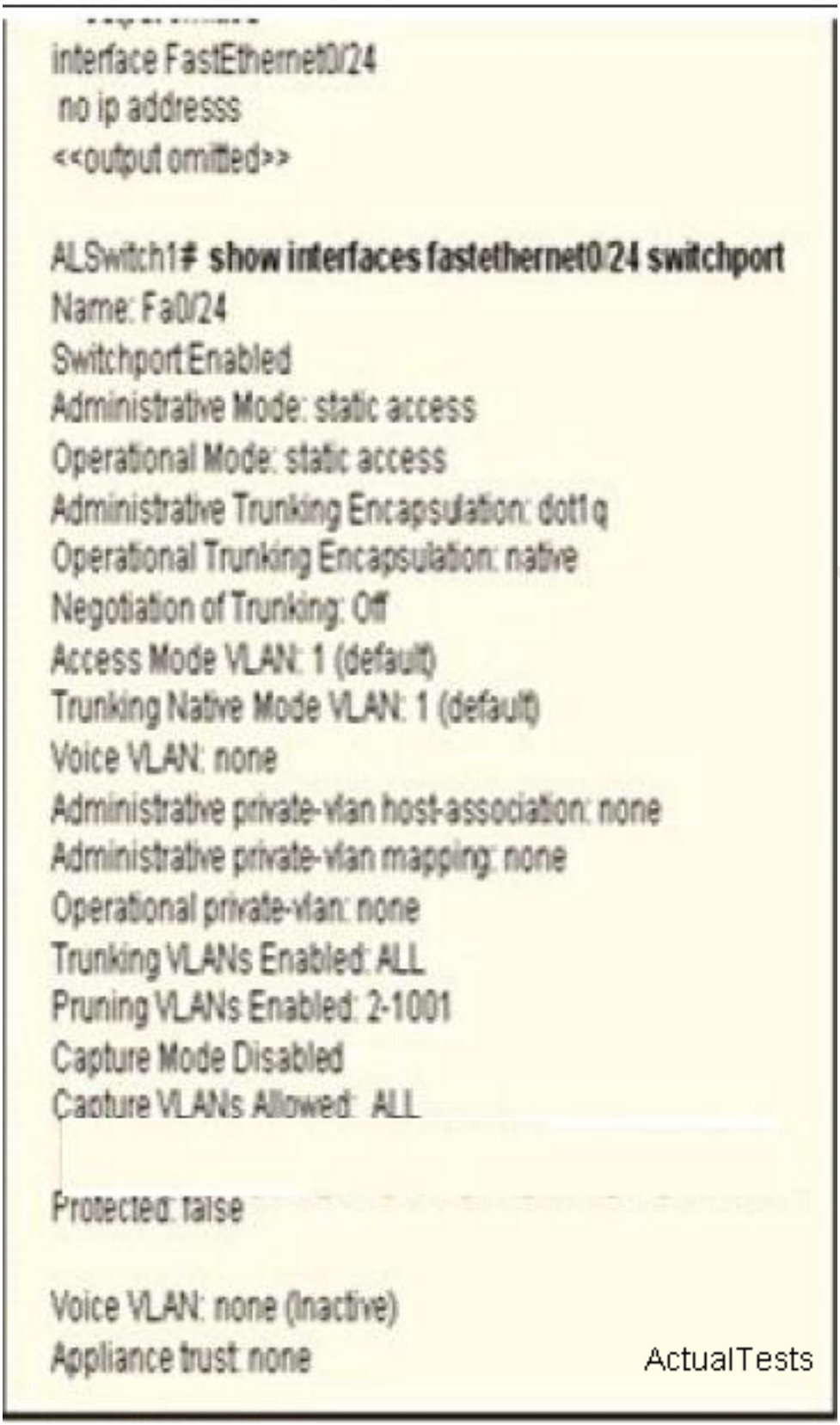


A. The path of the packets will be R3 to R2 to R1.
B. The path of the packets will be R3 to R1 to R2.
C. The path of the packets will be both R3 to R2 to R1 AND R3 to R1.
D. The path of the packets will be R3 to R1.

Answer: D

QUESTION NO: 609

Refer to the exhibit. Switch port FastEthemet 0/24 on ALSwitchl will be used to create an IEEE 802.1Q-compliant trunk to another switch. Based on the output shown, What is the reason the truck 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

QUESTION NO: 610

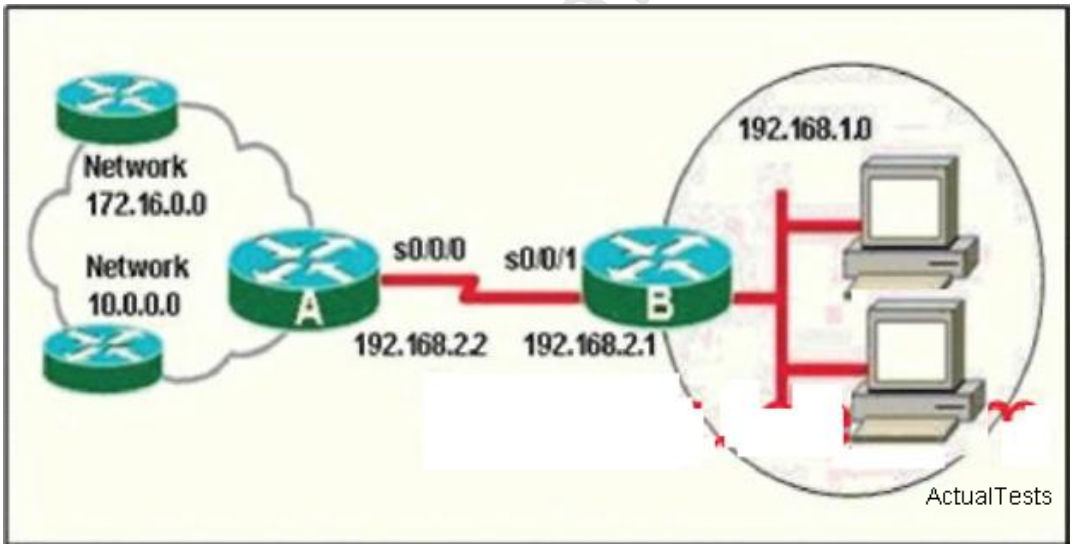
The output of the show frame-relay pvc command shows"PVC STATUS=INACTIVE". What does this mean?

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 the remote route.
C. The PVC is configured correctly, is operating normally.and is waiting for interesting 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 switch.

Answer: D

QUESTION NO: 611

Refer to the exhibit.Which command will created a default route on Router B to reach all networks beyond routerA?



A. ip route 0.0.0.0 0.0.0.0 192.168.2.2
B. ip route 192.168.1.0 255.255.255.0 192.168.2.1
C. ip route 192.168.1.0 255.255.255.0 s0/0/0
D. ip route 10.0.0.0 255.255.255.0 s0/0/0
E. ip route 0.0.0.0 255.255.255.0 192.168.2.2

Answer: A

QUESTION NO: 612

Which of the following IP addresses can be assigned to host devices?(Choose two)

A. 205.7.8.32/27
B. 191.168.10.2/23
C. 127.0.0.1
D. 224.0.0.10
E. 203.123.45.47/28
F. 10.10.0/13

Answer: B,F

QUESTION NO: 613

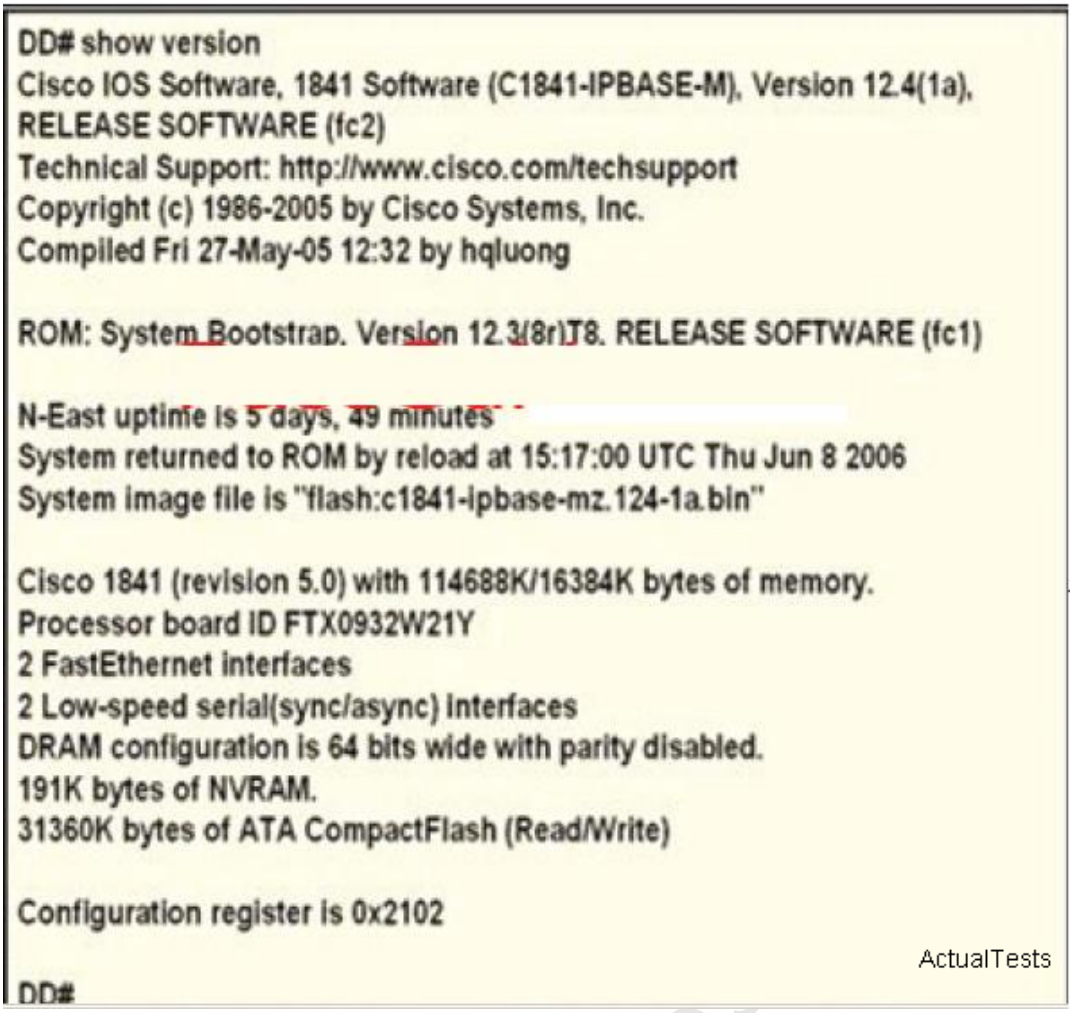
What is a vaild reason for a switch to deny port access to new devices when port security is enabled?

A. The denied MAC addresses have already been learned or configured on another secure interface in the same VLAN.
B. The denied MAC addresses are statically cofigured on the port.
C. The minimum MAC threshold has been reached.
D. The absolute aging times for the denied MAC addresses have expired.

Answer: B

QUESTION NO: 614

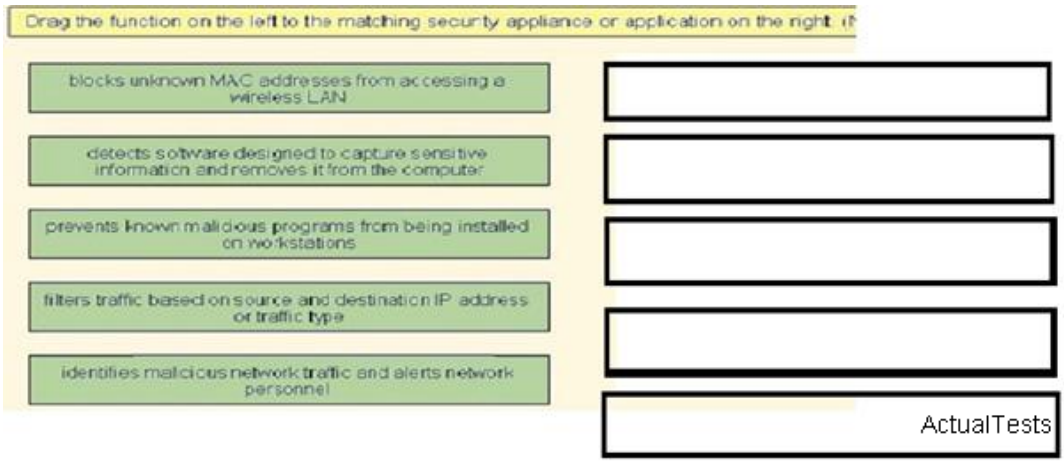
Refer to the digram.What is the largest configuration file that can be stored on this router?



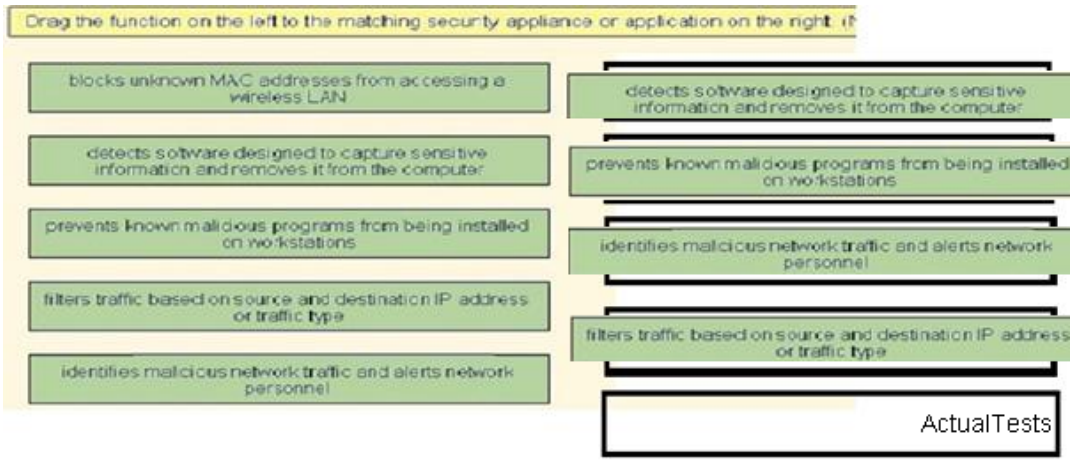
A. 191 Kbytes
B. 16384K bytes
C. cK bytes
D. 114688K bytes

Answer: A

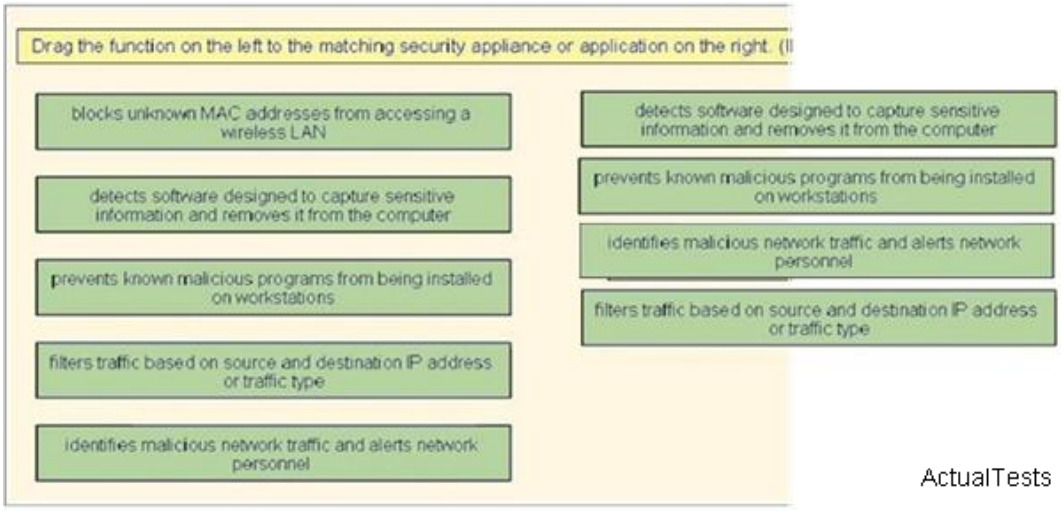
QUESTION NO: 615 DRAG DROP



Answer:

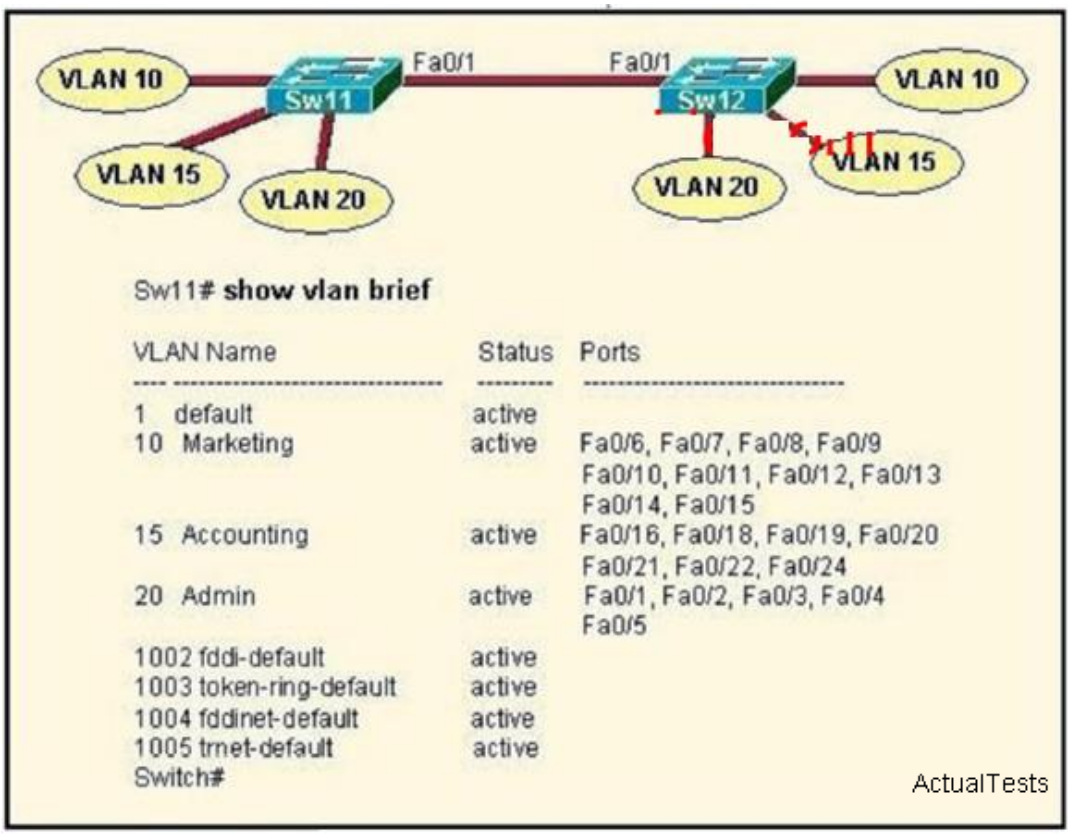


Explanation:



QUESTION NO: 616

Refer to the topology and router output shown in the exhibit. A technician is troubleshooting host connectivity issues on the Sw11 are unable to communicate with hosts in the same VLANs on Sw12. Hosts in the Admin VLAN are able to communicate identical on the two switches. What could be the problem?

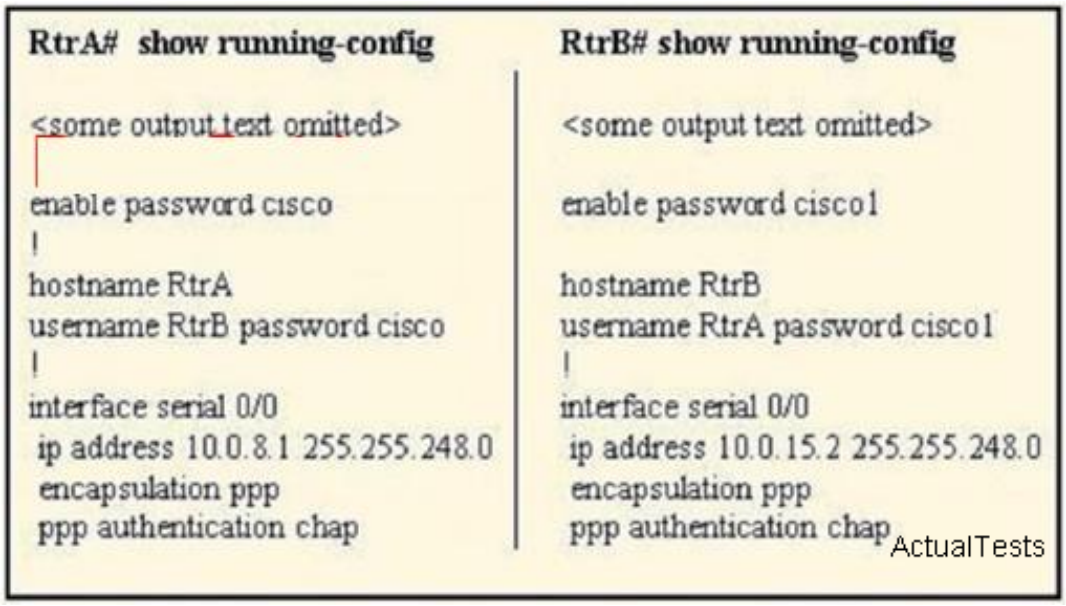


A. The Fa0/1 port is not operational on one of the switches
B. The link connecting the switches has not been configured as a trunk
C. At least one port needs to be configured in VLAN 1 for VLANs 10 and 15 to be able to communicate
D. Port FastEthernet 0/1 needs to be configured as an access link on both switches
E. A router is required for hosts on SW1 in VLANs 10 and 15 to communicate with hosts in the same VLAN on SW12.

Answer: B

QUESTION NO: 617

The administrator is unable to establish connectivity between two Cisco routers. Upon reviewing the command output of both the problem?



A. Authentication needs to be changed to PAP for both routers.

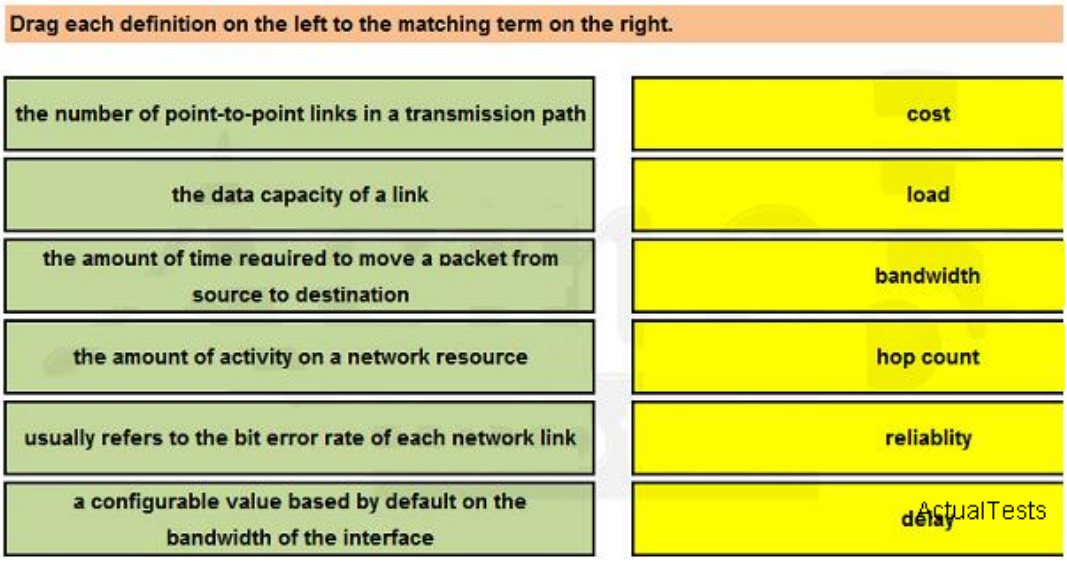
B. Serial ip addresses of routers are not on the same subnet.

C. Username/password is incorrectly configured.

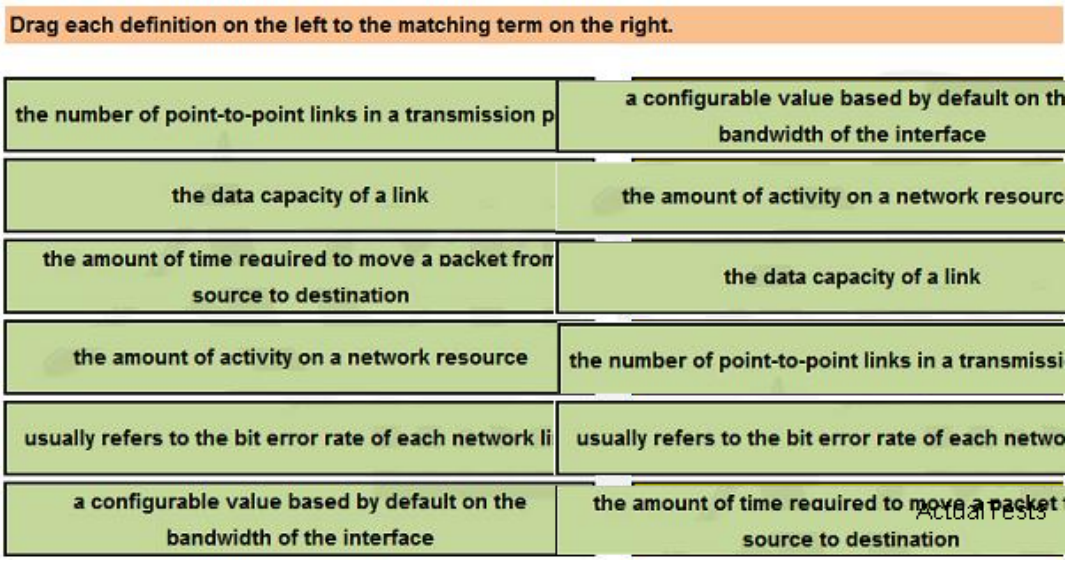
D. Router names are incorrectly configured.

Answer: C

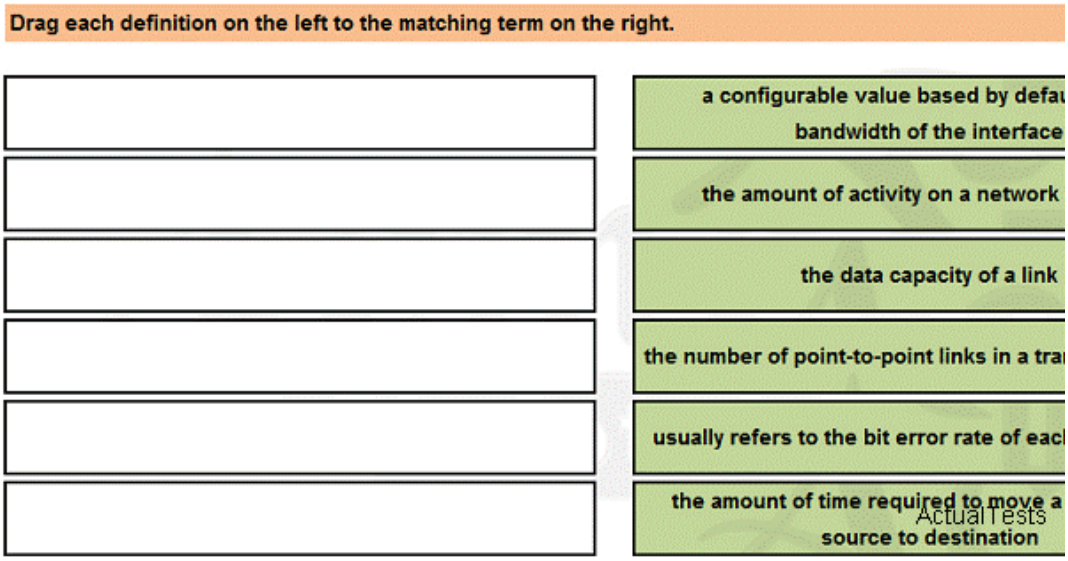
QUESTION NO: 618 DRAG DROP



Answer:

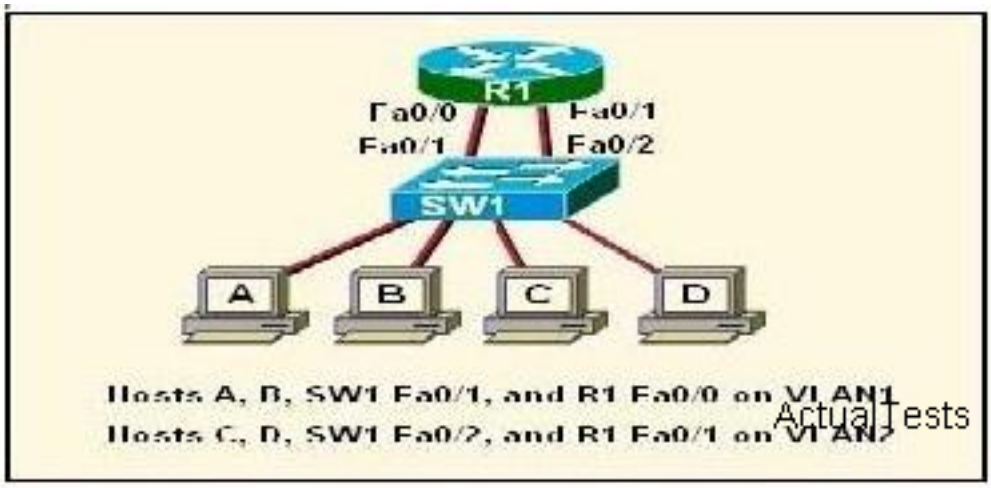


Explanation:



QUESTION NO: 619

Refer to the exhibit. A network administrator needs to add a new VLAN. named VLAN3. to the network shown. Unfortunately, there is not another FastEthernet interface on R1 to connect to the new VLAN3. Which approach is the most cost effective solution for this problem?



A. Purchase a new FastEthernet module and install it on R1.
B. Replace R1 with a new router that has at least three FastEthernet interfaces.
C. Configure a second switch to support VLAN3 with a VLAN trunk between SW1 and the new switch.
D. Configure a single VLAN trunk between R1 and SW1 and configure a subinterface on the R1 interface for each VLAN.
E. Connect another router to a serial interface of R1. Use a FastEthernet interface on the new router for VLAN3.

Answer: D

QUESTION NO: 620

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

QUESTION NO: 621

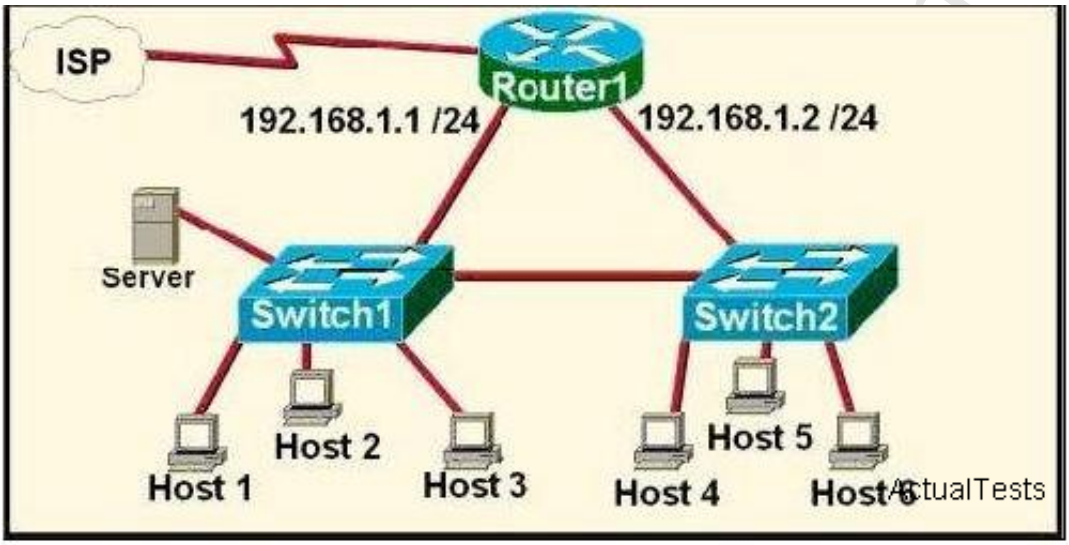
All WAN links inside the ABC University network use PPP with CHAP for authentication security. Which command will display the CHAP authentication process as it occurs between two routers in the network?

A. show CHAP authentication
B. show interface serialO
C. debug PPP authentication
D. debug CHAP authentication
E. show ppp authentication chap

Answer: C

QUESTION NO: 622

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?

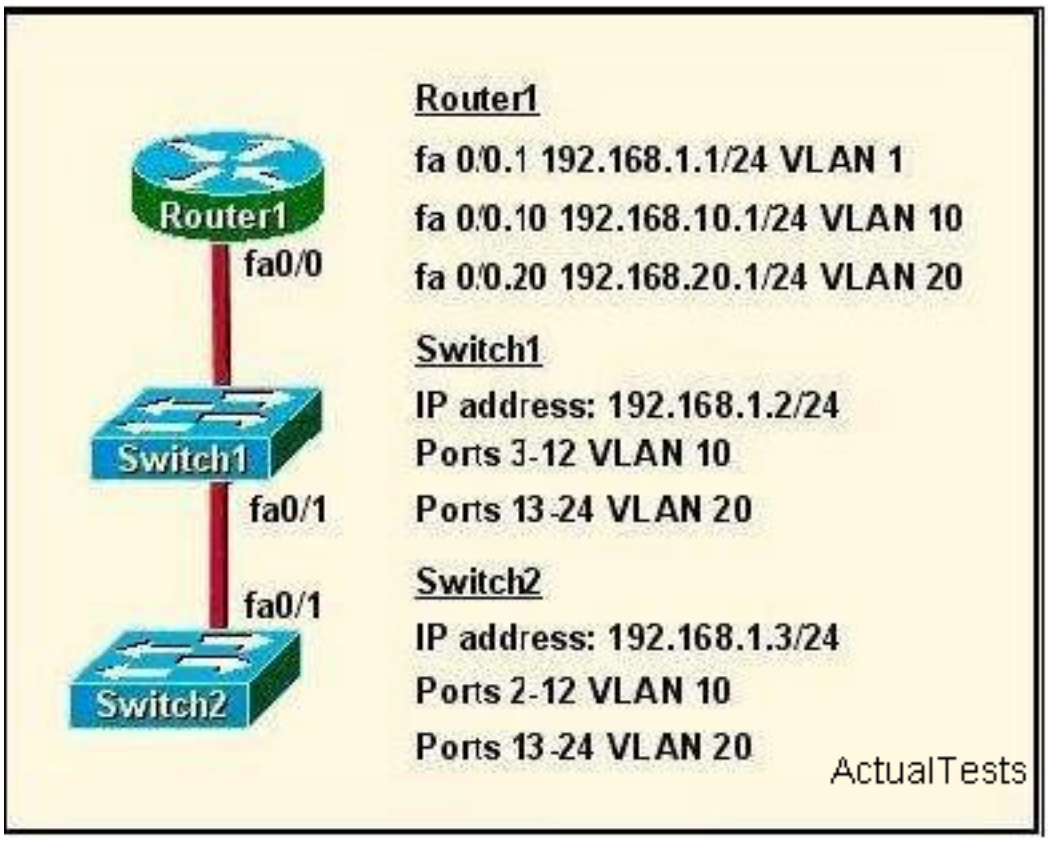


A. This design will function as intended.
B. Spanning-tree will need to be used.
C. The router will not accept the addressing scheme.
D. The connection between switches should be a trunk.
E. The router interfaces must be encapsulated with the 802.1Q protocol.

Answer: C

QUESTION NO: 623

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

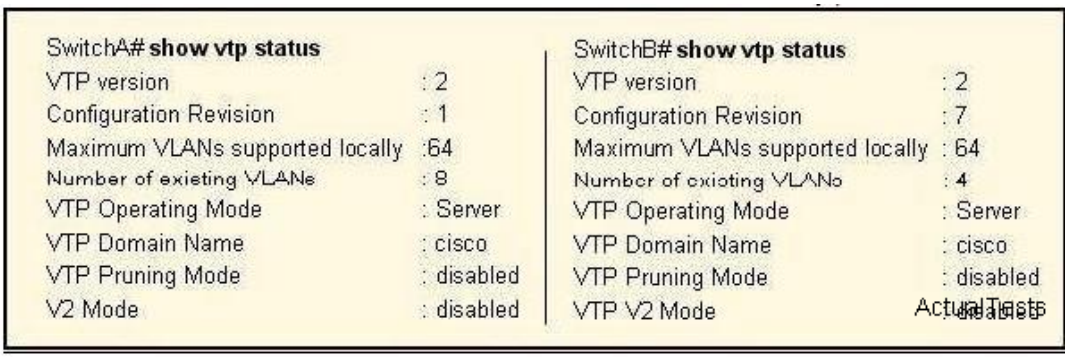


A. The ports only need to be connected by a crossover cable.
B. SwitchX(config)#interface fastethernet 0/1 SwitchX(config-if)#switchport mode trunk
C. SwitchX(config)# interface fastethernet 0/1 SwitchX(config-if)#switchport mode access SwitchX(config-if)#switchport access vlan 1
D. SwitchX(config)#interface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

QUESTION NO: 624

Refer to the exhibit. After SwitchB was added to the network, VLAN connectivity problems started to occur. What caused this problem?



A. Both switches are in server mode in the same domain.
B. The revision number of SwitchB was higher than the revision number of SwitchA.
C. SwitchA was not rebooted prior to adding SwitchB to the network.
D. V2-mode is not enabled.
E. VTP pruning is not activated, so the new paths in the network have not been recalculated.

Answer: B

QUESTION NO: 625

Refer to the exhibit.A router boots to the prompt shown in the exhibit.What does this signify,and how should the network administrator respond?

A. This prompt signifies that the configuration file was not found in NVRAM.The network administrator should follow the prompts to enter a basic configuration.
B. This prompt signifies that the configuration file was not found in flash memory.The network administrator should use TFTP to transfer a configuration file to the router.
C. This prompt signifies that the IOS image in flash memory is invalid or corrupt.The network administrator should use TFTP to transfer anlOS image to the router.
D. This prompt signifies that the router could not authenticate the user.The network administrator should modify the IOS mage and reboot the router.

Answer: B

QUESTION NO: 626

Exhibit and option E. added.
Refer to the exhibit. 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 not be blocked by STP.
B. Remote access management of this switch will not be possible without configuration change.
C. Moer 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.
E. As FastEthernet0/12 will be the last to come up, it will be blocked by STP.

Answer: C

QUESTION NO: 627

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

A. Only the default VLANs are configured on SwitchA.
B. SwitchA does not have a VTP domain name configured.
C. VTP pruning needs to be enabled on SwitchA.
D. SwitchC needs to have the VTP domain name configured.
E. SwitchB is in transparent mode.

Answer: B

QUESTION NO: 628

What can be done to secure the virtual terminal interfaces on a router? (Choose two.)

A. Administrabvely shut down the interface.
B. PhysicalAb secure the interface
C. Create an access list and apply t to the virfcAJal terminal interfaces with the access-group command
D. ConRgure a virtual temminal password and bgin process.
E. Enter an access list and apply it to the virtual terminal interlaces using the aceess-class command

Answer: D,E

QUESTION NO: 629

Refer to the exhibit. In this YLSM 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

QUESTION NO: 630

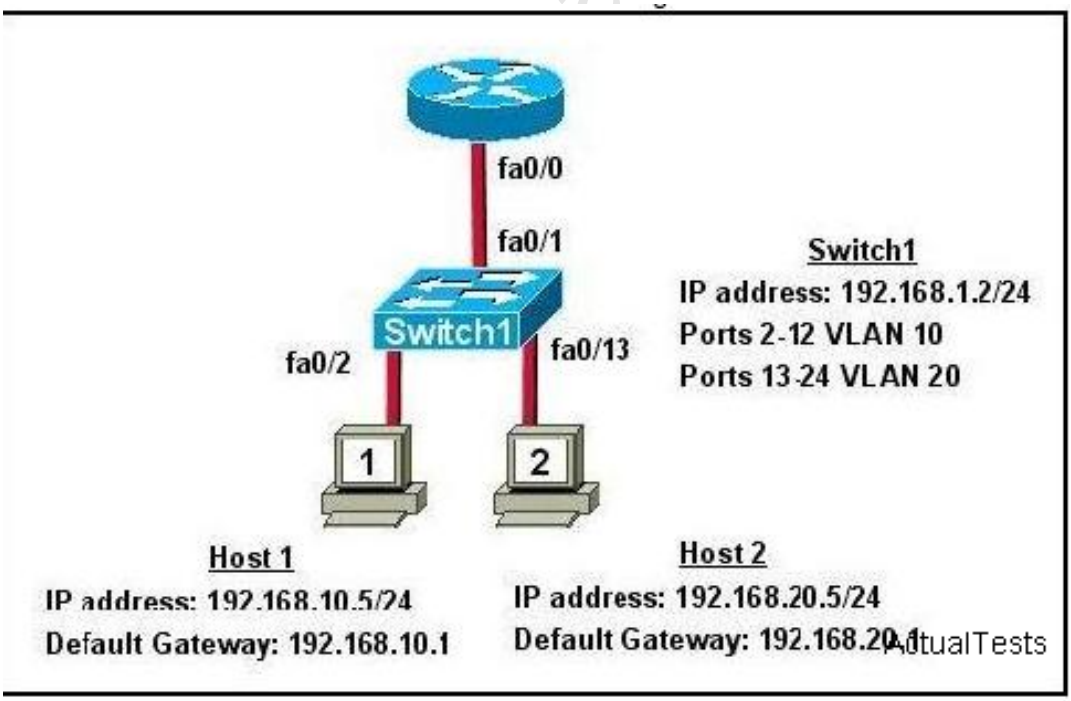
Refer to the exhibit. Given the output for this command, if the muter ID has not been manually set what muter ID will OSPF use for this ROUTER?

A. 10 1 1.2
B. 10.154.154.1
C. 172.16.5.1
D. 192.168.5.3

Answer: C

QUESTION NO: 631

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.)

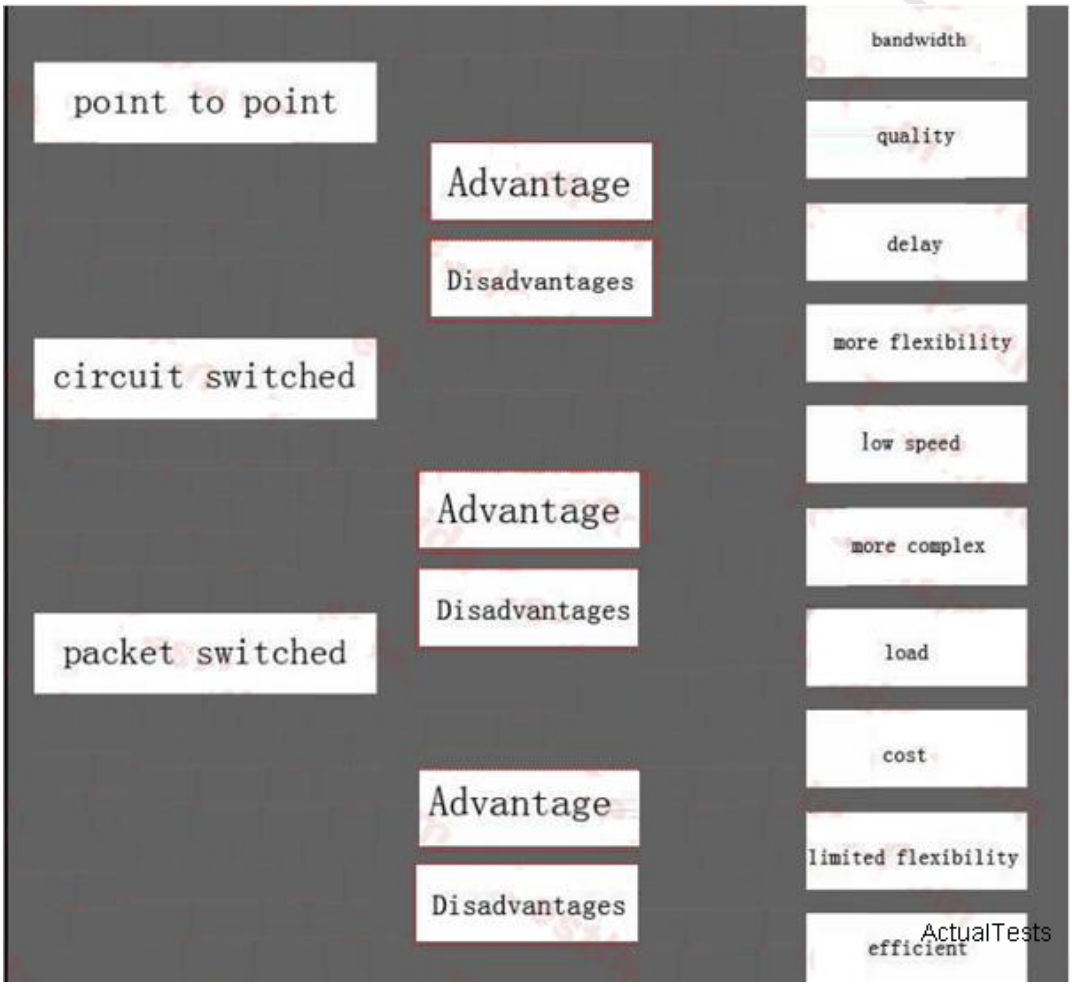


A. Router(config)# interface fastethernet 0/0 Router(config-if)# ip address 192 168 11 255 255 255 0 Router(config-if)# no shut down

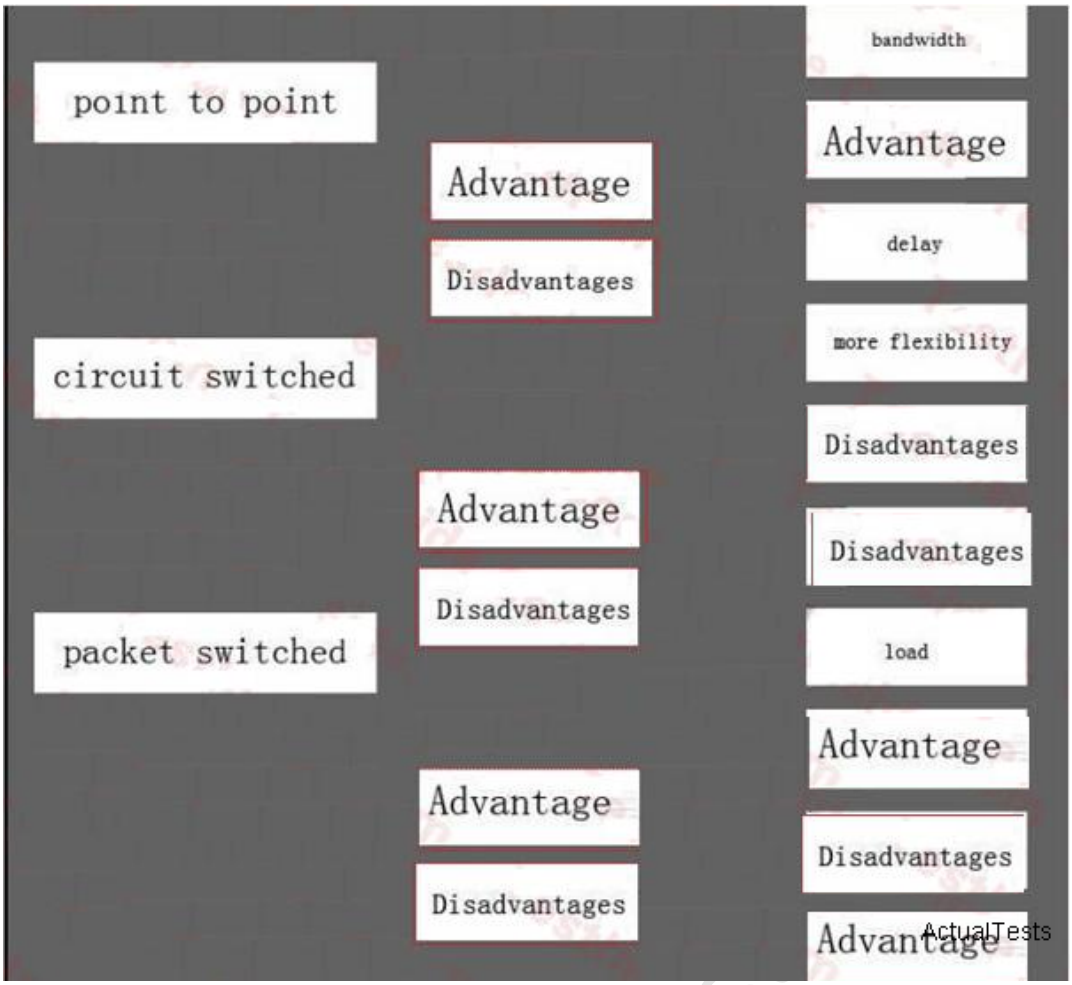
B. Router(config)# interface fastethernet 0/0 Router(config-if)# no shut down Router(config)# interface fastethernet 0/0.1 Router(config-subif)# encapsulation dot1q 10 Router(config-subif)# ip address 192.168.10.1 255.255.255.0 Router(config)# interface fastethernet 0/0.2 Router(config-subif)# encapsulation 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 Switch 1(config-vlan)#vtp domain XYZ Switch 1(config-vlan)#vtp server
E. Switch 1(config)# interface fastethernet 0/1 Switch 1(config-if)# switchport mode trunk
F. Switch 1(config)# interface vlan 1 Switch 1(config-if)#ip default-gateway 192.168.1.1

Answer: B,E

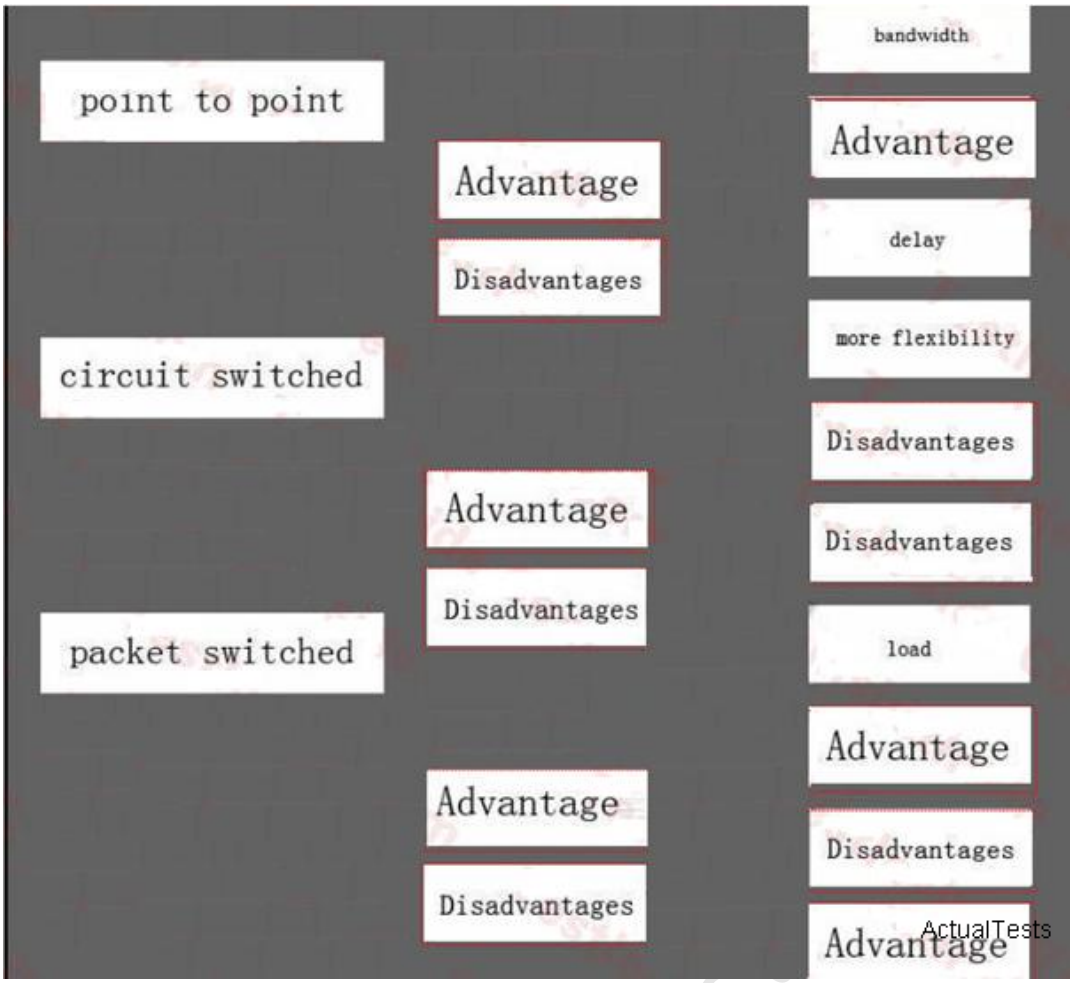
QUESTION NO: 632 DRAG DROP



Answer:



Explanation:



QUESTION NO: 633

What destination layer 2 address will be used in the frame the host 172.30.0.4?

A. 767
B. 682
C. 455
D. 46

Answer: B

QUESTION NO: 634

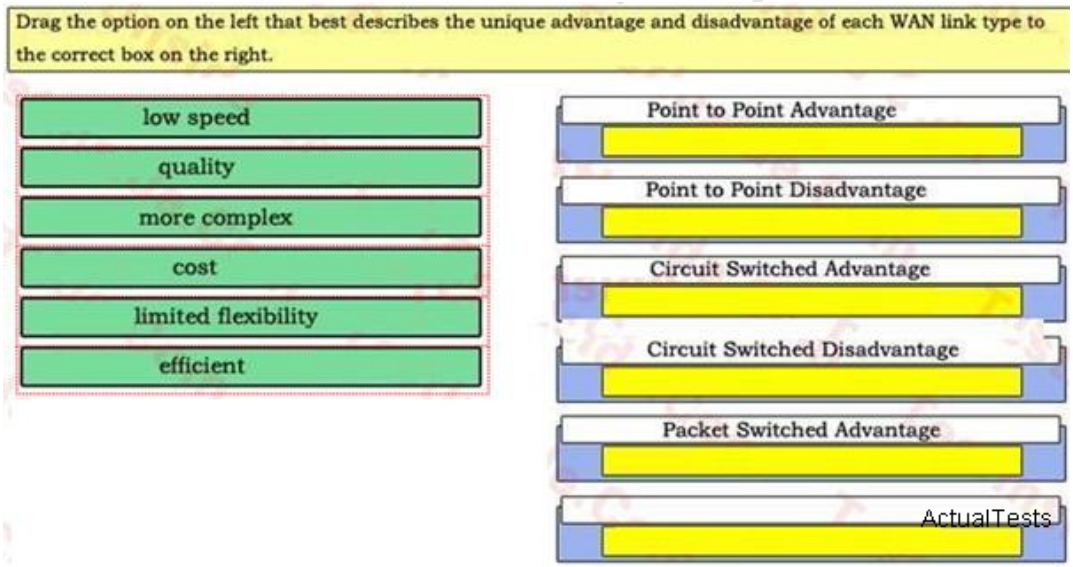
Refer to the exhibit.

A router interface is being configured for Frame Relay. However, as the exhibt shows, the router will not accept the command to configure the LMI type. What is the problem?

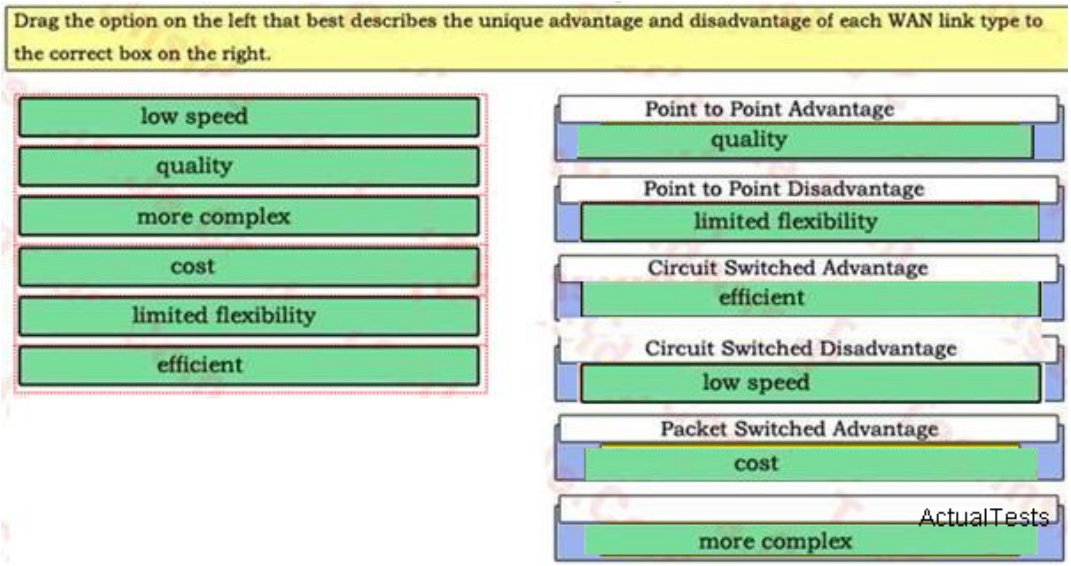
A. The interface does not support Frame Relay connections.
B. The interface does not have an ip address assigned to it yet.
C. The interface requires that the no shutdown command be configured first.
D. The interface requires that the encapsulation frame-relay command be configured first.

Answer: D

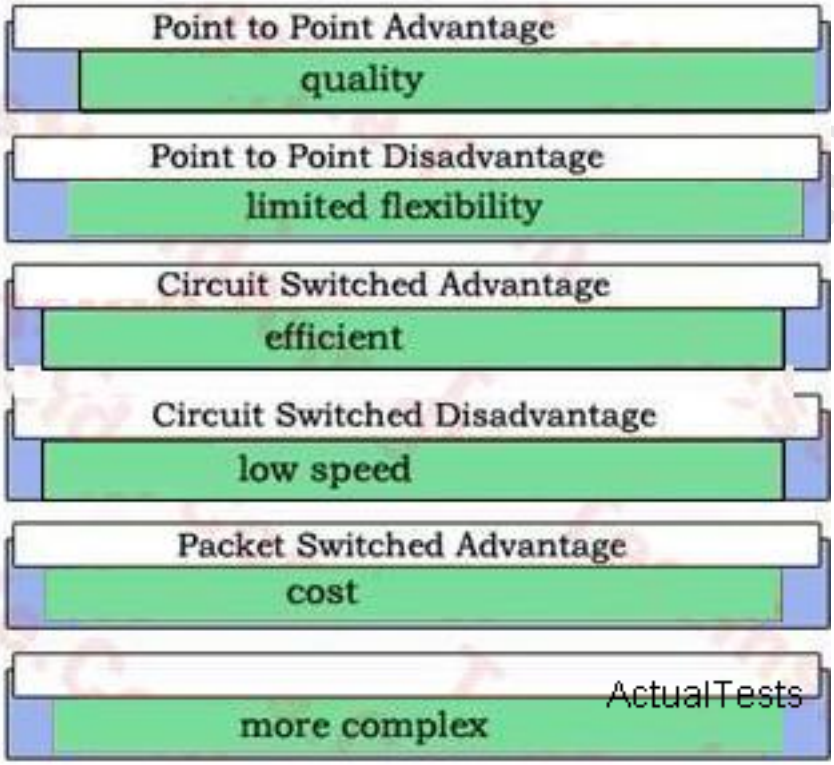
QUESTION NO: 635 DRAG DROP



Answer:



Explanation:



QUESTION NO: 636

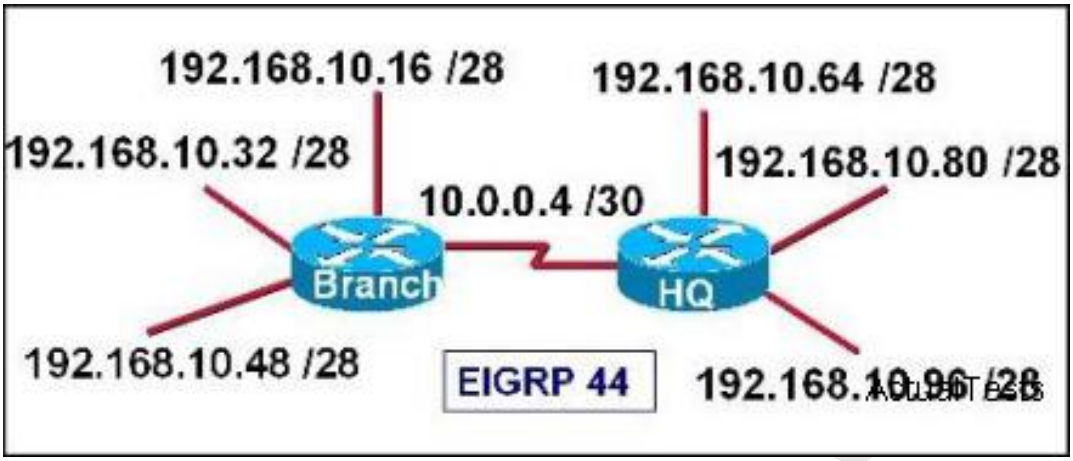
A network administrator is verifying the configuration of a newly installed host by establishing an FTP connection to a remote server. What is the hightest layer of the protocol stack that the network administrator is using for this operation?

A. Application
B. Presentation
C. Session

D. Transport
E. Internet
F. Data link

Answer: A

QUESTION NO: 637



An internetwork has been configured as shown in the diagram, with both routers using EIGRP routing for AS 44. Users on the Branch router are unable to reach any of the subnets on the HO router. Which of ttie following commands is necessary to fix this problem?

A. Branch(config-router)# eigrp log-neighbor-changes
B. Branch(config-router)# redistribute eigrp 44
C. Branch(config-router)# version 2
D. Branch(config-router)# no auto-summary
E. Branch(config-router)# default-information originate

Answer: D

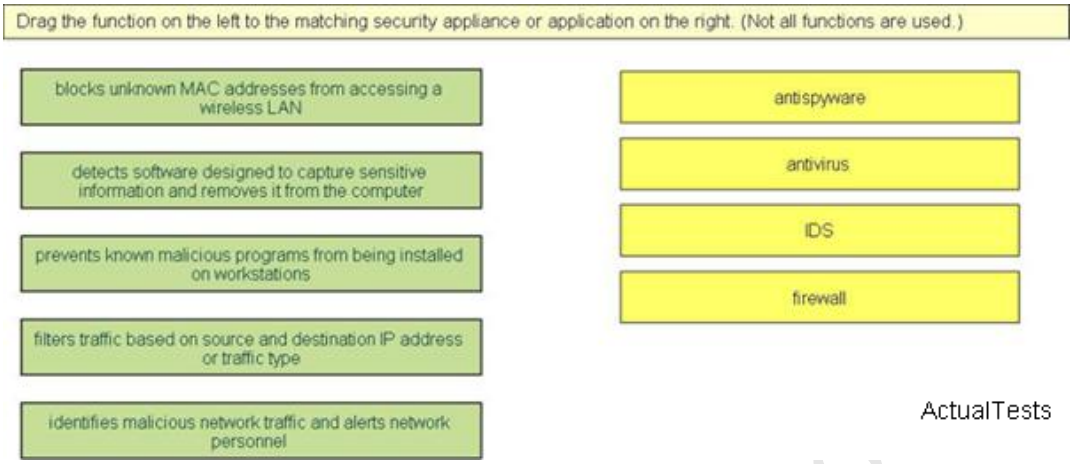
Explanation:
There are two ways to inject a default route into a normal area. If the ASBR already has the default route in its routing table, you can advertise the existing 0.0.0.0/0 into the OSPF domain with the default-information originate router configuration command. If the ASBR doesn't have a default route, you can add the keyword always to the default-information originate command (default-information originate always).
This command will advertise a default route into the OSPF domain, regardless of whether it has a route to 0.0.0.0. Another benefit of adding always keyword is that it can add stability to the internetwork. For example, if the ASBR is learning a default route from another routing domain such as RIP and this route is flapping, then without the always keyword, each time the route flaps, the ASBR will send a new Type 5 LSA into the OSPF domain causing some instability inside the OSPF domain. With the always keyword, the ASBR will advertise the default inside the OSPF domain always, and thus the flapping of the default route from the RIP domain will not cause any

instability inside the OSPF domain.

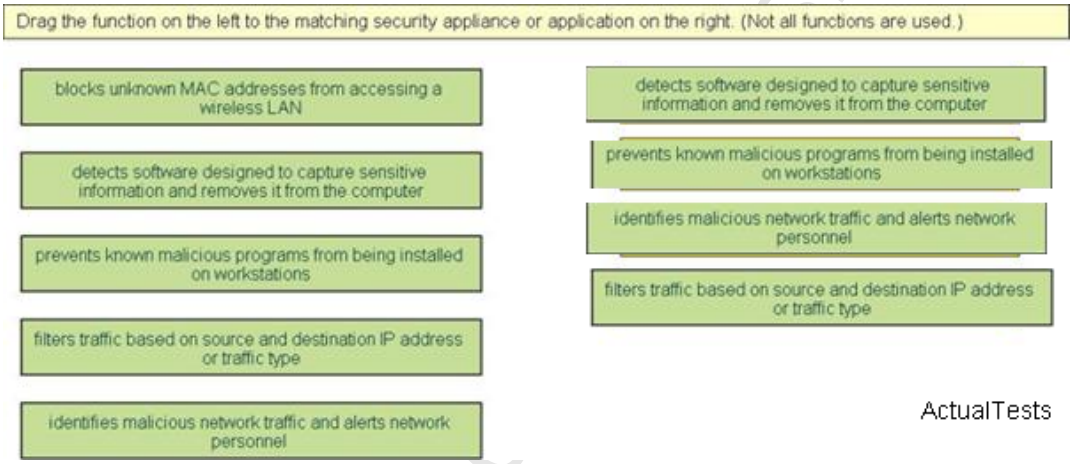
In the example shown here, only choice D is correct as the wildcard mask correctly specifies the 10.10.2.16 0.0.0.15 networks, which include all IP addresses in the 10.10.2.16-10.10.2.31 range.

Reference: http://www.cisco.com/warp/public/104/21.html

QUESTION NO: 638 DRAG DROP

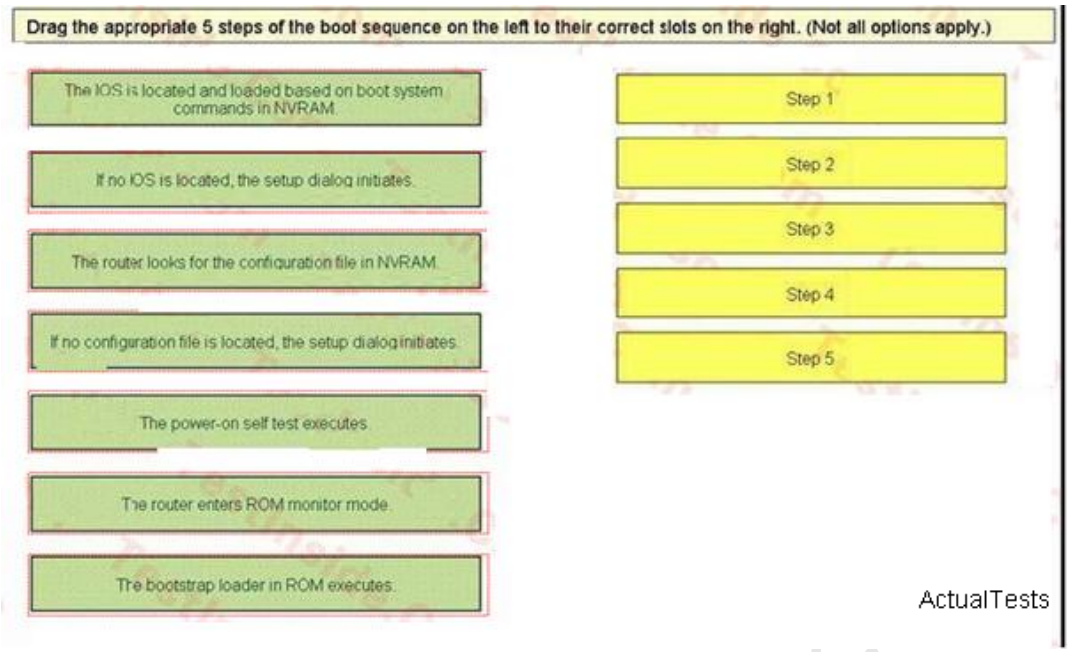


Answer:

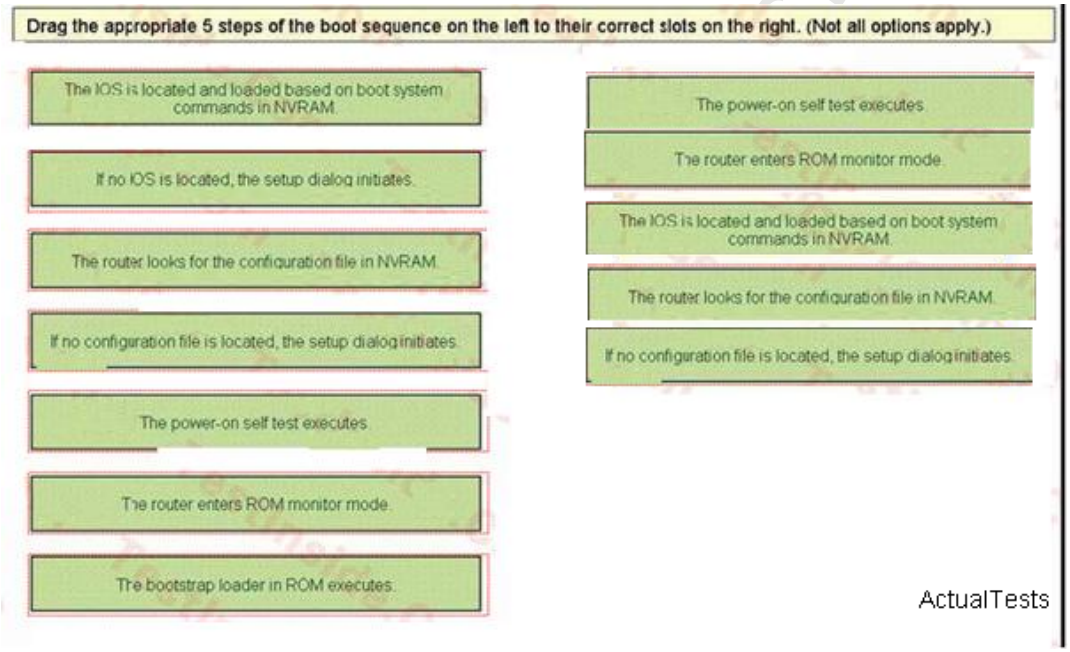


Explanation:

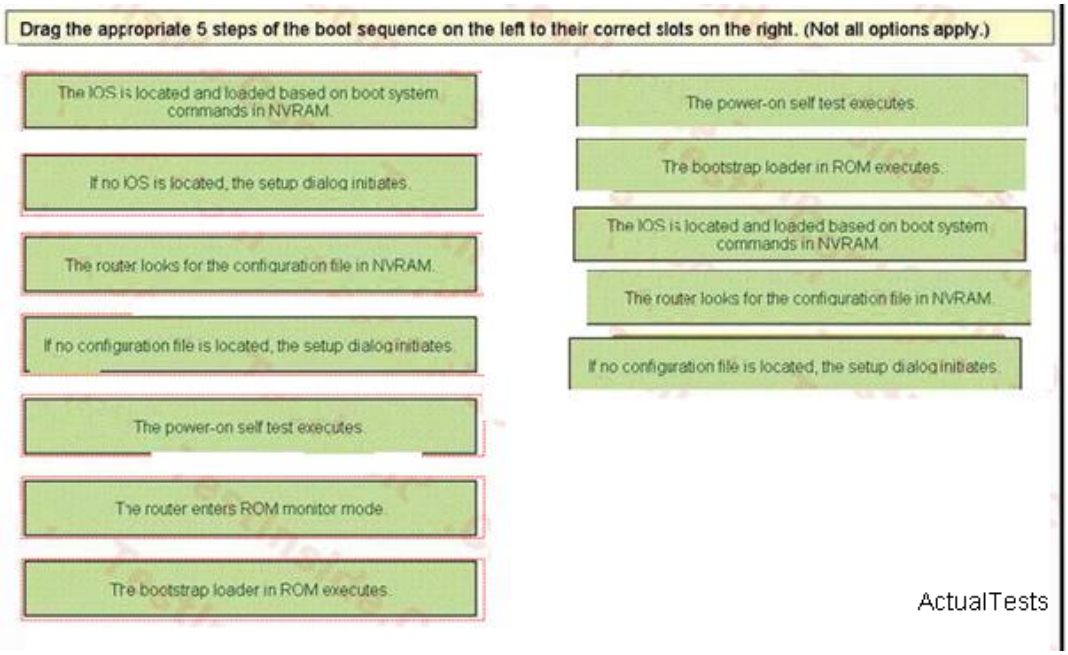
QUESTION NO: 639 DRAG DROP



Answer:



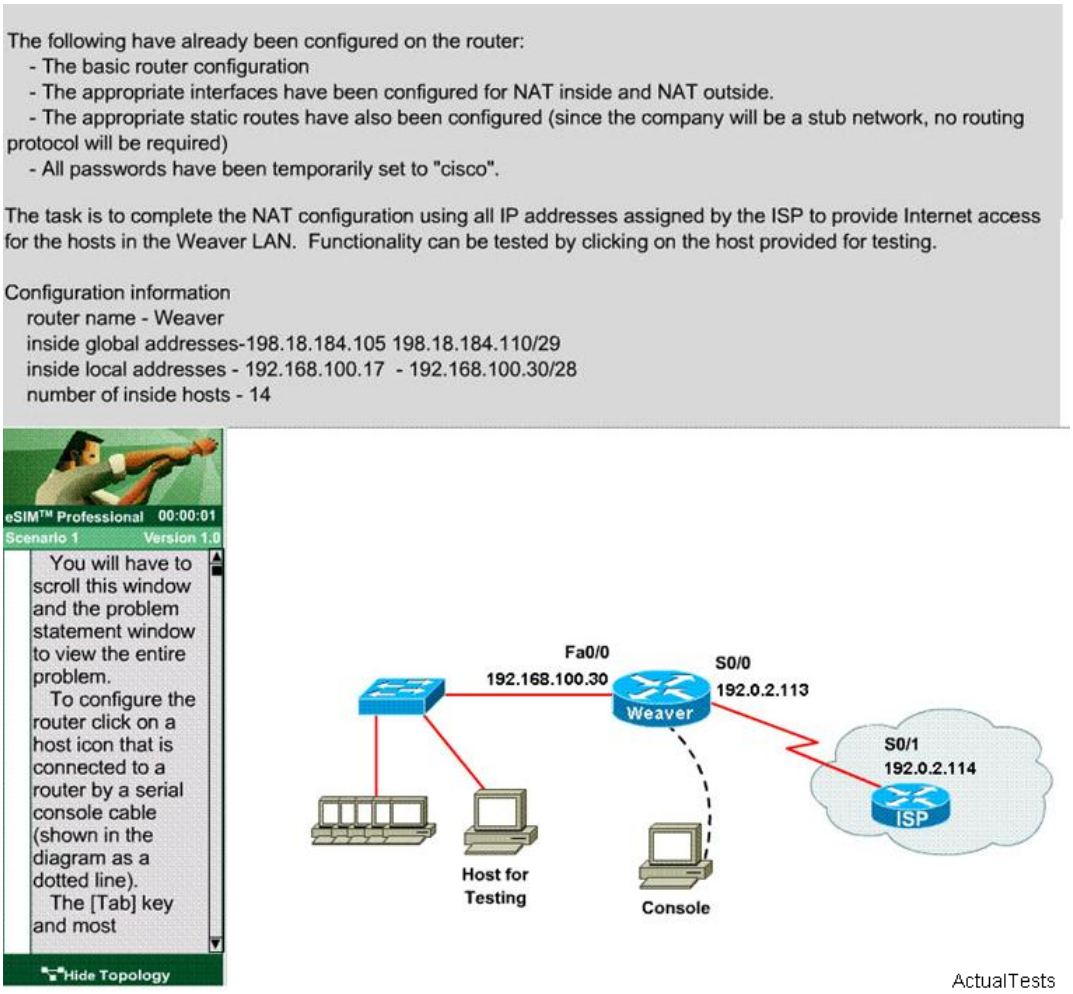
Explanation:



QUESTION NO: 640

LAB - SIMULATION

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.



Explanation:

Solution:

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

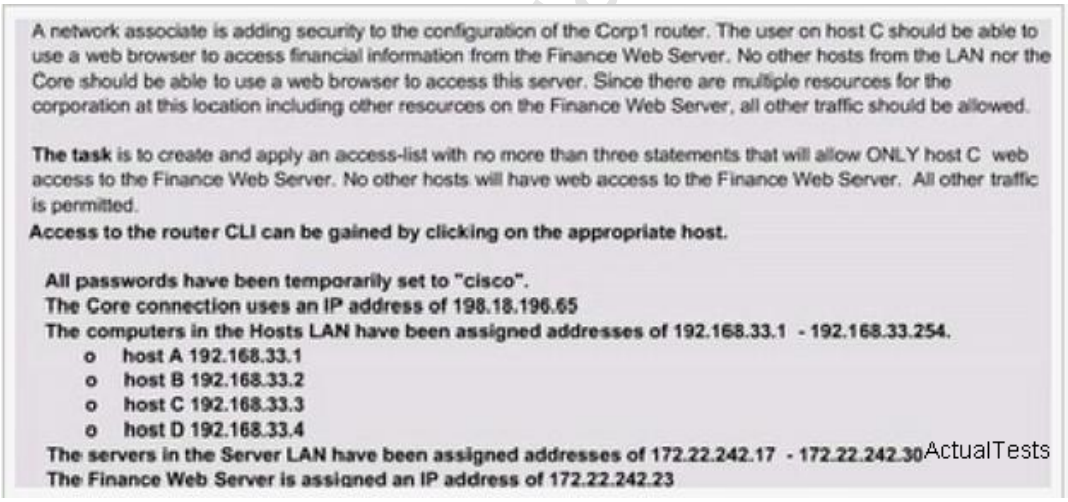
Weaver(config)#ip nat inside source list 1 pool mypool overload

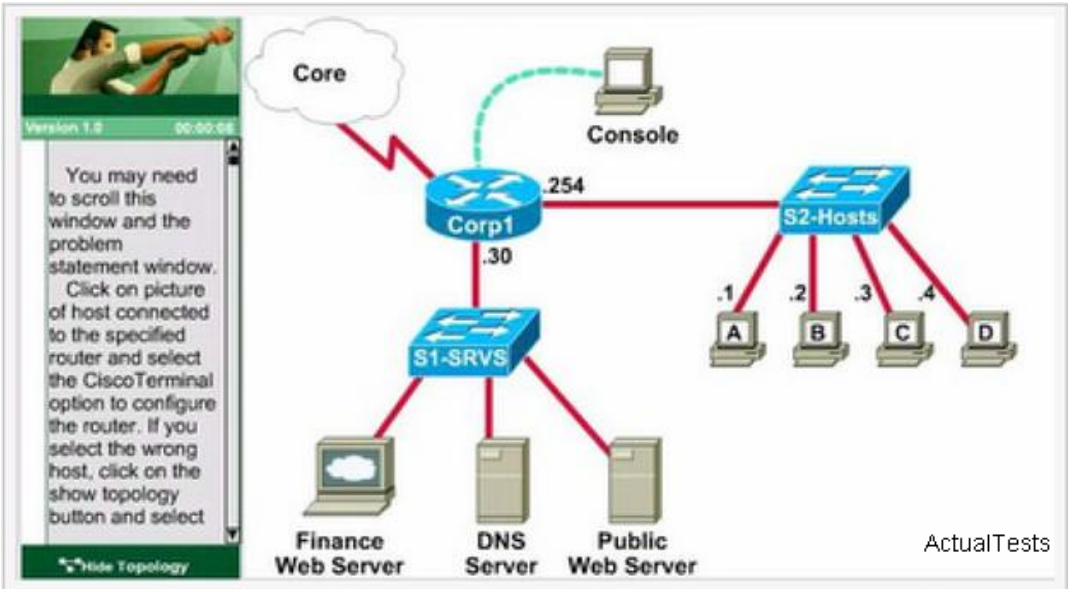
This command translates all source addresses that pass access list 1, which

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: 641

LAB - SIMULATION





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 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: 642

LAB - SIMULATION

A network associate is configuring a router for the network company to provide Internet access. The ISP has provided the company with six public IP addresses of 198.18.237.225 198.18.237.230. 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 192.168.16.33 -192.168.16.46.

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 Bomar LAN. You have successfully completed this exercise when the host PC can ping the ISP.

Configuration information
router namE. R
inside global addresses- 198.18.237.225 198.18.237.230/29
inside local addresses - 198.18.16.33 192.168.16.46/28
number of inside hosts - 14

Explanation:

```
Router>enable
Router#config terminal
Router(config)#hostname P4S-R
      R(config)#interface fa0/0
      Rconfig-if)#ip nat inside
      R(config)#interface S0/0
      R(config-if)#ip nat outside
      R(config-if)#exit
      R(config)#access-list 1 permit 192.168.16.33 0.0.0.15
      R(config)#access-list 1 deny any
      R(config)#ip nat pool nat_test 198.18.237.225 198.18.237.230 prefix-length 29
      R(config)#ip nat inside source list 1 pool nat_test overload
```


QUESTION NO: 643

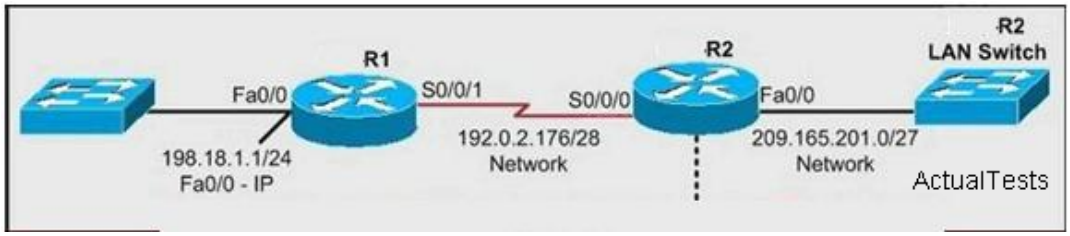
LAB - SIMULATION

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 ciscol
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



Explanation:

```
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 fa0/0
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
```

ActualTests

QUESTION NO: 644

LAB - SIMULATION

After adding Router2 router, no routing updates are being exchanged between ROUTER1 and the new location. All other inter connectivity 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 to provide full connectivity between the routers.

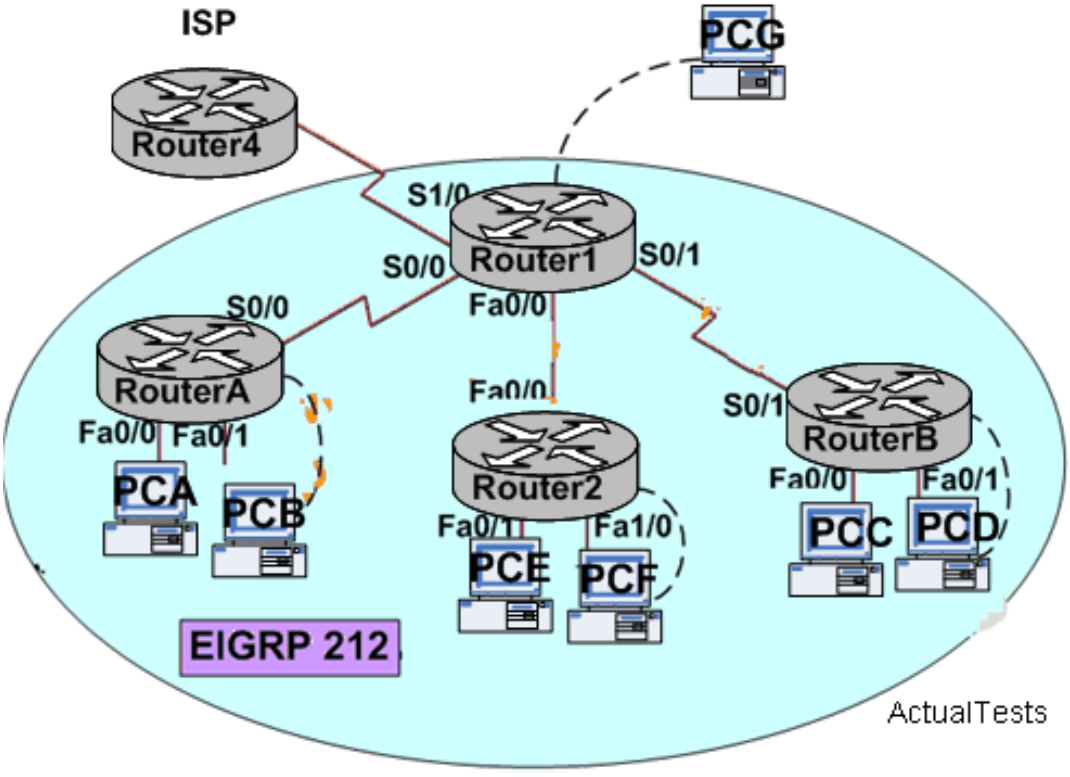
Access to the router CLI can be gained by clicking on the appropriate host. All passwords on all routers are cisco.

IP addresses are listed in the chart below.

Router1	Router2
Fa0/0 – 192.168.77.33 S1/0 – 198.0.18.6 S0/1 - 192.160.60.25	Fa0/0 – 192.168.77.34 Fa1/0 – 192.168.60.81 Fa0/1 – 192.168.60.65

RouterA	RouterB
Fa0/0 – 192.168.60.97 Fa0/1 – 192.168.60.113 S0/0 – 192.168.36.14	Fa0/0 – 192.168.60.129 Fa0/1 – 192.168.60.145 S0/1 – 192.168.60.26

Click that host-G, complete the configuration of the router in the pop-up CLI



****

RouterA# show run

interface FastEthernet0/0

ip address 192.168.60.97 255.255.255.240

!

interface FastEthernet0/1

ip address 192.168.60.113 255.255.255.240

!

interface Serial0/0

Ip address 192.168.36.14 255.255.255.252
Clockrate 64000

!
router eigrp 212
Network 192.168.36.0
Network 192.168.60.0
No auto-summary
!

RouterA# show ip route
192.168.36.0/30 is subnetted, 1 subnets
C 192.168.36.12 is directly connected, Serial0/0
192.168.60.0/24 is variably subnetted, 5 subnets, 2 masks
C 192.168.60.96/28 is directly connected, FastEthernet0/0
C 192.168.60.112/28 is directly connected, FastEthernet0/1
D 192.168.60.128/28 [90/21026560] via 192.168.36.13, 00:00:57, Serial0/0
D 192.168.60.144/28 [90/21026560] via 192.168.36.13, 00:00:57, Serial0/0
D 192.168.60.24/30 [90/21026560] via 192.168.36.13, 00:00:57, Serial0/0
D* 198.0.18.0 [90/21024000] via 192.168.36.13, 00:00:57, Serial0/0

****

Router2# show run
!
!
interface FastEthernet0/0
ip address 192.168.77.34 255.255.255.252
!
interface FastEtherner0/1
ip address 192.168.60.65 255.255.255.240
!
interface FastEthernet1/0
ip address 192.168.60.81 255.255.255.240
!
!
router eigrp 22
network 192.168.60.0
network 192.168.77.0
no auto-summary

Router2# show ip route

192.168.60.0/28 is subnetted, 2 subnets
C 192.168.60.80 is directly connected, FastEthernet1/0
C 192.168.60.64 is directly connected, FastEthernet0/1
192.168.77.0/30 is subnetted, 1 subnets
C 192.168.77.32 is directly connected, FastEthernet0/0
****

RouterB# show run

interface FastEthernet0/0
ip address 192.168.60.129 255.255.255.240
!
interface FastEthernet0/1
ip address 192.168.60.145 255.255.255.240
!
interface Serial0/1
ip address 192.168.60.26 255.255.255.252

router eigrp 212
network 192.168.60.0
network 192.168.60.0

RouterB# show ip route
192.168.60.0/24 is variably subnetted, 5 subnets, 2 masks
C 192.168.60.24/30 is directly connected, Serial0/1
C 192.168.60.128/28 is directly connected, FastEthernet0/0
C 192.168.60.144/28 is directly connected, FastEthernet0/1
D 192.168.60.96/28 [90/21026560] via 192.168.60.25, 00:00:57, Serial0/1
D 192.168.60.112/28 [90/21026560] via 192.168.60.25, 00:00:57, Serial0/1
192.168.36.0/30 is subnetted, 1 subnets
D 192.168.36.12 [90/21026560] via 192.168.60.25, 00:00:57, Serial0/1
D* 198.0.18.0 [90/21024000] via 192.168.60.25, 00:00:57, Serial0/1

****

ROUTER1# show run
!
interface FastEthernet0/0
ip address 192.168.77.33 255.255.255.252
!
interface Serial1/0

```
ip address 198.0.18.6 255.255.255.0
!
interface Serial0/0
ip address 192.168.36.13 255.255.255.252
clockrate 64000
!
interface Serial0/1
ip address 192.168.60.25 255.255.255.252
clockrate 64000
!
!
router eigrp 212
network 192.168.36.0
network 192.168.60.0
network 192.168.85.0
network 198.0.18.0
no auto-summary
!
ip classless
ip default-network 198.0.18.0
ip route 0.0.0.0 0.0.0.0 198.0.18.5
ip http server

ROUTER1# sh ip route
192.168.36.0/30 is subnetted, 1 subnets
C 192.168.36.12 is directly connected, Serial0/0
192.168.60.0/24 is variably subnetted, 5 subnets, 2 masks
C 192.168.60.24/30 is directly connected, Serial0/1
D 192.168.60.128/28 [ 90/21026560 ] via 192.168.60.26, 00:00:57, Serial0/1
D 192.168.60.144/28 [ 90/21026560 ] via 192.168.60.26, 00:00:57, Serial0/1
D 192.168.60.96/28 [ 90/21026560 ] via 192.168.36.14, 00:00:57, Serial0/0
192.168.77.0/30 is subnetted, 1 subnets
C 192.168.77.32 is directly connected, FastEthernet0/0
C 198.0.18.0/24 is directly connected, Serial1/0
*S 0.0.0.0 via 198.0.18.5
```

Explanation:

Please input commands here:

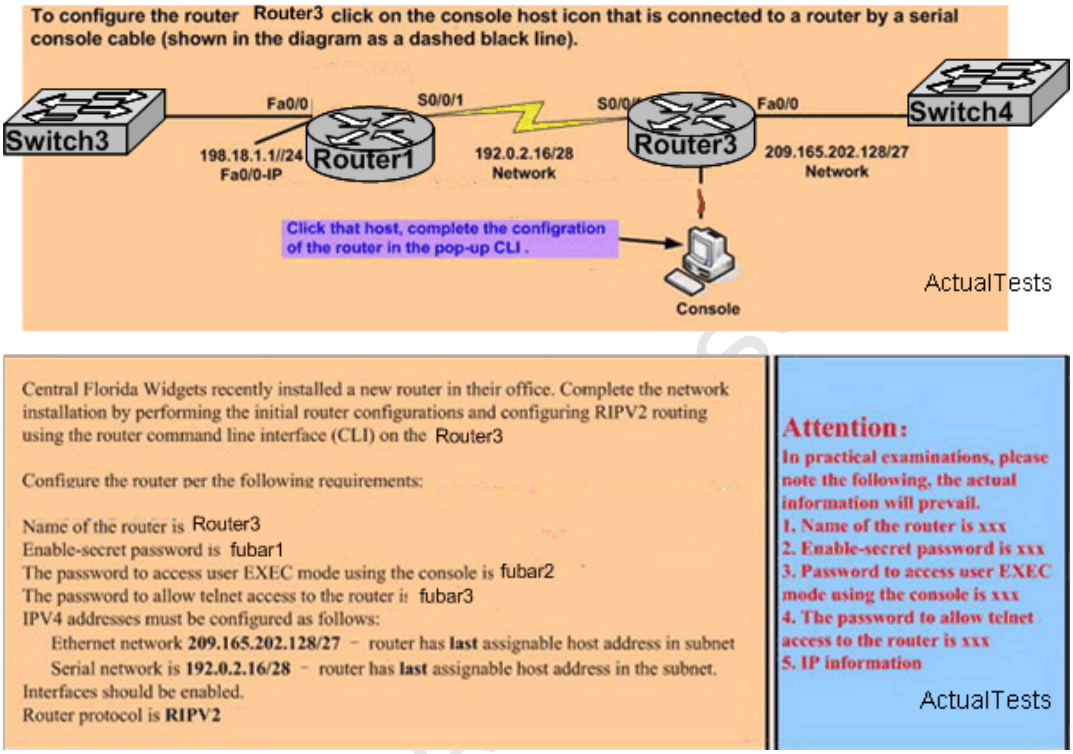
```
Router2>enable
Router2#config t
Router2(config)#no router eigrp 22
```

Router2(config)#router eigrp 212
Router2(config-router)#network 192.16.60.0
Router2(config-router)#network 192.16.77.0

ROUTER1>enable
ROUTER1#config t
ROUTER1(config)#router eigrp 212
ROUTER1(config-router)#network 192.16.77.0

QUESTION NO: 645

LAB - SIMULATION



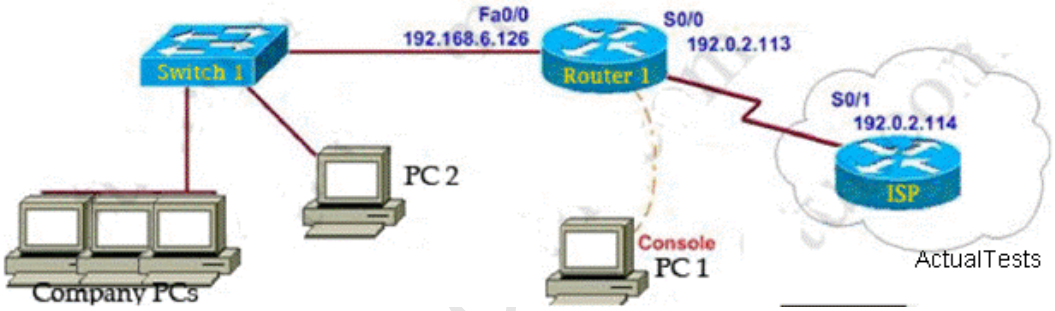
Please input command here:

Explanation:
Router>enable
Router#config terminal
Router(config)#hostname ROUTER3
ROUTER3(config)#enable secret fubar1
ROUTER3(config)#line console 0
ROUTER3(config-line)#password fubar2
ROUTER3(config-line)#exit
ROUTER3(config)#line vty 0 4
ROUTER3(config-line)#password p fubar3

```
ROUTER3(config-line)#login
ROUTER3(config-line)#exit
ROUTER3(config)#interface fa0/0
ROUTER3(config-if)#ip address 209.165.202.158 255.255.255.224
ROUTER3(config-if)#no shutdown
ROUTER3(config-if)#exit
ROUTER3(config)#interface s0/0/0
ROUTER3(config-if)#ip address 192.0.2.30 255.255.255.240
ROUTER3(config-if)#no shutdown
ROUTER3(config-if)#exit
ROUTER3(config)#router rip
ROUTER3(config-router)#version 2
ROUTER3(config-router)#network 209.165.202.128
ROUTER3(config-router)#network 192.0.2.16
ROUTER3(config-router)#end
ROUTER3#copy run start
```

QUESTION NO: 646

LAB - SIMULATION



You work as a network technician. Study the exhibit carefully. You are required to perform configurations to enable Internet access. The Router ISP has given you six public IP addresses in the 198.18.32.65 198.18.32.70/29 range.

Your Organization has 62 clients that needs to have simultaneous internet access. These local hosts use private IP addresses in the 192.168.6.65 - 192.168.6.126/26 range.
You need to configure Router1 using the PC1 console.
You have already made basic router configuration. You have also configured the appropriate NAT interfaces; NAT inside and NAT outside respectively.

Now you are required to finish the configuration of Router1.

Solution:

The company has 62 hosts that need to access the internet simultaneously but we just have 6 public IP addresses from 198.18.32.65 to 198.18.32.70/29 => we have to use NAT overload (or PAT)
Double click on PC1 to access Router1's command line interface
Router1>enable
Router1#configure terminal
Create a NAT pool of global addresses to be allocated with their netmask (notice that /29 = 248)
Router1(config)#ip nat pool mypool 198.18.32.65 198.18.32.70 netmask 255.255.255.248
Create a standard access control list that permits the addresses that are to be translated
Router1(config)#access-list 1 permit 192.168.6.64 0.0.0.63
Establish dynamic source translation, specifying the access list that was defined in the prior step
Router1(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 192.168.6.65 to 192.168.6.126, into an address from the pool named mypool (the pool contains addresses from 198.18.32.65 to 198.18.32.70)
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:
Router1(config)#interface fa0/0
Router1(config-if)#ip nat inside
Router1(config-if)#exit
Router1(config)#interface s0/0
Router1(config-if)#ip nat outside
Before leaving Router1, you should save the configuration:
Router1(config)#end (or Router1(config-if)#end)
Router1#copy running-config startup-config
Check your configuration by going to PC2 and type:

QUESTION NO: 647

Access List Lab.

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

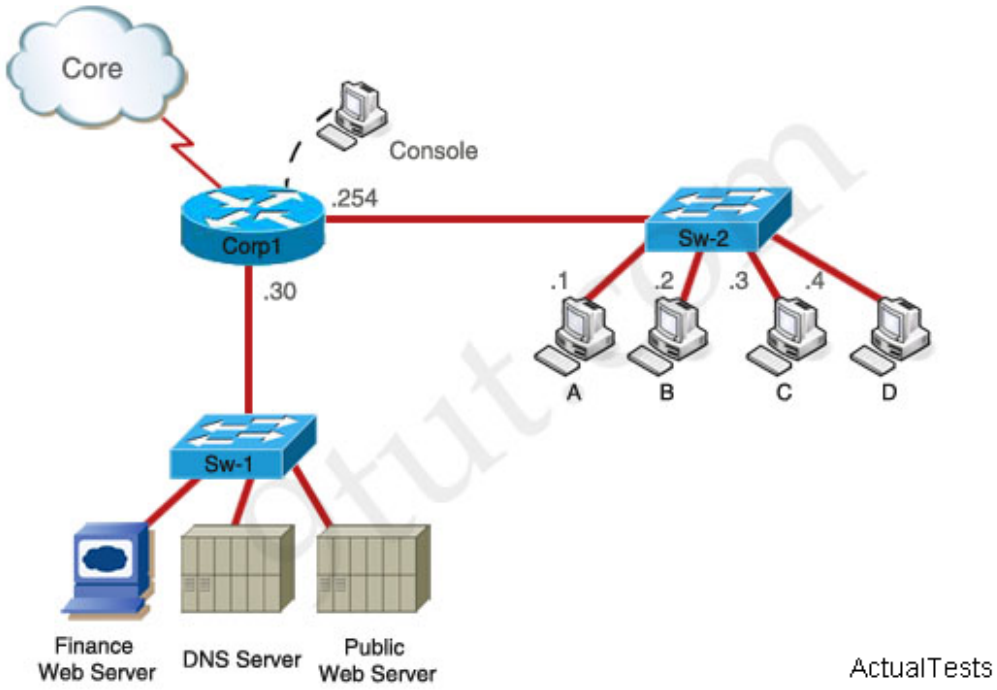
Host B 192.168.33.2

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.



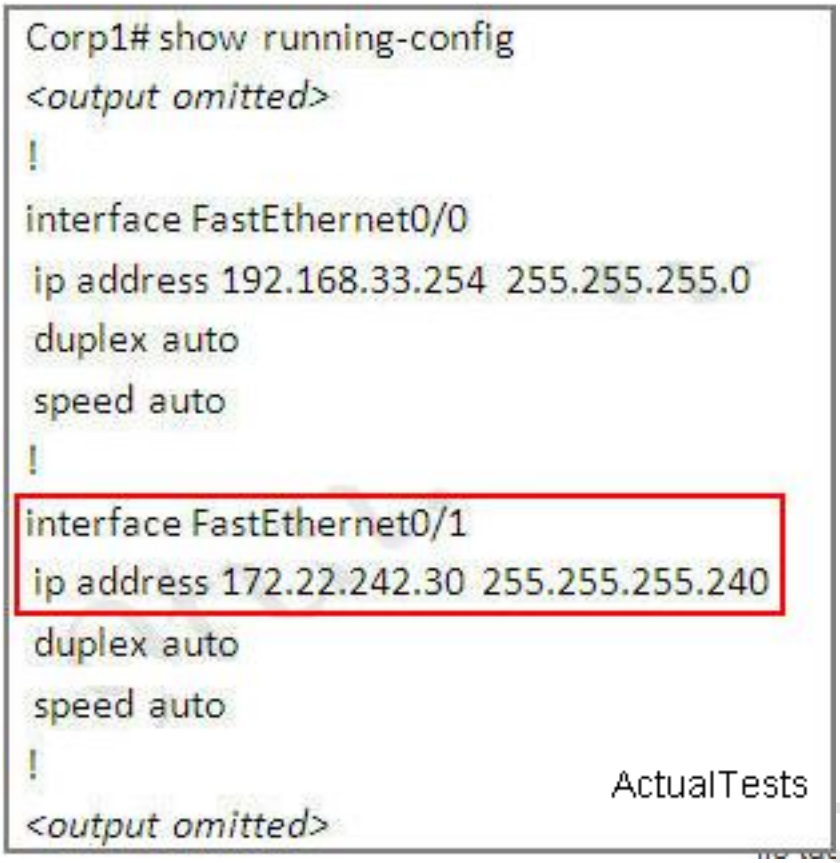
Explanation:

Corp1>enable (you may enter "cisco" as it passwords here)

We should create an access-list and apply it to the interface which is connected to the Server LAN because it can filter out traffic from both Sw-2 and Core networks. The Server LAN network has been assigned addresses of 172.22.242.17 - 172.22.242.30 so we can guess the interface connected to them has an IP address of 172.22.242.30 (.30 is the number shown in the figure).

Use the "show running-config" command to check which interface has the IP address of 172.22.242.30.

Corp1#show running-config



We learn that interface FastEthernet0/1 is the interface connected to Server LAN network. It is the interface we will apply our access-list (for outbound direction).

Corp1#configure terminal

Our access-list needs to allow host C - 192.168.33.3 to the Finance Web Server 172.22.242.23 via web (port 80)

Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80

Deny other hosts access to the Finance Web Server via web

Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80

All other traffic is permitted

Corp1(config)#access-list 100 permit ip any any

Apply this access-list to Fa0/1 interface (outbound direction)

Corp1(config)#interface fa0/1 Corp1(config-if)#ip access-group 100 out

Notice: We have to apply the access-list to Fa0/1 interface (not Fa0/0 interface) so that the access-list can filter traffic coming from the Core network.

Click on host C and open its web browser. In the address box type http://172.22.242.23 to check if you are allowed to access Finance Web Server or not. If your configuration is correct then you can access it.

Click on other hosts (A, B and D) and check to make sure you can't access Finance Web Server from these hosts.

Finally, save the configuration

Corp1(config-if)#end Corp1#copy running-config startup-config

(This configuration only prevents hosts from accessing Finance Web Server via web but if this server supports other traffic - like FTP, SMTP... then other hosts can access it, too.)