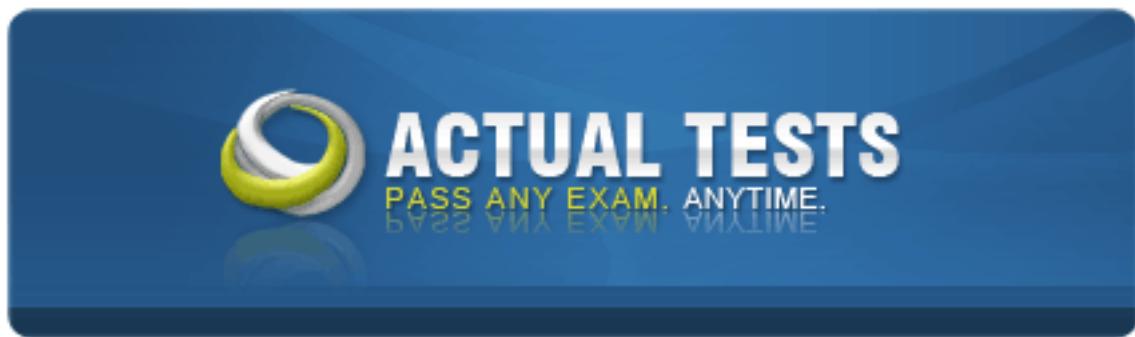


Cisco 100-101



Cisco Interconnecting Cisco Networking Devices Part 1 (ICND)

Version: 13.0

Topic 1, Operation of IP Data Networks**QUESTION NO: 1**

Which three statements are true about the operation of a full-duplex Ethernet network? (Choose three.)

- A. There are no collisions in full-duplex mode.
- B. A dedicated switch port is required for each full-duplex node.
- C. Ethernet hub ports are preconfigured for full-duplex mode.
- D. In a full-duplex environment, the host network card must check for the availability of the network media before transmitting.
- E. The host network card and the switch port must be capable of operating in full-duplex mode.

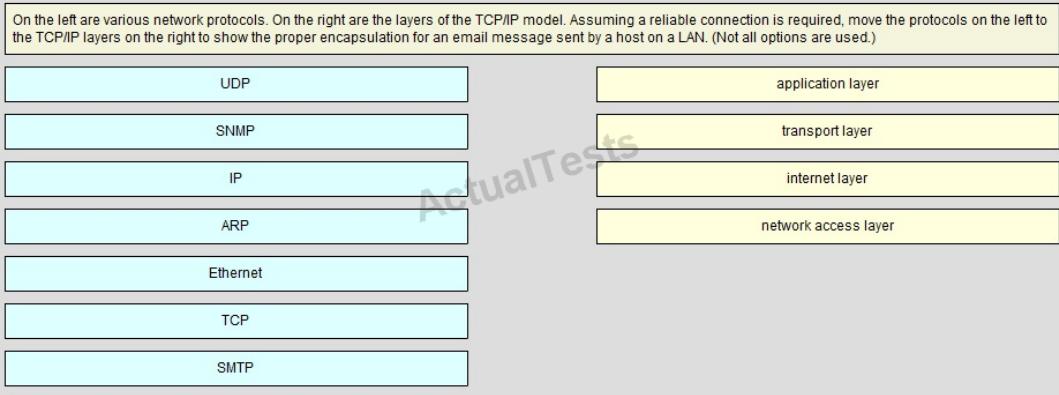
Answer: A,B,E**Explanation:**

Half-duplex Ethernet is defined in the original 802.3 Ethernet and Cisco says you only use one wire pair with a digital signal running in both directions on the wire. It also uses the CSMA/CD protocol to help prevent collisions and to permit retransmitting if a collision does occur. If a hub is attached to a switch, it must operate in half-duplex mode because the end stations must be able to detect collisions. Half-duplex Ethernet—typically 10BaseT—is only about 30 to 40 percent efficient as Cisco sees it, because a large 10BaseT network will usually only give you 3- to 4Mbps—at most.

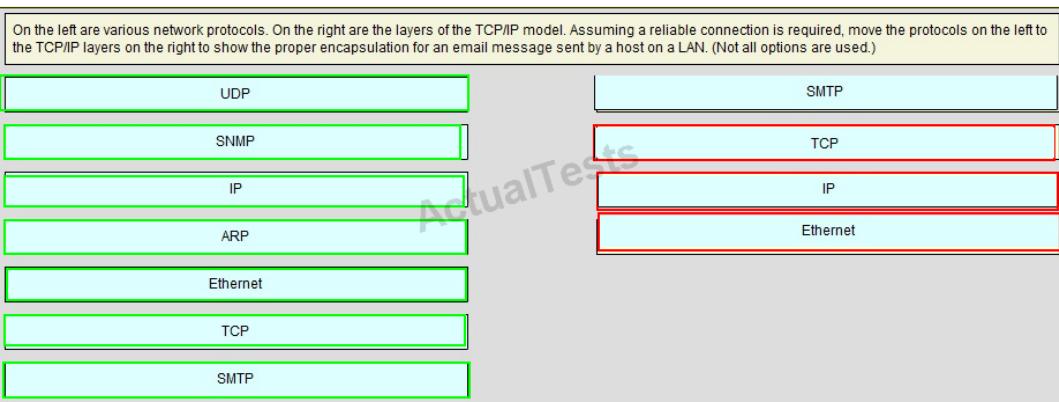
Full-duplex Ethernet uses two pairs of wires, instead of one wire pair like half duplex. Also, full duplex uses a point-to-point connection between the transmitter of the transmitting device and the receiver of the receiving device, which means that with full-duplex data transfer, you get a faster data transfer compared to half duplex. And because the transmitted data is sent on a different set of wires than the received data, no collisions occur. The reason you don't need to worry about collisions is because now Full-duplex Ethernet is like a freeway with multiple lanes instead of the single-lane road provided by half duplex. Full-duplex Ethernet is supposed to offer 100 percent efficiency in both directions; this means you can get 20Mbps with a 10Mbps Ethernet running full duplex, or 200Mbps for FastEthernet.

QUESTION NO: 2 DRAG DROP

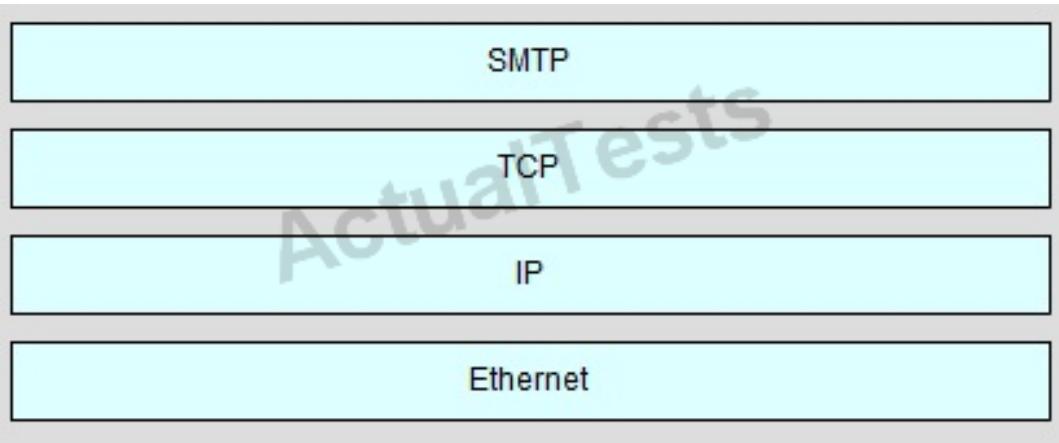
On the left are various network protocols. On the right are the layers of the TCP/IP model. Assuming a reliable connection is required, move the protocols on the left to the TCP/IP layers on the right to show the proper encapsulation for an email message sent by a host on a LAN. (Not all options are used.)



Answer:



Explanation:



QUESTION NO: 3

Which OSI layer header contains the address of a destination host that is on another network?

- A. application

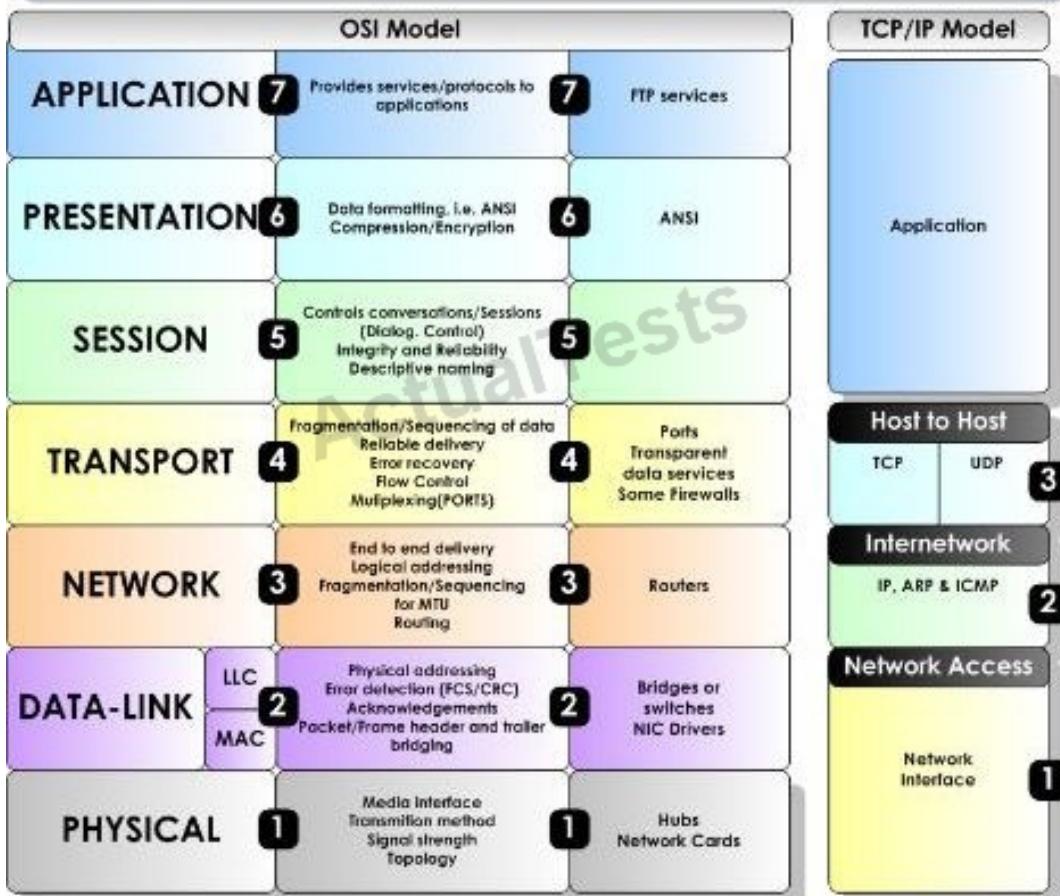
- B. session
- C. transport
- D. network
- E. data link
- F. physical

Answer: D

Explanation:

Only network address contains this information. To transmit the packets the sender uses network address and datalink address. But the layer 2 address represents just the address of the next hop device on the way to the sender. It is changed on each hop. Network address remains the same.

The OSI Model (Open Systems Interconnection)



QUESTION NO: 4

Which layer of the TCP/IP stack combines the OSI model physical and data link layers?

- A. Internet layer
- B. transport layer
- C. application layer
- D. network access layer

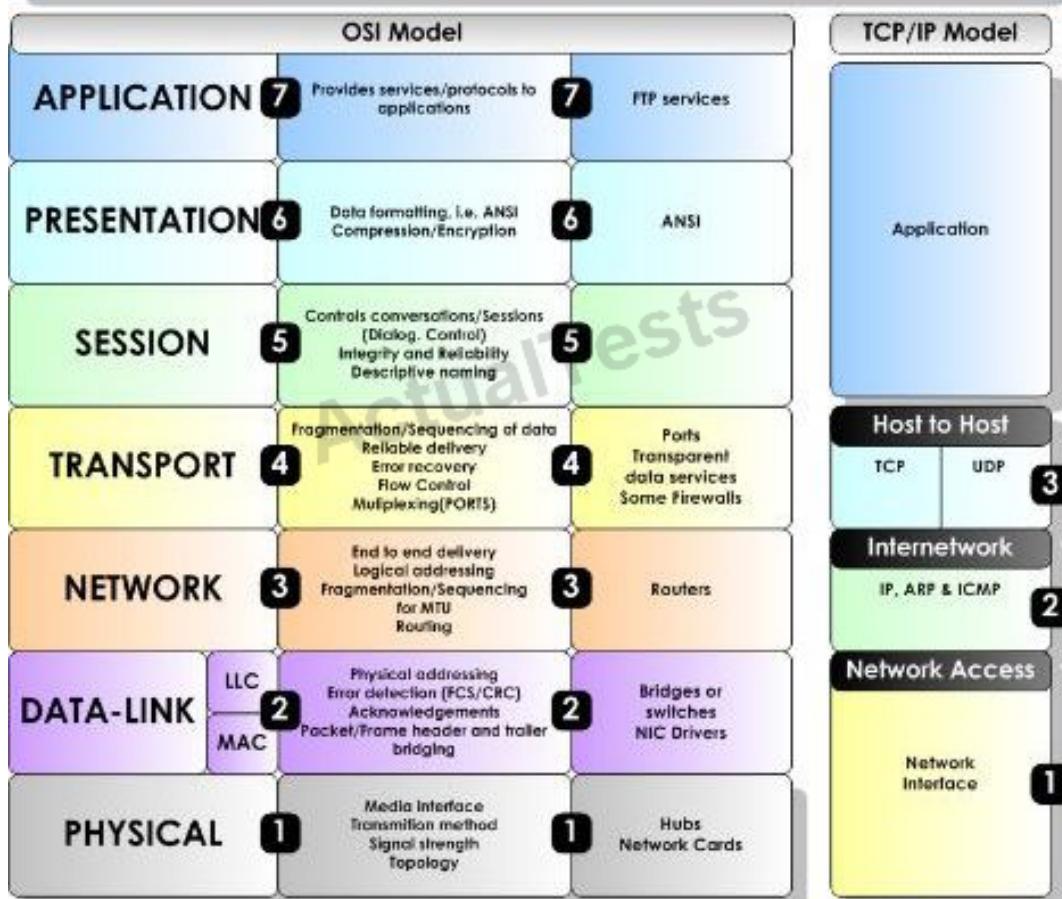
Answer: D

Explanation:

The Internet Protocol Suite, TCP/IP, is a suite of protocols used for communication over the internet. The TCP/ IP model was created after the OSI 7 layer model for two major reasons. First, the foundation of the Internet was built using the TCP/IP suite and through the spread of the World Wide Web and Internet, TCP/IP has been preferred. Second, a project researched by the Department of Defense (DOD) consisted of creating the TCP/IP protocols. The DOD's goal was to bring international standards which could not be met by the OSI model.

Since the DOD was the largest software consumer and they preferred the TCP/IP suite, most vendors used this model rather than the OSI. Below is a side by side comparison of the TCP/IP and OSI models.

The OSI Model (Open Systems Interconnection)



QUESTION NO: 5

Which protocol uses a connection-oriented service to deliver files between end systems?

- A. TFTP
- B. DNS
- C. FTP
- D. SNMP
- E. RIP

Answer: C

Explanation:

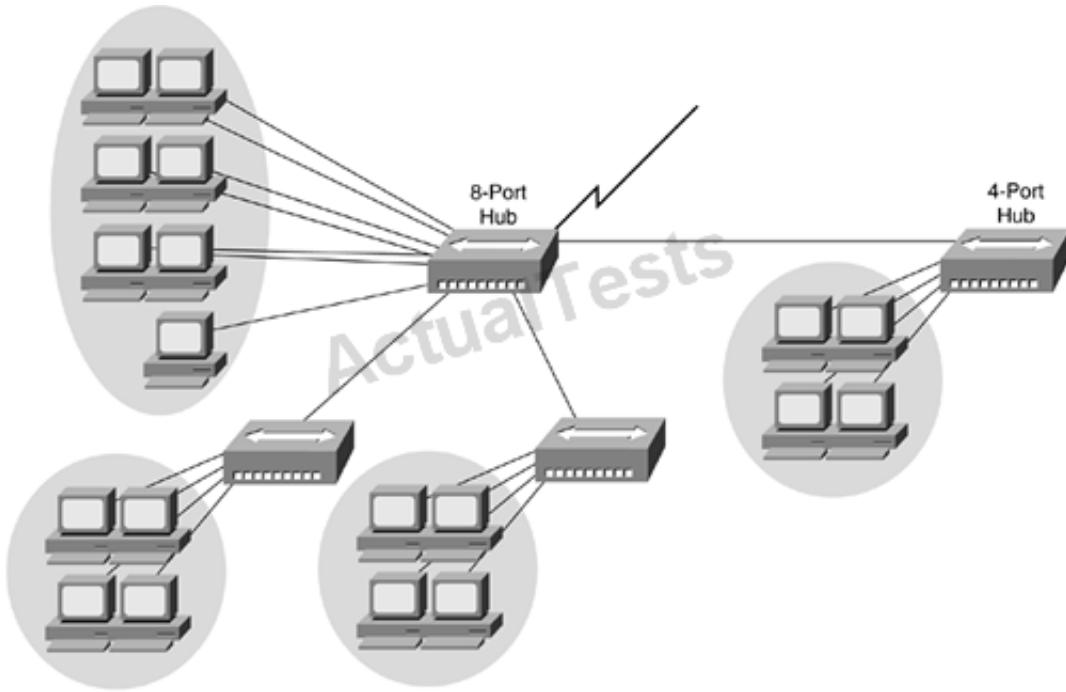
TCP is an example of a connection-oriented protocol. It requires a logical connection to be established between the two processes before data is exchanged. The connection must be maintained during the entire time that communication is taking place, then released afterwards. The process is much like a telephone call, where a virtual circuit is established--the caller must know the person's telephone number and the phone must be answered--before the message can be delivered.

TCP/IP is also a connection-oriented transport with orderly release. With orderly release, any data remaining in the buffer is sent before the connection is terminated. The release is accomplished in a three-way handshake between client and server processes. The connection-oriented protocols in the OSI protocol suite, on the other hand, do not support orderly release. Applications perform any handshake necessary for ensuring orderly release.

Examples of services that use connection-oriented transport services are telnet, rlogin, and ftp.

QUESTION NO: 6

Refer to the exhibit.



If the hubs in the graphic were replaced by switches, what would be virtually eliminated?

- A. broadcast domains
- B. repeater domains
- C. Ethernet collisions
- D. signal amplification
- E. Ethernet broadcasts

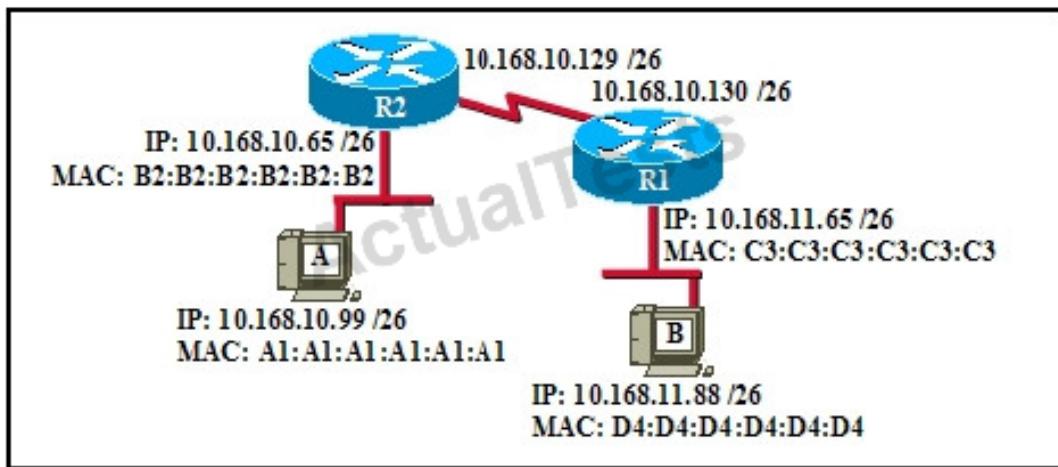
Answer: C

Explanation:

Modern wired networks use a network switch to eliminate collisions. By connecting each device directly to a port on the switch, either each port on a switch becomes its own collision domain (in the case of half duplex links) or the possibility of collisions is eliminated entirely in the case of full duplex links.

QUESTION NO: 7

Refer to the exhibit.



If host A sends an IP packet to host B, what will the source physical address be in the frame when it reaches host B?

- A. 10.168.10.99
- B. 10.168.11.88
- C. A1:A1:A1:A1:A1:A1
- D. B2:B2:B2:B2:B2:B2
- E. C3:C3:C3:C3:C3:C3
- F. D4:D4:D4:D4:D4:D4

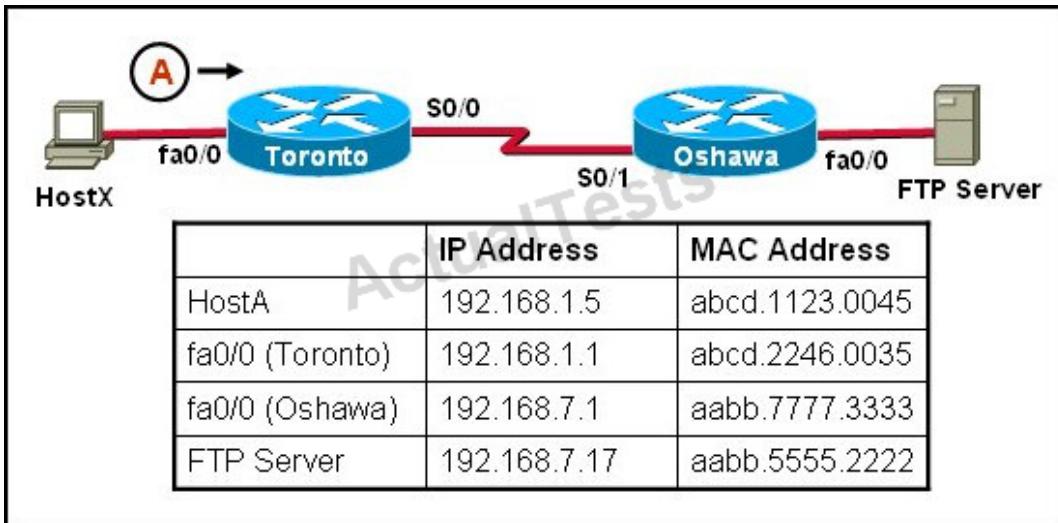
Answer: E

Explanation:

When packets transfer from one host to another across a routed segment, the source IP address always remains the same source IP address, and the source physical (MAC) address will be the existing router's interface address. Similarly, the destination IP address always remains the same and the destination physical (MAC) address is the destination router's interface address.

QUESTION NO: 8

Refer to the exhibit.



HostX is transferring a file to the FTP server. Point A represents the frame as it goes toward the Toronto router. What will the Layer 2 destination address be at this point?

- A. abcd.1123.0045
- B. 192.168.7.17
- C. aabb.5555.2222
- D. 192.168.1.1
- E. abcd.2246.0035

Answer: E

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 its default gateway, which is Toronto.

QUESTION NO: 9

Which network device functions only at Layer 1 of the OSI model?

A)



bridge

B)



hub

C)



NIC

D)



router

E)



switch

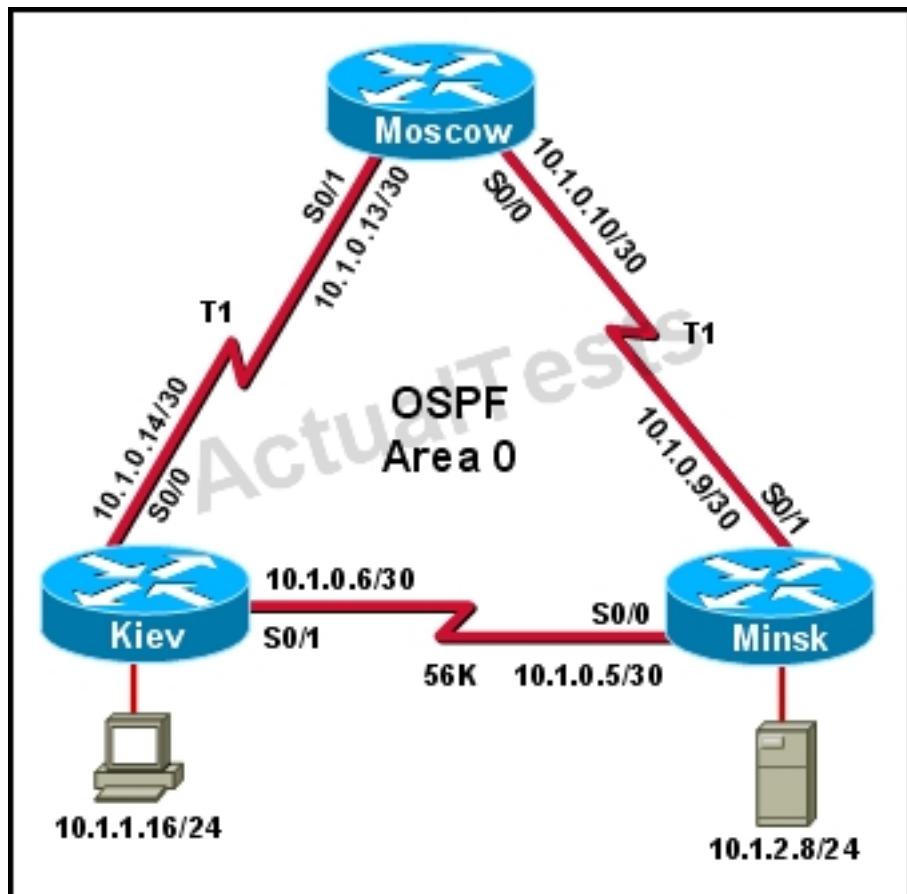
- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: B**Explanation:**

Most hubs are amplifying the electrical signal; therefore, they are really repeaters with several ports. Hubs and repeaters are Layer 1 (physical layer) devices.

QUESTION NO: 10

Refer to the exhibit.



The host in Kiev sends a request for an HTML document to the server in Minsk. What will be the source IP address of the packet as it leaves the Kiev router?

- A. 10.1.0.1
- B. 10.1.0.5
- C. 10.1.0.6
- D. 10.1.0.14
- E. 10.1.1.16
- F. 10.1.2.8

Answer: E

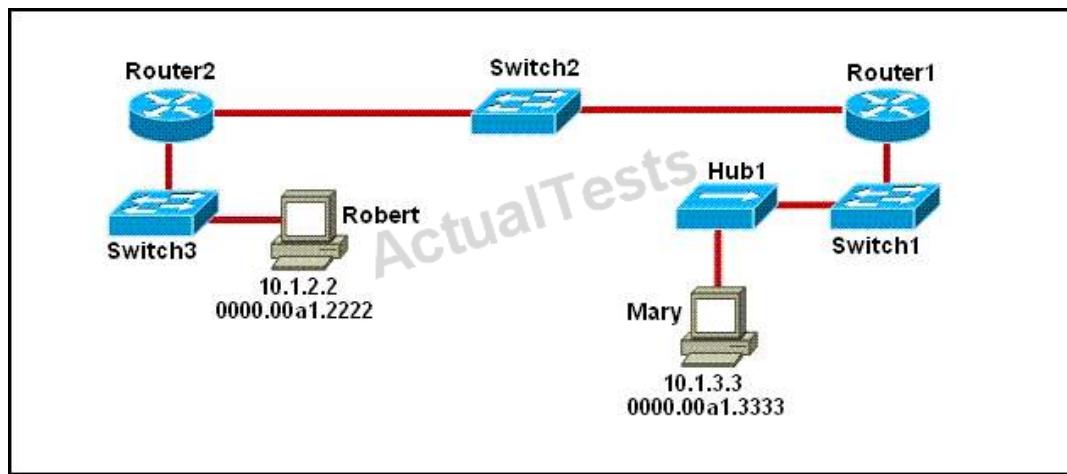
Explanation:

Although the source and destination MAC address will change as a packet traverses a network, the source and destination IP address will not unless network address translation (NAT) is being

done, which is not the case here.

QUESTION NO: 11

Refer to the exhibit.



As packets travel from Mary to Robert, which three devices will use the destination MAC address of the packet to determine a forwarding path? (Choose three.)

- A. Hub1
- B. Switch1
- C. Router1
- D. Switch2
- E. Router2
- F. Switch3

Answer: B,D,F

Explanation:

Switches use the destination MAC address information for forwarding traffic, while routers use the destination IP address information.

Local Area Networks employ Layer 2 Switches and Bridges to forward and filter network traffic. Switches and Bridges operate at the Data Link Layer of the Open System Interconnect Model (OSI). Since Switches and Bridges operate at the Layer 2 they operate more intelligently than hubs, which work at Layer 1 (Physical Layer) of the OSI. Because the switches and bridges are able to listen to the traffic on the wire to examine the source and destination MAC address. Being able to listen to the traffic also allows the switches and bridges to compile a MAC address table to better filter and forward network traffic.

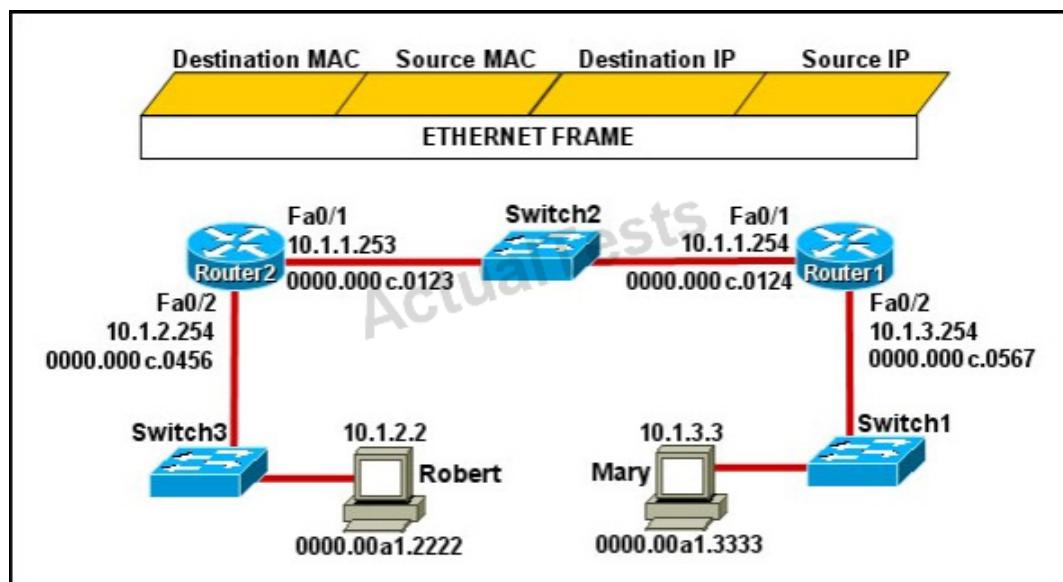
To accomplish the above functions switches and bridges carry out the following tasks:

MAC address learning by a switch or a bridge is accomplished by the same method. The switch or bridge listens to each device connected to each of its ports and scan the incoming frame for the source MAC address. This creates a MAC address to port map that is cataloged in the switches/bridge MAC database. Another name for the MAC address table is content addressable memory or CAM table.

When a switch or bridge is listening to the network traffic, it receives each frame and compares it to the MAC address table. By checking the MAC table the switch/ bridge are able to determine which port the frame came in on. If the frame is on the MAC table the frame is filtered or transmitted on only that port. If the switch determines that the frame is not on the MAC table, the frame is forwarded out to all ports except the incoming port.

QUESTION NO: 12

Refer to the exhibit.



Mary is sending an instant message to Robert. The message will be broken into a series of packets that will traverse all network devices. What addresses will populate these packets as they are forwarded from Router1 to Router2?

- A.
- | Destination MAC | Source MAC | Destination IP | Source IP |
|-----------------|----------------|----------------|-----------|
| 0000.00a1.2222 | 0000.00a1.3333 | 10.1.2.2 | 10.1.3.3 |
- B.
- | Destination MAC | Source MAC | Destination IP | Source IP |
|-----------------|----------------|----------------|-----------|
| 0000.000c.0123 | 0000.000c.0124 | 10.1.2.2 | 10.1.3.3 |
- C.
- | Destination MAC | Source MAC | Destination IP | Source IP |
|-----------------|----------------|----------------|------------|
| 0000.000c.0123 | 0000.000c.0124 | 10.1.1.253 | 10.1.1.254 |
- D.
- | Destination MAC | Source MAC | Destination IP | Source IP |
|-----------------|----------------|----------------|------------|
| 0000.00a1.2222 | 0000.00a1.3333 | 10.1.1.253 | 10.1.1.254 |
- E.
- | Destination MAC | Source MAC | Destination IP | Source IP |
|-----------------|----------------|----------------|-----------|
| 0000.000c.0456 | 0000.000c.0567 | 10.1.2.2 | 10.1.3.3 |

- A.** Option A
- B.** Option B
- C.** Option C
- D.** Option D
- E.** Option E

Answer: B

Explanation:

The Source and Destination IP address is not going to change. Host 1 IP address will stay as being the source IP and the Host 2 IP address will stay the destination IP address. Those two are not going to change.

For the MAC address it is going to change each time it goes from one host to another. (Except switches... they don't change anything)

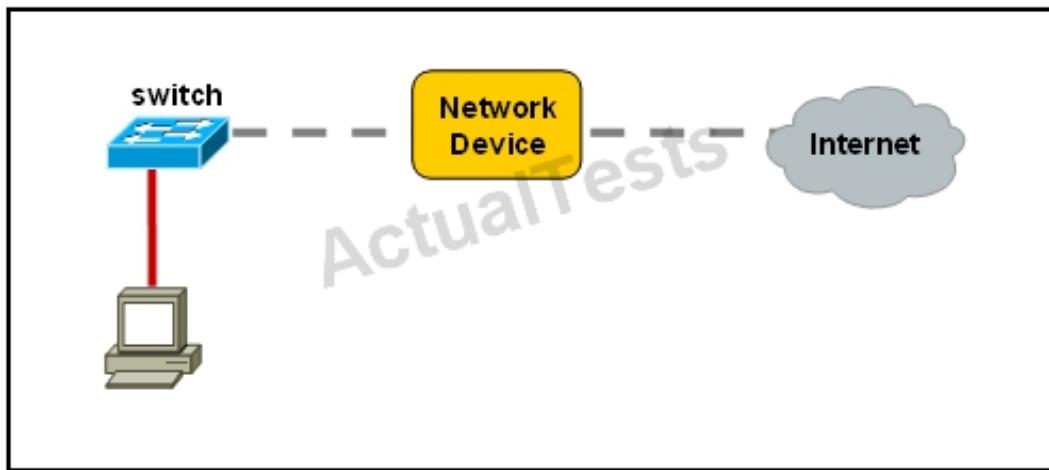
Frame leaving HOST 1 is going to have a source MAC of Host 1 and a destination MAC of Router 1.

Router 1 is going to strip that info off and then will make the source MAC address of Router1's exiting interface, and making Router2's interface as the destination MAC address.

Then the same will happen... Router2 is going to change the source/destination info to the source MAC being the Router2 interface that it is going out, and the destination will be Host2's MAC address.

QUESTION NO: 13

Refer to the exhibit.



A network device needs to be installed in the place of the icon labeled Network Device to accommodate a leased line attachment to the Internet. Which network device and interface configuration meets the minimum requirements for this installation?

- A. a router with two Ethernet interfaces
- B. a switch with two Ethernet interfaces
- C. a router with one Ethernet and one serial interface
- D. a switch with one Ethernet and one serial interface
- E. a router with one Ethernet and one modem interface

Answer: C

Explanation:

Only a router can terminate a leased line attachment access circuit, and only a router can connect two different IP networks. Here, we will need a router with two interfaces, one serial connection for the line attachment and one Ethernet interface to connect to the switch on the LAN.

QUESTION NO: 14

Which transport layer protocol provides best-effort delivery service with no acknowledgment

receipt required?

- A. HTTP
- B. IP
- C. TCP
- D. Telnet
- E. UDP

Answer: E

Explanation:

UDP provides a connectionless datagram service that offers best-effort delivery, which means that UDP does not guarantee delivery or verify sequencing for any datagrams. A source host that needs reliable communication must use either TCP or a program that provides its own sequencing and acknowledgment services.

QUESTION NO: 15

Which layer of the OSI model controls the reliability of communications between network devices using flow control, sequencing and acknowledgments?

- A. Physical
- B. Data-link
- C. Transport
- D. Network

Answer: C

Explanation:

Layer	Function	Examples
Application (Layer 7)	User interface	Telnet, HTTP
Presentation (Layer 6)	Handles encryption & changes to syntax	ASCII/EBCDIC, JPEG/MP3
Session (Layer 5)	Manages multiple applications and maintains synchronisation points	Operating systems, scheduling
Transport (Layer 4)	Provides reliable or best-effort delivery and (optional) error and flow control	TCP, UDP
Network (Layer 3)	Provides logical end-to-end addressing used by routers and hosts	IP
Data Link (Layer 2)	Creates frames from data bits, uses MAC addresses to access endpoints, and provides error detection but no correction	802.3, 802.2, HDLC, Frame Relay
Physical (Layer 1)	Specifies voltage, wire speed, and cable pin-outs	EIA/TIA, V.35

QUESTION NO: 16

Which statements are true regarding ICMP packets? (Choose two.)

- A. They acknowledge receipt of TCP segments.
- B. They guarantee datagram delivery.
- C. TRACERT uses ICMP packets.
- D. They are encapsulated within IP datagrams.
- E. They are encapsulated within UDP datagrams.

Answer: C,D

Explanation:

Ping may be used to find out whether the local machines are connected to the network or whether a remote site is reachable. This tool is a common network tool for determining the network connectivity, which uses ICMP protocol instead of TCP/IP and UDP/IP. This protocol is usually associated with the network management tools, which provide network information to network administrators, such as ping and traceroute (the later also uses the UDP/IP protocol).

ICMP is quite different from the TCP/IP and UDP/IP protocols. No source and destination ports are included in its packets. Therefore, usual packet-filtering rules for TCP/IP and UDP/IP are not applicable. Fortunately, a special "signature" known as the packet's Message type is included for denoting the purposes of the ICMP packet. Most commonly used message types are namely, 0, 3,

4, 5, 8, 11, and 12 which represent echo reply, destination unreachable, source quench, redirect, echo request, time exceeded, and parameter problem respectively.

In the ping service, after receiving the ICMP "echo request" packet from the source location, the destination

QUESTION NO: 17

Which statements accurately describe CDP? (Choose three.)

- A. CDP is an IEEE standard protocol.
- B. CDP is a Cisco proprietary protocol.
- C. CDP is a datalink layer protocol.
- D. CDP is a network layer protocol.
- E. CDP can discover directly connected neighboring Cisco devices.
- F. CDP can discover Cisco devices that are not directly connected.

Answer: B,C,E

Explanation:

CDP (Cisco Discovery Protocol) 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 containing useful info for troubleshooting and documenting the network.

QUESTION NO: 18

How does a switch differ from a hub?

- A. A switch does not induce any latency into the frame transfer time.
- B. A switch tracks MAC addresses of directly-connected devices.
- C. A switch operates at a lower, more efficient layer of the OSI model.
- D. A switch decreases the number of broadcast domains.
- E. A switch decreases the number of collision domains.

Answer: B

Explanation:

Some of the features and functions of a switch include:

A switch is essentially a fast, multi-port bridge, which can contain dozens of ports.

Rather than creating two collision domains, each port creates its own collision domain.

In a network of twenty nodes, twenty collision domains exist if each node is plugged into its own switch port.

If an uplink port is included, one switch creates twenty-one single-node collision domains.

A switch dynamically builds and maintains a Content-Addressable Memory (CAM) table, holding all of the necessary MAC information for each port.

For a detailed description of how switches operate, and their key differences to hubs, see the reference link below.

Reference: <http://www.cisco.com/warp/public/473/lan-switch-cisco.shtml>

QUESTION NO: 19

What must occur before a workstation can exchange HTTP packets with a web server?

- A.** A UDP connection must be established between the workstation and its default gateway.
- B.** A UDP connection must be established between the workstation and the web server.
- C.** A TCP connection must be established between the workstation and its default gateway.
- D.** A TCP connection must be established between the workstation and the web server.
- E.** An ICMP connection must be established between the workstation and its default gateway.
- F.** An ICMP connection must be established between the workstation and the web server.

Answer: D

Explanation:

HTTP uses TCP port 80, and a TCP port 80 connection must be established for HTTP communication to occur.

<http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/>

QUESTION NO: 20

How does TCP differ from UDP? (Choose two.)

- A.** TCP provides best effort delivery.

- B. TCP provides synchronized communication.
- C. TCP segments are essentially datagrams.
- D. TCP provides sequence numbering of packets.
- E. TCP uses broadcast delivery.

Answer: B,D

Explanation:

Because TCP is a connection-oriented protocol responsible for ensuring the transfer of a datagram from the source to destination machine (end-to-end communications), TCP must receive communications messages from the destination machine to acknowledge receipt of the datagram. The term virtual circuit is usually used to refer to the handshaking that goes on between the two end machines, most of which are simple acknowledgment messages (either confirmation of receipt or a failure code) and datagram sequence numbers.

Rather than impose a state within the network to support the connection, TCP uses synchronized state between the two endpoints. This synchronized state is set up as part of an initial connection process, so TCP can be regarded as a connection-oriented protocol. Much of the protocol design is intended to ensure that each local state transition is communicated to, and acknowledged by, the remote party.

Reference: http://en.wikibooks.org/wiki/Communication_Networks/TCP_and_UDP_Proocols

QUESTION NO: 21

A workstation has just resolved a browser URL to the IP address of a server. What protocol will the workstation now use to determine the destination MAC address to be placed into frames directed toward the server?

- A. HTTP
- B. DNS
- C. DHCP
- D. RARP
- E. ARP

Answer: E

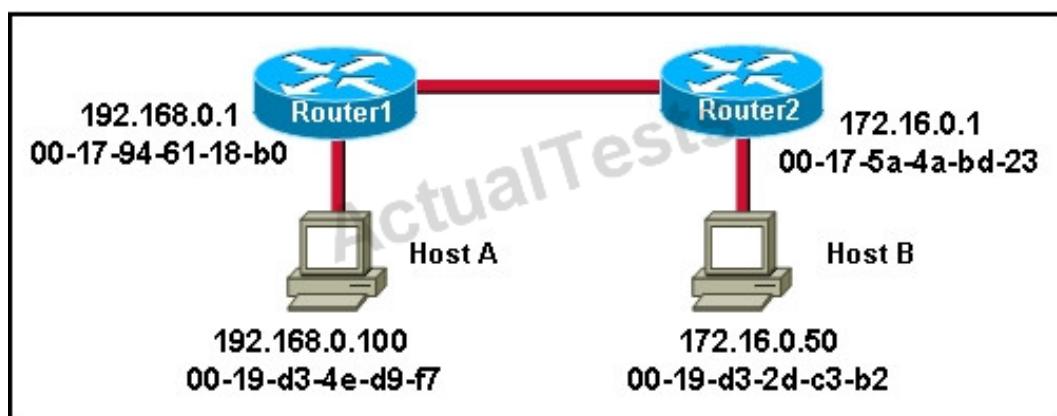
Explanation:

The RARP protocol is used to translate hardware interface addresses to protocol addresses. The RARP message format is very similar to the ARP format. When the booting computer sends the broadcast ARP request, it places its own hardware address in both the sending and receiving

fields in the encapsulated ARP data packet. The RARP server will fill in the correct sending and receiving IP addresses in its response to the message. This way the booting computer will know its IP address when it gets the message from the RARP server

QUESTION NO: 22

Refer to the exhibit.



Host A is sending a packet to Host B for the first time. What destination MAC address will Host A use in the ARP request?

- A. 192.168.0.1
- B. 172.16.0.50
- C. 00-17-94-61-18-b0
- D. 00-19-d3-2d-c3-b2
- E. ff-ff-ff-ff-ff-ff
- F. 255.255.255.255

Answer: E

Explanation:

For the initial communication, Host A will send a broadcast ARP (all F's) to determine the correct address to use to reach the destination.

ARP sends an Ethernet frame called an ARP request to every host on the shared link-layer segment. The Ethernet header includes the source host MAC address and a destination address of all Fs representing a broadcast frame. The ARP request contains the sender's MAC and IP address and the target (destination) IP address. The target's MAC address is set to all 0s.

ARP Request

Reference:

<http://www.technicalhowto.com/protocols/arp/arp.html>

QUESTION NO: 23

What are two common TCP applications? (Choose two.)

- A. TFTP
- B. SMTP
- C. SNMP
- D. FTP
- E. DNS

Answer: B,D

Explanation:

SMTP uses TCP port 25, while FTP uses TCP ports 20 and 21.

Reference: <http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/>

QUESTION NO: 24

Refer to the exhibit.

```
SwitchA# show mac-address-table
< non-essential output omitted >
      Destination Address  Address Type  VLAN  Destination Port
      -----  -----  -----  -----
      00b0.d056.fe4d    Dynamic     1    FastEthernet0/3
      00b0.d043.ac2e    Dynamic     1    FastEthernet0/4
      00b0.d0fe.ac32    Dynamic     1    FastEthernet0/5
      00b0.d0da.cb56    Dynamic     1    FastEthernet0/6
```

Frame received by SwitchA:

Source MAC	Destination MAC	Source IP	Destination IP
00b0.d056.fe4d	00b0.d0da.cb56	192.168.40.5	192.168.40.6

SwitchA receives the frame with the addressing shown. According to the command output also shown in the exhibit, how will SwitchA handle this frame?

- A. It will drop the frame.
- B. It will forward the frame out port Fa0/6 only.
- C. It will flood the frame out all ports.
- D. It will flood the frame out all ports except Fa0/3.

Answer: B

Explanation:

Switches keep the learned MAC addresses in a table, so that when a frame comes in with a destination MAC address that the switch has already learned, it will forward it to that port only. If a frame comes in with a destination MAC that is not already in the MAC address table, then the frame will be flooded to all ports except for the one that it came in on. In this case, Switch A already knows that 00b0.d0da.cb56 resides on port fa0/6, so it will forward the from out that port.

QUESTION NO: 25

Refer to the exhibit.

SwitchA# show mac-address-table				
< non-essential output omitted >				
Destination Address	Address Type	VLAN	Destination Port	
00b0.d056.fe4d	Dynamic	1	FastEthernet0/3	
00b0.d043.ac2e	Dynamic	1	FastEthernet0/4	
00b0.d0fe.ac32	Dynamic	1	FastEthernet0/5	
00b0.d0da.cb56	Dynamic	1	FastEthernet0/6	

Frame received by SwitchA:

Source MAC	Destination MAC	Source IP	Destination IP
00b0.d056.fe4d	00b0.d0da.cb56	192.168.40.5	192.168.40.6

SwitchA receives the frame with the addressing shown in the exhibit. According to the command output also shown in the exhibit, how will SwitchA handle this frame?

- A. It will drop the frame.

- B. It will forward the frame out port Fa0/6 only.
- C. It will forward the frame out port Fa0/3 only.
- D. It will flood the frame out all ports.
- E. It will flood the frame out all ports except Fa0/3.

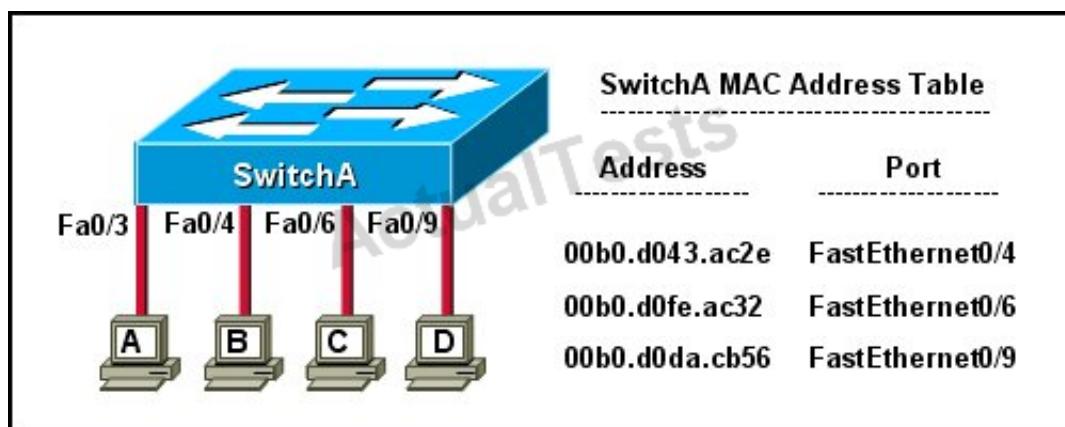
Answer: E

Explanation:

When frame receives the frame, it checks the source address on MAC table if MAC address found in MAC table it tries to forward if not in MAC table adds the Address on MAC table. After checking the source address, it checks the destination address on MAC table, if MAC address found on MAC table it forwards to proper ports otherwise floods on all ports except the source port.

QUESTION NO: 26

Refer to the exhibit.



The exhibit is showing the topology and the MAC address table. Host A sends a data frame to host D. What will the switch do when it receives the frame from host A?

- A. The switch will add the source address and port to the MAC address table and forward the frame to host D.
- B. The switch will discard the frame and send an error message back to host A.
- C. The switch will flood the frame out of all ports except for port Fa0/3.
- D. The switch will add the destination address of the frame to the MAC address table and forward the frame to host D.

Answer: A

Explanation:

When switch receives the data frame from the host not having the MAC address already on the MAC table, it will add the MAC address to source port on MAC address table and sends the data frame.

QUESTION NO: 27

Which two statements describe the operation of the CSMA/CD access method? (Choose two.)

- A. In a CSMA/CD collision domain, multiple stations can successfully transmit data simultaneously.
- B. In a CSMA/CD collision domain, stations must wait until the media is not in use before transmitting.
- C. The use of hubs to enlarge the size of collision domains is one way to improve the operation of the CSMA/CD access method.
- D. After a collision, the station that detected the collision has first priority to resend the lost data.
- E. After a collision, all stations run a random backoff algorithm. When the backoff delay period has expired, all stations have equal priority to transmit data.
- F. After a collision, all stations involved run an identical backoff algorithm and then synchronize with each other prior to transmitting data.

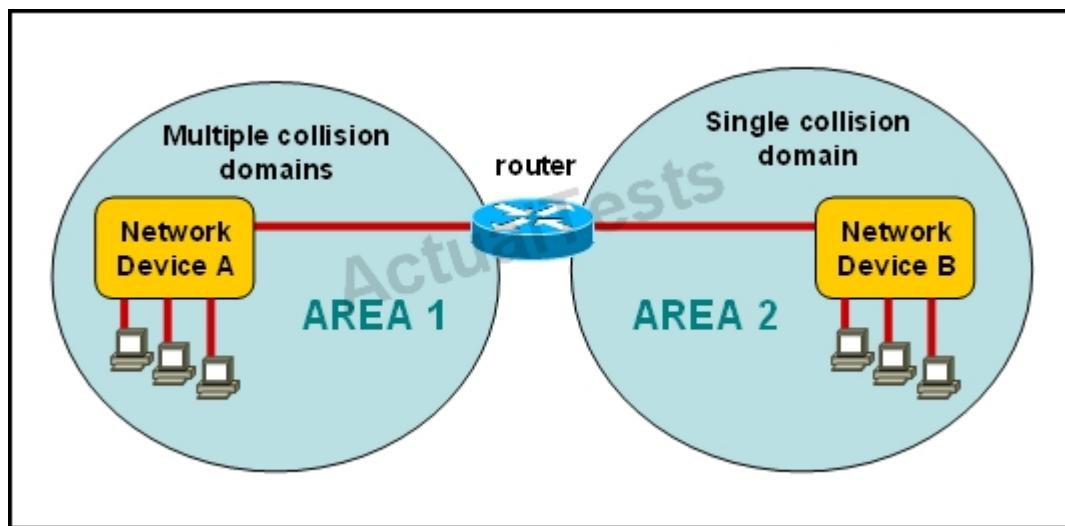
Answer: B,E

Explanation:

Ethernet networking uses Carrier Sense Multiple Access with Collision Detect (CSMA/CD), a protocol that helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium. CSMA/CD was created to overcome the problem of those collisions that occur when packets are transmitted simultaneously from different nodes. And trust me, good collision management is crucial, because when a node transmits in a CSMA/CD network, all the other nodes on the network receive and examine that transmission. Only bridges and routers can effectively prevent a transmission from propagating throughout the entire network! So, how does the CSMA/CD protocol work? Like this: when a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire. If all is clear (no other host is transmitting), the host will then proceed with its transmission. But it doesn't stop there. The transmitting host constantly monitors the wire to make sure no other hosts begin transmitting. If the host detects another signal on the wire, it sends out an extended jam signal that causes all nodes on the segment to stop sending data (think, busy signal). The nodes respond to that jam signal by waiting a while before attempting to transmit again. Backoff algorithms determine when the colliding stations can retransmit. If collisions keep occurring after 15 tries, the nodes attempting to transmit will then time out.

QUESTION NO: 28

Refer to the exhibit.



A network has been planned as shown. Which three statements accurately describe the areas and devices in the network plan? (Choose three.)

- A. Network Device A is a switch.
- B. Network Device B is a switch.
- C. Network Device A is a hub.
- D. Network Device B is a hub.
- E. Area 1 contains a Layer 2 device.
- F. Area 2 contains a Layer 2 device.

Answer: A,D,E

Explanation:

Switches use a separate collision domain for each port, so device A must be a switch. Hubs, however, place all ports in the same collision domain so device B is a hub. Switches reside in layer 2 while hubs are layer 1 devices.

QUESTION NO: 29

On a Cisco switch, which protocol determines if an attached VoIP phone is from Cisco or from another vendor?

- A. RTP
- B. TCP
- C. CDP
- D. UDP

Answer: C

Explanation:

The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.

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 the network.

CDP messages are generated every 60 seconds as multicast messages on each of its active interfaces.

The information shared in a CDP packet about a Cisco device includes the following:

Name of the device configured with the hostname command

IOS software version

Hardware capabilities, such as routing, switching, and/or bridging

Hardware platform, such as 2600, 2950, or 1900

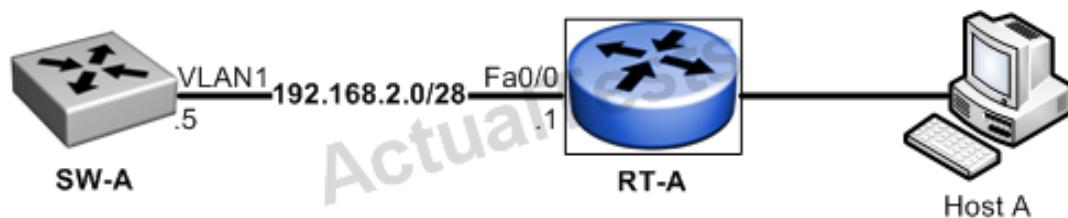
The layer-3 address(es) of the device

The interface the CDP update was generated on

Reference: <http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discoveryprotocol.html>

QUESTION NO: 30

Refer to the exhibit.



What must be configured to establish a successful connection from Host A to switch SW-A through router RT-A?

- A. VLAN 1 on RT-A
- B. IP routing on SW-A
- C. default gateway on SW-A
- D. crossover cable connecting SW-A and RT-A

Answer: C

Explanation:

In order for the switch to reach networks that are not local, such as networks attached to different interfaces of the router, it will need to set its default gateway to be the IP address of the attached router.

QUESTION NO: 31

At which layer of the OSI model does the protocol that provides the information that is displayed by the show cdp neighbors command operate?

- A. application
- B. transport
- C. network
- D. physical
- E. data link

Answer: E

Explanation:

CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols.

CDP allows devices to share basic configuration information without even configuring any protocol specific information and is enabled by default on all interfaces.

CDP is a Datalink Protocol occurring at Layer 2 of the OSI model.

CDP is not routable and can only go over to directly connected devices.

CDP is enabled, by default, on all Cisco devices. CDP updates are generated as multicasts every

60 seconds with a hold-down period of 180 seconds for a missing neighbor. The no cdp run command globally disables CDP, while the no cdp enable command disables CDP on an interface. Use show cdp neighbors to list out your directly connected Cisco neighboring devices. Adding the detail parameter will display the layer-3 addressing configured on the neighbor. Reference: <http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discoveryprotocol.html>

QUESTION NO: 32

Which two characteristics apply to Layer 2 switches? (Choose two.)

- A. Increases the number of collision domains
- B. Decreases the number of collision domains
- C. Implements VLAN
- D. Decreases the number of broadcast domains
- E. Uses the IP address to make decisions for forwarding data packets

Answer: A,C

Explanation:

Layer 2 switches offer a number of benefits to hubs, such as the use of VLANs and each switch port is in its own separate collision domain, thus eliminating collisions on the segment.

QUESTION NO: 33

Which two characteristics describe the access layer of the hierarchical network design model? (Choose two.)

- A. layer 3 support
- B. port security
- C. redundant components
- D. VLANs
- E. PoE

Answer: B,D

Explanation:

Access layer

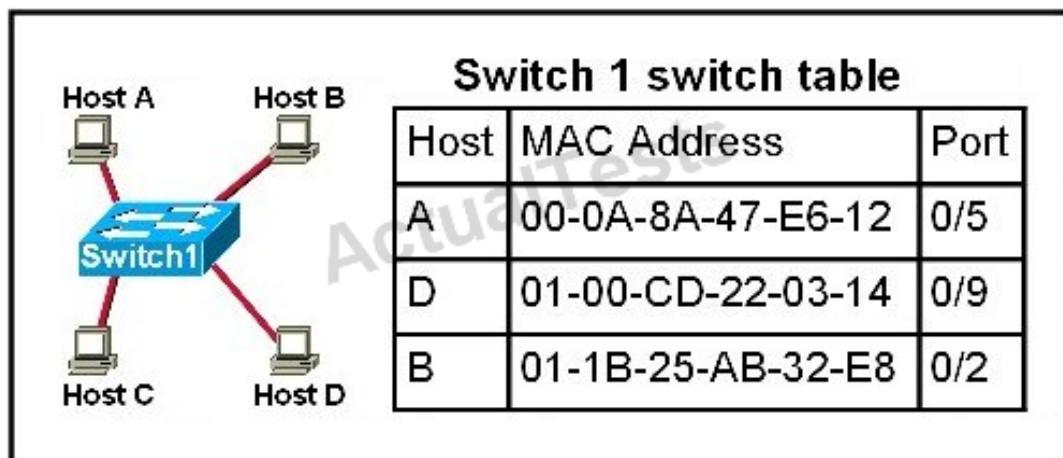
The main purpose of the access layer is to provide direct connection to devices on the network and controlling which devices are allowed to communicate over it. The access layer interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs, and wireless access points (AP).

Switch features in the Access layer:

References: <http://www.ciscopath.com/content/61/>
http://www.mcmcse.com/cisco/guides/hierarchical_model.shtml

QUESTION NO: 34

Refer to the topology and switching table shown in the graphic.



Host B sends a frame to Host C. What will the switch do with the frame?

- A. Drop the frame
- B. Send the frame out all ports except port 0/2
- C. Return the frame to Host B
- D. Send an ARP request for Host C
- E. Send an ICMP Host Unreachable message to Host B
- F. Record the destination MAC address in the switching table and send the frame directly to Host C

Answer: B

Explanation:

An Ethernet switch appears to use the same logic as a transparent bridge. However, the internal logic of the switch is optimized for performing the basic function of choosing when to forward and when to filter a frame. Just as with a transparent bridge, the basic logic of a LAN switch is as follows:

- Step 1** A frame is received.
- Step 2** If the destination is a broadcast or multicast, forward on all ports.
- Step 3** If the destination is a unicast and the address is not in the address table, forward on all ports.
- Step 4** If the destination is a unicast and the address is in the address table, forward the frame out the associated port, unless the MAC address is associated with the incoming port.

QUESTION NO: 35

Refer to the exhibit.

RouterA# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

- 172.16.0.0/24 is subnetted, 1 subnets
 - C 172.16.1.0 is directly connected, Ethernet0/1
 - 10.0.0.0/30 is subnetted, 1 subnets
 - C 10.255.255.200 is directly connected, Serial0/0
 - S* 0.0.0.0/0 is directly connected, Serial0/0

RouterA#

The output is from a router in a large enterprise. From the output, determine the role of the router.

- A. A Core router.

- B. The HQ Internet gateway router.
- C. The WAN router at the central site.
- D. Remote stub router at a remote site.

Answer: D

Explanation:

Since the routing table shows only a single default route using the single interface serial 0/0, we know that this is most likely a remote stub site with a single connection to the rest of the network. All the other answer options would mean that this router would have more connections, and would contain more routes.

QUESTION NO: 36

To what type of port would a cable with a DB-60 connector attach?

- A. Serial port
- B. Console port
- C. Ethernet port
- D. Fibre optic port

Answer: A

Explanation:

Serial Connection



The picture on the left shows a V.35 DTE cable with a male DB60 connector and a male standard

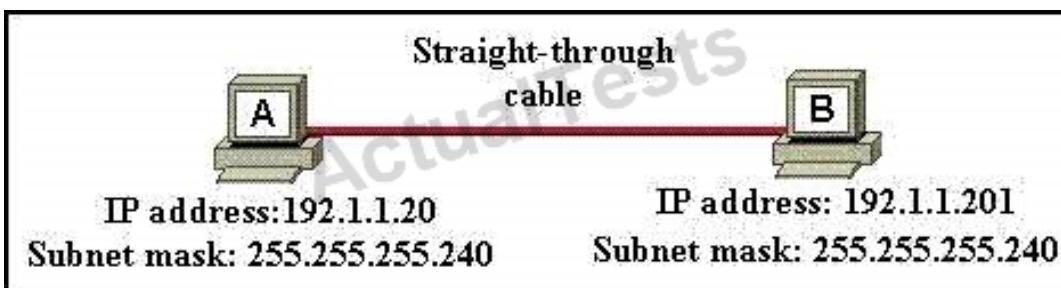
34-pin Winchester-type connector. The right picture shows a V.35 DCE serial cable with a male DB60 connector and a female 34-pin Winchester-type connector. As you probably guessed already, the male connector of the DTE cable is attached to the DCE cable's female connector, this is depicted in the picture below. This is known as a back-to-back connection, and 'simulates' a WAN link. In a real world setup, the DTE cable's male connector typically connects to a port on a CSU/DSU provided by a service provider (i.e. telco), which in turn connects to a CSU/DSU at another location, thru a T1 link for example. The DB60 connector connects to a Serial interface on a router.



Reference: http://www.techexams.net/techlabs/ccna/lab_hardware.shtml

QUESTION NO: 37

A 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. A crossover cable should be used in place of the straight-through cable.
- B. A rollover cable should be used in place of the straight-through cable.
- C. The subnet masks should be set to 255.255.255.192
- D. A default gateway needs to be set on each host.
- E. The hosts must be reconfigured to use private IP addresses for direct connections of this type.
- F. The subnet masks should be set to 255.255.255.0

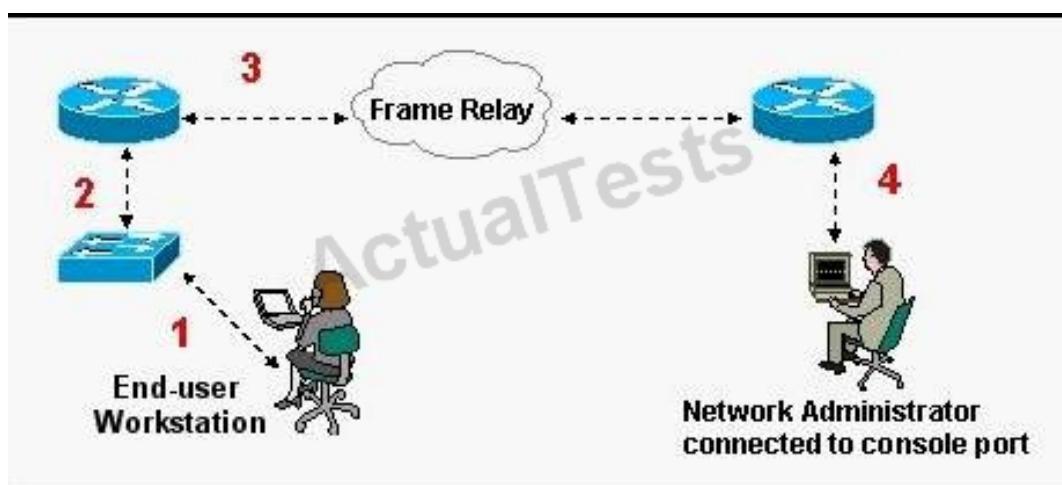
Answer: A,F**Explanation:**

If you need to connect two computers but you don't have access to a network and can't set up an ad hoc network, you can use an Ethernet crossover cable to create a direct cable connection. Generally speaking, a crossover cable is constructed by reversing (or crossing over) the order of the wires inside so that it can connect two computers directly. A crossover cable looks almost exactly like a regular Ethernet cable (a straight-through cable), so make sure you have a crossover cable before following these steps.

Both devices need to be on the same subnet, and since one PC is using 192.1.1.20 and the other is using 192.1.1.201, the subnet mask should be changed to 255.255.255.0.

QUESTION NO: 38

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 Crossover cable
 - 2 - Ethernet straight-through cable
 - 3 - Fiber Optic cable
 - 4 - Rollover cable
- B.**
 - 1 - Ethernet straight-through cable
 - 2 - Ethernet straight-through cable
 - 3 - Serial cable

- 4 - Rollover cable
- C.** 1 - Ethernet rollover cable
- 2 - Ethernet crossover cable
- 3 - Serial cable
- 4 - Null-modem cable
- D.** 1 - Ethernet straight-through cable
- 2 - Ethernet Crossover cable
- 3 - Serial cable
- 4 - Rollover cable
- E.** 1 - Ethernet straight-through cable
- 2 - Ethernet Crossover cable
- 3 - Serial cable
- 4 - Ethernet Straight-through cable

Answer: B

Explanation:

When connecting a PC to a switch, a standard Ethernet straight through cable should be used. This same cable should also be used for switch to router connections. Generally speaking, crossover cables are only needed when connecting two like devices (PC-PC, switch-switch, router-router, etc).

Routers connect to frame relay and other WAN networks using serial cables.

Rollover cables are special cables used for connecting to the console ports of Cisco devices.

QUESTION NO: 39

Which of the following are types of flow control? (Choose three.)

- A.** buffering
- B.** cut-through
- C.** windowing
- D.** congestion avoidance
- E.** load balancing

Answer: A,C,D

Explanation:

During Transfer of data, a high speed computer is generating data traffic a lot faster than the network device can handle in transferring to destination, so single gateway or destination device cannot handle much amount of traffic that is called "Congestion".

Buffering

The Technie is used to control the data transfer when we have congestion, when a network device receive a data it stores in memory section and then transfer to next destination this process called "Buffering".

Windowing Whereas Windowing is used for flow control by the Transport layer.

Say the sender device is sending segments and the receiver device can accommodate only a fixed number of segments before it can accept more, the two devices negotiate the window size during the connection setup.

This is done so that the sending device doesn't overflow the receiving device's buffer.

Also the receiving device can send a single acknowledgement for the segments it has received instead of sending an acknowledgement after every segment received.

Also, this window size is dynamic meaning, the devices can negotiate and change the window size in the middle of a session. So if initially the window size is three and the receiving device thinks that it can accept more number of segments in its buffer it can negotiate with the sending device and it increases it to say 5 for example.

Windowing is used only by TCP since UDP doesn't use or allow flow control.

Reference: <http://www.info-it.net/cisco/ccna/exam-tips/flow-control.php>

QUESTION NO: 40

Refer to the exhibit.

SwitchA# show mac-address-table				
< non-essential output omitted >				
Destination Address	Address Type	VLAN	Destination Port	
00b0.d056.fe4d	Dynamic	1	FastEthernet0/3	
00b0.d043.ac2e	Dynamic	1	FastEthernet0/4	
00b0.d0fe.ac32	Dynamic	1	FastEthernet0/5	
00b0.d0da.cb56	Dynamic	1	FastEthernet0/6	

Frame received by SwitchA:

Source MAC	Destination MAC	Source IP	Destination IP
00b0.d056.fe4d	00b0.d0da.895a	192.168.40.5	192.168.40.6

Which option describes how SwitchA will handle the frame just received?

- A. It will drop the frame.
- B. It will forward the frame out of port Fa0/3 only.
- C. It will flood the frame out all ports.
- D. It will flood the frame out of all the ports except Fa0/3.

Answer: D

Explanation:

Topic 2, LAN Switching Technologies

QUESTION NO: 41

Which two options will help to solve the problem of a network that is suffering a broadcast storm?
(Choose two.)

- A. a bridge
- B. a router
- C. a hub
- D. a Layer 3 switch
- E. an access point

Answer: B,D

Explanation:

Routers and layer 3 switches will not propagate broadcast traffic beyond the local segment, so the use of these devices is the best method for eliminating broadcast storms.

QUESTION NO: 42

A switch receives a frame on one of its ports. There is no entry in the MAC address table for the destination MAC address. What will the switch do with the frame?

- A. drop the frame
- B. forward it out of all ports except the one that received it
- C. forward it out of all ports
- D. store it until it learns the correct port

Answer: B

Explanation:

Understanding this concept is prime for understanding that when switch receives the data frame from the host not having the MAC address already in the MAC table, it will add the MAC address to the source port on the MAC address table and sends the data frame. If the switch already has the MAC address in its table for the destination, it will forward the frame directly to the destination port. If it was not already in its MAC table, then they frame would have been flooded out all ports except for the port that it came from.

QUESTION NO: 43

Which address type does a switch use to make selective forwarding decisions?

- A. Source IP address
- B. Destination IP address
- C. Source and destination IP address
- D. Source MAC address
- E. Destination MAC address

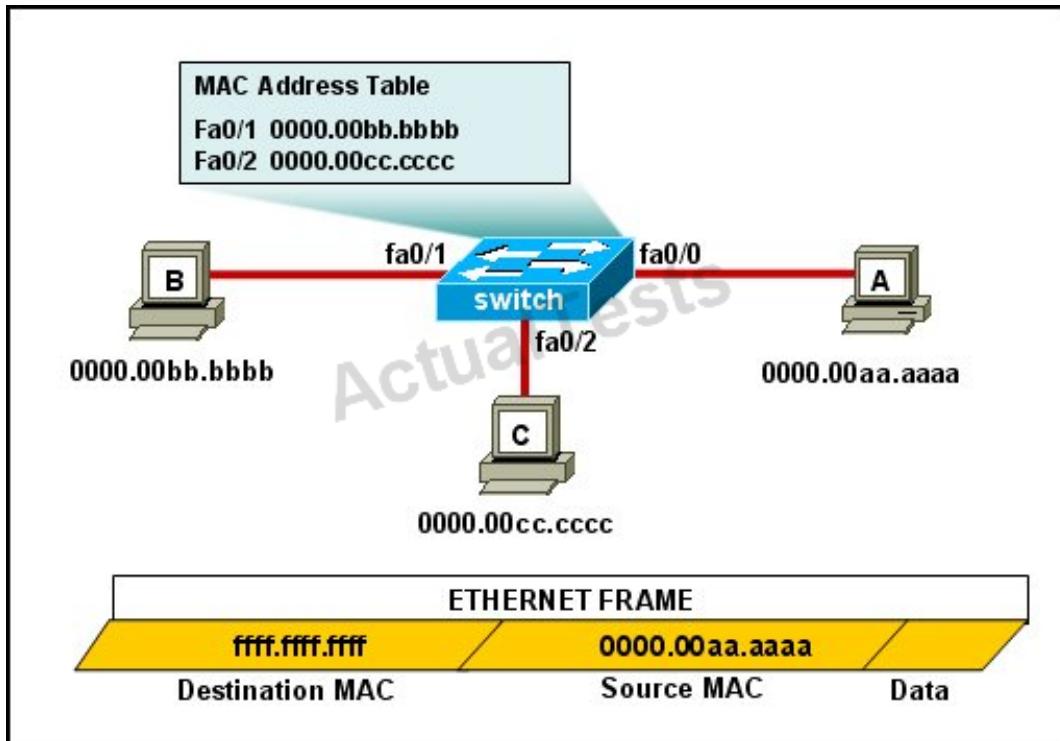
Answer: E

Explanation:

Switches analyze the destination MAC to make its forwarding decision since it is a layer 2 device. Routers use the destination IP address to make forwarding decisions.

QUESTION NO: 44

Refer to the exhibit.



The MAC address table is shown in its entirety. The Ethernet frame that is shown arrives at the switch.

What two operations will the switch perform when it receives this frame? (Choose two.)

- A. The switch will not forward a frame with this destination MAC address.
- B. The MAC address of 0000.00aa.aaaa will be added to the MAC Address Table.
- C. The MAC address of ffff.ffff.ffff will be added to the MAC address table.
- D. The frame will be forwarded out of all the active switch ports except for port fa0/0.
- E. The frame will be forwarded out of fa0/0 and fa0/1 only.
- F. The frame will be forwarded out of all the ports on the switch.

Answer: B,D

Explanation:

If the switch already has the MAC address in its table for the destination, it will forward the frame directly to the destination port. If it was not already in its MAC table, then the frame would have been flooded out all ports except for the port that it came from.

QUESTION NO: 45

What does a host on an Ethernet network do when it is creating a frame and it does not have the

destination address?

- A. Drops the frame
- B. Sends out a Layer 3 broadcast message
- C. Sends a message to the router requesting the address
- D. Sends out an ARP request with the destination IP address

Answer: D

Explanation:

In this case, it will send out an ARP request for MAC address of the destination IP (assuming it doesn't already have it in its table) and then address it to the destination's MAC address.

QUESTION NO: 46

A switch has 48 ports and 4 VLANs. How many collision and broadcast domains exist on the switch (collision, broadcast)?

- A. 4, 48
- B. 48, 4
- C. 48, 1
- D. 1, 48
- E. 4, 1

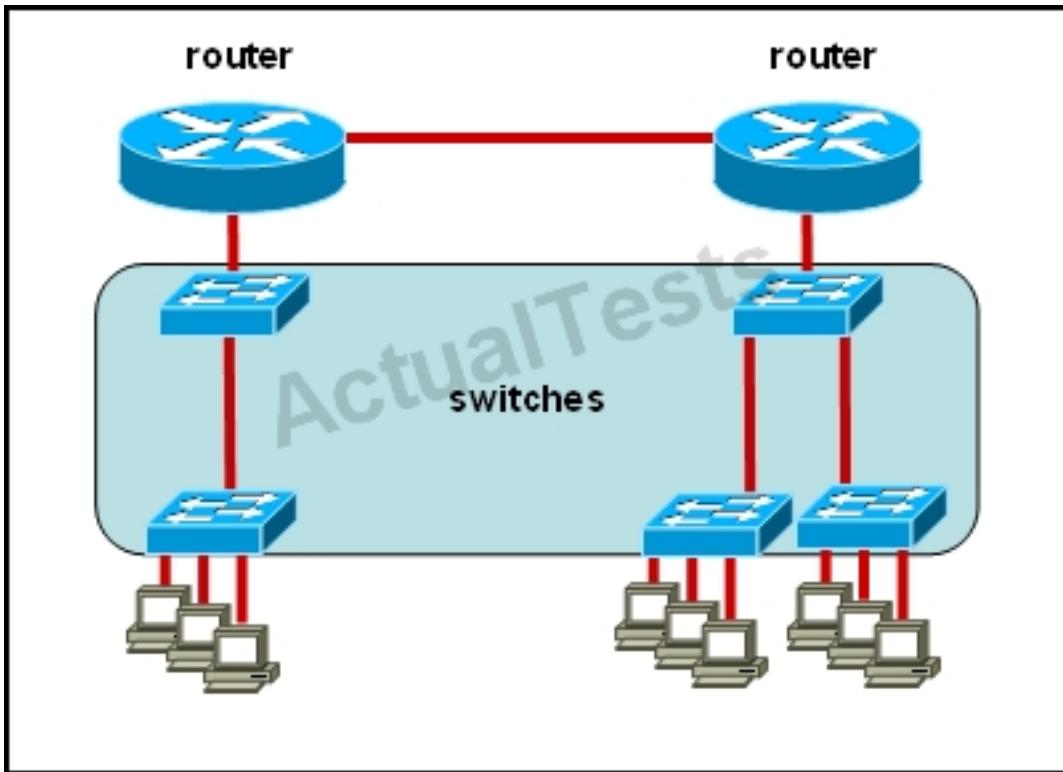
Answer: B

Explanation:

A switch uses a separate collision domain for each port, and each VLAN is a separate broadcast domain.

QUESTION NO: 47

Refer to the exhibit.



All devices attached to the network are shown. How many collision domains are present in this network?

- A. 2
- B. 3
- C. 6
- D. 9
- E. 15

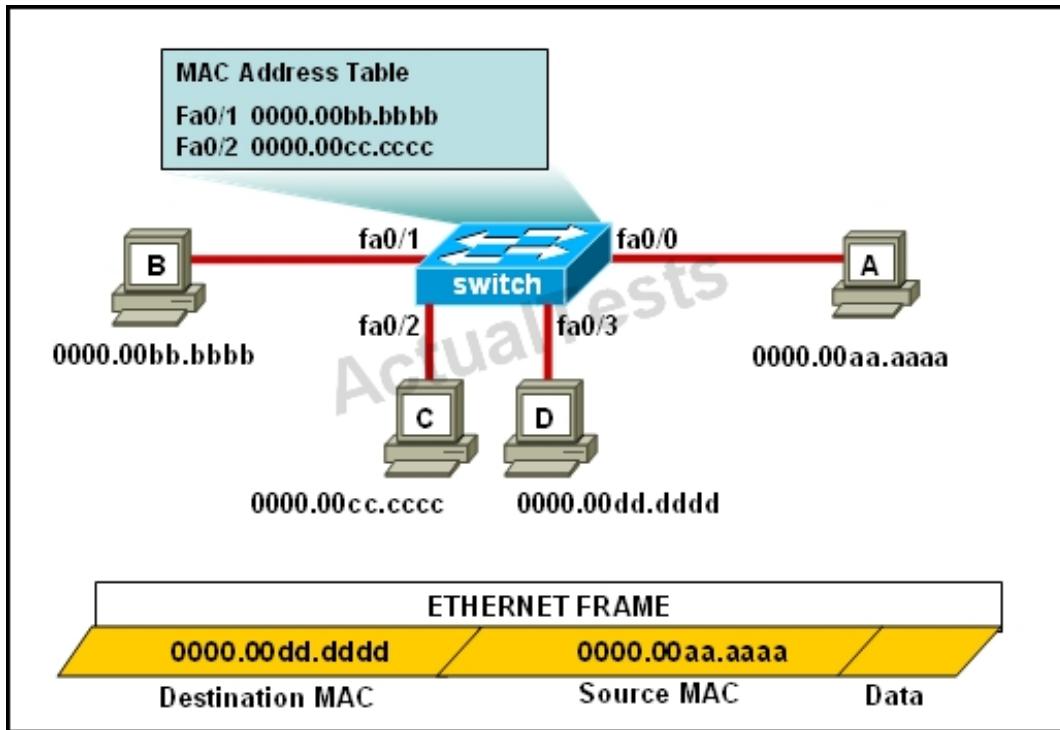
Answer: E

Explanation:

A switch uses a separate collision domain for each port so there are a total of 9 for each device shown. In addition to this, the switch to switch connections (3) are a separate collision domain. Finally, we add the switch to router connections (2) and the router to router connection (1) for a total of 15.

QUESTION NO: 48

Refer to the exhibit.



The ports that are shown are the only active ports on the switch. The MAC address table is shown in its entirety. The Ethernet frame that is shown arrives at the switch.

What two operations will the switch perform when it receives this frame? (Choose two.)

- A. The MAC address of 0000.00aa.aaaa will be added to the MAC address table.
- B. The MAC address of 0000.00dd.dddd will be added to the MAC address table.
- C. The frame will be forwarded out of port fa0/3 only.
- D. The frame will be forwarded out of fa0/1, fa0/2, and fa0/3.
- E. The frame will be forwarded out of all the active ports.

Answer: A,D

Explanation:

If the switch already has the MAC address in its table for the destination, it will forward the frame directly to the destination port. If it was not already in its MAC table, then the frame would have been flooded out all ports except for the port that it came from. It will also add the MAC address of the source device to its MAC address table.

QUESTION NO: 49

How many simultaneous Telnet sessions does a Cisco router support by default?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5
- F. 6

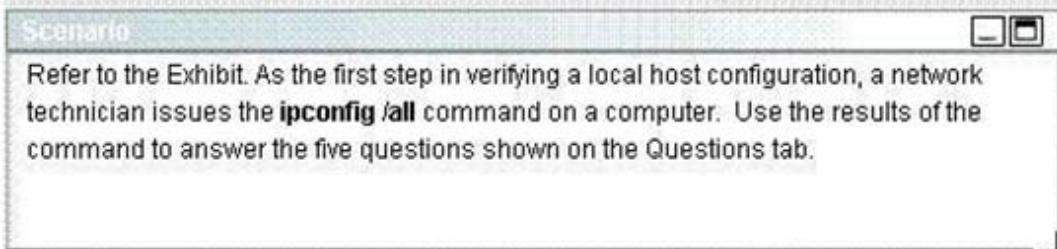
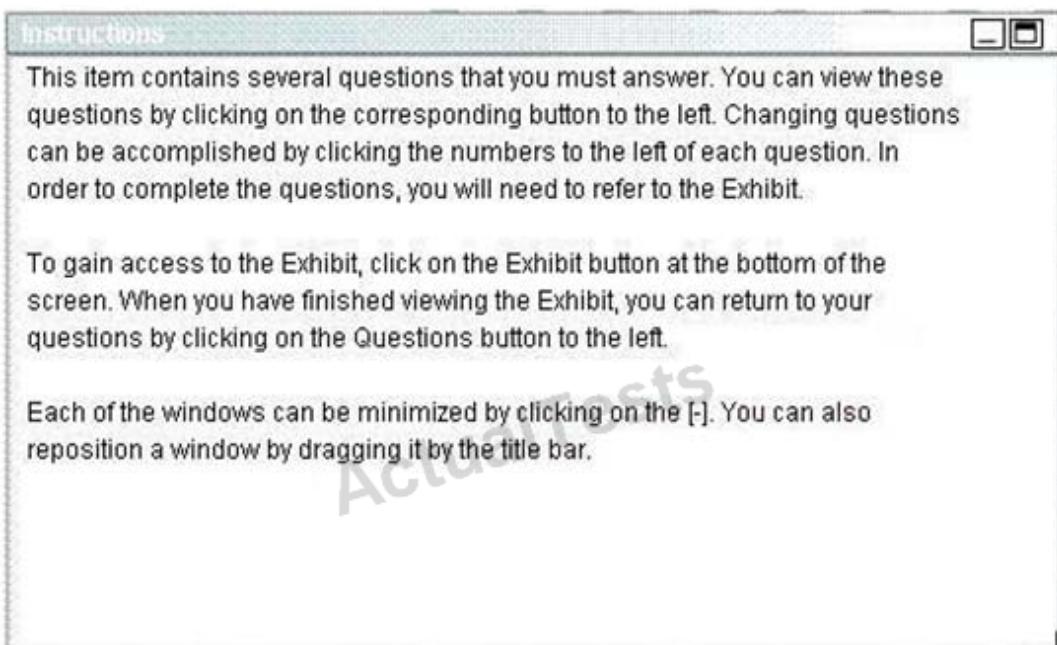
Answer: E

Explanation:

By default, Cisco routers support virtual terminal interfaces 0-4 (5 total) which are used for telnet sessions.

QUESTION NO: 50

Refer to the exhibit.



Exhibit

```
C:\> C:\WINNT\system32\cmd.exe

Connection-specific DNS Suffix . . . . . : cisco.com
Description . . . . . : Intel(R) PRO/1000 MT Mobile
Physical Address . . . . . : 00-0D-60-FD-F0-34
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address . . . . . : 172.16.236.227
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.236.1
DHCP Server . . . . . : 172.16.3.2
DNS Servers . . . . . : 10.4.8.1
                           10.5.2.22
Primary WINS Server . . . . . : 10.69.2.87
Secondary WINS Server . . . . . : 10.69.235.228
Lease Obtained . . . . . : Monday, June 11, 2007 9:26:45 AM
Lease Expires . . . . . : Thursday, June 14, 2007 9:26:45 AM

Ethernet adapter Local Area Connection:

Media State . . . . . : Cable Disconnected
Description . . . . . : Cisco Systems Wireless LAN Adapter
Physical Address . . . . . : 00-0E-9B-48-86-2A
```

What two things can the technician determine by successfully pinging from this computer to the IP address 172.16.236.1? (Choose two)

- A. The network card on the computer is functioning correctly.
- B. The default static route on the gateway router is correctly configured.
- C. The correct default gateway IP address is configured on the computer.
- D. The device with the IP address 172.16.236.1 is reachable over the network.
- E. The default gateway at 172.16.236.1 is able to forward packets to the internet.

Answer: A,D

Explanation:

The source and destination addresses are on the same network therefore, a default gateway is not necessary for communication between these two addresses.

QUESTION NO: 51

What is the purpose of flow control?

- A. To ensure data is retransmitted if an acknowledgement is not received.
- B. To reassemble segments in the correct order at the destination device.
- C. To provide a means for the receiver to govern the amount of data sent by the sender.
- D. To regulate the size of each segment.

Answer: C

Explanation:

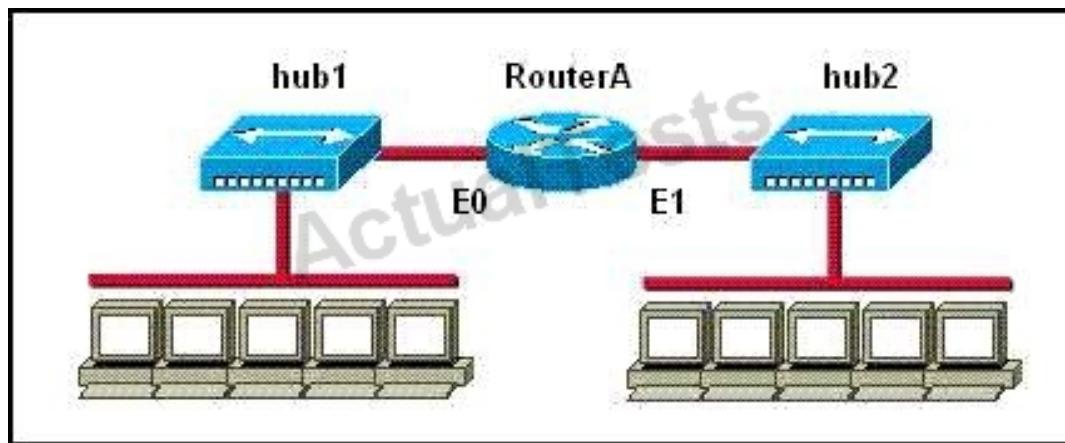
Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted. For serial data transmission locally or in a network, the Xon/Xoff protocol can be used. For modem connections, either Xon/Xoff or CTS/RTS (Clear to Send/Ready to Send) commands can be used to control data flow.

In a network, flow control can also be applied by refusing additional device connections until the flow of traffic has subsided.

Reference: <http://whatis.techtarget.com/definition/flow-control>

QUESTION NO: 52

Refer to the exhibit.



How many collision domains are shown?

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

Answer: B

Explanation:

Hubs create single collision and broadcast domains, so in this case there will be a single collision domain for each of the two hubs.

Topic 3, IP addressing (IPv4 / IPv6)

QUESTION NO: 53

Which IP addresses are valid for hosts belonging to the 10.1.160.0/20 subnet? (Choose three.)

- A. 10.1.168.0
- B. 10.1.176.1
- C. 10.1.174.255
- D. 10.1.160.255
- E. 10.1.160.0
- F. 10.1.175.255

Answer: A,C,D

Explanation:

All IP address in IP ranges between: 10.1.160.1 and 10.1.175.254 are valid as shown below

Address: 10.1.160.0 00001010.00000001.1010 0000.00000000

Netmask: 255.255.240.0 = 20 11111111.11111111.1111 0000.00000000

Wildcard: 0.0.15.255 00000000.00000000.0000 1111.11111111

Which implies that:

Network: 10.1.160.0/20 00001010.00000001.1010 0000.00000000

HostMin: 10.1.160.1 00001010.00000001.1010 0000.00000001

HostMax: 10.1.175.254 00001010.00000001.1010 1111.11111110

Broadcast: 10.1.175.255 00001010.00000001.1010 1111.11111111

QUESTION NO: 54

Given an IP address of 192.168.1.42 255.255.255.248, what is the subnet address?

- A. 192.168.1.8/29

- B. 192.168.1.32/27
- C. 192.168.1.40/29
- D. 192.168.1.16/28
- E. 192.168.1.48/29

Answer: C

Explanation:

248 mask uses 5 bits (1111 1000)

42 IP in binary is (0010 1010)

The base subnet therefore is the lowest binary value that can be written without changing the output of an AND operation of the subnet mask and IP...

1111 1000 AND

0010 1010 equals

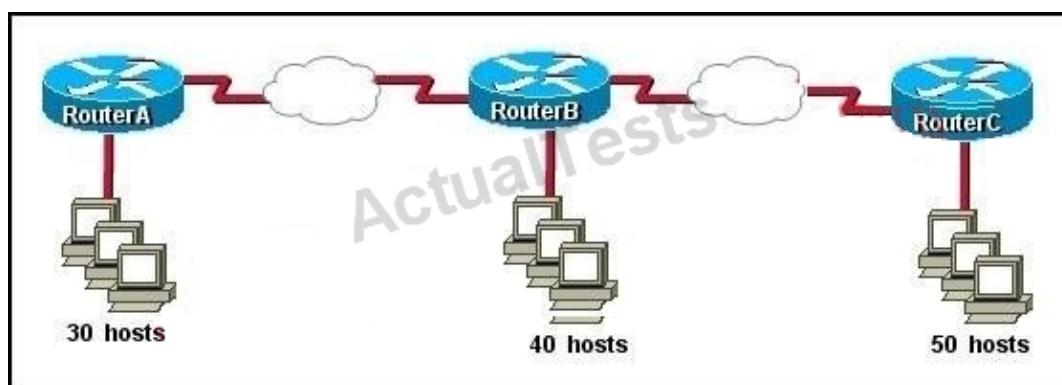
0010 1000 - which is .40

/24 is standard class C mask.

Adding the 5 bits from the .248 mask gives /29

QUESTION NO: 55

Refer to the exhibit.



The enterprise has decided to use the network address 172.16.0.0. The network administrator needs to design a classful addressing scheme to accommodate the three subnets, with 30, 40, and 50 hosts, as shown. What subnet mask would accommodate this network?

- A. 255.255.255.192
- B. 255.255.255.224
- C. 255.255.255.240
- D. 255.255.255.248

E. 255.255.255.252

Answer: A

Explanation:

Subnet mask A i.e. 255.255.255.192 with CIDR of /26 which means 64 hosts per subnet which are sufficient to accommodate even the largest subnet of 50 hosts.

Net Bits	Subnet Mask	Total-Address Per Subnet
/20	255.255.240.0	4096
/21	255.255.248.0	2048
/22	255.255.252.0	1024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4

QUESTION NO: 56

Which two statements describe the IP address 10.16.3.65/23? (Choose two.)

- A. The subnet address is 10.16.3.0 255.255.254.0.
- B. The lowest host address in the subnet is 10.16.2.1 255.255.254.0.

- C. The last valid host address in the subnet is 10.16.2.254 255.255.254.0
- D. The broadcast address of the subnet is 10.16.3.255 255.255.254.0.
- E. The network is not subnetted.

Answer: B,D

Explanation:

The mask 255.255.254.0 (/23) used with a Class A address means that there are 15 subnet bits and 9 host bits. The block size in the third octet is 2 (256 - 254). So this makes the subnets in 0, 2, 4, 6, etc., all the way to 254. The host 10.16.3.65 is in the 2.0 subnet. The next subnet is 4.0, so the broadcast address for the 2.0 subnet is 3.255. The valid host addresses are 2.1 through 3.254

QUESTION NO: 57

Given a Class C IP address subnetted with a /30 subnet mask, how many valid host IP addresses are available on each of the subnets?

- A. 1
- B. 2
- C. 4
- D. 8
- E. 252
- F. 254

Answer: B

Explanation:

/30 CIDR corresponds to mask 255.255.255.252 whose binary is 11111100 which means 6 subnet bits and 2 host bits which means 62 subnets and 2 hosts per subnet.

QUESTION NO: 58

Which one of the following IP addresses is the last valid host in the subnet using mask 255.255.255.224?

- A. 192.168.2.63
- B. 192.168.2.62
- C. 192.168.2.61

- D. 192.168.2.60
- E. 192.168.2.32

Answer: B

Explanation:

With the 224 there are 8 networks with increments of 32

One of these is 32 33 62 63 where 63 is broadcast so 62 is last valid host out of given choices.

QUESTION NO: 59

What is the subnet address of 172.16.159.159/22?

- A. 172.16.0.0
- B. 172.16.128.0
- C. 172.16.156.0
- D. 172.16.159.0
- E. 172.16.159.128
- F. 172.16.192.0

Answer: C

Explanation:

Converting to binary format it comes to 11111111.11111111.11111100.00000000 or 255.255.252.0 Starting with 172.16.0.0 and having increment of 4 we get.

QUESTION NO: 60

What is the subnet address for the IP address 172.19.20.23/28?

- A. 172.19.20.0
- B. 172.19.20.15
- C. 172.19.20.16
- D. 172.19.20.20
- E. 172.19.20.32

Answer: C

Explanation:

From the /28 we can get the following:

Increment: 16 (/28 = 11111111.11111111.11111111.11110000)

Network address: 172.19.20.16 (because 16 < 23)

Broadcast address: 172.19.20.31 (because 31 = 16 + 16 – 1)

QUESTION NO: 61

An administrator is working with the 192.168.4.0 network, which has been subnetted with a /26 mask. Which two addresses can be assigned to hosts within the same subnet? (Choose two.)

- A. 192.168.4.61
- B. 192.168.4.63
- C. 192.168.4.67
- D. 192.168.4.125
- E. 192.168.4.128
- F. 192.168.4.132

Answer: C,D

Explanation:

Increment: 64 (/26 = 11111111.11111111.11111111.11000000)

The IP 192.168.4.0 belongs to class C. The default subnet mask of class C is /24 and it has been subnetted with a /26 mask so we have $2^{(26-24)} = 2^2 = 4$ sub-networks:

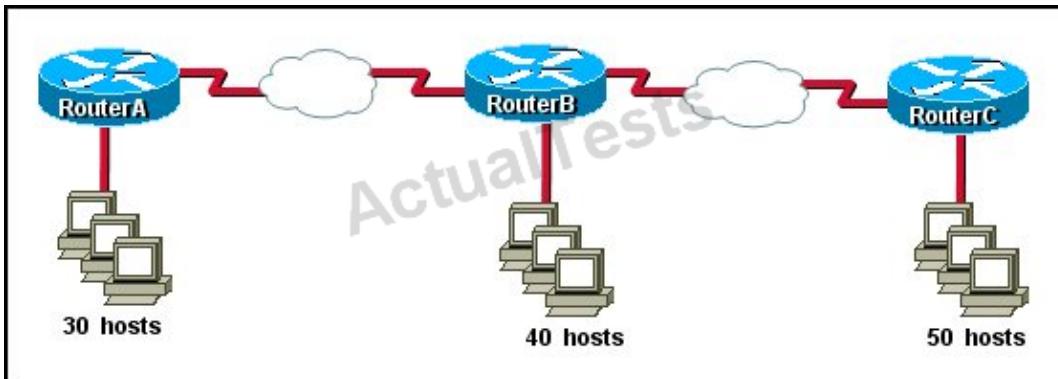
- 1st subnet: 192.168.4.0 (to 192.168.4.63)
- 2nd subnet: 192.168.4.64 (to 192.168.4.127)
- 3rd subnet: 192.168.4.128 (to 192.168.4.191)
- 4th subnet: 192.168.4.192 (to 192.168.4.225)

In all the answers above, only answer C and D are in the same subnet.

Therefore only IPs in this range can be assigned to hosts.

QUESTION NO: 62

Refer to the exhibit.



The internetwork is using subnets of the address 192.168.1.0 with a subnet mask of 255.255.255.224. The routing protocol in use is RIP version 1. Which address could be assigned to the FastEthernet interface on RouterA?

- A. 192.168.1.31
- B. 192.168.1.64
- C. 192.168.1.127
- D. 192.168.1.190
- E. 192.168.1.192

Answer: D

Explanation:

Subnet mask 255.255.255.224 with CIDR of /27 which results in 32 hosts per.

192.168.1.31 is the broadcast address for subnet '0'

192.168.1.64 is the network address for subnet '2'

192.168.1.127 is the broadcast address for subnet '3'

192.168.1.192 is the network address for subnet '6'

Subnet	Network Address	Starting Host	End Host	Broadcast	Netmask
0	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31	255.255.255.224
1	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63	255.255.255.224
2	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95	255.255.255.224
3	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127	255.255.255.224
4	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159	255.255.255.224
5	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191	255.255.255.224
6	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223	255.255.255.224
7	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255	255.255.255.224

QUESTION NO: 63

What is the network address for the host with IP address 192.168.23.61/28?

- A. 192.168.23.0
- B. 192.168.23.32
- C. 192.168.23.48
- D. 192.168.23.56
- E. 192.168.23.60

Answer: C

Explanation:

Convert bit-length prefix to quad-dotted decimal representation, then from it find the number of bits used for subnetting you can find previously calculated number of subnets by separating subnets each having value of last bit used for subnet masking Find that your IP address is in which subnet, that subnet's first address is network address and last address is broadcast address.

Based on above steps the answer is option C

QUESTION NO: 64

The network manager has requested a 300-workstation expansion of the network. The workstations are to be installed in a single broadcast domain, but each workstation must have its own collision domain. The expansion is to be as cost-effective as possible while still meeting the requirements.

Which three items will adequately fulfill the request? (Choose three).

- A. One IP subnet with a mask of 255.255.254.0
- B. Two IP subnets with a mask of 255.255.255.0
- C. Seven 48-port hubs
- D. Seven 48-port switches
- E. One router interface
- F. Seven router interfaces

Answer: A,D,E

Explanation:

To support 300 workstations in a single broadcast domain, we need to use a subnet mask which supports 512 hosts = $2^9 \rightarrow /23$ or 255.255.254.0 in decimal form -> A is correct.

If we use 48-port switches we need $300/48 = 6.25 \rightarrow$ seven 48-port switches are enough because we also need trunking between them -> D is correct.

We only need one router interface and it is connected with one of seven switches -> E is correct.

QUESTION NO: 65

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

- A. provides local hosts with a default gateway address
- B. allows remote management of the switch
- C. allows the switch to respond to ARP requests between two hosts
- D. ensures that hosts on the same LAN can communicate with each other

Answer: B

Explanation:

A 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: 66

An administrator must assign static IP addresses to the servers in a network. For network 192.168.20.24/29, the router is assigned the first usable host address while the sales server is given the last usable host address.

Which of the following should be entered into the IP properties box for the sales server?

- A. IP address: 192.168.20.14
Subnet Mask: 255.255.255.248
Default Gateway: 192.168.20.9
- B. IP address: 192.168.20.254
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.20.1

- C.** IP address: 192.168.20.30
 Subnet Mask: 255.255.255.248
 Default Gateway: 192.168.20.25
- D.** IP address: 192.168.20.30
 Subnet Mask: 255.255.255.240
 Default Gateway: 192.168.20.17
- E.** IP address: 192.168.20.30
 Subnet Mask: 255.255.255.240
 Default Gateway: 192.168.20.25

Answer: C**Explanation:**

With network 192.168.20.24/29 we have:

Increment: $8 / 29 = 255.255.255.248 = 11111000$ for the last octet)

Network address: 192.168.20.24 (because $24 = 8 * 3$)

Broadcast address: 192.168.20.31 (because $31 = 24 + 8 - 1$)

Therefore the first usable IP address is 192.168.20.25 (assigned to the router) and the last usable IP address is 192.168.20.30 (assigned to the sales server). The IP address of the router is also the default gateway of the sales server.

QUESTION NO: 67

Which IP address is a private address?

- A.** 12.0.0.1
B. 168.172.19.39
C. 172.20.14.36
D. 172.33.194.30
E. 192.169.42.34

Answer: C**Explanation:**

Private IP Address Ranges (RFC 1918)

Class	From	To	CIDR Mask	Decimal Mask
Class A (24 Bit)	10.0.0.0	10.255.255.255	/8	255.0.0.0
Class B (20 Bit)	172.16.0.0	172.31.255.255	/12	255.240.0.0
Class C (16 Bit)	192.168.0.0	192.168.255.255	/16	255.255.0.0

QUESTION NO: 68

Which command can you use to manually assign a static IPV6 address to a router interface?

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

Answer: D

Explanation:

An example of configuring IPv6 on an interface is shown below:

```
Router(config)# interface fastethernet 0/1  
Router(config-if)# ipv6 address 3000::2222:1/64
```

QUESTION NO: 69

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

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

Answer: B,C

Explanation:

A single interface may be assigned multiple addresses of any type (unicast, anycast, multicast).

Every IPv6-enabled interface must contain at least one loopback and one link-local address.

Optionally, every interface can have multiple unique local and global addresses.

IPv6 host addresses can be assigned in multiple ways:

Static configuration

Stateless autoconfiguration

DHCPv6

When IPv6 is used over Ethernet networks, the Ethernet MAC address can be used to generate the 64-bit interface ID for the host. This is called the EUI-64 address.

Since MAC addresses use 48 bits, additional bits must be inserted to fill the 64 bits required.

Reference:

http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8026003d.pdf

QUESTION NO: 70

Which option is a valid IPv6 address?

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

Answer: D

Explanation:

IPv6 Address Notation

IPv6 addresses are denoted by eight groups of hexadecimal quartets separated by colons in between them.

Following is an example of a valid IPv6 address: 2001:cdba:0000:0000:0000:3257:9652

Any four-digit group of zeroes within an IPv6 address may be reduced to a single zero or altogether omitted.

Therefore, the following IPv6 addresses are similar and equally valid:

2001:cdba:0000:0000:0000:3257:9652

2001:cdba:0:0:0:3257:9652

2001:cdba::3257:9652

Reference: <http://www.ipv6.com/articles/general/IPv6-Addressing.htm>

QUESTION NO: 71

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

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

Answer: D

Explanation:

One of the key advantages IPv6 brings is the exponentially larger address space. The following will outline the basic address architecture of IPv6.

128-bit-long addresses

Represented in hexadecimal format:

Uses CIDR principles: prefix/prefix length

x:x:x:x:x:x:x:x, where x is a 16-bit hex field

The last 64 bits are used for the interface ID

http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8026003d.pdf

QUESTION NO: 72

Which three approaches can be used while migrating from an IPv4 addressing scheme to an IPv6 scheme? (Choose three)

- A. static mapping of IPv4 address to IPv6 addresses
- B. configuring IPv4 tunnels between IPv6 islands
- C. use DHCPv6 to map IPv4 addresses to IPv6 addresses
- D. use proxying and translation (NAT-PT) to translate IPv6 packets into IPv4 packets
- E. configure IPv6 directly
- F. enable dual-stack routing

Answer: B,D,F

Explanation:

Connecting IPv6 islands with tunnels

An IPv6 island is a network made of IPv6 links directly connected by IPv6 routers. In the early days of IPv6 deployment, there are many IPv6 islands. IPv6 in IPv4 tunnels are used to connect those islands together. In each island, one (or more) dual stack routers are designated to encapsulate and decapsulate IPv6 packets within IPv4 packets. Different mechanisms have been developed to manage tunnels: automatic tunnels³, configured tunnels³, tunnel brokers³, 6over4³, 6to4³, ...

Reference 2:

<http://www.petri.co.il/ipv6-transition.htm>

Network Address Translation - Protocol Translation (NAT-PT)

The NAT-PT method enables the ability to either statically or dynamically configure a translation of a IPv4 network address into an IPv6 network address and vice versa. For those familiar with more typically NAT implementations, the operation is very similar but includes a protocol translation function. NAT-PT also ties in an Application Layer Gateway (ALG) functionality that converts Domain Name System (DNS) mappings between protocols.

Dual Stack

The simplest approach when transitioning to IPv6 is to run IPv6 on all of the devices that are currently running IPv4. If this is something that is possible within the organizational network, it is very easy to implement.

However, for many organizations, IPv6 is not supported on all of the IPv4 devices; in these situations other methods must be considered.

Reference: <http://www.opus1.com/ipv6/howdoitransitiontoipv6.html>

QUESTION NO: 73

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

Explanation:

IPv6 has three types of addresses, which can be categorized by type and scope:

Unicast addresses. A packet is delivered to one interface.

Multicast addresses. A packet is delivered to multiple interfaces.

Anycast addresses. A packet is delivered to the nearest of multiple interfaces (in terms of routing distance).

IPv6 does not use broadcast messages.

Unicast and anycast addresses in IPv6 have the following scopes (for multicast addresses, the scope are built into the address structure):

Link-local. The scope is the local link (nodes on the same subnet).

Site-local. The scope is the organization (private site addressing).

Global. The scope is global (IPv6 Internet addresses).

In addition, IPv6 has special addresses such as the loopback address. The scope of a special address depends on the type of special address.

Much of the IPv6 address space is unassigned.

[http://technet.microsoft.com/en-us/library/cc757359\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc757359(v=ws.10).aspx)

QUESTION NO: 74

Which command enables IPv6 forwarding on a Cisco router?

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

Answer: B

Explanation:

Enabling IPv6 on Cisco IOS Software Technology

<http://www.ciscopress.com/articles/article.asp?p=31948&seqNum=4>

The first step of enabling IPv6 on a Cisco router is the activation of IPv6 traffic forwarding to forward unicast IPv6 packets between network interfaces. By default, IPv6 traffic forwarding is disabled on Cisco routers.

The `ipv6 unicast-routing` command is used to enable the forwarding of IPv6 packets between interfaces on the router. The syntax for this command is as follows:

Router(config)#`ipv6 unicast-routing` The `ipv6 unicast-routing` command is enabled on a global basis.

QUESTION NO: 75

Identify the four valid IPv6 addresses. (Choose four.)

- A. ::
- B. ::192:168:0:1
- C. 2000::

- D. 2001:3452:4952:2837::
- E. 2002:c0a8:101::42
- F. 2003:dead:beef:4dad:23:46:bb:101

Answer: A,B,E,F

Explanation:

<http://www.intermapper.com/ipv6validator>

http://www.ripe.net/lir-services/new-lir/ipv6_reference_card.pdf

Address	Value	Description
Global	2000::/3	These are assigned by the IANA and used on public networks. They are equivalent to IPv4 global (sometimes called public) addresses. ISPs summarize these to provide scalability in the Internet.
Reserved	(range)	Reserved addresses are used for specific types of anycast as well as for future use. Currently about 1/256th of the IPv6 address space is reserved.
Private	FE80::/10	Like IPv4, IPv6 supports private addressing, which is used by devices that don't need to access a public network. The first two digits are FE, and the third digit can range from 8 to F.
Loopback	::1	Like the 127.0.0.1 address in IPv4, 0:0:0:0:0:0:1, or ::1, is used for local testing functions; unlike IPv4, which dedicates a complete A class block of addresses for local testing, only one is used in IPv6.
Unspecified	::	0.0.0.0 in IPv4 means "unknown" address. In IPv6, this is represented by 0:0:0:0:0:0, or ::, and is typically used in the source address field of the packet when an interface doesn't have an address and is trying to acquire one dynamically.

QUESTION NO: 76

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

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

Answer: A,D

Explanation:

Address	Value	Description
Global	2000::/3	These are assigned by the IANA and used on public networks. They are equivalent to IPv4 global (sometimes called public) addresses. ISPs summarize these to provide scalability in the Internet.
Reserved	(range)	Reserved addresses are used for specific types of anycast as well as for future use. Currently about 1/256th of the IPv6 address space is reserved.
Private	FE80::/10	Like IPv4, IPv6 supports private addressing, which is used by devices that don't need to access a public network. The first two digits are FE, and the third digit can range from 8 to F.
Loopback	::1	Like the 127.0.0.1 address in IPv4, 0:0:0:0:0:0:1, or ::1, is used for local testing functions; unlike IPv4, which dedicates a complete A class block of addresses for local testing, only one is used in IPv6.
Unspecified	::	0.0.0.0 in IPv4 means "unknown" address. In IPv6, this is represented by 0:0:0:0:0:0:, or ::, and is typically used in the source address field of the packet when an interface doesn't have an address and is trying to acquire one dynamically.

QUESTION NO: 77

Which statement is true?

- A. An IPv6 address is 64 bits long and is represented as hexadecimal characters.
- B. An IPv6 address is 32 bits long and is represented as decimal digits.
- C. An IPv6 address is 128 bits long and is represented as decimal digits.
- D. An IPv6 address is 128 bits long and is represented as hexadecimal characters.

Answer: D

Explanation:

http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aec8026003d.pdf

One of the key advantages IPv6 brings is the exponentially larger address space. The following will outline the basic address architecture of IPv6.

128-bit-long addresses

Represented in hexadecimal format:

Uses CIDR principles: prefix/prefix length

x:x:x:x:x:x:x, where x is a 16-bit hex field

The last 64 bits are used for the interface ID

QUESTION NO: 78

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

Answer: C

Explanation:

Each octet represents eight bits. The bits, in turn, represent (from left to right): 128, 64, 32 , 16 , 8, 4, 2, 1

Add them up and you get 255. Add one for the all zeros option, and the total is 256.

Now, take away one of these for the network address (all zeros) and another for the broadcast address (all ones). Each octet represents 254 possible hosts. Or 254 possible networks. Unless you have subnet zero set on your network gear, in which case you could conceivably have 255. The CIDR addressing format (/20) tells us that 20 bits are used for the network portion, so the maximum number of networks are 2^{20} minus one if you have subnet zero enabled, or minus 2 if not.

You asked about the number of hosts. That will be 32 minus the number of network bits, minus two. So calculate it as $(2^{(32-20)})-2$, or $(2^{12})-2 = 4094$

QUESTION NO: 79

Which statements are TRUE regarding Internet Protocol version 6 (IPv6) addresses? (Choose three.)

- A. An IPv6 address is divided into eight 16-bit groups.
- B. A double colon (:) can only be used once in a single IPv6 address.
- C. IPv6 addresses are 196 bits in length.
- D. Leading zeros cannot be omitted in an IPv6 address.

E. Groups with a value of 0 can be represented with a single 0 in IPv6 address.

Answer: A,B,E

Explanation:

IPv6 addresses are divided into eight 16-bit groups, a double colon (:) can only be used once in an IPv6 address, and groups with a value of 0 can be represented with a single 0 in an IPv6 address.

The following statements are also true regarding IPv6 address:

IPv6 addresses are 128 bits in length.

Eight 16-bit groups are divided by a colon (:).

Multiple groups of 16-bit 0s can be represented with double colon (::).

Double colons (::) represent only 0s.

Leading zeros can be omitted in an IPv6 address.

The option stating that IPv6 addresses are 196 bits in length is incorrect. IPv6 addresses are 128 bits in length.

The option stating that leading zeros cannot be omitted in an IPv6 address is incorrect. Leading zeros can be omitted in an IPv6 address.

QUESTION NO: 80

Which of the following IP addresses are valid Class B host addresses if a default Class B mask is in use? (Choose two.)

- A. 10.6.8.35
- B. 133.6.5.4
- C. 192.168.5.9
- D. 127.0.0.1
- E. 190.6.5.4

Answer: B,E

Explanation:

The IP addresses 133.6.5.4 and 190.6.5.4 are both valid Class B addresses when a default mask is in use.

The Class B default mask is 255.255.0.0 and the range of valid addresses is 128.0.0.0 - 191.255.255.255.

The IP address 10.6.8.35 is a Class A address. The Class A default mask is 255.0.0.0 and the range of valid addresses is 1.0.0.0 - 127.255.255.255, with the exception of the range 127.0.0.1 - 127.255.255.255, which is reserved and cannot be assigned.

The IP address 192.168.5.9 is a Class C address. The Class C default mask is 255.255.255.0 and the range of valid addresses is 192.0.0.0 - 223.255.255.255.

The IP address 127.0.0.1 is a Class A address, but it comes from a reserved portion that cannot be assigned.

The range 127.0.0.1 - 127.255.255.255 is used for diagnostics, and although any address in the range will work as a diagnostic address, 127.0.0.1 is known as the loopback address. If you can ping this address, or any address in the 127.0.0.1 - 127.255.255.255 range, then the NIC is working and TCP/IP is installed. The Class A default mask is 255.0.0.0 and the range of valid addresses is 1.0.0.0 - 127.255.255.255, with the exception of the range 127.0.0.1 - 127.255.255.255, which is reserved and cannot be assigned.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

Topic 4, IP Routing Technologies

QUESTION NO: 81

What two things does a router do when it forwards a packet? (Choose two.)

- A. switches the packet to the appropriate outgoing interfaces
- B. computes the destination host address
- C. determines the next hop on the path
- D. updates the destination IP address
- E. forwards ARP requests

Answer: A,C

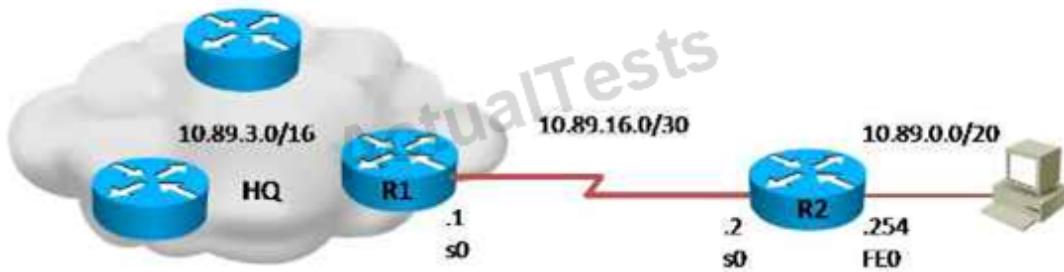
Explanation:

A primary function of a router is to forward packets toward their destination. This is accomplished by using a switching function, which is the process used by a router to accept a packet on one interface and forward it out of another interface. A key responsibility of the switching function is to encapsulate packets in the appropriate data link frame type for the outgoing data link and

determining the next hop device to send the frame to.

QUESTION NO: 82

Refer to the exhibit.



What is the simplest way to configure routing between the regional office network 10.89.0.0/20 and the corporate network?

- A. router1(config)#ip route 10.89.0.0 255.255.240.0 10.89.16.2
- B. router2(config)#ip route 10.89.3.0 255.255.0.0 10.89.16.2
- C. router1(config)#ip route 10.89.0.0 255.255.240.0 10.89.16.1
- D. router2(config)#ip route 0.0.0.0 0.0.0.0 10.89.16.1

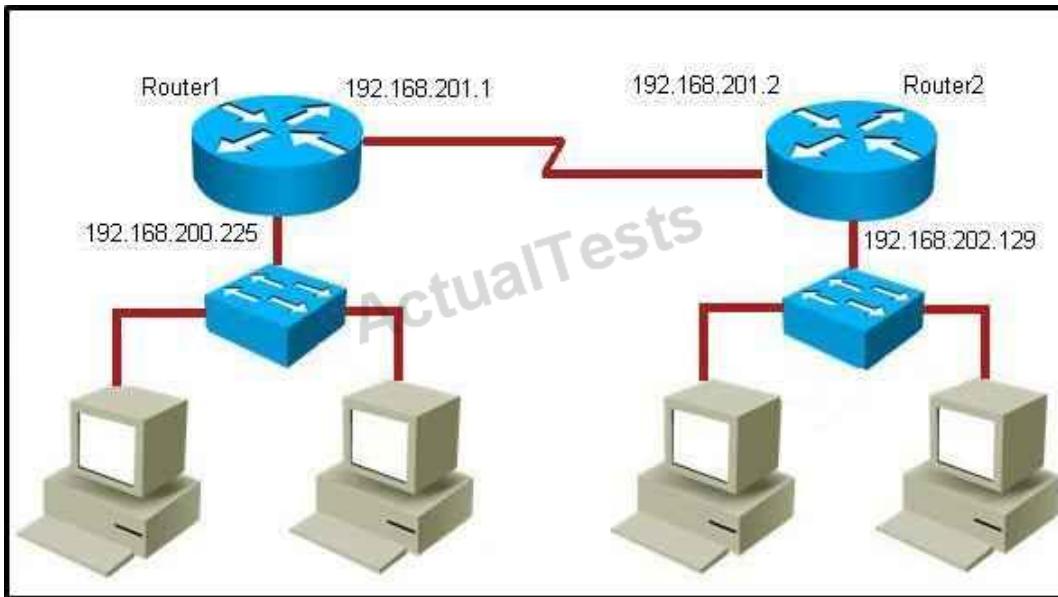
Answer: D

Explanation:

The next hop of the static route should be 10.89.16.1, which is the IP address for router R1 in this example. Since this router is a stub router with only a single connection to the WAN, the simplest thing to do is to configure a single static default route back to the HQ network.

QUESTION NO: 83

Refer to the exhibit.



Which command would you use to configure a static route on Router1 to network 192.168.202.0/24 with a nondefault administrative distance?

- A. router1(config)#ip route 1 192.168.201.1 255.255.255.0 192.168.201.2
- B. router1(config)#ip route 192.168.202.0 255.255.255.0 192.168.201.2 1
- C. router1(config)#ip route 5 192.168.202.0 255.255.255.0 192.168.201.2
- D. router1(config)#ip route 192.168.202.0 255.255.255.0 192.168.201.2 5

Answer: D

Explanation:

The default AD for a static route is 1. To change this, configure a different value to be used as the AD at the very end of the “ip route” statement.

QUESTION NO: 84

What does administrative distance refer to?

- A. the cost of a link between two neighboring routers
- B. the advertised cost to reach a network
- C. the cost to reach a network that is administratively set
- D. a measure of the trustworthiness of a routing information source

Answer: D

Explanation:

Reference:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094195.shtml

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

Administrative distance is the first criterion that a router uses to determine which routing protocol to use if two protocols provide route information for the same destination. Administrative distance is a measure of the trustworthiness of the source of the routing information. The smaller the administrative distance value, the more reliable the protocol.

QUESTION NO: 85

Which IOS command is used to initiate a login into a VTY port on a remote router?

- A. router# login
- B. router# telnet
- C. router# trace
- D. router# ping
- E. router(config)# line vty 0 5
- F. router(config-line)# login

Answer: B

Explanation:

VTY ports are telnet ports hence command B will initiate login to the telnet port.

QUESTION NO: 86

The command ip route 192.168.100.160 255.255.255.224 192.168.10.2 was issued on a router. No routing protocols or other static routes are configured on the router. Which statement is true about this command?

- A. The interface with IP address 192.168.10.2 is on this router.
- B. The command sets a gateway of last resort for the router.
- C. Packets that are destined for host 192.168.100.160 will be sent to 192.168.10.2.
- D. The command creates a static route for all IP traffic with the source address 192.168.100.160.

Answer: C

Explanation:

With 160 it's actually network address of /27 so any address within the range of .160-.191 network will be sent to 192.168.10.2

QUESTION NO: 87

Which two of these functions do routers perform on packets? (Choose two.)

- A. Examine the Layer 2 headers of inbound packets and use that information to determine the next hops for the packets
- B. Update the Layer 2 headers of outbound packets with the MAC addresses of the next hops
- C. Examine the Layer 3 headers of inbound packets and use that information to determine the next hops for the packets
- D. Examine the Layer 3 headers of inbound packets and use that information to determine the complete paths along which the packets will be routed to their ultimate destinations
- E. Update the Layer 3 headers of outbound packets so that the packets are properly directed to valid next hops
- F. Update the Layer 3 headers of outbound packets so that the packets are properly directed to their ultimate destinations

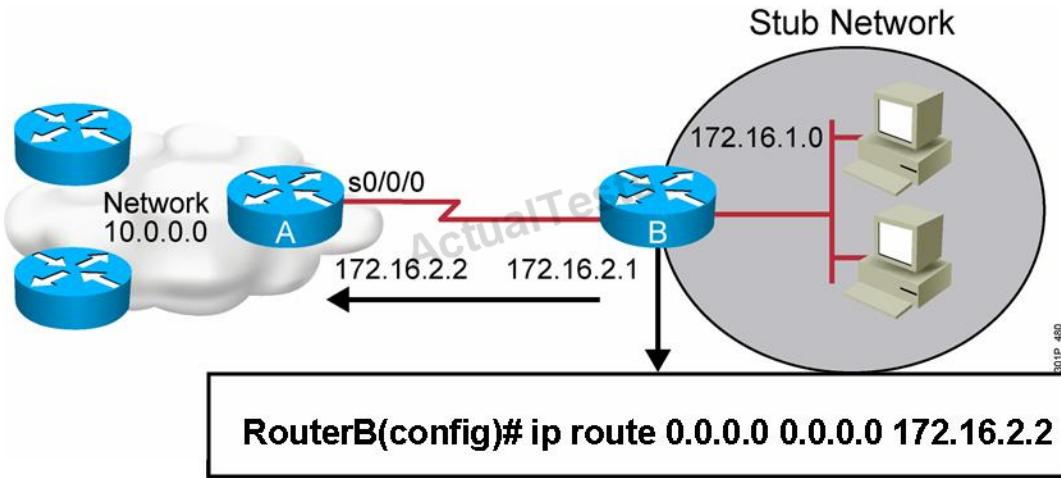
Answer: B,C

Explanation:

This is the basic function of the router to receive incoming packets and then forward them to their required destination. This is done by reading layer 3 headers of inbound packets and update the info to layer 2 for further hopping.

QUESTION NO: 88

Refer to the exhibit.



Which two statements are correct? (Choose two.)

- A. This is a default route.
- B. Adding the subnet mask is optional for the ip route command.
- C. This will allow any host on the 172.16.1.0 network to reach all known destinations beyond RouterA.
- D. This command is incorrect, it needs to specify the interface, such as s0/0/0 rather than an IP address.
- E. The same command needs to be entered on RouterA so that hosts on the 172.16.1.0 network can reach network 10.0.0.0.

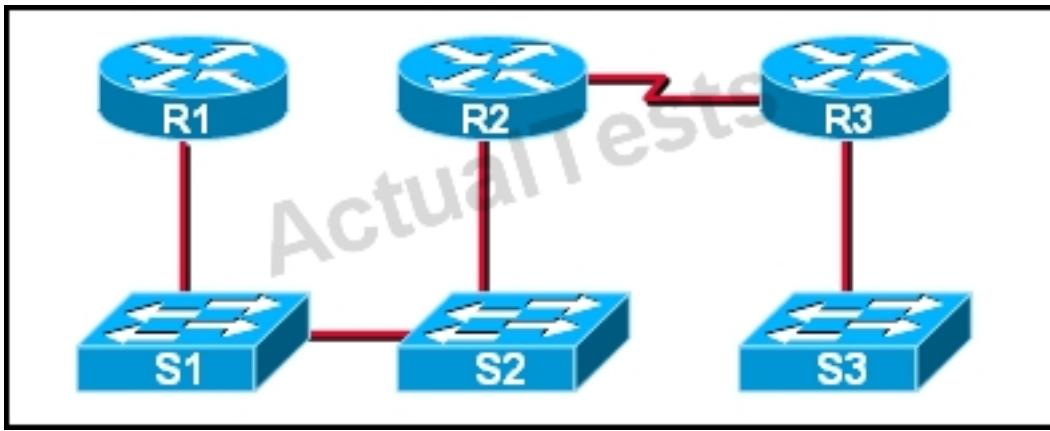
Answer: A,C

Explanation:

This is obviously the default route which is set between the routers and since it is entered in such a manner that it ensures connectivity between the stub network and any host lying beyond RouterA.

QUESTION NO: 89

Refer to the exhibit.



If CDP is enabled on all devices and interfaces, which devices will appear in the output of a show cdp neighbors command issued from R2?

- A. R2 and R3
- B. R1 and R3
- C. R3 and S2
- D. R1, S1, S2, and R3
- E. R1, S1, S2, R3, and S3

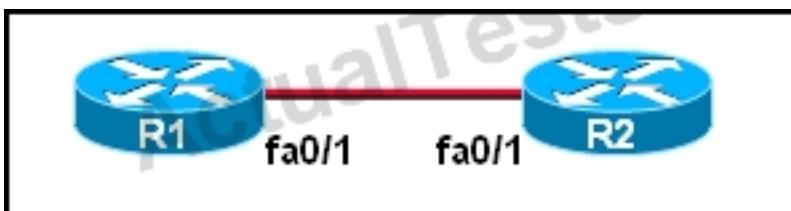
Answer: C

Explanation:

A Cisco device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighbors. Since it is a layer two protocol, these packets are not routed. So the devices detected would be immediate connected neighbors.

QUESTION NO: 90

Refer to the exhibit.



The two routers have had their startup configurations cleared and have been restarted. At a minimum, what must the administrator do to enable CDP to exchange information between R1 and R2?

- A. Configure the router with the cdp enable command.
- B. Enter no shutdown commands on the R1 and R2 fa0/1 interfaces.
- C. Configure IP addressing and no shutdown commands on both the R1 and R2 fa0/1 interfaces.
- D. Configure IP addressing and no shutdown commands on either of the R1 or R2 fa0/1 interfaces.

Answer: B

Explanation:

If the no shut down commands are not entered, then CDP can exchange information between the two routers. By default, all Cisco device interfaces and ports are shut down and need to be manually enabled.

QUESTION NO: 91

Which two commands will display the current IP address and basic Layer 1 and 2 status of an interface? (Choose two.)

- A. router#show version
- B. router#show ip interface
- C. router#show protocols
- D. router#show controllers
- E. router#show running-config

Answer: B,C

Explanation:

The outputs of “show protocols” and “show ip interface” are shown below:

Global values:Internet Protocol routing is enabledSerial0/0 is up, line protocol is downInternet address is 10.1.1.1/30Serial0/1 is up, line protocol is downInternet address is 209.65.200.225/30Serial0/2 is up, line protocol is downSerial0/3 is up, line protocol is downNVI0 is up, line protocol is upInterface is unnumbered. Using address of NVI0 (0.0.0.0)Loopback0 is up, line protocol is upInternet address is 10.1.10.1/32Loopback1 is up, line protocol is upInternet address is 10.1.2.1/27Loopback6 is up, line protocol is up

Serial0/0 is up, line protocol is downInternet address is 10.1.1.1/30Broadcast address is 255.255.255.255Address determined by non-volatile memoryMTU is 1500 bytesHelper address is

not setDirected broadcast forwarding is disabledMulticast reserved groups joined:
224.0.0.5Outgoing access list is not setInbound access list is not setProxy ARP is enabledLocal
Proxy ARP is disabledSecurity level is defaultSplit horizon is disabledICMP redirects are always
sentICMP unreachables are always sentICMP mask replies are never sentIP fast switching is
enabledIP fast switching on the same interface is enabledIP Flow switching is disabledIP CEF
switching is disabledIP Feature Fast switching turbo vectorIP multicast fast switching is enabledIP
multicast distributed fast switching is disabledIP route-cache flags are FastRouter Discovery is
disabledIP output packet accounting is disabledIP access violation accounting is disabledTCP/IP
header compression is disabledRTP/IP header compression is disabledPolicy routing is
disabledNetwork address translation is enabled, interface in domain insideBGP Policy Mapping is
disabledWCCP Redirect outbound is disabledWCCP Redirect inbound is disabledWCCP Redirect
exclude is disabled

QUESTION NO: 92

An administrator is in the process of changing the configuration of a router. What command will allow the administrator to check the changes that have been made prior to saving the new configuration?

- A. Router# show startup-config
- B. Router# show current-config
- C. Router# show running-config
- D. Router# show memory
- E. Router# show flash
- F. Router# show processes

Answer: C

Explanation:

This command followed by the appropriate parameter will show the running config hence the admin will be able to see what changes have been made, and then they can be saved.

QUESTION NO: 93

On a live network, which commands will verify the operational status of router interfaces? (Choose two.)

- A. Router# show interfaces
- B. Router# show ip protocols
- C. Router# debug interface
- D. Router# show ip interface brief
- E. Router# show start

Answer: A,D

Explanation:

Only two commands “show interfaces” and “show ip interface brief” reveal the status of router interfaces (up/up, for example).

QUESTION NO: 94

Which router command will configure an interface with the IP address 10.10.80.1/19?

- A. router(config-if)# ip address 10.10.80.1/19
- B. router(config-if)# ip address 10.10.80.1 255.255.0.0
- C. router(config-if)# ip address 10.10.80.1 255.255.255.0
- D. router(config-if)# ip address 10.10.80.1 255.255.224.0
- E. router(config-if)# ip address 10.10.80.1 255.255.240.0
- F. router(config-if)# ip address 10.10.80.1 255.255.255.240

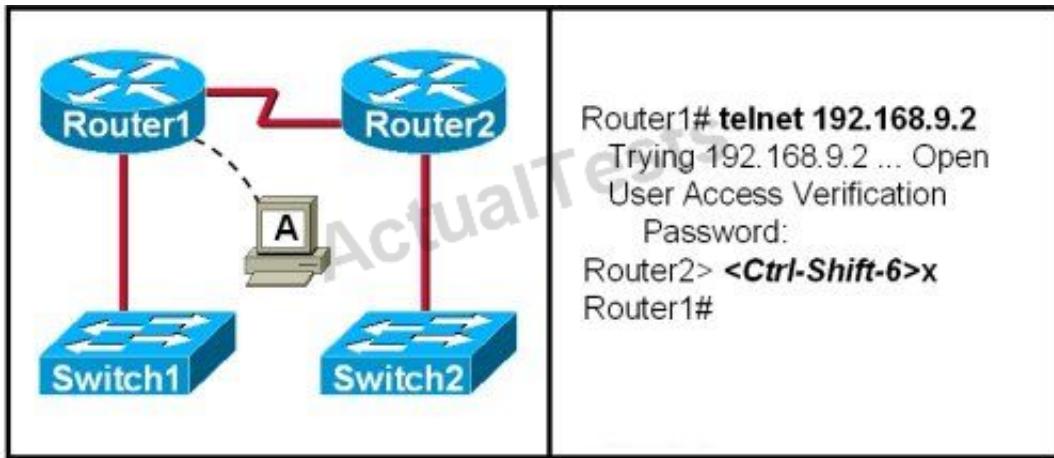
Answer: D

Explanation:

255.255.224 equal /19 in CIDR format hence the answer

QUESTION NO: 95

Refer to the exhibit.



If the resume command is entered after the sequence that is shown in the exhibit, which router prompt will be displayed?

- A. Router1>
- B. Router1#
- C. Router2>
- D. Router2#

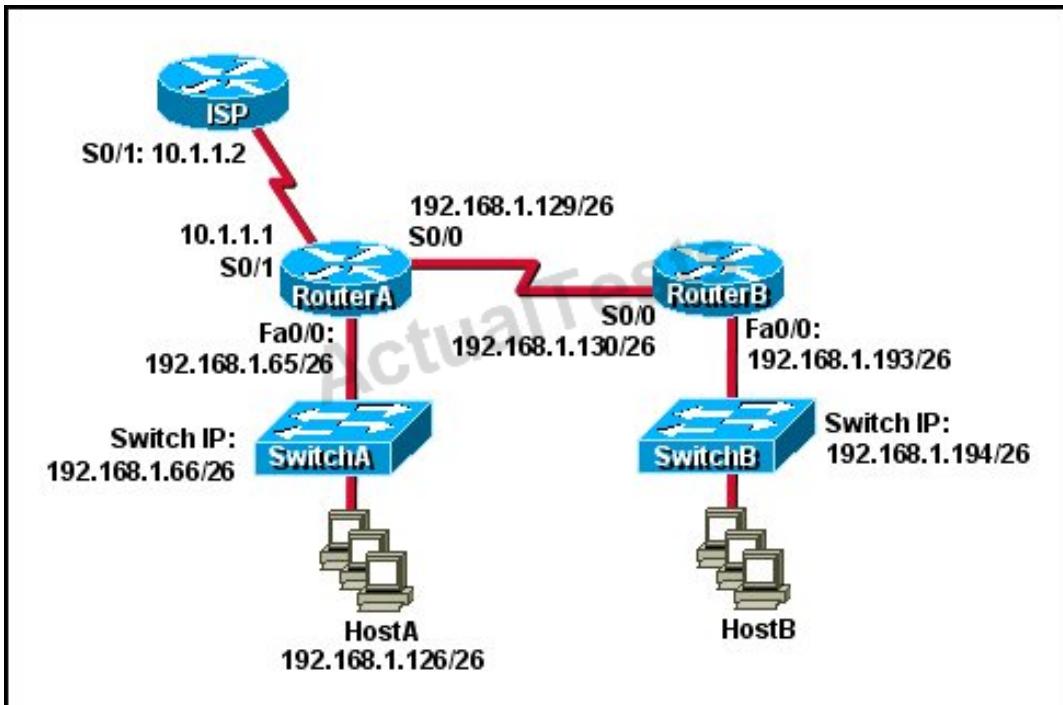
Answer: C

Explanation:

After resuming the telnet session by using the Enter key after it has been suspended, it will resume back to the telnet session so it will be back to the router2> prompt.

QUESTION NO: 96

Refer to the exhibit.



Which default gateway address should be assigned to HostA?

- A. 192.168.1.1
- B. 192.168.1.65
- C. 192.168.1.66
- D. 192.168.1.129
- E. 10.1.1.1
- F. 10.1.1.2

Answer: B

Explanation:

The default gateway will be the IP address of the router that it connects to, not the switch.

QUESTION NO: 97

Refer to the output of the corporate router routing table shown in the graphic.

```

Corp#show ip route
...
Gateway of last resort is not set

C 192.168.13.0/24 is directly connected, Serial0/1
C 192.168.14.0/24 is directly connected, FastEthernet0/0
C 192.168.15.0/24 is directly connected, Serial0/0.102
C 192.168.20.0/24 is directly connected, Serial0/0.117
R 192.168.21.0/24 [120/3] via 192.168.15.2, 00:00:05, Serial0/0.102
R 192.168.21.0/24 [120/3] via 192.168.15.2, 00:00:05, Serial0/0.102
R 192.168.21.0/24 [120/3] via 192.168.20.2, 00:00:25, Serial0/0.117
R 192.168.21.0/24 [120/3] via 192.168.20.2, 00:00:25, Serial0/0.117
R 192.168.21.0/24 [120/3] via 192.168.20.2, 00:00:25, Serial0/0.117
R 192.168.214.0/24 [120/1] via 192.168.14.2, 00:00:22, FastEthernet0/0

```

The corporate router receives an IP packet with a source IP address of 192.168.214.20 and a destination address of 192.168.22.3.

What will the router do with this packet?

- A. It will encapsulate the packet as Frame Relay and forward it out interface Serial 0/0.117.
- B. It will discard the packet and send an ICMP Destination Unreachable message out interface FastEthernet 0/0.
- C. It will forward the packet out interface Serial 0/1 and send an ICMP Echo Reply message out interface serial 0/0.102.
- D. It will change the IP packet to an ARP frame and forward it out FastEthernet 0/0.

Answer: B

Explanation:

Since the destination network is not in the routing table, and no default gateway has been configured, the router will discard the packet and send an ICMP Destination Unreachable message out interface FastEthernet 0/0. It knows to send it out Fa 0/0 because the routing table for the source IP address of 192.168.214.20 shows it was learned from the Fa 0/0 interface.

QUESTION NO: 98

What is the default administrative distance of the OSPF routing protocol?

- A. 90
- B. 100

- C. 110
- D. 120
- E. 130
- F. 170

Answer: C

Explanation:

Default Distance Value Table

This table lists the administrative distance default values of the protocols that Cisco supports:

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

If the administrative distance is 255, the router does not believe the source of that route and does not install the route in the routing table.

QUESTION NO: 99

To allow or prevent load balancing to network 172.16.3.0/24, which of the following commands

could be used in R2? (Choose two.)

Instructions

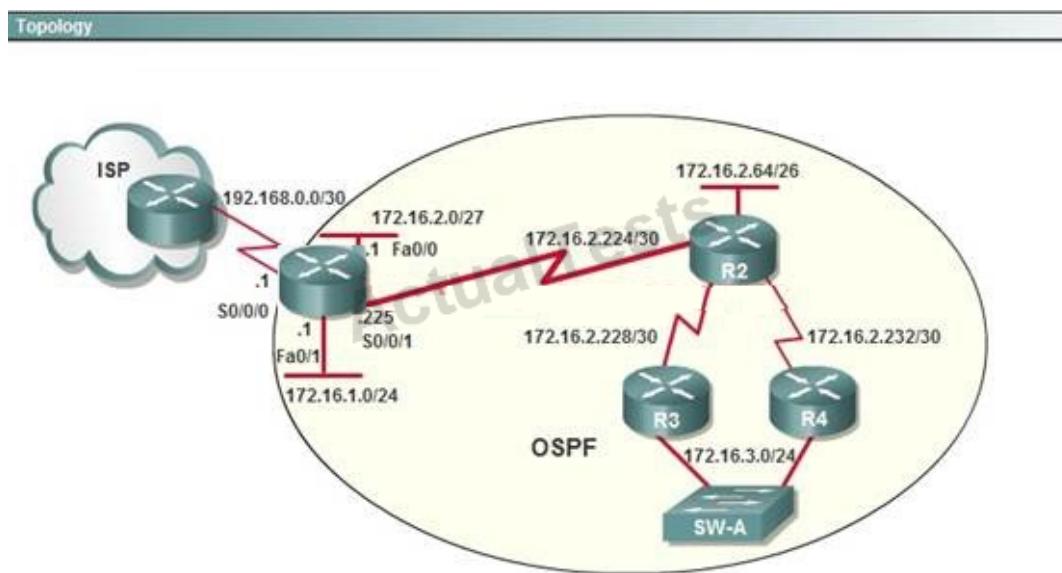
This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the topology.

To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by **clicking on the Questions button to the left**.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Scenario

Refer to the topology. Using the information shown, answer the four questions shown on the Questions tab.



- A. R2(config-if)#clock rate
- B. R2(config-if)#bandwidth
- C. R2(config-if)#ip ospf cost
- D. R2(config-if)#ip ospf priority
- E. R2(config-router)#distance ospf

Answer: B,C

Explanation:

The cost (also called metric) of an interface in OSPF is an indication of the overhead required to send packets across a certain interface. The cost of an interface is inversely proportional to the bandwidth of that interface. A higher bandwidth indicates a lower cost. There is more overhead (higher cost) and time delays involved in crossing a 56k serial line than crossing a 10M Ethernet line. The formula used to calculate the cost is:

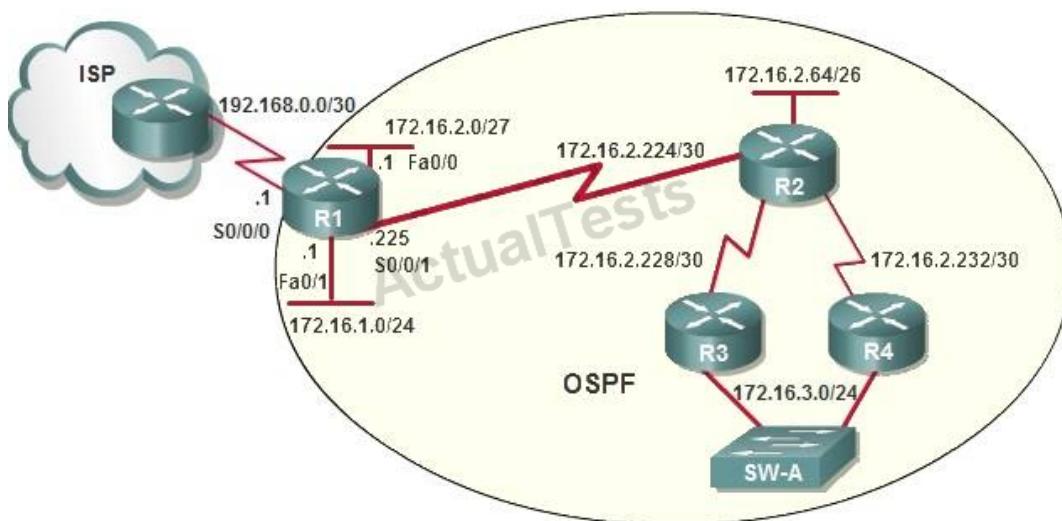
$$\text{Cost} = 10000 \text{ 0000}/\text{bandwidth in bps}$$

For example, it will cost $10 \text{ EXP8}/10 \text{ EXP7} = 10$ to cross a 10M Ethernet line and will cost $10 \text{ EXP8}/1544000 = 64$ to cross a T1 line.

By default, the cost of an interface is calculated based on the bandwidth; you can force the cost of an interface with the `ip ospf cost <value>` interface subconfiguration mode command.

QUESTION NO: 100

After the network has converged, what type of messaging, if any, occurs between R3 and R4?



- A. No messages are exchanged
- B. Hellos are sent every 10 seconds.
- C. The full database from each router is sent every 30 seconds.
- D. The routing table from each router is sent every 60 seconds.

Answer: B

Explanation:

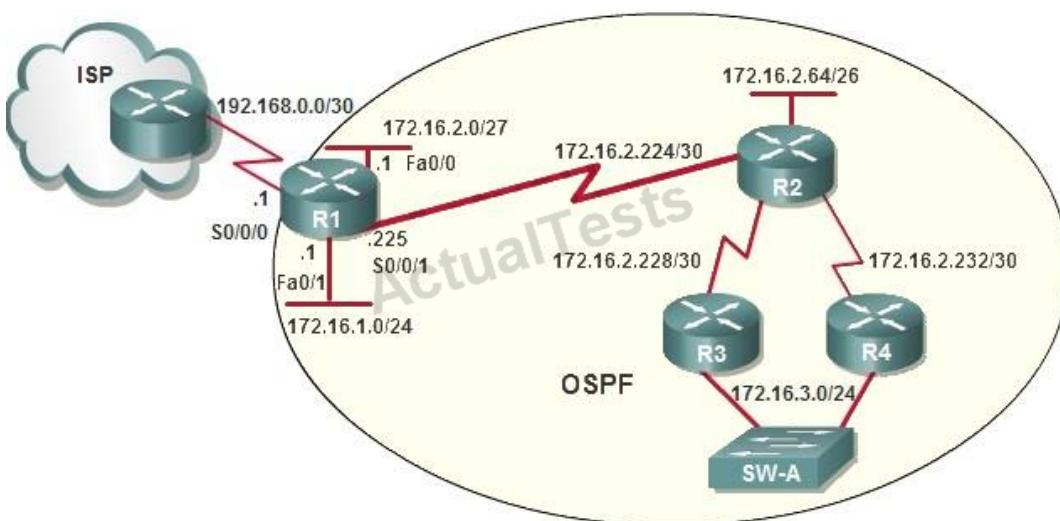
HELLO messages are used to maintain adjacent neighbors so even when the network is

converged, hellos are still exchanged. On broadcast and point-to-point links, the default is 10 seconds, on NBMA the default is 30 seconds.

Although OSPF is a link-state protocol the full database from each router is sent every 30 minutes (not seconds) therefore, C and D are not correct.

QUESTION NO: 101

OSPF is configured using default classful addressing. With all routers and interfaces operational, how many networks will be in the routing table of R1 that are indicated to be learned by OSPF?



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

Answer: C

Explanation:

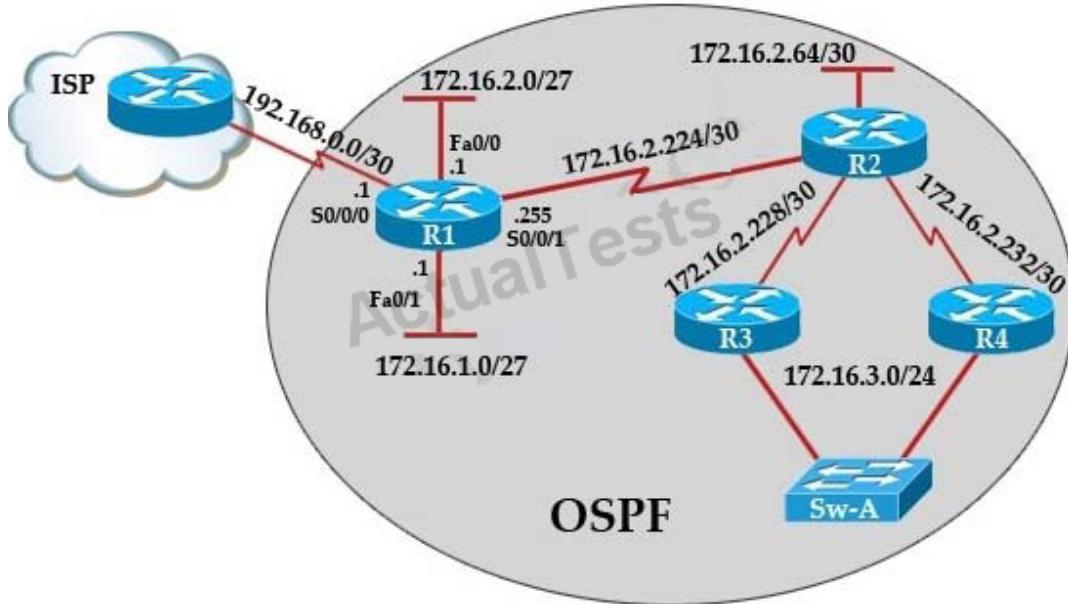
Although OSPF is configured using default classful addressing but OSPF is a link-state routing protocol so it will always send the subnet mask of each network in their advertised routes.

Therefore R1 will learn the the complete subnets. Four networks list below will be in the routing table of R1: + 172.16.2.64/30 + 172.16.2.228/30 + 172.16.2.232/30 + 172.16.3.0/24

Note: Other networks will be learned as “Directly connected” networks (marked with letter “C”)

QUESTION NO: 102

R1 is configured with the default configuration of OSPF. From the following list of IP addresses configured on R1, which address will the OSPF process select as the router ID?



- A. 192.168.0.1
- B. 172.16.1.1
- C. 172.16.2.1
- D. 172.16.2.225

Answer: A

Explanation:

The Router ID (RID) is an IP address used to identify the router and is chosen using the following sequence.

- + The highest IP address assigned to a loopback (logical) interface. + If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen.
- + The router ID can be manually assigned

In this case, because a loopback interface is not configured so the highest active IP address 192.168.0.1 is chosen as the router ID.

QUESTION NO: 103

ROUTER# show ip route

```
192.168.12.0/24 is variably subnetted, 9 subnets, 3 masks
C 192.168.12.64 /28 is directly connected, Loopback1
C 192.168.12.32 /28 is directly connected, Ethernet0
C 192.168.12.48 /28 is directly connected, Loopback0
O 192.168.12.236 /30 [110/128] via 192.168.12.233, 00:35:36, Serial0
C 192.168.12.232 /30 is directly connected, Serial0
O 192.168.12.245 /30 [110/782] via 192.168.12.233, 00:35:36, Serial0
O 192.168.12.240 /30 [110/128] via 192.168.12.233, 00:35:36, Serial0
O 192.168.12.253 /30 [110/782] via 192.168.12.233, 00:35:37, Serial0
O 192.168.12.249 /30 [110/782] via 192.168.12.233, 00:35:37, Serial0
O 192.168.12.240/30 [110/128] via 192.168.12.233, 00:35:36, Serial 0
```

To what does the 128 refer to in the router output above?

- A. OSPF cost
- B. OSPF priority
- C. OSPF hop count
- D. OSPF ID number
- E. OSPF administrative distance

Answer: A

Explanation:

The first parameter is the Administrative Distance of OSPF (110) while the second parameter is the cost of OSPF.

QUESTION NO: 104

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 globally significant.
- C. It is needed to identify a unique instance of an OSPF database.
- D. It is an optional parameter required only if multiple OSPF processes are running on the router.
- E. All routers in the same OSPF area must have the same process ID if they are to exchange routing information.

Answer: A,C

Explanation:

<https://learningnetwork.cisco.com/thread/6248>

They are locally significant only, and have no bearing on the structure of any OSPF packet or LSA update. So you can have a separate process-id on every single router in your network if you so desire.

QUESTION NO: 105

Which address are OSPF hello packets addressed to on point-to-point networks?

- A. 224.0.0.5
- B. 172.16.0.1
- C. 192.168.0.5
- D. 223.0.0.1
- E. 254.255.255.255

Answer: A

Explanation:

Why does the show ip ospf neighbor Command Reveal Neighbors in the Init State?

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f11.shtml

OSPF hello packets have a destination address of 224.0.0.5 (the all ospf routers multicast address).

QUESTION NO: 106

Some routers have been configured with default routes. What are some of the advantages of

using default routes? (Choose two)

- A. They establish routes that will never go down.
- B. They keep routing tables small.
- C. They require a great deal of CPU power.
- D. They allow connectivity to remote networks that are not in the routing table
- E. They direct traffic from the internet into corporate networks.

Answer: B,D

Explanation:

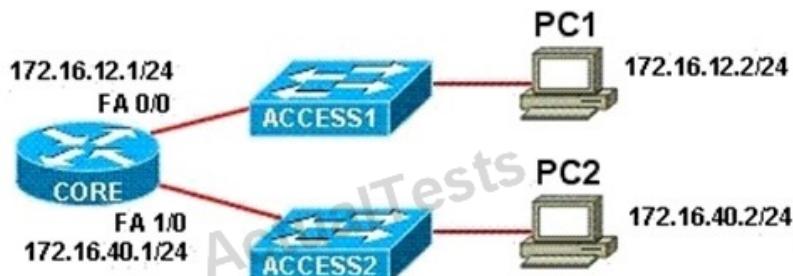
Cisco administration 101: What you need to know about default routes

Reference:

<http://www.techrepublic.com/article/cisco-administration-101-what-you-need-to-know-about-default-routes/>

QUESTION NO: 107

Refer to the exhibit.



Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.12.1	-	0001.4210.3BA9	ARPA	FastEthernet0/0
Internet	172.16.12.2	0	0010.111A.7AB0	ARPA	FastEthernet0/0
Internet	172.16.40.1	-	00D0.FF59.4A85	ARPA	FastEthernet1/0
Internet	172.16.40.2	0	00E0.B0B7.EAB1	ARPA	FastEthernet1/0

PC1 pings PC2. What three things will CORE router do with the data that is received from PC1? (Choose three.)

- A. The data frames will be forwarded out interface FastEthernet0/1 of CORE router.
- B. The data frames will be forwarded out interface FastEthernet1/0 of CORE router.
- C. CORE router will replace the destination IP address of the packets with the IP address of PC2.
- D. CORE router will replace the MAC address of PC2 in the destination MAC address of the

frames.

- E. CORE router will put the IP address of the forwarding FastEthernet interface in the place of the source IP address in the packets.
- F. CORE router will put the MAC address of the forwarding FastEthernet interface in the place of the source MAC address.

Answer: B,D,F

Explanation:

The router will forward the frames out the interface toward the destination – B is correct.

Since the router will have the end station already in its MAC table as seen by the “show arp” command, it will replace the destination MAC address to that of PC2 – D is correct.

The router will then replace the source IP address to 172.16.40.1 – E is correct.

QUESTION NO: 108

Which three statements are correct about RIP version 2? (Choose three)

- A. It uses broadcast for its routing updates.
- B. It supports authentication.
- C. It is a classless routing protocol.
- D. It has a lower default administrative distance than RIP version 1.
- E. It has the same maximum hop count as RIP version 1.
- F. It does not send the subnet mask in updates.

Answer: B,C,E

Explanation:

A and E are correct according to the theory of RIP.

RIP version 1 updates are broadcasts, and RIP version 2 updates are multicast to 224.0.0.9 -> B is not correct.

RIP v1 is a classful routing protocol but RIP v2 is a classless routing protocol -> C is correct.

RIPv1 and RIPv2 have the same default administrative distance of 120 -> D is not correct.

RIPv2 is a classless routing protocol so it does send the subnet mask in updates -> F is not correct.

QUESTION NO: 109

Refer to the exhibit.

Neighbor_ID	Pri	State	Dead Time	Address	Interface
208.149.23.194	1	Full/DR	00:00:33	190.172.32.10	Ethernet1
208.149.23.60	1	Full/BDR	00:00:33	190.172.32.10	Ethernet0
208.149.23.130	1	Full/DR	00:00:39	190.172.32.10	Ethernet0

Why are two OSPF designated routers identified on Core-Router?

- A. Core-Router is connected to more than one multi-access network.
- B. The router at 208.149.23.130 is a secondary DR in case the primary fails.
- C. Two router IDs have the same OSPF priority and are therefore tied for DR election
- D. The DR election is still underway and there are two contenders for the role.

Answer: A

Explanation:

OSPF elects one DR per multi-access network. In the exhibit there are two DR so there must have more than one multi-access network.

QUESTION NO: 110

What is the OSPF default frequency, in seconds, at which a Cisco router sends hello packets on a multi-access network?

- A. 10
- B. 40
- C. 30
- D. 20

Answer: A

Explanation:

On broadcast multiaccess and point-to-point links, the default is 10 seconds. On NBMA, the default is 30 seconds.

QUESTION NO: 111

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

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

Answer: A

Explanation:

The well-known formula to calculate OSPF cost is

$$\text{Cost} = 108 / \text{Bandwidth}$$

QUESTION NO: 112

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

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

Answer: B,C,D

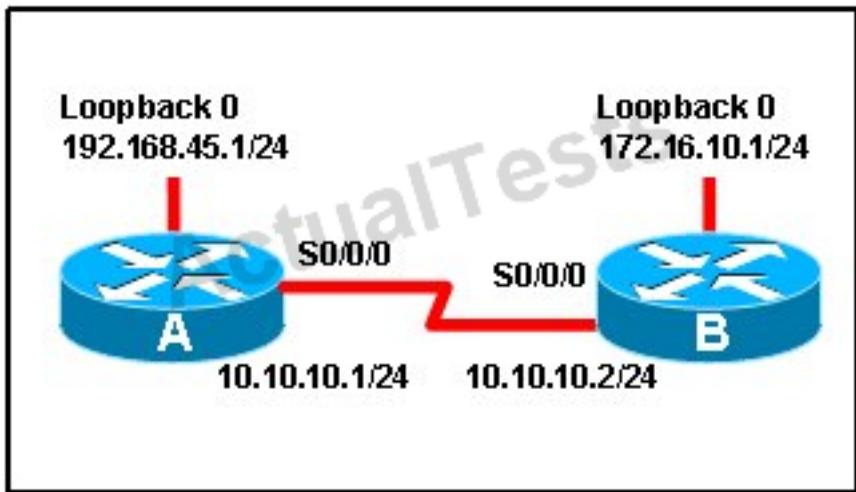
Explanation:

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

The hierarchical approach is used to achieve the following:

QUESTION NO: 113

Refer to the exhibit.



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

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

Answer: B

Explanation:

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

QUESTION NO: 114

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

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

Answer: B

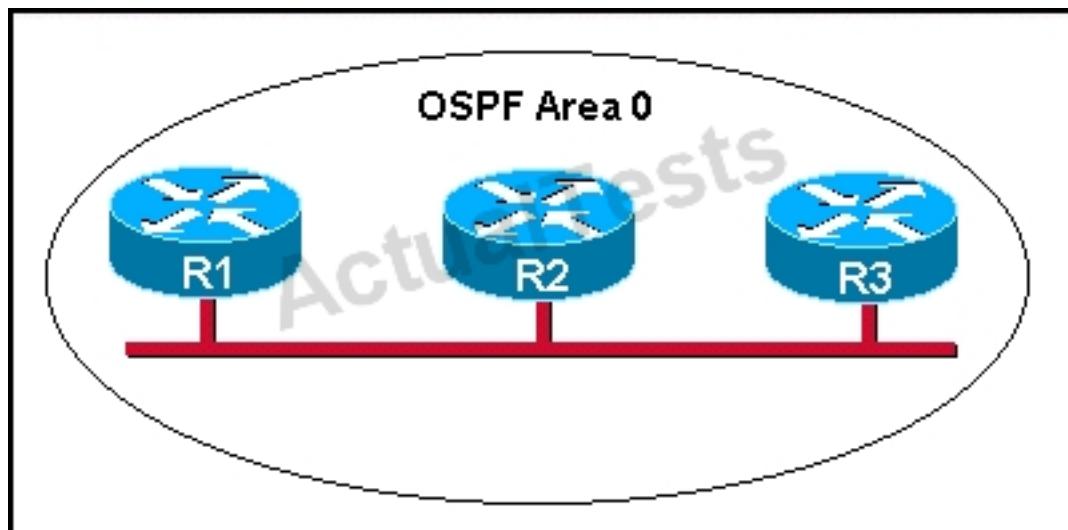
Explanation:

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

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

QUESTION NO: 115

Refer to the graphic.



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

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

- B. R1 and R2 are the DR and BDR, so OSPF will not establish neighbor adjacency with R3.
- C. A static route has been configured from R1 to R3 and prevents the neighbor adjacency from being established.
- D. The hello and dead interval timers are not set to the same values on R1 and R3.
- E. EIGRP is also configured on these routers with a lower administrative distance.
- F. R1 and R3 are configured in different areas.

Answer: D,F

Explanation:

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

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

1. The area ID and its types;
2. Hello and failure time interval timer;
3. OSPF Password (Optional);

QUESTION NO: 116

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

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

Answer: D

Explanation:

The “show ip ospf database” command displays the link states. Here is an example:

Here is the lsa database on R2.

R2#show ip ospf database

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

Router Link States (Area 0)

Link ID ADV Router Age Seq# Checksum Link count

2.2.2.2 2.2.2.2 793 0x80000003 0x004F85 2

10.4.4.4 10.4.4.4 776 0x80000004 0x005643 1

111.111.111.111 111.111.111.111 755 0x80000005 0x0059CA 2

133.133.133.133 133.133.133.133 775 0x80000005 0x00B5B1 2

Net Link States (Area 0)

Link ID ADV Router Age Seq# Checksum 10.1.1.1 111.111.111.111 794 0x80000001 0x001E8B
 10.2.2.3 133.133.133.133 812 0x80000001 0x004BA9
 10.4.4.1 111.111.111.111 755 0x80000001 0x007F16
 10.4.4.3 133.133.133.133 775 0x80000001 0x00C31F

QUESTION NO: 117

Refer to the exhibit.

```
City#show ip interface brief
```

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

```
City#
```

A network associate has configured OSPF with the command:

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

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

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

Answer: B,C,D

Explanation:

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

- + Increment: 64 (/26= 1111 1111.1111 1111.1111 1111.1100 0000)
- + Network address: 192.168.12.64
- + Broadcast address: 192.168.12.127

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

QUESTION NO: 118

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

- A. It supports VLSM.
- B. It is used to route between autonomous systems.
- C. It confines network instability to one area of the network.
- D. It increases routing overhead on the network.
- E. It allows extensive control of routing updates.
- F. It is simpler to configure than RIP v2.

Answer: A,C,E

Explanation:

Routing overhead is the amount of information needed to describe the changes in a dynamic network topology.

All routers in an OSPF area have identical copies of the topology database and the topology database of one area is hidden from the rest of the areas to reduce routing overhead because fewer routing updates are sent and smaller routing trees are computed and maintained (allow extensive control of routing updates and confine network instability to one area of the network).

QUESTION NO: 119

What is the default administrative distance of OSPF?

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

Answer: C**Explanation:**

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

Default Distance Value Table

This table lists the administrative distance default values of the protocols that Cisco supports:

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

QUESTION NO: 120

Refer to the exhibit.

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

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

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

Answer: C

Explanation:

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

QUESTION NO: 121

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

```
Router(config)# router ospf 1
```

- A. All OSPF routers in an area must have the same process ID.
- B. Only one process number can be used on the same router.
- C. Different process identifiers can be used to run multiple OSPF processes

- D. The process number can be any number from 1 to 65,535.
- E. Hello packets are sent to each neighbor to determine the processor identifier.

Answer: C,D

Explanation:

Multiple OSPF processes can be configured on a router using multiple process ID's.

The valid process ID's are shown below:

```
Edge-B(config)#router ospf  
<1-65535> Process ID
```

QUESTION NO: 122

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

- A. Router(config)# router ospf 0
- B. Router(config)# router ospf 1
- C. Router(config)# router ospf area 0
- D. Router(config-router)# network 192.168.16.0 0.0.0.255 0
- E. Router(config-router)# network 192.168.16.0 0.0.0.255 area 0
- F. Router(config-router)# network 192.168.16.0 255.255.255.0 area 0

Answer: B,E

Explanation:

In the router ospf command, the ranges from 1 to 65535 so 0 is an invalid number -> but To configure OSPF, we need a wildcard in the “network” statement, not a subnet mask. We also need to assign an area to this process.

QUESTION NO: 123

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

- A. 2

- B. 8
- C. 16
- D. unlimited

Answer: B

Explanation:

Maximum-paths (OSPF)

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

Syntax Description

maximum

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

Command Default

8 *paths*

QUESTION NO: 124

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

```
Router(config)# router ospf 1
```

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

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

Answer: C

Explanation:

When configuring OSPF, the mask used for the network statement is a wildcard mask similar to an

access list. In this specific example, the correct syntax would have been “network 10.0.0.0 0.0.0.255 area 0.”

QUESTION NO: 125

A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common Ethernet link.

R1:	Ethernet0 is up, line protocol is up Internet address 192.168.1.2/24, Area 0 Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 10 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 192.168.31.33, Interface address 192.168.1.2 No backup designated router on this network Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
R2:	Ethernet0 is up, line protocol is up Internet address 192.168.1.1/24, Area 0 Process ID 2, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 10 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1 No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

The graphic shows the output of the show ip ospf interface e0 command for routers R1 and R2. Based on the information in the graphic, what is the cause of this problem?

- A. The OSPF area is not configured properly.
- B. The priority on R1 should be set higher.
- C. The cost on R1 should be set higher.
- D. The hello and dead timers are not configured properly.
- E. A backup designated router needs to be added to the network.
- F. The OSPF process ID numbers must match.

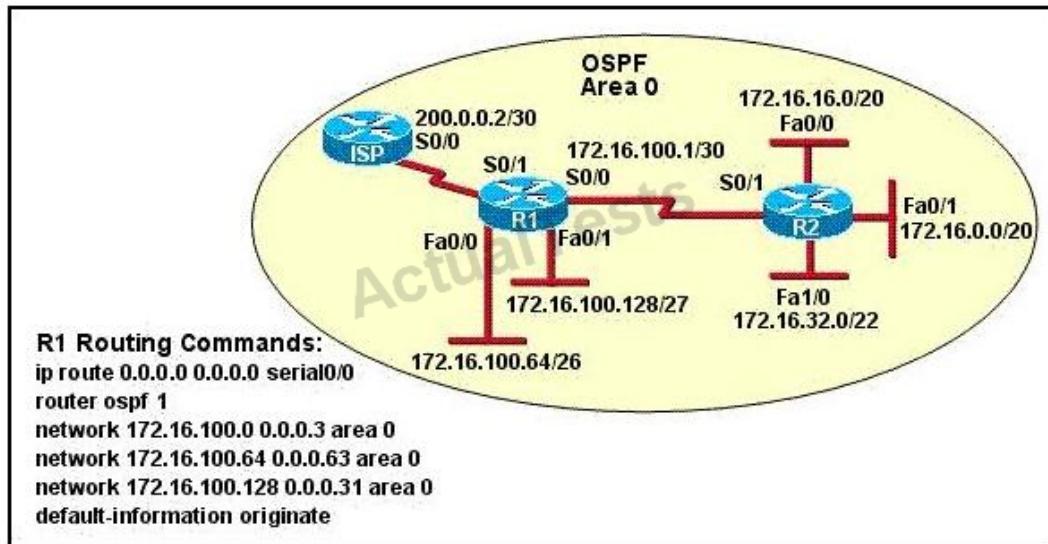
Answer: D

Explanation:

In OSPF, the hello and dead intervals must match and here we can see the hello interval is set to 5 on R1 and 10 on R2. The dead interval is also set to 20 on R1 but it is 40 on R2.

QUESTION NO: 126

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

Explanation:

First, notice that the more-specific routes will always be favored over less-specific routes regardless of the administrative distance set for a protocol. In this case, because we use OSPF for three networks (172.16.100.0 0.0.0.3, 172.16.100.64 0.0.0.63, 172.16.100.128 0.0.0.31) so the packets destined for these networks will not be affected by the default route.

The default route configured on R1 “ip route 0.0.0.0 0.0.0.0 serial0/0 will send any packet whose destination network is not referenced in the routing table of router R1 to R2, it doesn’t drop anything. These routes are declared in R1 and the question says that “OSPF has been correctly configured on router R2, so network directly connected to router R2 can communicate with those

three subnetworks.

As said above, the default route configured on R1 will send any packet destined for a network that is not referenced in its routing table to R2; R2 in turn sends it to R1 because it is the only way and a routing loop will occur.

QUESTION NO: 127

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

Explanation:

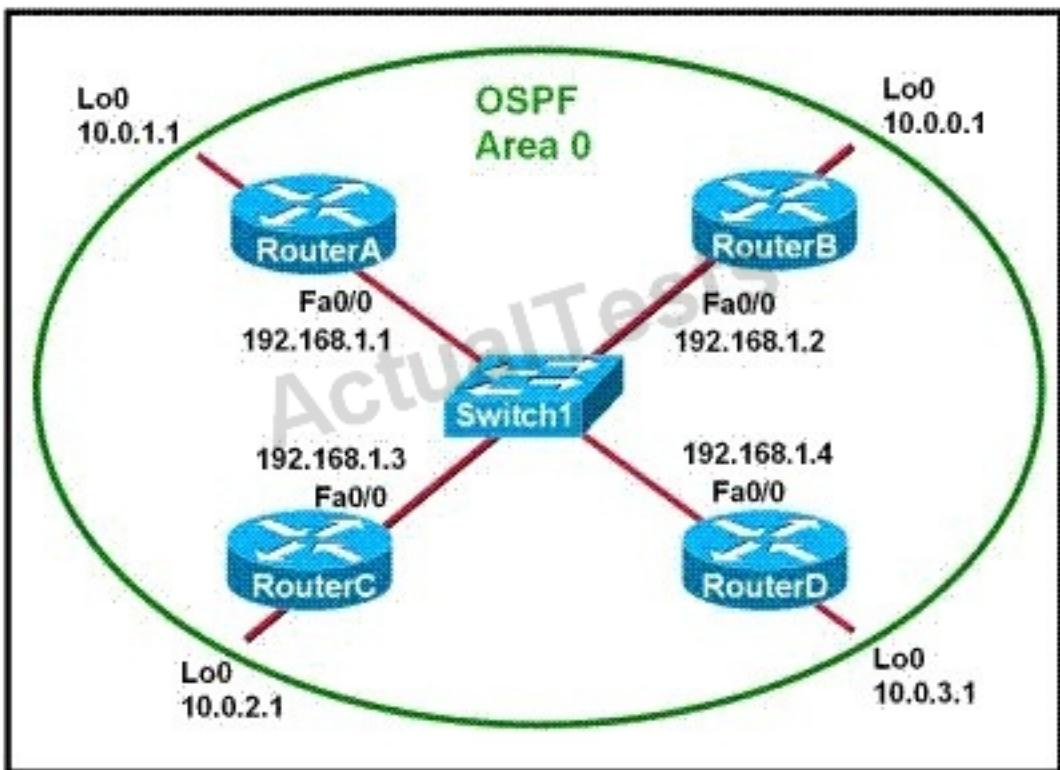
Definition of OSPF areas: An OSPF network may be structured, or subdivided, into routing *areas* to simplify administration and optimize traffic and resource utilization. Areas are identified by 32-bit numbers, expressed either simply in decimal, or often in octet-based dot-decimal notation, familiar from IPv4 address notation.

See discussion following Cisco Learning discussion.

<https://learningnetwork.cisco.com/message/90832>

QUESTION NO: 128

Refer to the exhibit.



Which two statements are true about the loopback address that is configured on RouterB?
(Choose two.)

- A. It ensures that data will be forwarded by RouterB.
- B. It provides stability for the OSPF process on RouterB.
- C. It specifies that the router ID for RouterB should be 10.0.0.1.
- D. It decreases the metric for routes that are advertised from RouterB.
- E. It indicates that RouterB should be elected the DR for the LAN.

Answer: B,C

Explanation:

A loopback interface never comes down even if the link is broken so it provides stability for the OSPF process (for example we use that loopback interface as the router-id) -

The router-ID is chosen in the order below:

- + The highest IP address assigned to a loopback (logical) interface.
 - + If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen.
- > The loopback interface will be chosen as the router ID of RouterB -

QUESTION NO: 129

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

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

Answer: A,C,D

Explanation:

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

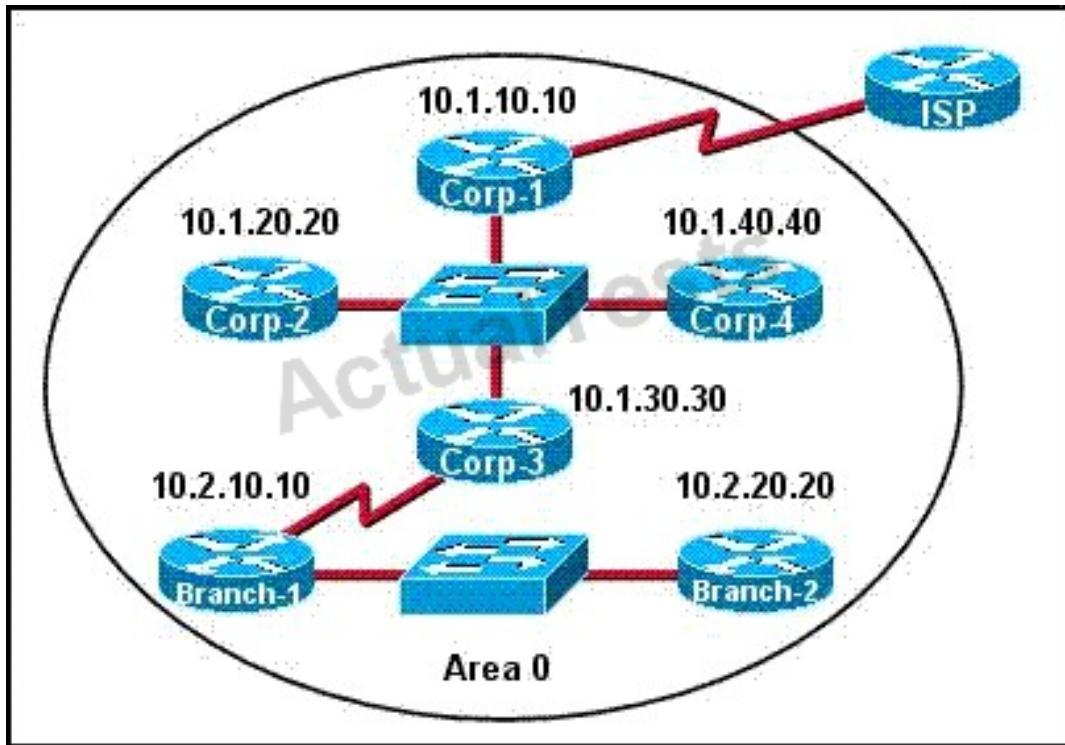
Link-state routing protocols generate routing updates only (not the whole routing table) when a change occurs in the network topology so

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

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

QUESTION NO: 130

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:

There are 2 segments on the topology above which are separated by Corp-3 router. Each segment will have a DR so we have 2 DRs.

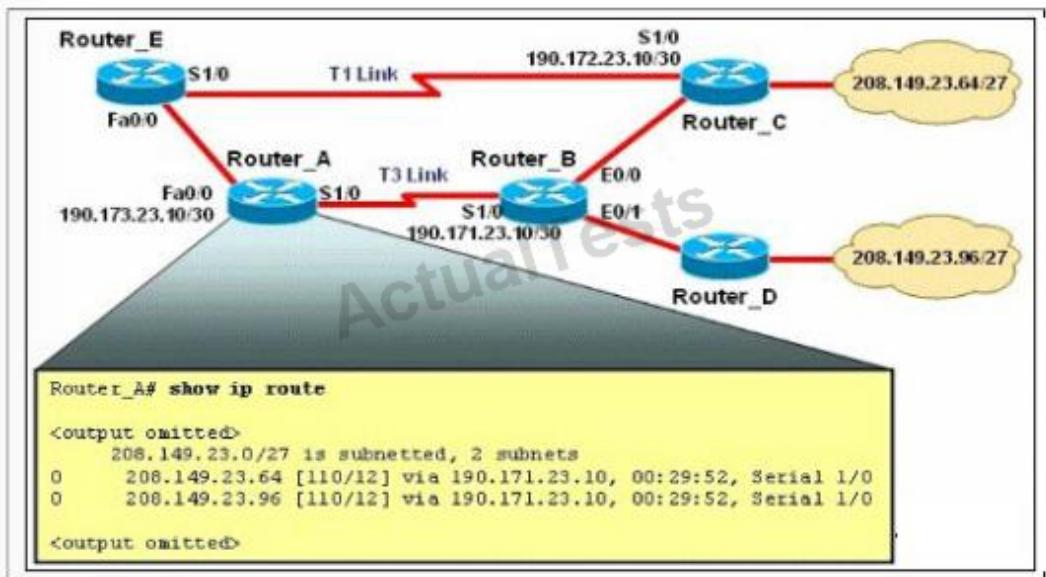
To select which router will become DR they will compare their router-IDs. The router with highest (best) router-ID will become DR. The router-ID is chosen in the order below:

- + The highest IP address assigned to a loopback (logical) interface.
- + If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen.

In this question, the IP addresses of loopback interfaces are not mentioned so we will consider IP addresses of all active router's physical interfaces. Router Corp-4 (10.1.40.40) & Branch-2 (10.2.20.20) have highest "active" IP addresses so they will become DRs.

QUESTION NO: 131

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, FastEthernet0/0
208.149.23.96[110/13] via 190.173.23.10, 00:00:16, FastEthernet0/0
- 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, FastEthernet0/0
- 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, FastEthernet0/0
- 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

Explanation:

Router_E learns two subnets 208.149.23.64 and 208.149.23.96 via Router_A through FastEthernet interface. The interface cost is calculated with the formula $108 / \text{Bandwidth}$. For FastEthernet it is $108 / 100 \text{ Mbps} = 108 / 100,000,000 = 1$. Therefore the cost is **12** (learned from

Router_A) + 1 = 13 for both subnets ->

The cost through T1 link is much higher than through T3 link (T1 cost = 108 / 1.544 Mbps = 64; T3 cost = 108 / 45 Mbps = 2) so surely OSPF will choose the path through T3 link -> Router_E will choose the path from Router_A through FastEthernet0/0, not Serial1/0.

In fact, we can quickly eliminate answers B, C and D because they contain at least one subnet learned from Serial1/0 -> they are surely incorrect.

QUESTION NO: 132

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

Answer: A,C

Explanation:

Reference 1:

<http://www.ciscopress.com/articles/article.asp?p=24090&seqNum=4>

Link state protocols, sometimes called shortest path first or distributed database protocols, are built around a well-known algorithm from graph theory, E. W. Dijkstra's shortest path algorithm.

Examples of link state routing protocols are:

Open Shortest Path First (OSPF) for IP

The ISO's Intermediate System to Intermediate System (IS-IS) for CLNS and IP

DEC's DNA Phase V

Novell's NetWare Link Services Protocol (NLSP)

Although link state protocols are rightly considered more complex than distance vector protocols, the basic functionality is not complex at all:

1. Each router establishes a relationship—an adjacency—with each of its neighbors.
2. Each router sends link state advertisements (LSAs), some
3. Each router stores a copy of all the LSAs it has seen in a database. If all works well, the databases in all routers should be identical.
4. The completed topological database, also called the link state database, describes a graph of the internetwork. Using the Dijkstra algorithm, each router calculates the shortest path to each

network and enters this information into the route table.

OSPF Tutorial

QUESTION NO: 133

What are two benefits of using a single OSPF area network design? (Choose two.)

- A. It is less CPU intensive for routers in the single area.
- B. It reduces the types of LSAs that are generated.
- C. It removes the need for virtual links.
- D. It increases LSA response times.
- E. It reduces the number of required OSPF neighbor adjacencies.

Answer: B,C

Explanation:

OSPF uses a LSDB (link state database) and fills this with LSAs (link state advertisement). The link types are as follows:

If all routers are in the same area, then many of these LSA types (Summary ASBR LSA, external LSA, etc) will not be used and will not be generated by any router.

All areas in an Open Shortest Path First (OSPF) autonomous system must be physically connected to the backbone area (Area 0). In some cases, where this is not possible, you can use a virtual link to connect to the backbone through a non-backbone area. You can also use virtual links to connect two parts of a partitioned backbone through a non-backbone area. The area through which you configure the virtual link, known as a transit area, must have full routing information. The transit area cannot be a stub area. Virtual links are not ideal and should really only be used for temporary network solutions or migrations. However, if all locations are in a single OSPF area this is not needed.

QUESTION NO: 134

What command sequence will configure a router to run OSPF and add network 10.1.1.0 /24 to area 0?

- A. router ospf area 0
network 10.1.1.0 255.255.255.0 area 0
- B. router ospf
network 10.1.1.0 0.0.0.255
- C. router ospf 1
network 10.1.1.0 0.0.0.255 area 0
- D. router ospf area 0
network 10.1.1.0 0.0.0.255 area 0
- E. router ospf
network 10.1.1.0 255.255.255.0 area 0
- F. router ospf 1
network 10.1.1.0 0.0.0.255

Answer: C

Explanation:

Enabling OSPF **SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router ospf process-id**
4. **network ip-address wildcard-mask area area-id**
5. **end**

DETAILED STEPS

Command or Action

Purpose

Step 1

enable

Example:

Device> enable

Enables privileged EXEC mode.

Step 2

configure terminal

Example:

Device# configure terminal

Enters global configuration mode.

Step 3

router ospf process-id

Example:

```
Device(config)# router ospf 109
```

Enables OSPF routing and enters router configuration mode.

Step 4

```
network ip-address wildcard-mask area area-id
```

Example:

```
Device(config-router)# network 192.168.129.16 0.0.0.3 area 0
```

Defines an interface on which OSPF runs and defines the area ID for that interface.

Step 5

```
end
```

Example:

```
Device(config-router)# end
```

Exits router configuration mode and returns to privileged EXEC mode.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/12-4t/iro-12-4t-book/iro-cfg.html#GUID-588D1301-F63C-4DAC-BF1C-C3735EB13673

QUESTION NO: 135

Refer to the exhibit.

Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/0	192.168.1.1	YES manual up	up
FastEthernet0/1	172.16.1.1	YES manual up	up
Loopback0	1.1.1.1	YES manual up	up
Loopback1	2.2.2.2	YES manual up	up
Vlan1	unassigned	YES unset administratively down down	

If the router Cisco returns the given output and has not had its router ID set manually, what value will OSPF use as its router ID?

- A. 192.168.1.1
- B. 172.16.1.1
- C. 1.1.1.1
- D. 2.2.2.2

Answer: D

Explanation:

If a router-id is not configured manually in the OSPF routing process the router will automatically configure a router-id determined from the highest IP address of a logical interface (loopback interface) or the highest IP address of an active interface. If more than one loopback interfaces are configured, the router will compare the IP addresses of each of the interfaces and choose the highest IP address from the loopbacks.

QUESTION NO: 136

What OSPF command, when configured, will include all interfaces into area 0?

- A. network 0.0.0.0 255.255.255.255 area 0
- B. network 0.0.0.0 0.0.0.0 area 0
- C. network 255.255.255.255 0.0.0.0 area 0
- D. network all-interfaces area 0

Answer: A

Explanation:

Example 3-1 displays OSPF with a process ID of 1 and places all interfaces configured with an IP address in area 0. The network command **network 0.0.0.0 255.255.255.255 area 0** dictates that you do not care (255.255.255.255) what the IP address is, but if an IP address is enabled on any interface, place it in area 0.

Example 3-1 Configuring OSPF in a Single Area

```
router ospf 1  
network 0.0.0.0 255.255.255.255 area 0
```

Reference: <http://www.ciscopress.com/articles/article.asp?p=26919&seqNum=3>

QUESTION NO: 137

Which statement describes the process ID that is used to run OSPF on a router?

- A. It is globally significant and is used to represent the AS number.
- B. It is locally significant and is used to identify an instance of the OSPF database.
- C. It is globally significant and is used to identify OSPF stub areas.
- D. It is locally significant and must be the same throughout an area.

Answer: B

Explanation:

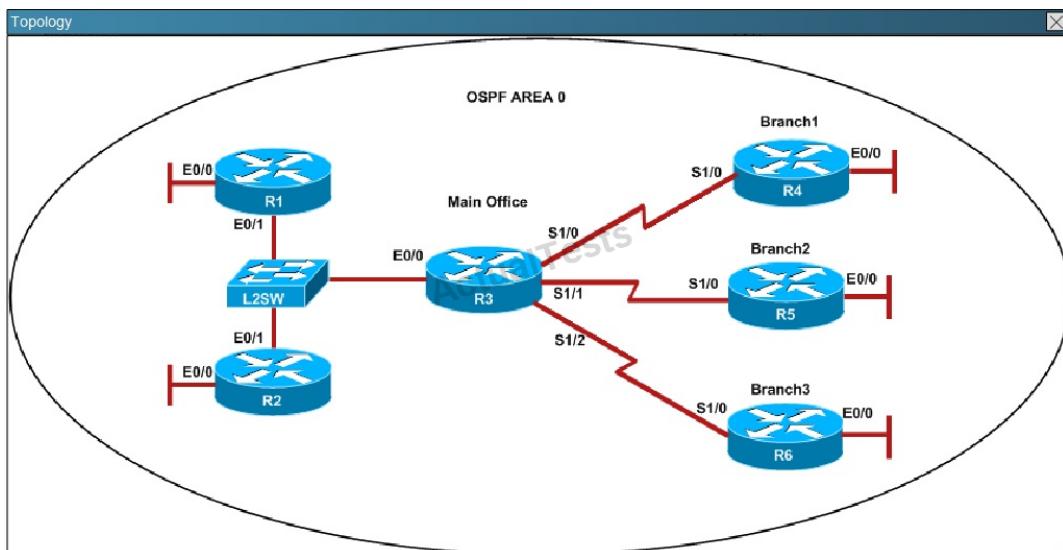
The Process ID for OSPF on a router is only locally significant and you can use the same number on each router, or each router can have a different number-it just doesn't matter. The numbers you can use are from 1 to 65,535. Don't get this confused with area numbers, which can be from 0 to 4.2 billion.

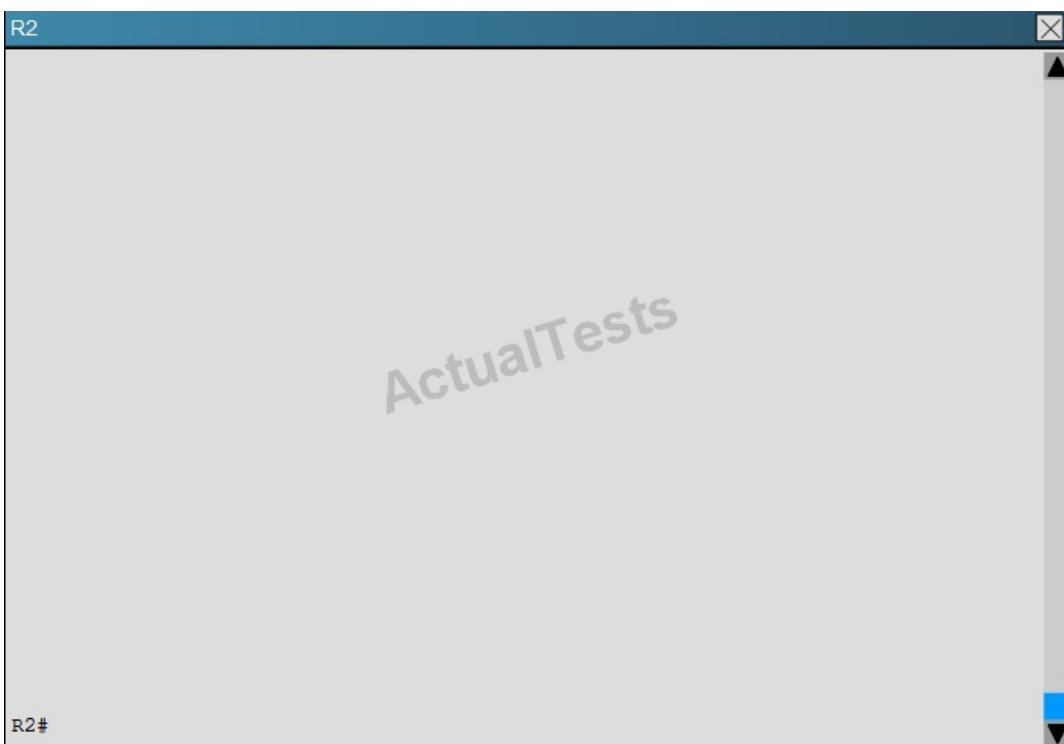
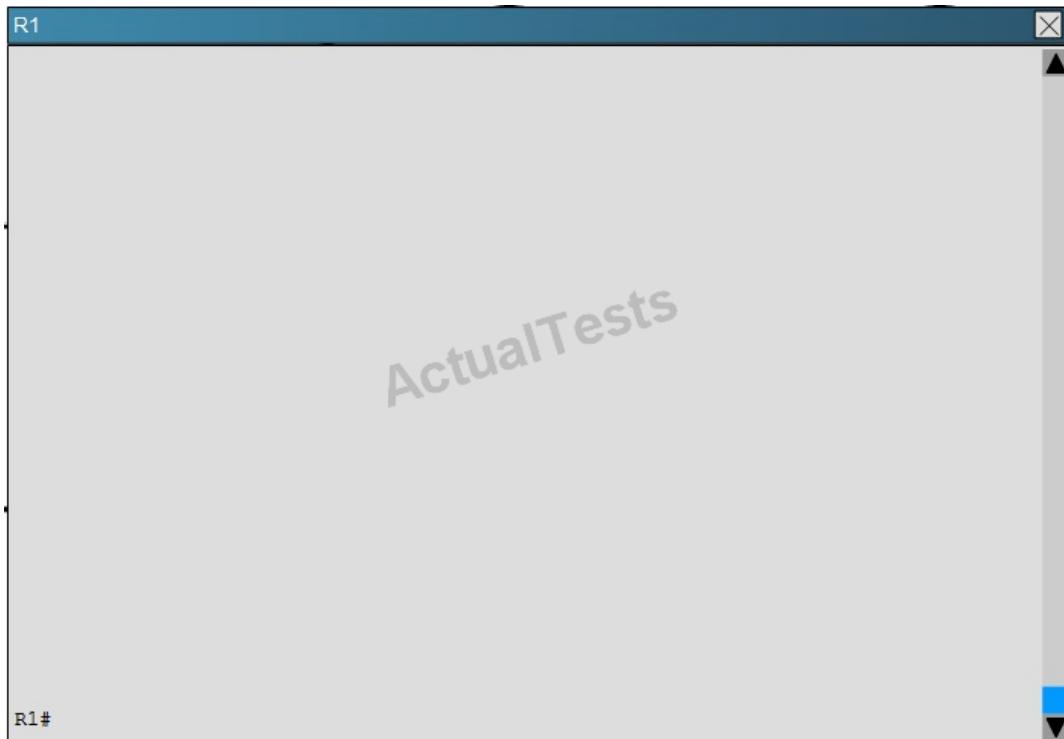
QUESTION NO: 138

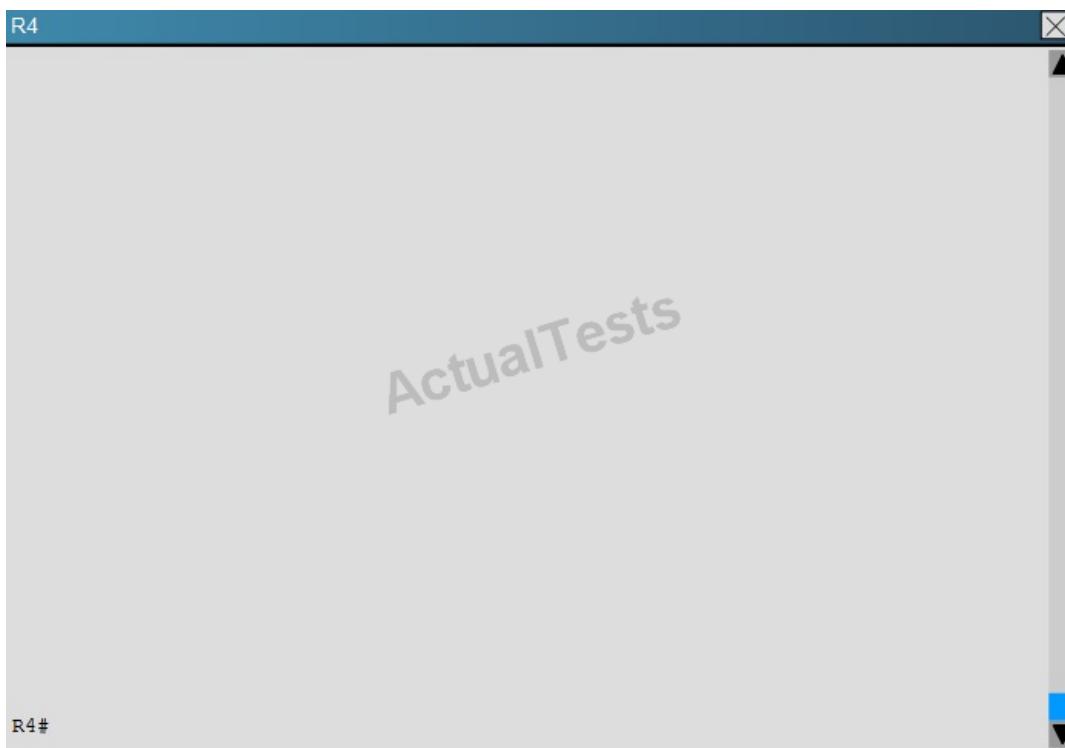
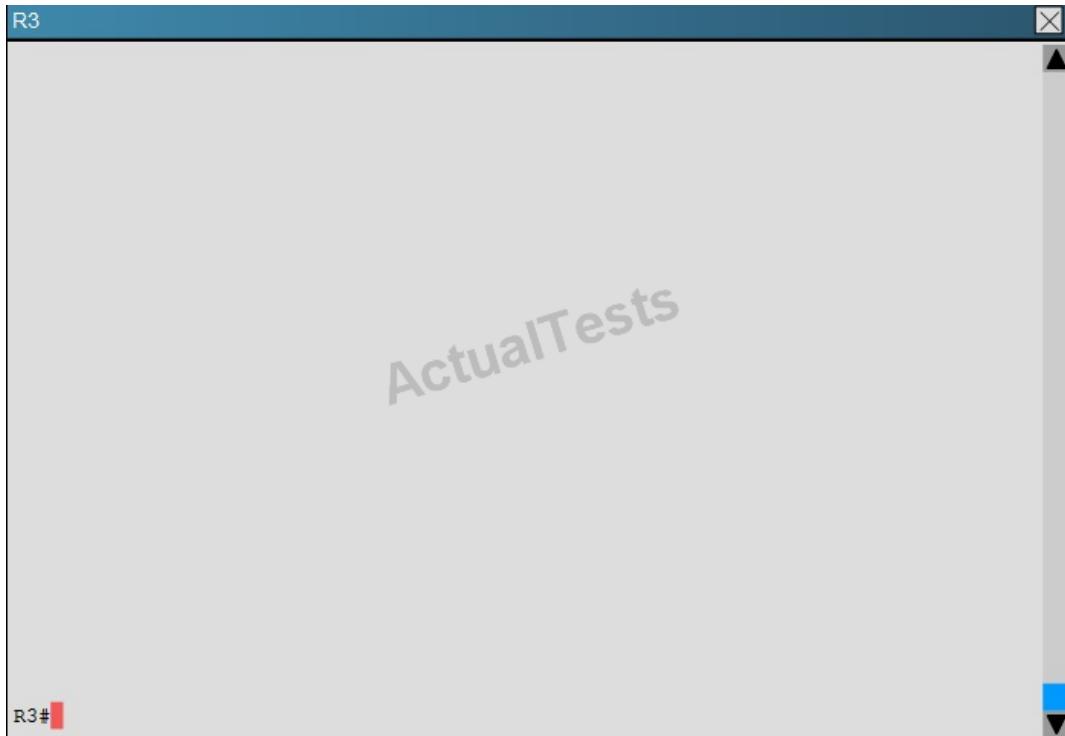
Scenario

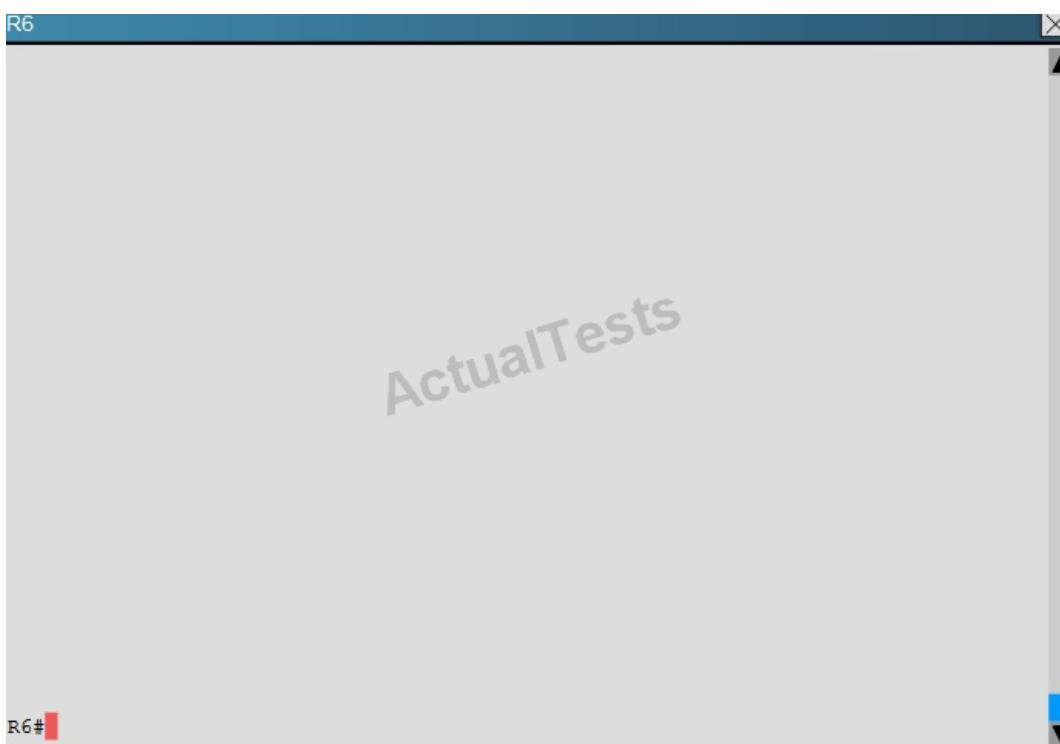
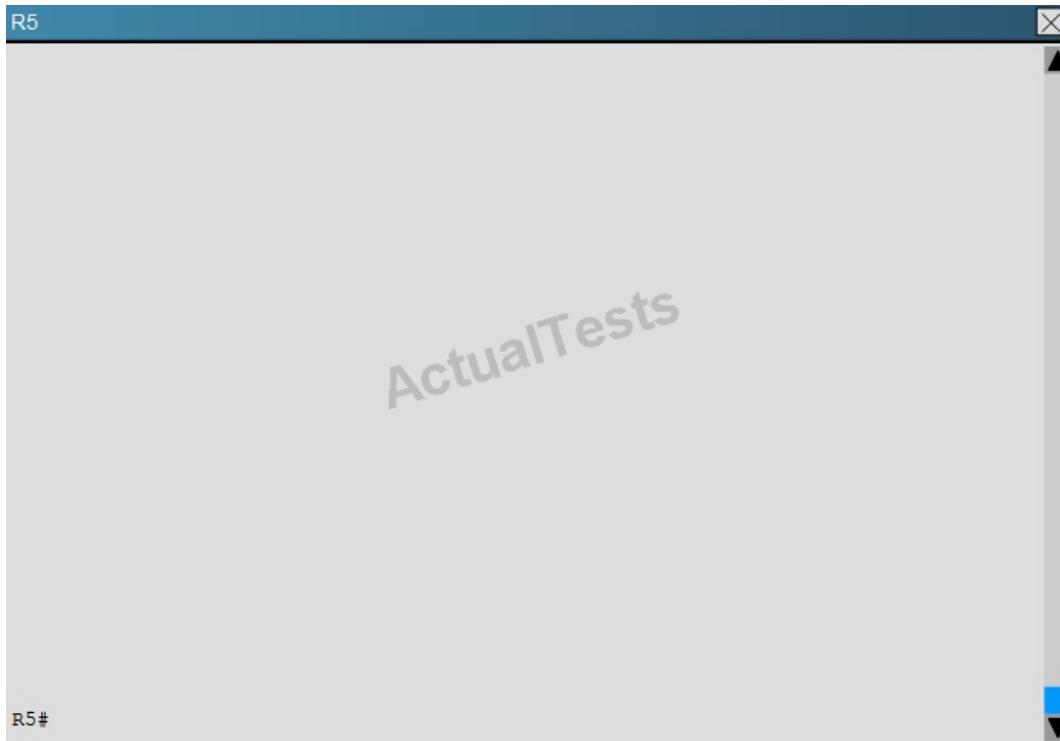
Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.

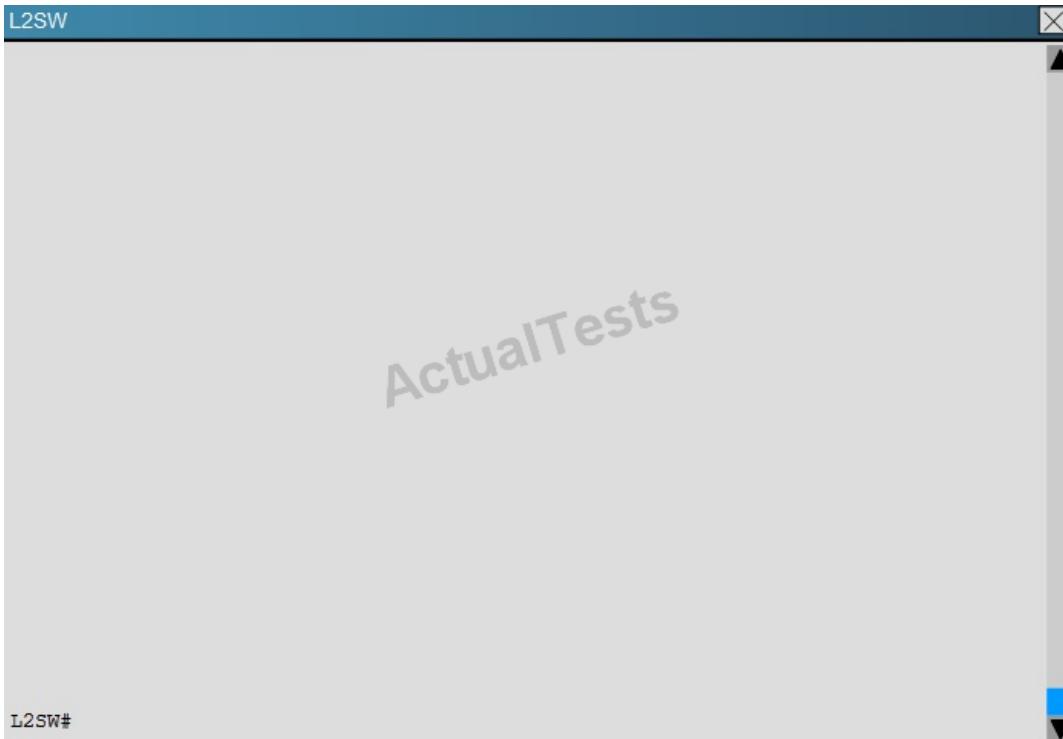
You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.











An OSPF neighbor adjacency is not formed between R3 in the main office and R5 in the Branch2 office. What is causing the problem?

- A. There is an area ID mismatch.
- B. There is a PPP authentication issue; a password mismatch.
- C. There is an OSPF hello and dead interval mismatch.
- D. There is a missing network command in the OSPF process on R5.

Answer: C

Explanation:

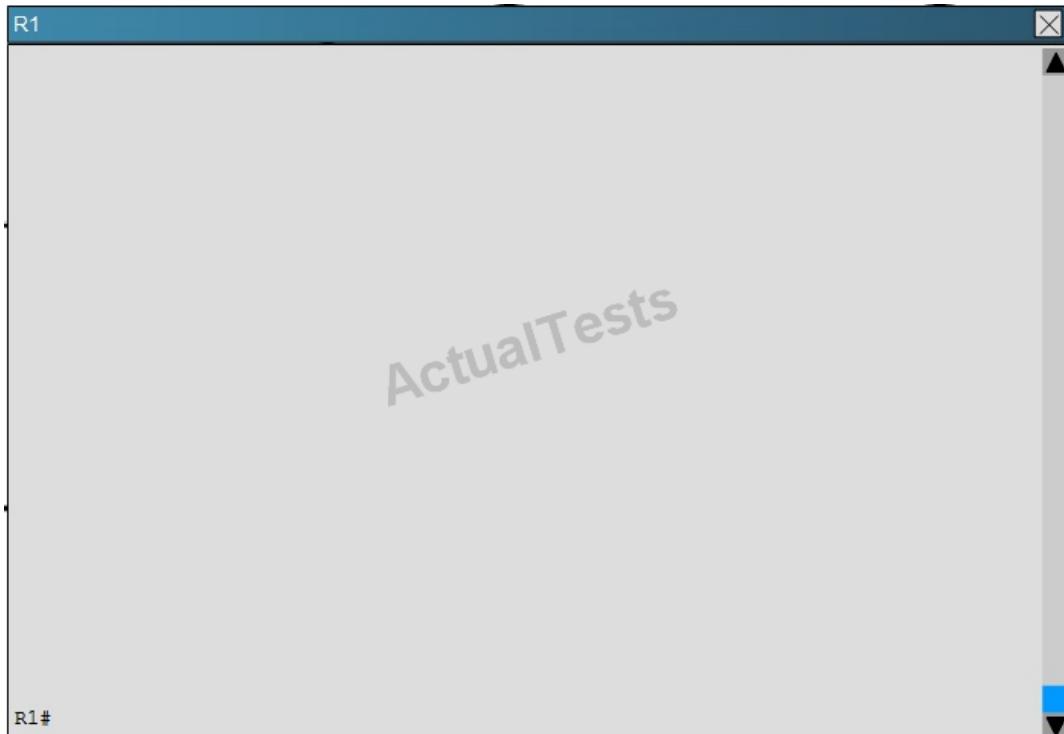
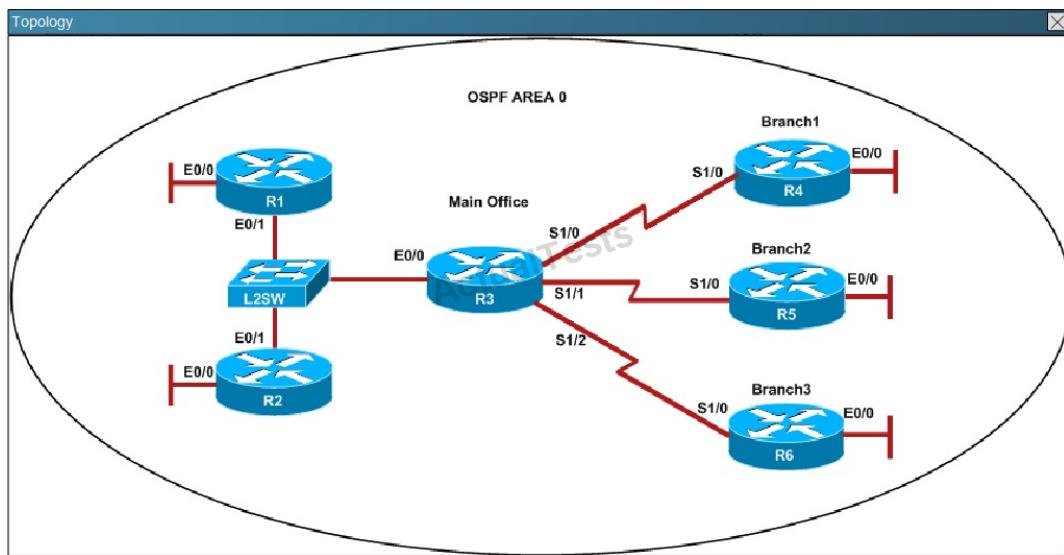
The “show ip ospf interface” command on R3 and R5 shows that the hello and dead intervals do not match. They are 50 and 200 on R3 and 10 and 40 on R5.

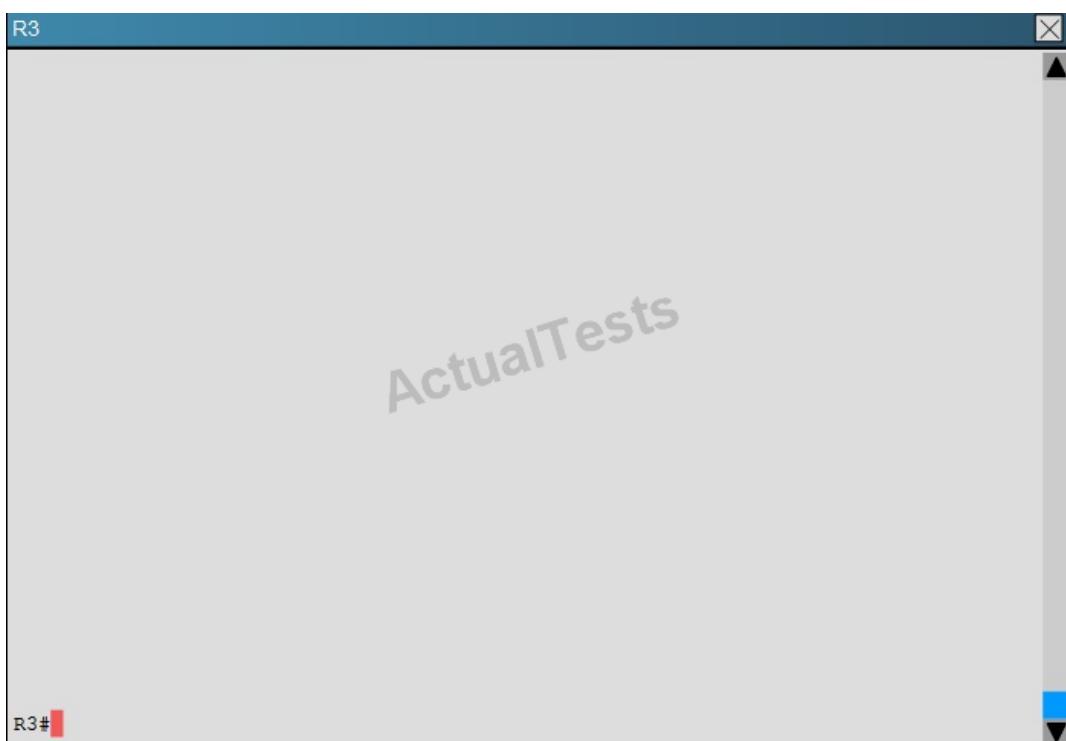
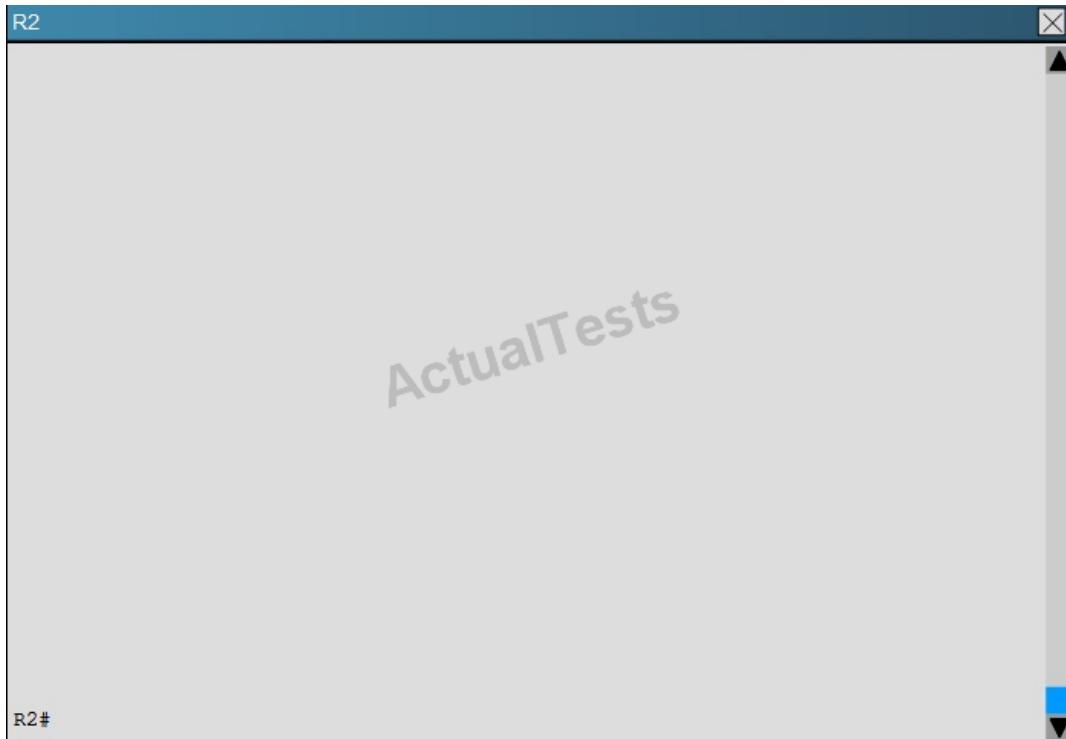
R3	R5
Suppress hello for 0 neighbor(s)	
Serial1/1 is up, line protocol is up	0 1 no no Base
Internet Address 10.10.240.5/30, Area 0, Attached via Interface	Enabled by interface config, including secondary ip addresses
Process ID 3, Router ID 192.168.3.3, Network Type POINT_TO_POINT	Loopback interface is treated as a stub Host
Topology-MTID Cost Disabled Shutdown Topology Name	Serial1/0 is up, line protocol is up
0 64 no no no Base	Internet Address 10.10.240.6/30, Area 0, Attached via Interface Enable
Enabled by interface config, including secondary ip addresses	Process ID 5, Router ID 192.168.5.5, Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT	Topology-MTID Cost Disabled Shutdown Topology Name
Time intervals configured, Hello 50, Dead 200, Wait 200, Retransmit 5	0 64 no no no Base
oob-resync timeout 200	Enabled by interface config, including secondary ip addresses
Hello due in 00:00:39	Transmit Delay is 1 sec, State POINT_TO_POINT
Supports Link-local Signaling (LLS)	Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Cisco NSF helper support enabled	oob-resync timeout 40
IEFT NSF helper support enabled	Hello due in 00:00:08
Index 4/4, flood queue length 0	Supports Link-local Signaling (LLS)
Next 0x0(0)/0x0(0)	Cisco NSF helper support enabled
Last flood scan length is 0, maximum is 0	IEFT NSF helper support enabled
Last flood scan time is 0 msec, maximum is 0 msec	Index 3/3, flood queue length 0
Neighbor Count is 0, Adjacent neighbor count is 0	Next 0x0(0)/0x0(0)
Suppress hello for 0 neighbor(s)	Last flood scan length is 0, maximum is 0
Serial1/0 is up, line protocol is up	Last flood scan time is 0 msec, maximum is 0 msec
Internet Address 10.10.240.1/30, Area 0, Attached via Interface	Neighbor Count is 0, Adjacent neighbor count is 0
Process ID 3, Router ID 192.168.3.3, Network Type POINT_TO_POINT	Suppress hello for 0 neighbor(s)
Topology-MTID Cost Disabled Shutdown Topology Name	Ethernet0/0 is up, line protocol is up
	Internet Address 172.16.114.1/24, Area 0, Attached via Interface Enable
--- More (37) ---	
	R5#

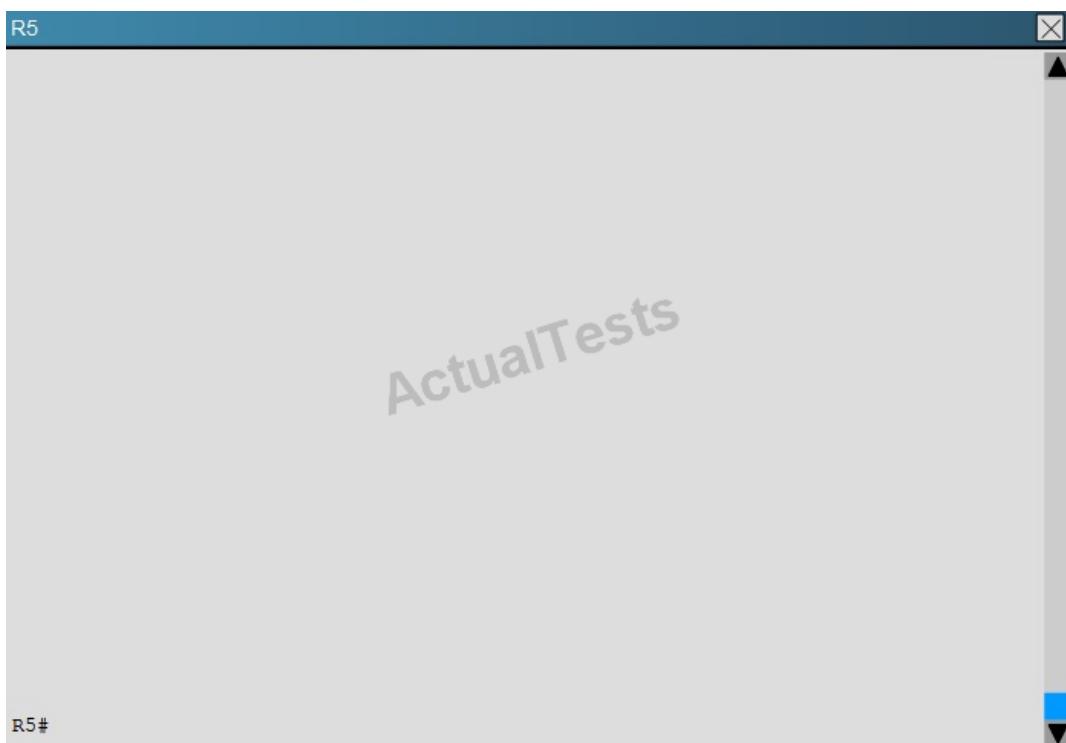
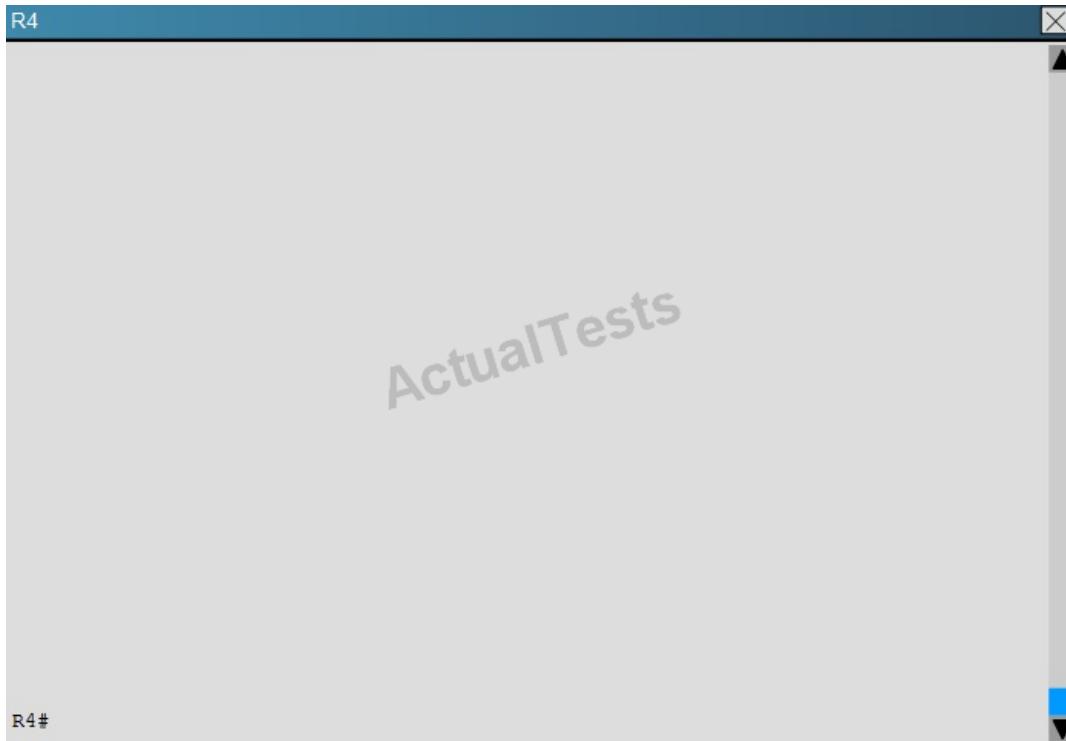
QUESTION NO: 139**Scenario**

Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.

You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.







R6#

L2SW#

R1 does not form an OSPF neighbor adjacency with R2. Which option would fix the issue?

- A. R1 ethernetO/1 is shutdown. Configure no shutdown command.
- B. R1 ethernetO/1 configured with a non-default OSPF hello interval of 25: configure no ip ospf hello-interval 25
- C. R2 ethernetO/1 and R3 ethernetO/O are configured with a non-default OSPF hello interval of 25; configure no ip ospf hello-interval 25
- D. Enable OSPF for R1 ethernetO/1; configure ip ospf 1 area 0 command under ethernetO/1

Answer: B**Explanation:**

Looking at the configuration of R1, we see that R1 is configured with a hello interval of 25 on interface Ethernet 0/1 while R2 is left with the default of 10 (not configured).

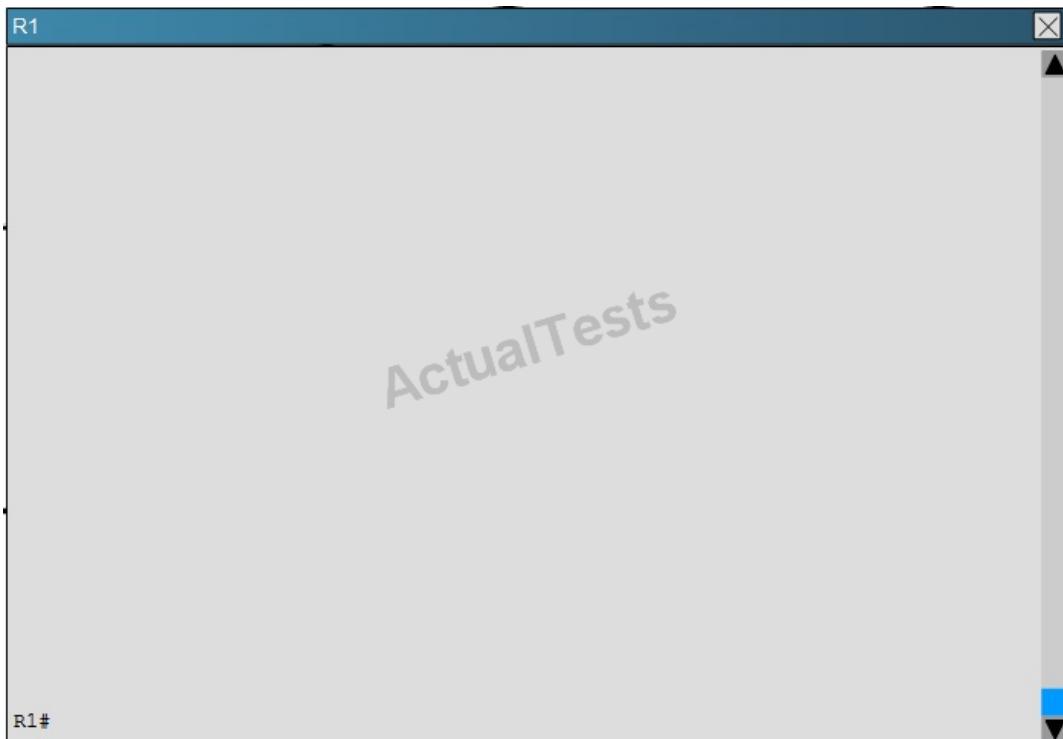
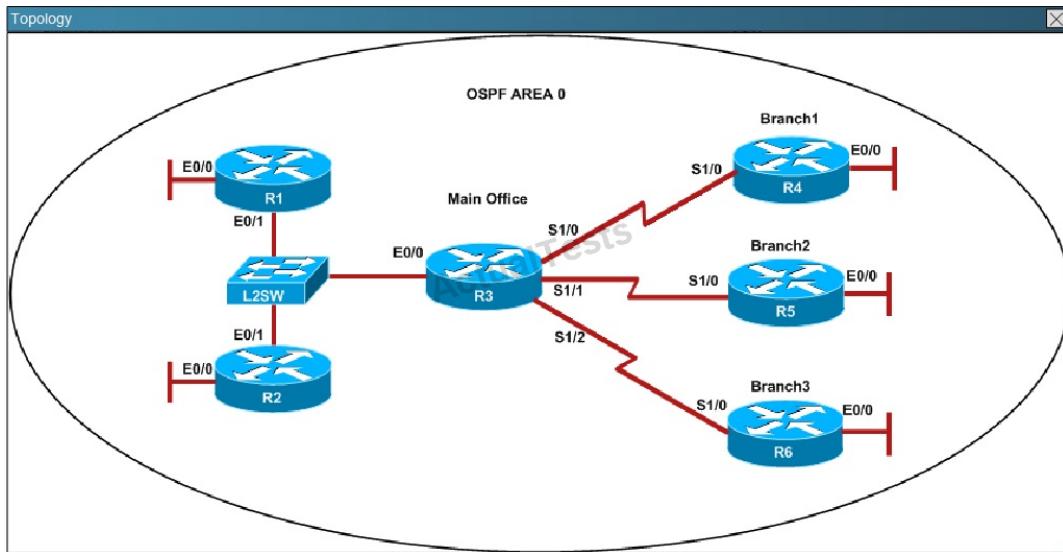
R1	R2
<pre> ! ! ! ! interface Loopback0 description ***Loopback*** ip address 192.168.1.1 255.255.255.255 ip ospf 1 area 0 ! interface Ethernet0/0 description ***Connected to R1-LAN*** ip address 10.10.110.1 255.255.255.0 ip ospf 1 area 0 ! interface Ethernet0/1 description ***Connected to L2SW*** ip address 10.10.230.1 255.255.255.0 ip ospf hello-interval 25 ip ospf 1 area 0 ! interface Ethernet0/2 no ip address shutdown --- More (35) --- </pre>	<pre> ! ! ! ! interface Loopback0 description ***Loopback*** ip address 192.168.2.2 255.255.255.255 ip ospf 2 area 0 ! interface Ethernet0/0 description ***Connected to R2-LAN*** ip address 10.10.120.1 255.255.255.0 ip ospf 2 area 0 ! interface Ethernet0/1 description ***Connected to L2SW*** ip address 10.10.230.2 255.255.255.0 ip ospf 2 area 0 ! interface Ethernet0/2 no ip address shutdown --- More (35) --- </pre>

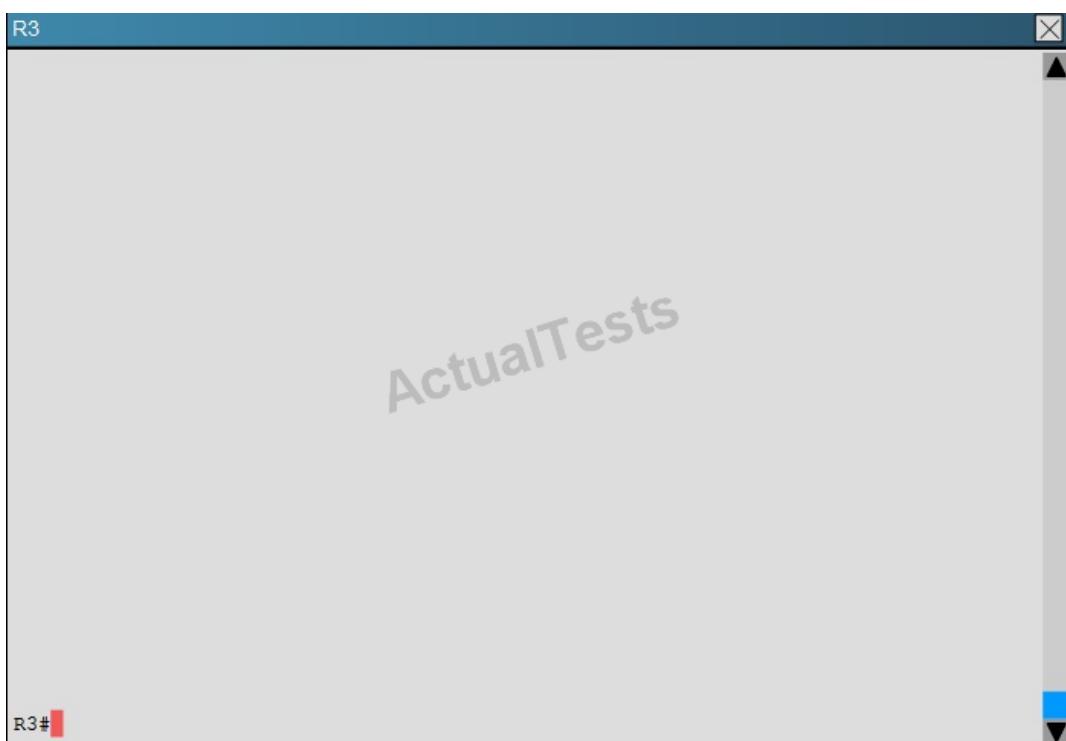
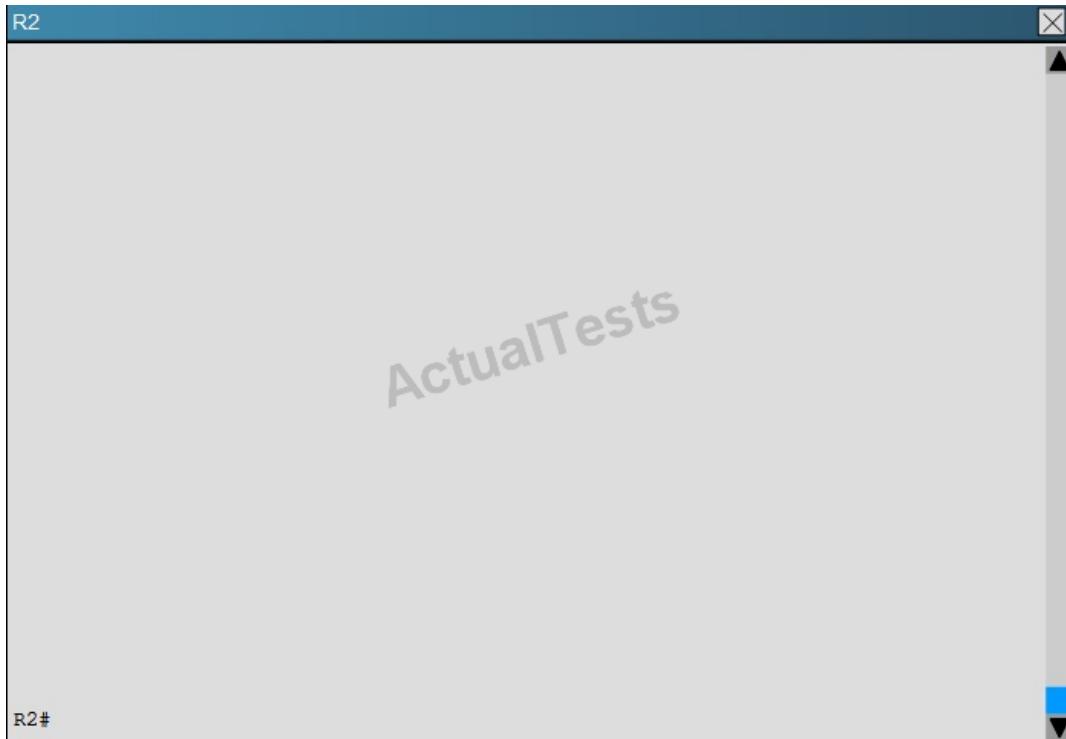
QUESTION NO: 140

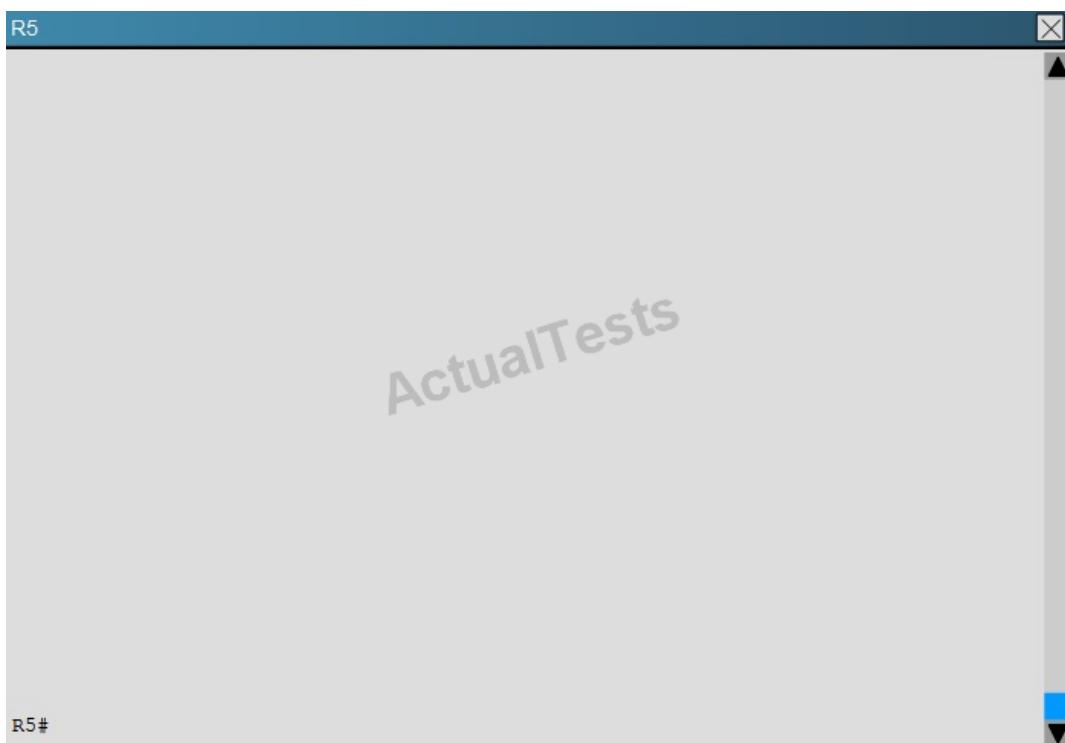
Scenario

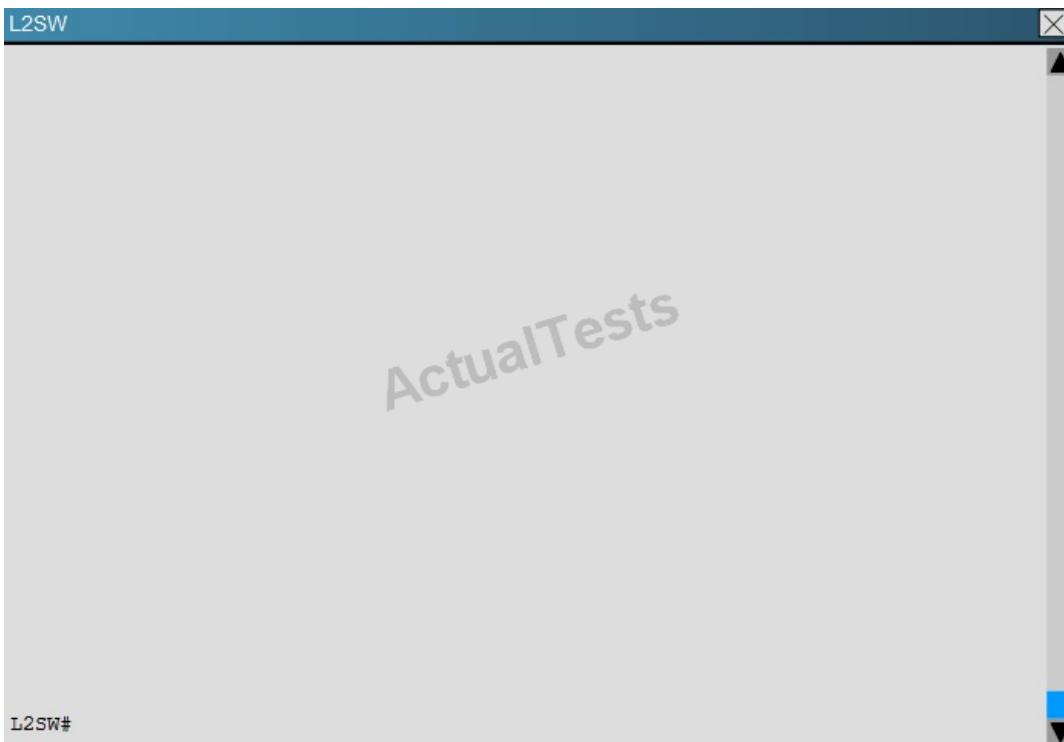
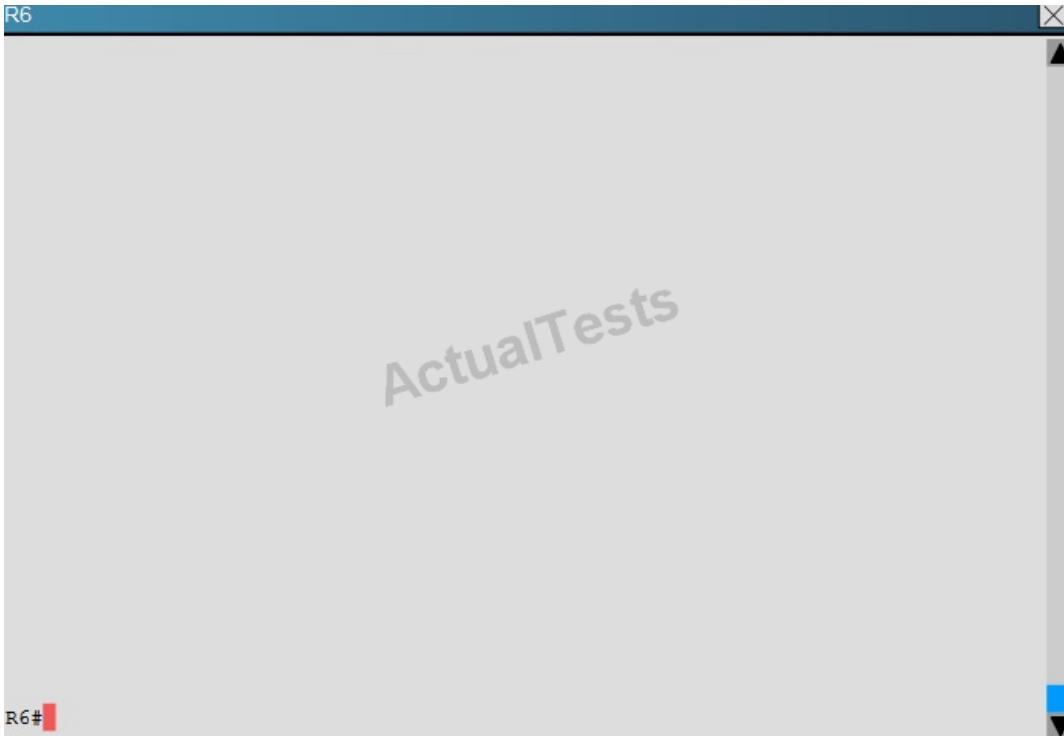
Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.

You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.









An OSPF neighbor adjacency is not formed between R3 in the main office and R6 in the Branch3 office. What is causing the problem?

- A.** There is an area ID mismatch.
- B.** There is a PPP authentication issue; the username is not configured on R3 and R6.
- C.** There is an OSPF hello and dead interval mismatch.
- D.** The R3 router ID is configured on R6.

Answer: D**Explanation:**

Using the show running-config command we see that R6 has been incorrectly configured with the same router ID as R3 under the router OSPF process.

R3	R6
<pre> ip address 10.10.240.5 255.255.255.252 encapsulation ppp ip ospf hello-interval 50 ip ospf 3 area 0 ppp authentication chap serial restart-delay 0 ! interface Serial1/2 description ***Connected to R6-Branch3 office*** ip address 10.10.240.9 255.255.255.252 encapsulation ppp ip ospf 3 area 0 ppp authentication chap serial restart-delay 0 ! interface Serial1/3 no ip address shutdown serial restart-delay 0 ! router ospf 3 router-id 192.168.3.3 ! ip forward-protocol nd ! !</pre>	<pre> no ip address shutdown serial restart-delay 0 ! interface Serial1/2 no ip address shutdown serial restart-delay 0 ! interface Serial1/3 no ip address shutdown serial restart-delay 0 ! router ospf 6 router-id 192.168.3.3 ! ip forward-protocol nd ! no ip http server no ip http secure-server ! !</pre>

Topic 5, IP Services

QUESTION NO: 141

What is the best practice when assigning IP addresses in a small office of six hosts?

- A. Use a DHCP server that is located at the headquarters.
- B. Use a DHCP server that is located at the branch office.
- C. Assign the addresses by using the local CDP protocol.
- D. Assign the addresses statically on each node.

Answer: D**Explanation:**

Its best to use static addressing scheme where the number of systems is manageable rather than using a dynamic method such as DHCP as it is easy to operate and manage.

QUESTION NO: 142 DRAG DROP

Various protocols are listed on the left. On the right are applications for the use of those protocols. Drag the protocol on the left to an associated function for that protocol on the right. (Not all options are used.)

Various protocols are listed on the left. On the right are applications for the use of those protocols. Drag the protocol on the left to an associated function for that protocol on the right. (Not all options are used.)

ICMP	A PC sends packets to the default gateway IP address the first time since the PC turned on.
DHCP	The network administrator is checking basic IP connectivity from a workstation to a server.
RARP	The TCP/IP protocol stack must find an IP address for packets destined for a URL.
UDP	A network device will automatically assign IP addresses to workstations.
DNS	
ARP	

Answer:

Various protocols are listed on the left. On the right are applications for the use of those protocols. Drag the protocol on the left to an associated function for that protocol on the right. (Not all options are used.)

ICMP	ARP
DHCP	ICMP
RARP	DNS
UDP	DHCP
DNS	
ARP	

Explanation:

ARP

ICMP

DNS

DHCP

QUESTION NO: 143 DRAG DROP

Move the protocol or service on the left to a situation on the right where it would be used. (Not all options are used.)

Move the protocol or service on the left to a situation on the right where it would be used. (Not all options are used.)

OSPF

A PC with address 10.1.5.10 must access devices on the Internet.

ARP

Only routers and servers require static IP addresses. Easy IP administration is required.

NAT

A PC only knows a server as //MediaServer . IP needs to send data to that server.

DNS

A protocol is needed to replace current static routes with automatic route updates.

SQL

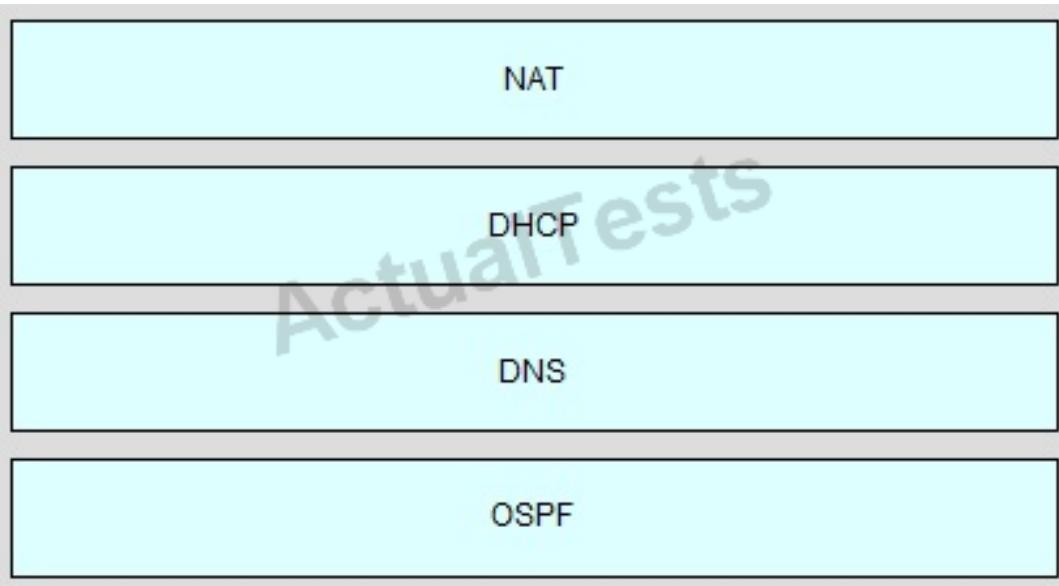
DHCP

Answer:

Move the protocol or service on the left to a situation on the right where it would be used. (Not all options are used.)

OSPF	NAT
ARP	DHCP
NAT	DNS
DNS	OSPF
SQL	
DHCP	

Explanation:



QUESTION NO: 144 DRAG DROP

Drag the definition on the left to the correct term on the right. Not all definitions on the left will be used.

Drag the definition on the left to the correct term on the right. Not all definitions on the left will be used.

a protocol that converts human-readable names into machine-readable addresses	SNMP
used to assign IP addresses automatically and set parameters such as subnet mask and default gateway	FTP
a protocol for using HTTP or HTTPS to exchange XML-based messages over computer networks	TFTP
a connectionless service that uses UDP to transfer files between systems	DNS
a protocol used to monitor and manage network devices	DHCP
a reliable, connection-oriented service that uses TCP to transfer files between systems	

Answer:

Drag the definition on the left to the correct term on the right. Not all definitions on the left will be used.	
a protocol that converts human-readable names into machine-readable addresses	a protocol used to monitor and manage network devices
used to assign IP addresses automatically and set parameters such as subnet mask and default gateway	a reliable, connection-oriented service that uses TCP to transfer files between systems
a protocol for using HTTP or HTTPS to exchange XML-based messages over computer networks	a connectionless service that uses UDP to transfer files between systems
a connectionless service that uses UDP to transfer files between systems	a protocol that converts human-readable names into machine-readable addresses
a protocol used to monitor and manage network devices	used to assign IP addresses automatically and set parameters such as subnet mask and default gateway
a reliable, connection-oriented service that uses TCP to transfer files between systems	

Explanation:

a protocol used to monitor and manage network devices

a reliable, connection-oriented service that uses TCP to transfer files between systems

a connectionless service that uses UDP to transfer files between systems

a protocol that converts human-readable names into machine-readable addresses

used to assign IP addresses automatically and set parameters such as subnet mask and default gateway

QUESTION NO: 145

In the configuration of NAT, what does the keyword overload signify?

- A. When bandwidth is insufficient, some hosts will not be allowed to access network translation.
- B. The pool of IP addresses has been exhausted.
- C. Multiple internal hosts will use one IP address to access external network resources.
- D. If the number of available IP addresses is exceeded, excess traffic will use the specified address pool.

Answer: C**Explanation:**

The keyword **overload** used in the **ip nat inside source list 1 pool ovrid overload** example command allows NAT to translate multiple inside devices to the single address in the pool.

The types of NAT include:

Static address translation (static NAT)—Allows one-to-one mapping between local and global addresses.

Dynamic address translation (dynamic NAT)—Maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.

Overloading—Maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as Port Address Translation (PAT). By using overloading, thousands of users can be connected to the Internet by using only one real global IP address.

QUESTION NO: 146

What happens when computers on a private network attempt to connect to the Internet through a Cisco router running PAT?

- A.** The router uses the same IP address but a different TCP source port number for each connection.
- B.** An IP address is assigned based on the priority of the computer requesting the connection.
- C.** The router selects an address from a pool of one-to-one address mappings held in the lookup table.
- D.** The router assigns a unique IP address from a pool of legally registered addresses for the duration of the connection.

Answer: A**Explanation:**

Reference:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/nat_staticpat.html

Static PAT translations allow a specific UDP or TCP port on a global address to be translated to a specific port on a local address. That is, both the address and the port numbers are translated.

Static PAT is the same as static NAT, except that it enables you to specify the protocol (TCP or UDP) and port for the real and mapped addresses. Static PAT enables you to identify the same mapped address across many different static statements, provided that the port is different for each statement. You cannot use the same mapped address for multiple static NAT statements.

Port Address Translation makes the PC connect to the Internet but using different TCP source port.

QUESTION NO: 147

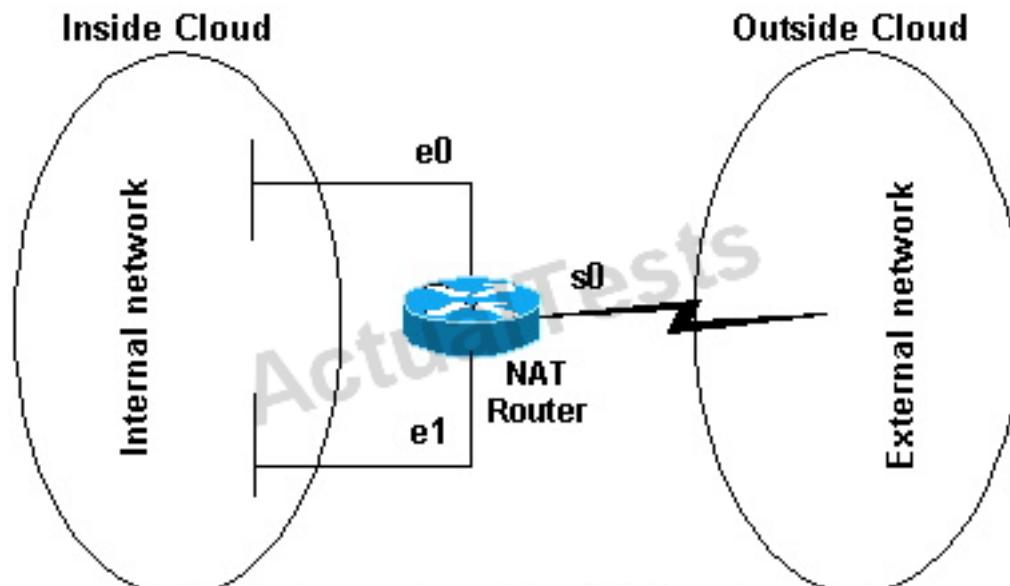
When configuring NAT, the Internet interface is considered to be what?

- A. local
- B. inside
- C. global
- D. outside

Answer: D

Explanation:

The first step to deploy NAT is to define NAT inside and outside interfaces. You may find it easiest to define your internal network as inside, and the external network as outside. However, the terms internal and external are subject to arbitration as well. This figure shows an example of this.



In this figure, ethernet 0 and ethernet 1 will be defined as NAT inside interfaces and serial 0 will be defined as a NAT outside interface.

Reference: <http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772->

QUESTION NO: 148

The ip helper-address command does what?

- A. assigns an IP address to a host
- B. resolves an IP address from a DNS server
- C. relays a DHCP request across networks
- D. resolves an IP address overlapping issue

Answer: C

Explanation:

<http://cisco.net.com/tcpip/dhcp/107-how-to-use-ip-helper-address-to-connect-remote-dhcp-server.html>

When the DHCP client sends the DHCP request packet, it doesn't have an IP address. So it uses the all-zeroes address, 0.0.0.0, as the IP source address. And it doesn't know how to reach the DHCP server, so it uses a general broadcast address, 255.255.255.255, for the destination. So the router must replace the source address with its own IP address, for the interface that received the request. And it replaces the destination address with the address specified in the ip helper-address command. The client device's MAC address is included in the payload of the original DHCP request packet, so the router doesn't need to do anything to ensure that the server receives this information. The router then relays the DHCP request to the DHCP server.

QUESTION NO: 149

The network administrator is using a Windows PC application that is called putty.exe for remote communication to a switch for network troubleshooting. Which two protocols could be used during this communication? (Choose two.)

- A. SNMP
- B. HTTP
- C. Telnet
- D. RMON
- E. SSH

Answer: C,E

Explanation:

PuTTY is a free implementation of Telnet and SSH for Windows and Unix platforms, and is used to connect to Cisco and other networking devices using SSH or Telnet.

QUESTION NO: 150

A network administrator cannot connect to a remote router by using SSH. Part of the show interfaces command is shown.

router#show interfaces

Serial0/1/0 is up, line protocol is down

At which OSI layer should the administrator begin troubleshooting?

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

Answer: B

Explanation:

<https://learningnetwork.cisco.com/thread/12389>

I think the indication here is "Serial 0 is up, line protocol is down". What causes this indication? Correct me if I am wrong. When you have this indication, a cable unplugged is not a correct answer. If you check the output of your "show interface serial 0" command again, you should notice it as "Serial 0 is down, line protocol is down. Under the "show ip int brief" you should see status = down and protocol = down as opposed to up, down. Because you disconnected the cable, layer 1 will go down, which is indicated by the serial 0 down status. The line protocol status is for layer 2. So, a cable unplugged is not a correct answer to "Serial 0 is up, line protocol is down". Up/down means that the physical layer is OK, but there is a problem with the data link link (line protocol).

QUESTION NO: 151

Which of the following statements are TRUE regarding Cisco access lists? (Choose two.)

- A. In an inbound access list, packets are filtered as they enter an interface.
- B. In an inbound access list, packets are filtered before they exit an interface.
- C. Extended access lists are used to filter protocol-specific packets.
- D. You must specify a deny statement at the end of each access list to filter unwanted traffic.
- E. When a line is added to an existing access list, it is inserted at the beginning of the access list.

Answer: A,C

Explanation:

In an inbound access list, packets are filtered as they enter an interface. Extended access lists are used to filter protocol specific packets. Access lists can be used in a variety of situations when the router needs to be given guidelines for decision-making. These situations include:

Filtering traffic as it passes through the router

To control access to the VTY lines (Telnet)

To identify "interesting" traffic to invoke Demand Dial Routing (DDR) calls

To filter and control routing updates from one router to another

There are two types of access lists, standard and extended. Standard access lists are applied as close to the destination as possible (outbound), and can only base their filtering criteria on the source IP address. The number used while creating an access list specifies the type of access list created. The range used for standard access lists is 1 to 99 and 1300 to 1999. Extended access lists are applied as close to the source as possible (inbound), and can base their filtering criteria on the source or destination IP address, or on the specific protocol being used. The range used for extended access lists is 100 to 199 and 2000 to 2699.

Other features of access lists include:

Inbound access lists are processed before the packet is routed.

Outbound access lists are processed after the packet has been routed to an exit interface.

An "implicit deny" is at the bottom of every access list, which means that if a packet has not matched any preceding access list condition, it will be filtered (dropped).

Access lists require at least one permit statement, or all packets will be filtered (dropped).

One access list may be configured per direction for each Layer 3 protocol configured on an interface. The option stating that in an inbound access list, packets are filtered before they exit an interface is incorrect.

Packets are filtered as they exit an interface when using an outbound access list.

The option stating that a deny statement must be specified at the end of each access list in order to filter unwanted traffic is incorrect. There is an implicit deny at the bottom of every access list.

When a line is added to an existing access list, it is not inserted at the beginning of the access list. It is inserted at the end. This should be taken into consideration. For example, given the following

access list, executing the command access-list 110 deny tcp 192.168.5.0 0.0.0.255 any eq www would have NO effect on the packets being filtered because it would be inserted at the end of the list, AFTER the line that allows all traffic.

```
access-list 110 permit ip host 192.168.5.1 any
access-list 110 deny icmp 192.168.5.0 0.0.0.255 any echo
access-list 110 permit any any
```

QUESTION NO: 152

What does the "Inside Global" address represent in the configuration of NAT?

- A. the summarized address for all of the internal subnetted addresses
- B. the MAC address of the router used by inside hosts to connect to the Internet
- C. a globally unique, private IP address assigned to a host on the inside network
- D. a registered address that represents an inside host to an outside network

Answer: D

Explanation:

NAT: Local and Global Definitions

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094837.shtml

Cisco defines these terms as:

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 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 owner.

The address is allocated from a globally routable address or network space.

These 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

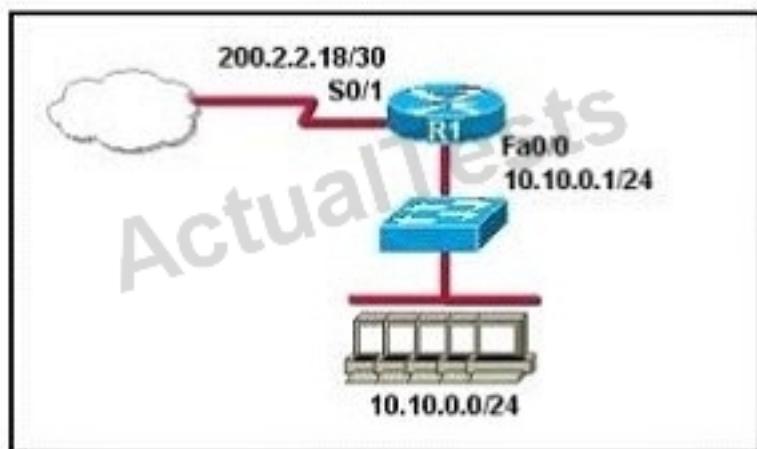
NAT configuration commands, ip nat inside destination and ip nat outside source . Networks to which these interfaces connect can then be thought of as inside networks or outside networks, respectively.

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: 153

Refer to the exhibit.



A company wants to use NAT in the network shown. Which commands will apply the NAT configuration to the proper interfaces? (Choose two.)

- A.** R1(config)# interface serial0/1
R1(config-if)# ip nat inside
- B.** R1(config)# interface serial0/1
R1(config-if)# ip nat outside
- C.** R1(config)# interface fastethernet0/0
R1(config-if)# ip nat inside
- D.** R1(config)# interface fastethernet0/0
R1(config-if)# ip nat outside
- E.** R1(config)# interface serial0/1
R1(config-if)# ip nat outside source pool 200.2.2.18 255.255.255.252
- F.** R1(config)# interface fastethernet0/0
R1(config-if)# ip nat inside source 10.10.0.0 255.255.255.0

Answer: **B,C**

Explanation:

For NAT, you need to define which interfaces are inside and which are outside. The outside interface is the one that connects to the external network, and the one that will be used for translating addresses. The inside interface is for the internal network, and defines the network IP addresses that will get translated to the one specified in the outside network.

QUESTION NO: 154

How many addresses will be available for dynamic NAT translation when a router is configured with the following commands?

```
Router(config)#ip nat pool TAME 209.165.201.23 209.165.201.30 netmask 255.255.255.224
```

```
Router(config)#ip nat inside source list 9 pool TAME
```

- A. 7
- B. 8
- C. 9
- D. 10
- E. 24
- F. 32

Answer: B

Explanation:

209.165.201.23 to 209.165.201.30 provides for 8 addresses.

Topic 6, Network Device Security

QUESTION NO: 155

Refer to the exhibit.

```

Router# configure terminal
Router(config)# hostname Router1
Router1(config)# enable secret sanfran
Router1(config)# enable password cisco
Router1(config)# line vty 0 4
Router1(config-line)# password sanjose
Router1(config-line)#

```

The network administrator made the entries that are shown and then saved the configuration. From a console connection, what password or password sequence is required for the administrator to access privileged mode on Router1?

- A. cisco
- B. sanfran
- C. sanjose
- D. either cisco or sanfran
- E. either cisco or sanjose
- F. sanjose and sanfran

Answer: B

Explanation:

The enable secret password takes precedence over the enable password, so sanfran will be used.

QUESTION NO: 156 DRAG DROP

Drag the appropriate command on the left to the configuration task it accomplishes. (Not all options are used.)

Drag the appropriate command on the left to the configuration task it accomplishes. (Not all options are used.)

login password cantComeIn

encrypt all clear text passwords

enable password uwi11NeverNo

protect access to the user mode prompt

service password-encryption

set privileged mode encrypted password

line console 0
password friendS0nly

set password to allow Telnet connections

enable secret noWay1n4u

set privileged mode clear text password

line vty 0 4
password 2hard2Guess

Answer:

Drag the appropriate command on the left to the configuration task it accomplishes. (Not all options are used.)

login password cantComeIn	service password-encryption
enable password uwi11NeverNo	line console 0 password friend\$Only
service password-encryption	enable secret noWay1n4u
line console 0 password friend\$Only	line vty 0 4 password 2hard2Guess
enable secret noWay1n4u	enable password uwi11NeverNo
line vty 0 4 password 2hard2Guess	

Explanation:

service password-encryption
line console 0 password friend\$Only
enable secret noWay1n4u
line vty 0 4 password 2hard2Guess
enable password uwi11NeverNo

QUESTION NO: 157

The following commands are entered on the router:

```
Burbank(config)# enable secret fortress
```

```
Burbank(config)# line con 0
```

```
Burbank(config-line)# login
```

```
Burbank(config-line)# password n0way1n  
Burbank(config-line)# exit  
Burbank(config)# service password-encryption
```

What is the purpose of the last command entered?

- A. to require the user to enter an encrypted password during the login process
- B. to prevent the vty, console, and enable passwords from being displayed in plain text in the configuration files
- C. to encrypt the enable secret password
- D. to provide login encryption services between hosts attached to the router

Answer: B

Explanation:

Certain types of passwords, such as Line passwords, by default appear in clear text in the configuration file. You can use the service password-encryption command to make them more secure. Once this command is entered, each password configured is automatically encrypted and thus rendered illegible inside the configuration file (much as the Enable/Enable Secret passwords are). Securing Line passwords is doubly important in networks on which TFTP servers are used, because TFTP backup entails routinely moving config files across networks—and config files, of course, contain Line passwords.

QUESTION NO: 158

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

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

Answer: E

Explanation:

Encryption further adds a level of security to the system as anyone having access to the database of passwords cannot reverse the process of encryption to know the actual passwords which isn't

the case if the passwords are stored simply.

QUESTION NO: 159

An administrator has connected devices to a switch and, for security reasons, wants the dynamically learned MAC addresses from the address table added to the running configuration.

What must be done to accomplish this?

- A. Enable port security and use the keyword sticky.
- B. Set the switchport mode to trunk and save the running configuration.
- C. Use the switchport protected command to have the MAC addresses added to the configuration.
- D. Use the no switchport port-security command to allow MAC addresses to be added to the configuration.

Answer: A

Explanation:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/port_sec.pdf

One can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts, hence enabling security as desired.

QUESTION NO: 160

A company has placed a networked PC in a lobby so guests can have access to the corporate directory.

A security concern is that someone will disconnect the directory PC and re-connect their laptop computer and have access to the corporate network. For the port servicing the lobby, which three configuration steps should be performed on the switch to prevent this? (Choose three.)

- A. Enable port security.
- B. Create the port as a trunk port.

- C. Create the port as an access port.
- D. Create the port as a protected port.
- E. Set the port security aging time to 0.
- F. Statically assign the MAC address to the address table.
- G. Configure the switch to discover new MAC addresses after a set time of inactivity.

Answer: A,C,F

Explanation:

If port security is enabled and the port is only designated as access port, and finally static MAC address is assigned, it ensures that even if a physical connection is done by taking out the directory PC and inserting personal laptop or device, the connection cannot be made to the corporate network, hence ensuring safety.

QUESTION NO: 161

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

- A. to prevent unauthorized Telnet access to a switch port
- B. to prevent unauthorized hosts from accessing the LAN
- C. to limit the number of Layer 2 broadcasts on a particular switch port
- D. block unauthorized access to the switch management interfaces

Answer: B

Explanation:

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.

QUESTION NO: 162

How can you ensure that only the MAC address of a server is allowed by switch port Fa0/1?

- A. Configure port Fa0/1 to accept connections only from the static IP address of the server.
- B. Configure the server MAC address as a static entry of port security.
- C. Use a proprietary connector type on Fa0/1 that is incomputable with other host connectors.
- 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.

Answer: B

Explanation:

When the MAC address is configured as static entry, no other address is allowed.

QUESTION NO: 163

What should be part of a comprehensive network security plan?

- A. Allow users to develop their own approach to network security.
- B. Physically secure network equipment from potential access by unauthorized individuals.
- C. Encourage users to use personal information in their passwords to minimize the likelihood of passwords being forgotten.
- D. Delay deployment of software patches and updates until their effect on end-user equipment is well known and widely reported.
- E. Minimize network overhead by deactivating automatic antivirus client updates.

Answer: B

Explanation:

From Cisco CCENT Exam Essentials study guide by Todd Lammle:

Know what the first part of a comprehensive network security plan is. The first part of your comprehensive network security plan is to physically secure network equipment from potential access by unauthorized individuals.

List the recommended ways of protecting network devices from outside network security threats. Use a firewall to restrict access from the outside to the network devices, and use SSH or another encrypted and authenticated transport to access device configurations.

Reference:

CCENT Cisco Certified Entry Networking Technician Study Guide: (ICND1 Exam 640-822), 2nd

Edition

by Todd Lammle

Published by Sybex, 2013

QUESTION NO: 164

What is the purpose of the switchport command?

Switch(config-if)# switchport port-security maximum 1

Switch(config-if)# switchport port-security mac-address 0018.DE8B.4BF8

- A. It ensures that only the device with the MAC address 0018.DE8B.4BF8 will be able to connect to the port that is being configured.
- B. It informs the switch that traffic destined for MAC address 0018.DE8B.4BF8 should only be sent to the port that is being configured.
- C. It will act like an access list and the port will filter packets that have a source or destination MAC of 0018.DE8B.4BF8.
- D. The switch will shut down the port of any traffic with source MAC address of 0018.DE8B.4BF8.

Answer: A

Explanation:

The first command configures the maximum number of secure MAC addresses on a port to one. The next command specifies that MAC addresses that are allowed with port security; in this case it is just the one single device MAC. If any other device connects on that port the port will be shut down by the port security feature.

QUESTION NO: 165

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.

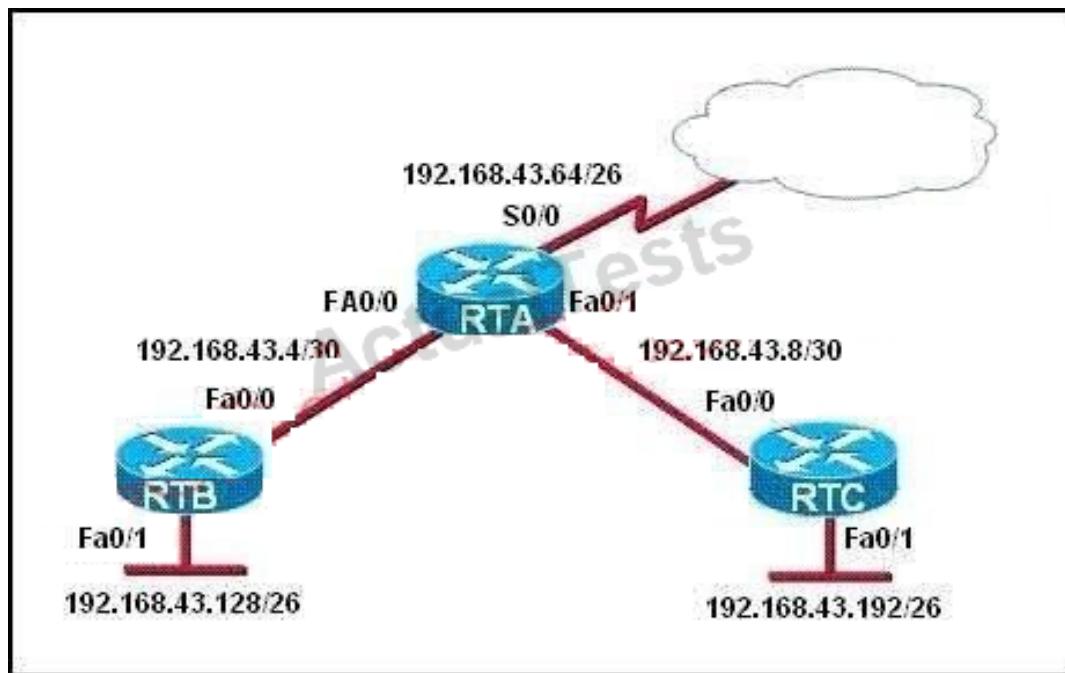
Answer: B,D

Explanation:

Using a firewall is a must for networks of any size to protect the internal network from outside threats and unauthorized access. SSH traffic is encrypted while telnet is not, so it is always recommended to use SSH.

QUESTION NO: 166

Refer to the exhibit.



For security reasons, information about RTA, including platform and IP addresses, should not be accessible from the Internet. This information should, however, be accessible to devices on the internal networks of RTA.

Which command or series of commands will accomplish these objectives?

- A. RTA(config)#no cdp run
- B. RTA(config)#no cdp enable

- C. RTA(config)#interface s0/0
 RTA(config-if)#no cdp run
 D. RTA(config)#interface s0/0
 RTA(config-if)#no cdp enable

Answer: D

Explanation:

http://www.cisco.com/en/US/tech/tk962/technologies_tech_note09186a00801aa000.shtml#topicenab

When CDP is enabled globally using the cdp run command, it is enabled by default on all supported interfaces (except for Frame Relay multipoint subinterfaces) to send and receive CDP information. You can disable CDP on an interface that supports CDP with the no cdp enable command.

Router#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	Holddme	Capability	Platform	Port ID
R2-AGS	Ser 1	129	R	2500	Ser 0
R6-2500	Eth 0	144	R	4000	Eth 0

Router#

On this router, CDP is enabled on Serial 1 and Ethernet 0 interfaces. Disable CDP on the Serial 1 interface and

verify if the neighbor device is discovered on the serial 1 interface, as this output shows:

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface s1

Router(config-if)#no cdp enable

Router(config-if)# Z

Router#4w5D. %SYS-5-CONFIG_I: Configured from console by console

QUESTION NO: 167

From which of the following attacks can Message Authentication Code (MAC) shield your

network?

- A. DoS
- B. DDoS
- C. spoofing
- D. SYN floods

Answer: C

Explanation:

Message Authentication Code (MAC) can shield your network from spoofing attacks. Spoofing, also known as masquerading, is a popular trick in which an attacker intercepts a network packet, replaces the source address of the packets header with the address of the authorized host, and reinserts fake information which is sent to the receiver. This type of attack involves modifying packet contents. MAC can prevent this type of attack and ensure data integrity by ensuring that no data has changed. MAC also protects against frequency analysis, sequence manipulation, and ciphertext-only attacks.

MAC is a secure message digest that requires a secret key shared by the sender and receiver, making it impossible for sniffers to change both the data and the MAC as the receiver can detect the changes.

A denial-of-service (DoS) attack floods the target system with unwanted requests, causing the loss of service to users. One form of this attack generates a flood of packets requesting a TCP connection with the target, tying up all resources and making the target unable to service other requests. MAC does not prevent DoS attacks. Stateful packet filtering is the most common defense against a DoS attack.

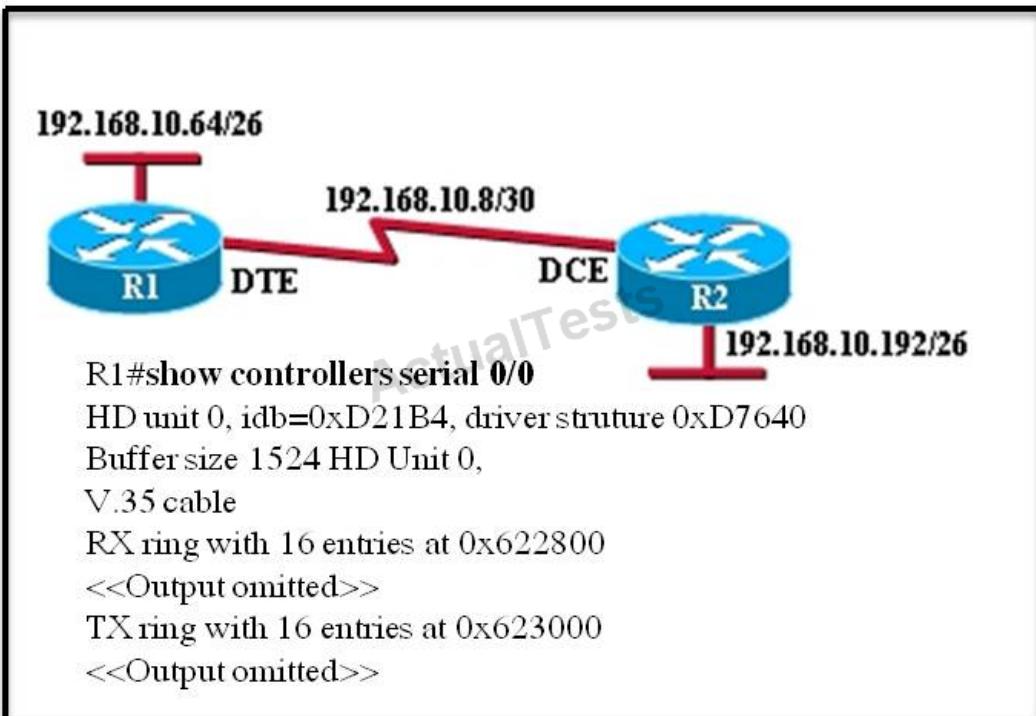
A Distributed Denial of Service attack (DDoS) occurs when multiple systems are used to flood the network and tax the resources of the target system. Various intrusion detection systems, utilizing stateful packet filtering, can protect against DDoS attacks.

In a SYN flood attack, the attacker floods the target with spoofed IP packets and causes it to either freeze or crash. A SYN flood attack is a type of denial of service attack that exploits the buffers of a device that accept incoming connections and therefore cannot be prevented by MAC. Common defenses against a SYN flood attack include filtering, reducing the SYN-RECEIVED timer, and implementing SYN cache or SYN cookies.

Topic 7, Troubleshooting

QUESTION NO: 168

Refer to the exhibit.



An administrator cannot connect from R1 to R2. To troubleshoot this problem, the administrator has entered the command shown in the exhibit. Based on the output shown, what could be the problem?

- A. The serial interface is configured for half duplex.
- B. The serial interface does not have a cable attached.
- C. The serial interface has the wrong type of cable attached.
- D. The serial interface is configured for the wrong frame size.
- E. The serial interface has a full buffer.

Answer: C

Explanation:

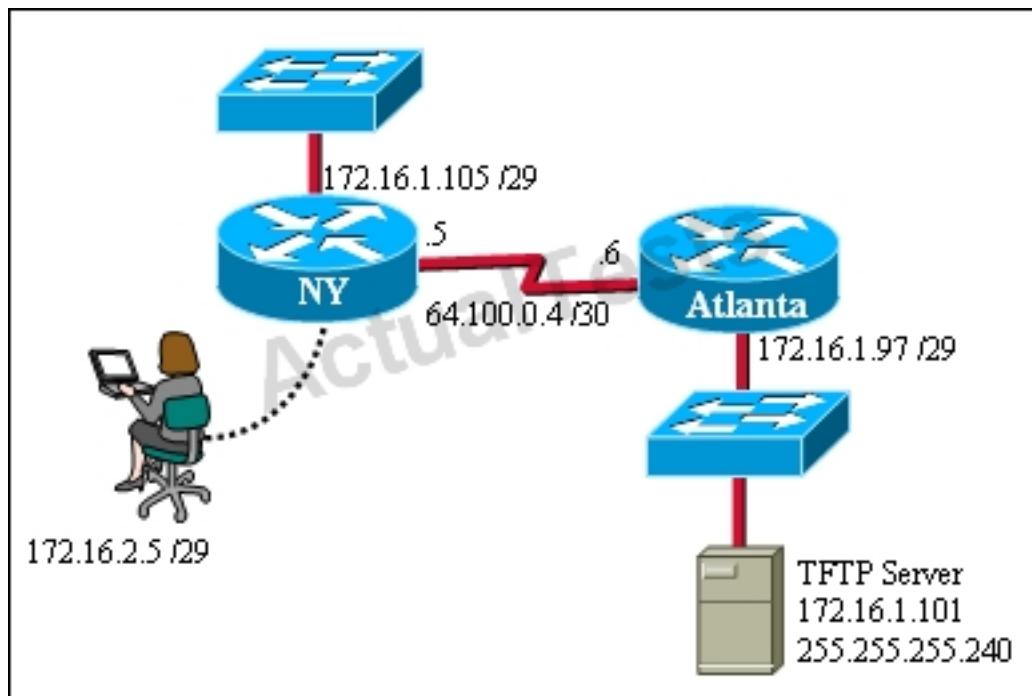
<http://www.thebryantadvantage.com/CCNACertificationExamTutorialDirectlyConnectedSerialInterfaces.htm>

Since the output is not forthcoming it shows that the type of cable attached is wrong, though the cable is connected since it shows the cable type.

According to the figure DTE cable should connect to R1 on interface but while examining using show controllers serial 0/0 command it showing that a DCE is connected so the wrong type of cable is being used.

QUESTION NO: 169

Refer to the exhibit.



A TFTP server has recently been installed in the Atlanta office. The network administrator is located in the NY office and has made a console connection to the NY router. After establishing the connection they are unable to backup the configuration file and IOS of the NY router to the TFTP server. What is the cause of this problem?

- A.** The NY router has an incorrect subnet mask.
- B.** The TFTP server has an incorrect IP address.
- C.** The TFTP server has an incorrect subnet mask.
- D.** The network administrator computer has an incorrect IP address.

Answer: C

Explanation:

The TFTP server is using a mask of 255.255.255.240 (/28) while the router is configured with a /29. Because of this, the Atlanta router does not see the TFTP server as being in the same subnet.

QUESTION NO: 170

If a host experiences intermittent issues that relate to congestion within a network while remaining connected, what could cause congestion on this LAN?

- A. half-duplex operation
- B. broadcast storms
- C. network segmentation
- D. multicasting

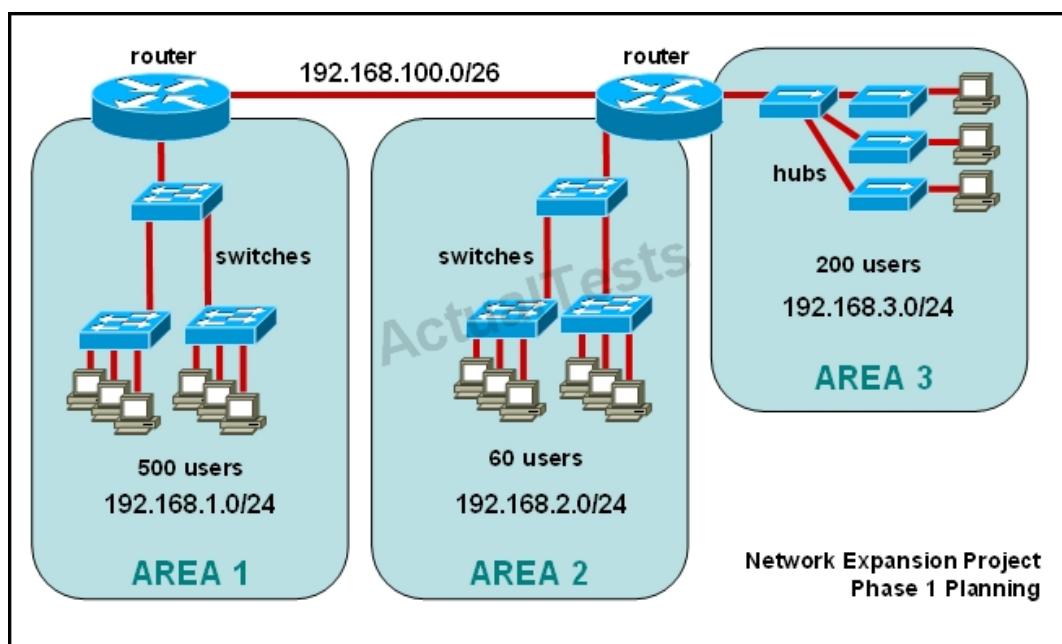
Answer: B

Explanation:

A broadcast storm can consume sufficient network resources so as to render the network unable to transport normal traffic.

QUESTION NO: 171

Refer to the exhibit.



The junior network support staff provided the diagram as a recommended configuration for the first phase of a four-phase network expansion project. The entire network expansion will have over 1000 users on 14 network segments and has been allocated this IP address space.

192.168.1.1 through 192.168.5.255

192.168.100.1 through 192.168.100.255

What are three problems with this design? (Choose three.)

- A. The AREA 1 IP address space is inadequate for the number of users.
- B. The AREA 3 IP address space is inadequate for the number of users.
- C. AREA 2 could use a mask of /25 to conserve IP address space.
- D. The network address space that is provided requires a single network-wide mask.
- E. The router-to-router connection is wasting address space.
- F. The broadcast domain in AREA 1 is too large for IP to function.

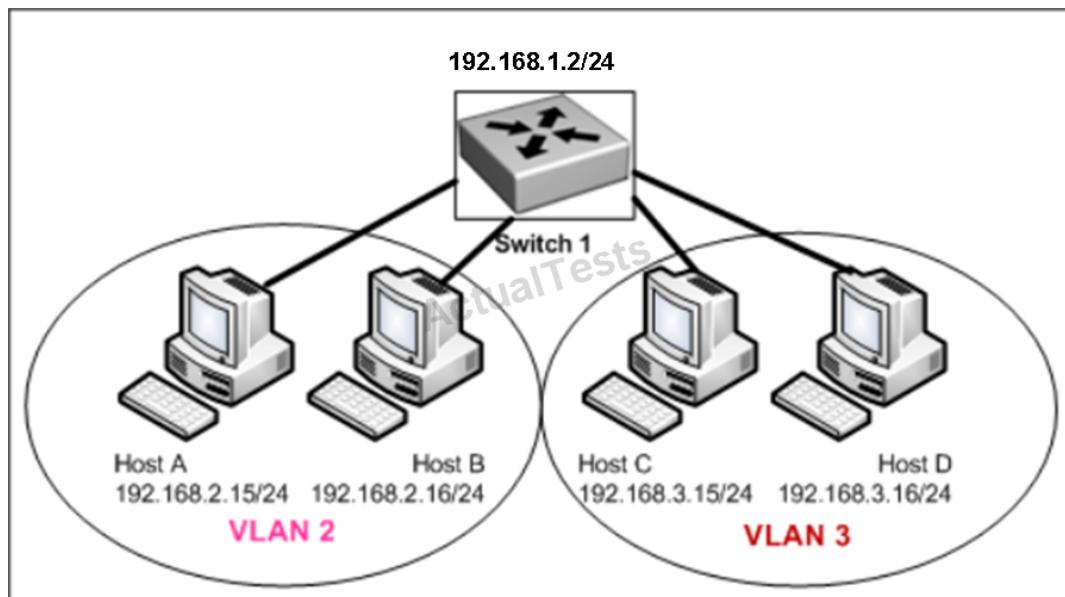
Answer: A,C,E

Explanation:

The given IP addresses of areas 1 and 3 along with network masks of /24 cannot accommodate 500 users so are inadequate, while the area 2 is having over capacity so its network mask can be reduced to /25 to accommodate the only 60 users it has.

QUESTION NO: 172

Refer to the exhibit.



Host A can communicate with Host B but not with Hosts C or D. How can the network administrator solve this problem?

- A. Configure Hosts C and D with IP addresses in the 192.168.2.0 network.
- B. Install a router and configure a route to route between VLANs 2 and 3.
- C. Install a second switch and put Hosts C and D on that switch while Hosts A and B remain on the original switch.
- D. Enable the VLAN trunking protocol on the switch.

Answer: B**Explanation:**

Two VLANs require a router in between otherwise they cannot communicate. Different VLANs and different IP subnets need a router to route between them.

QUESTION NO: 173

Refer to the exhibit.

```
interface vlan 1
ip address 192.168.17.253 255.255.255.240
no shutdown
exit
ip default-gateway 192.168.17.1
line vty 0 15
password cisco
login
exit
```

A network administrator has configured a Catalyst 2950 switch for remote management by pasting into the console the configuration commands that are shown in the exhibit. However, a Telnet session cannot be successfully established from a remote host. What should be done to fix this problem?

- A. Change the first line to interface fastethernet 0/1.
- B. Change the first line to interface vlan 0/1.
- C. Change the fifth line to ip default-gateway 192.168.17.241.
- D. Change the fifth line to ip route 0.0.0.0 0.0.0.0 192.168.17.1.
- E. Change the sixth line to line con 0.

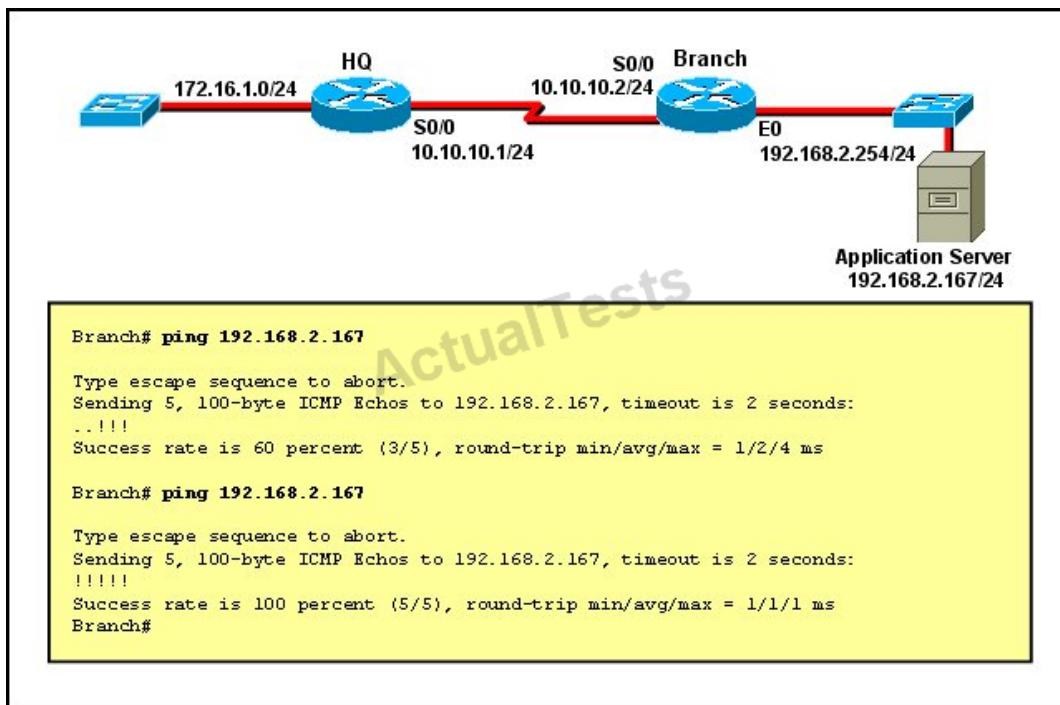
Answer: C**Explanation:**

The default gateway must reside on the same IP subnet as the device. Here, the subnet mask for the VLAN interface is /228. Only choice C will fix this issue, as then the default gateway is on the

same subnet as the 2950.

QUESTION NO: 174

Refer to the exhibit.



The network administrator is testing connectivity from the branch router to the newly installed application server. What is the most likely reason for the first ping having a success rate of only 60 percent?

- A. The network is likely to be congested, with the result that packets are being intermittently dropped.
- B. The branch router had to resolve the application server MAC address.
- C. There is a short delay while NAT translates the server IP address.
- D. A routing table lookup delayed forwarding on the first two ping packets.
- E. The branch router LAN interface should be upgraded to FastEthernet.

Answer: B

Explanation:

Initially the MAC address had to be resolved, but once it is resolved and is in the ARP table of the router, pings go through immediately.

QUESTION NO: 175**Instructions**

For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

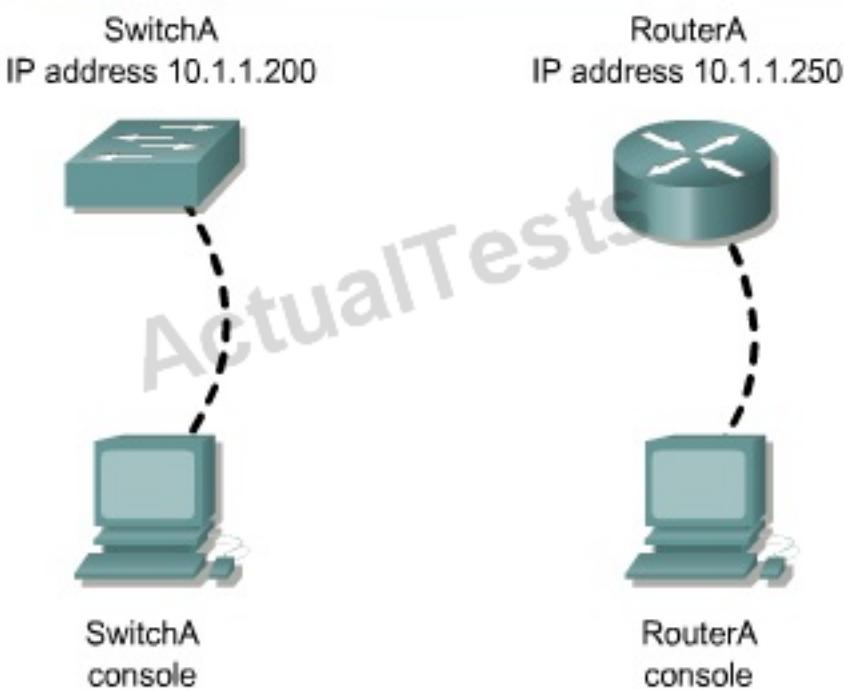
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.

Topology

Select two options which are security Issues which need to be modified before RouterA is used?
(Choose two.)

- A. unencrypted weak password is configured to protect privilege mode
- B. inappropriate wording in banner message
- C. the virtual terminal lines have a weak password configured
- D. virtual terminal lines have a password, but it will not be used
- E. configuration supports un-secure web server access

Answer: B,D

Explanation:

QUESTION NO: 176

Instructions



For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

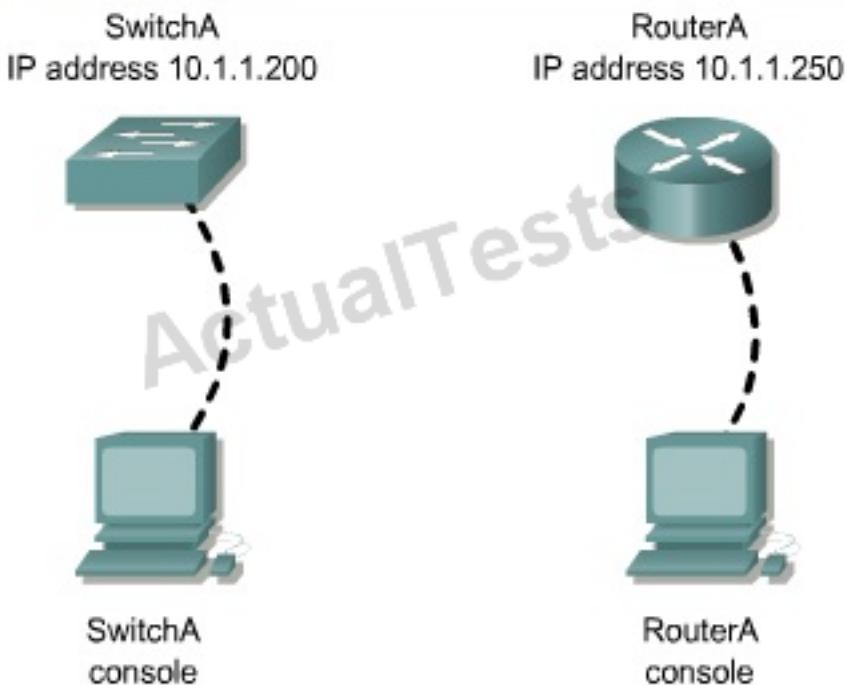
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.

Topology

Select three options which are security issues with the current configuration of SwitchA. (Choose three.)

- A. Privilege mode is protected with an unencrypted password
- B. Inappropriate wording in banner message
- C. Virtual terminal lines are protected only by a password requirement
- D. Both the username and password are weak
- E. Telnet connections can be used to remotely manage the switch
- F. Cisco user will be granted privilege level 15 by default

Answer: A,B,D

Explanation:

QUESTION NO: 177

Instructions

For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

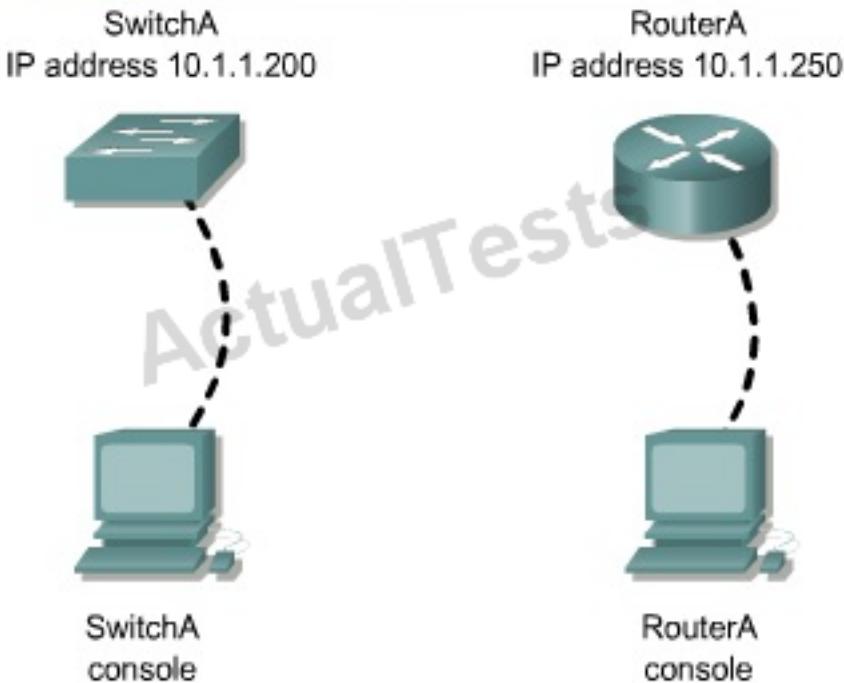
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.

Topology

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

- A. At least 5 simultaneous remote connections are possible
- B. Only telnet protocol connections to RouterA are supported
- C. Remote connections to RouterA using telnet will succeed
- D. Console line connections will never time out due to inactivity

- E. Since DHCP is not used on Fa0/1 there is not a need to use the NAT protocol

Answer: A,C

Explanation:

QUESTION NO: 178

Instructions



For both the Router and the Switch the simulated console mode needs to start and remain in enabled mode.

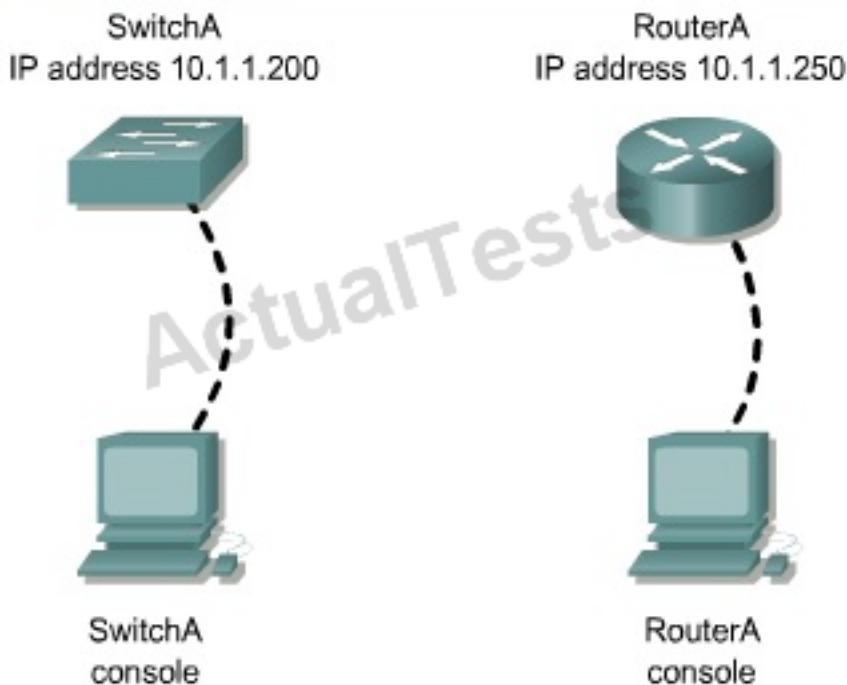
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

You will connect to RouterA and SwitchA via the console devices that are attached to each.

There are 4 multiple-choice questions with this task. Be sure to answer all of them before leaving this item. In order to score the maximum points you will need to have accessed both SwitchA and RouterA.

NOTE: The configuration command has been disabled for both the router and switch in this simulation.

Topology

Which of the following is true regarding the configuration of SwitchA?

- A. only 5 simultaneous remote connections are possible
- B. remote connections using ssh will require a username and password
- C. only connections from the local network will be possible
- D. console access to SwitchA requires a password

Answer: B

Explanation:

QUESTION NO: 179

Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

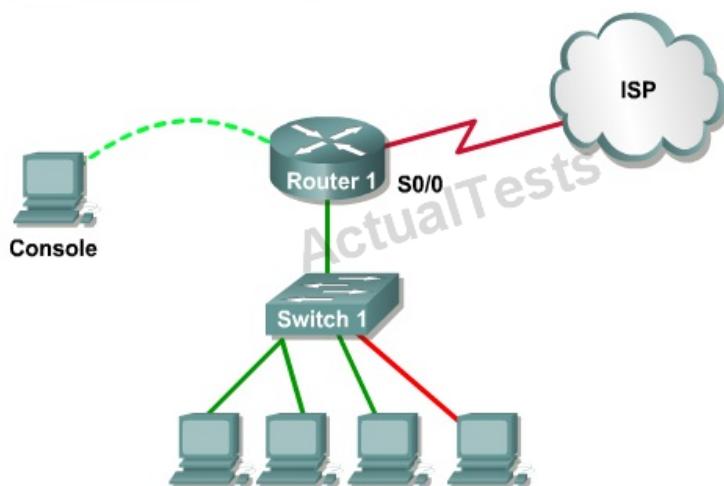
Scenario

This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

NOTE: The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.

Topology

R1

ActualTests

```
Press RETURN to get started!
Router1>
```

What is the subnet broadcast address of the LAN connected to Router1?

- A. 192.168.8.15
- B. 192.168.8.31
- C. 192.168.8.63
- D. 192.168.8.127

Answer: A

Explanation:

The IP address assigned to FA0/1 is 192.168.8.9/29, making 192.168.8.15 the broadcast address.

QUESTION NO: 180

Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

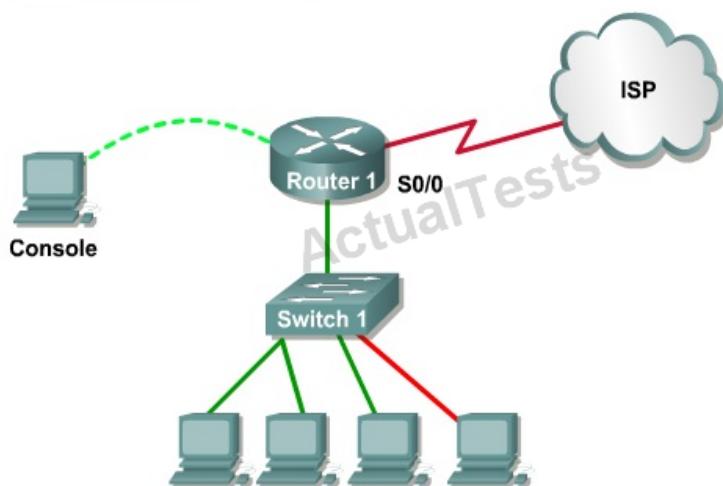
Scenario

This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

NOTE: The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.

Topology

```
R1
Press RETURN to get started!
Router1>
```

What is the bandwidth on the WAN interface of Router 1?

- A. 16 Kbit/sec
- B. 32 Kbit/sec
- C. 64 Kbit/sec
- D. 128 Kbit/sec
- E. 512 Kbit/sec
- F. 1544 Kbit/sec

Answer: A

Explanation:

Use the “show interface s0/0” to see the bandwidth set at 16 Kbit/sec.

The show interface s0/0 command results will look something like this and the bandwidth will be represented by the "BW" on the fourth line as seen below where BW equals 1544 Kbits/sec.

R2#show interface serial 0/0

Serial0/0 is up, line protocol is down

Hardware is GT96K Serial

Internet address is 10.1.1.5/30

MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 uses.

QUESTION NO: 181

Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

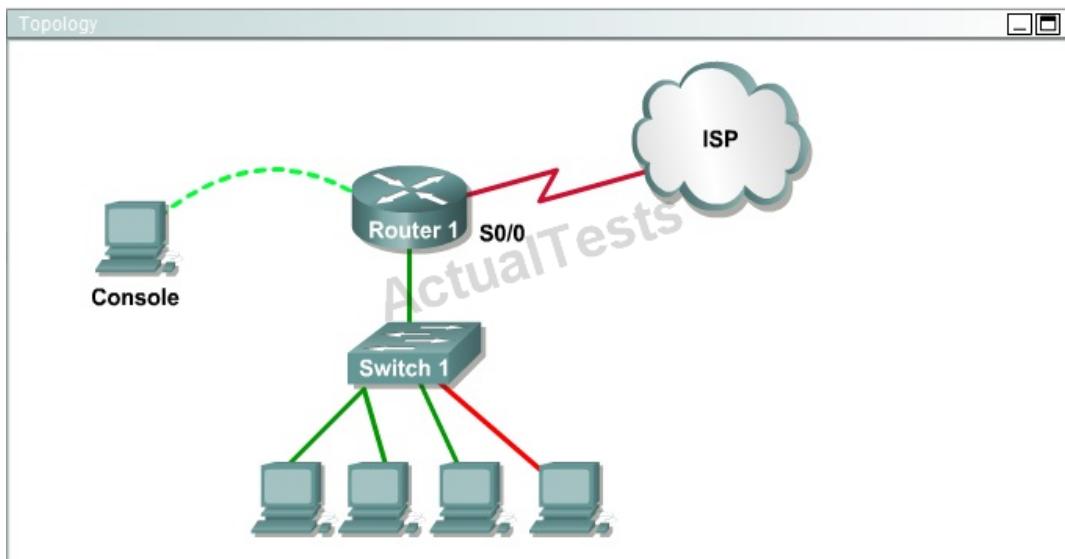
Scenario

This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

NOTE: The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.



R1

ActualTests

```
Press RETURN to get started!
Router1>
```

Including the address on the Routed Ethernet interface, how many hosts can have IP addresses on the LAN to which Routed is connected?

- A. 6
- B. 30
- C. 62
- D. 126

Answer: A

Explanation:

This is a /29 address, so there are 6 usable IP's on this subnet.

QUESTION NO: 182

Instructions

You can click on the grey buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

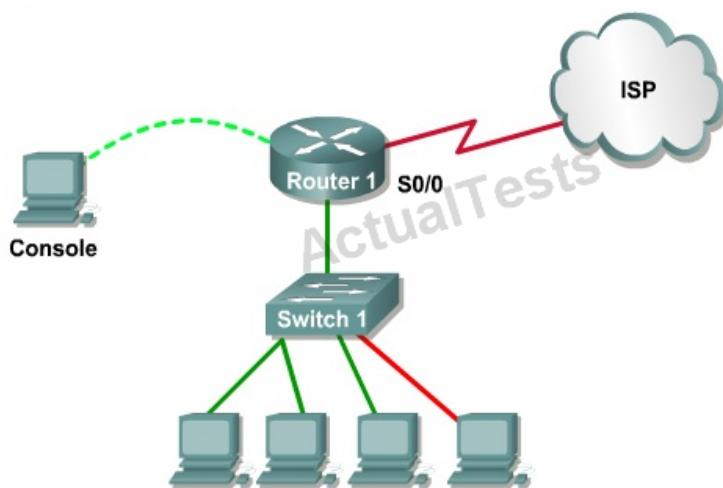
Scenario

This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

NOTE: The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.

Topology

```
R1
Press RETURN to get started!
Router1>
```

The hosts in the LAN are not able to connect to the Internet. Which commands will correct this issue?

- Router1(conf)# interface fa0/0
Router1(conf-if)# no shutdown
- Router1(conf)# interface fa0/1
Router1(conf-if)# no shutdown
- Router1(conf)# interface s0/0
Router1(conf-if)# no shutdown
- Router1(conf)# interface s0/1
Router1(conf-if)# no shutdown
- Router1(conf)# interface s0/0
Router1(conf-if)# ip address 10.11.12.13 255.255.255.252
- Router1(conf)# interface s0/1
Router1(conf-if)# ip address 10.100.1.1255.255.255.252

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: B

Explanation:

Do a “show ip int brief” and you will see that Fa0/1 has an IP address assigned, but it is shut down.

QUESTION NO: 183

The network administrator has found the following problem.

```
Central# debug ip rip
```

```
<some output text omitted>
```

```
Central#debug ip rip
```

```
1d00h: RIP: received v1 update from 172.16.100.2 on Serial0/0
1d00h:    172.16.10.0 in 1 hops
1d00h:    172.16.20.0 in 1 hops
1d00h:    172.16.30.0 in 1 hops
```

```
Central# show ip route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/24 is subnetted, 8 subnets
C    172.16.150.0 is directly connected, FastEthernet0/0
C    172.16.220.0 is directly connected, Loopback2
C    172.16.210.0 is directly connected, Loopback1
C    172.16.200.0 is directly connected, Loopback0
R    172.16.30.0 [120/1] via 172.16.100.2, 00:00:07, Serial0/0
S    172.16.20.0 [1/0] via 172.16.150.15
R    172.16.10.0 [120/1] via 172.16.100.2, 00:00:07, Serial0/0
C    172.16.100.0 is directly connected, Serial0/0
```

The remote networks 172.16.10.0, 172.16.20.0, and 172.16.30.0 are accessed through the Central router's serial 0/0 interface. No users are able to access 172.16.20.0. After reviewing the command output shown in the graphic, what is the most likely cause of the problem?

- A. no gateway of last resort on Central
- B. Central router's not receiving 172.16.20.0 update

- C. incorrect static route for 172.16.20.0
- D. 172.16.20.0 not located in Central's routing table

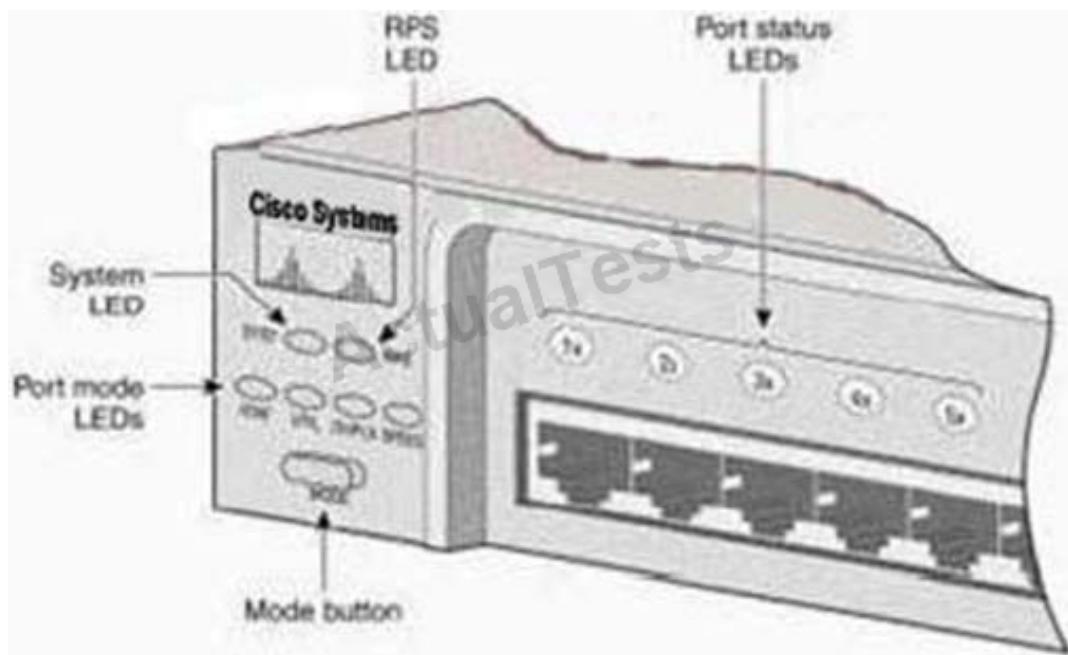
Answer: C

Explanation:

If we use 172.16.20.0 to route to 172.16.150.15, then the packet will route back. To clear this error we have to use **#no ip route 172.16.20.0 255.255.255.0 172.16.150.15** command in configuration mode.

QUESTION NO: 184

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

Answer: C**Explanation:**

http://www.cisco.com/en/US/products/hw/switches/ps607/products_tech_note09186a0080125913.shtml

Each time you power up the switch, eight Power-On Self Tests (POSTs) run automatically. POSTs check the most important system components before the switch begins to forward packets. When the switch begins the POST, the port status LEDs display amber for two seconds, and then display green. As each test runs, the port status LEDs go out. 1x is the first to go out. The port status LEDs for ports 2x through 8x go out sequentially as the system completes a test.

When the POST completes successfully, the port status LEDs go out. This indicates that the switch is operational. If a test fails, the port status LED associated with the test displays amber. The system LED also displays amber.

Not E: From Cisco IOS Software Release 11.2(8.5) SA6 onwards, the port and system LEDs both remain amber after a POST failure. In the earlier Cisco IOS Software Releases, only the LEDs of failed linked ports remained amber.

QUESTION NO: 185

Refer to the exhibit.

```
WG1R2#show ru
% Ambiguous command:  "show ru"
WG1R2#_
```

Why did the device return this message?

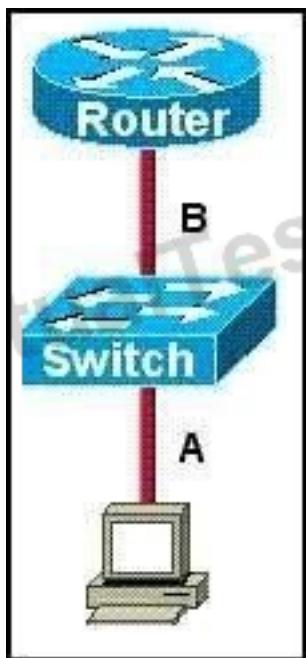
- A. The command requires additional options or parameters
- B. There is no show command that starts with ru.
- C. The command is being executed from the wrong router mode.
- D. There is more than one show command that starts with the letters ru.

Answer: D**Explanation:**

Answer D is correct because when you type the incomplete command it will not autocomplete if there is more than one option for completing the command. In this case, there is another command that also starts with "show ru"

QUESTION NO: 186

Refer to the exhibit.



The two connected ports on the switch are not turning orange or green. What would be the most effective steps to troubleshoot this physical layer problem? (Choose three.)

- A. Ensure that the Ethernet encapsulations match on the interconnected router and switch ports.
- B. Ensure that cables A and B are straight-through cables.
- C. Ensure cable A is plugged into a trunk port.
- D. Ensure the switch has power.
- E. Reboot all of the devices.
- F. Reseat all cables.

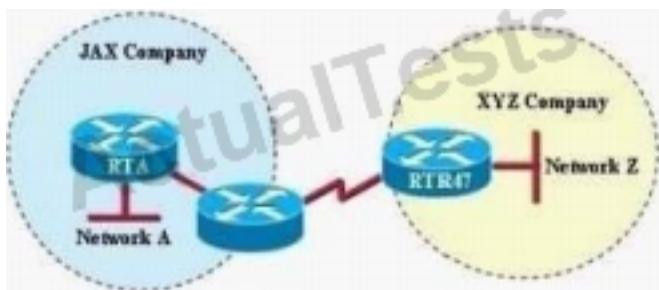
Answer: B,D,F

Explanation:

The ports on the switch are not up indicating it is a layer 1 (physical) problem so we should check cable type, power and how they are plugged in.

QUESTION NO: 187

Refer to the exhibit.



A person is trying to send a file from a host on Network A of the JAX Company to a server on Network Z of the XYZ Company. The file transfer fails. The host on Network A can communicate with other hosts on Network A.

Which command, issued from router RTA, would be the most useful for troubleshooting this problem?

- A. show flash:**
- B. show history**
- C. show version**
- D. show interfaces**
- E. show controllers serial**

Answer: D

Explanation:

The most useful thing to check on RTA would be the show interfaces command to see if the interface toward the WAN link is up. The most likely scenario is that the local LAN interface is up, but the other interface toward the XYZ company is down.

QUESTION NO: 188

Refer to the exhibit.

```
C:\>ipconfig /all
Windows IP Configuration

Host Name . . . . . : home-pc
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection 3:

Connection-Specifics DNX suffix . . . . . :
Description . . . . . : Wired Network Connection
Physical Address . . . . . : 00-13-CE-9B-33-93
Dhcp Enabled . . . . . : No
IP address . . . . . : 10.10.10.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.1

C:\>
```

A user cannot reach any web sites on the Internet, but others in the department are not having a problem.

What is the most likely cause of the problem?

- A.** IP routing is not enabled.
- B.** The default gateway is not in the same subnet.
- C.** A DNS server address is not reachable by the PC.
- D.** A DHCP server address is not reachable by the PC.
- E.** NAT has not been configured on the router that connects to the Internet.

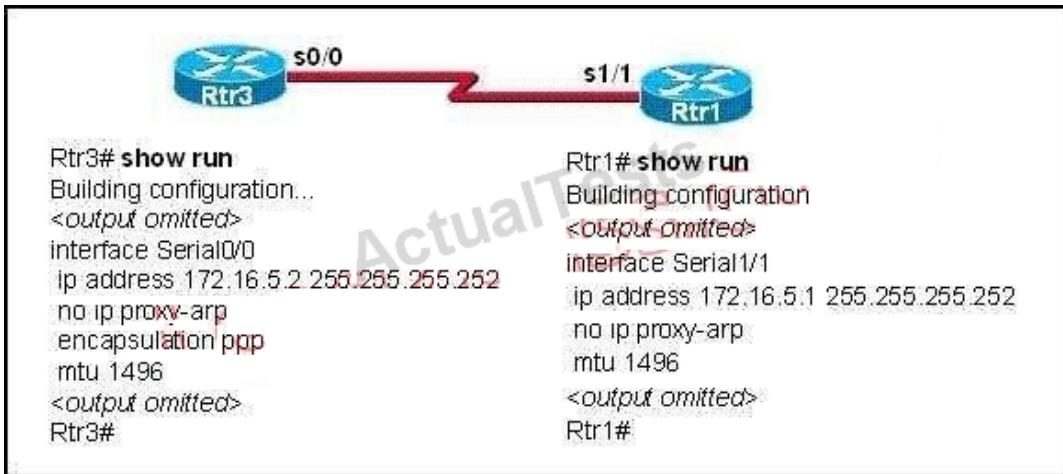
Answer: C

Explanation:

Answer C is only answer that makes sense. IP routing does not need to be enabled on PC's, this is a router function. We can see from the output that the PC and default gateway are on the same subnet. DHCP has not been enabled on this PC so it has been configured with a static address so reaching the DHCP server is not the issue. Finally, NAT must be configured correctly or the other users in the department would also be having issues.

QUESTION NO: 189

Refer to the exhibit.



A network administrator is troubleshooting a connectivity problem on the serial interfaces. The output from the show interfaces command on both routers shows that the serial interface is up, line protocol is down. Given the partial output for the show running-config in the exhibit, what is the most likely cause of this problem?

- A.** The serial cable is bad.
- B.** The MTU is incorrectly configured.
- C.** The Layer 2 framing is misconfigured.
- D.** The IP addresses are not in the same subnet.

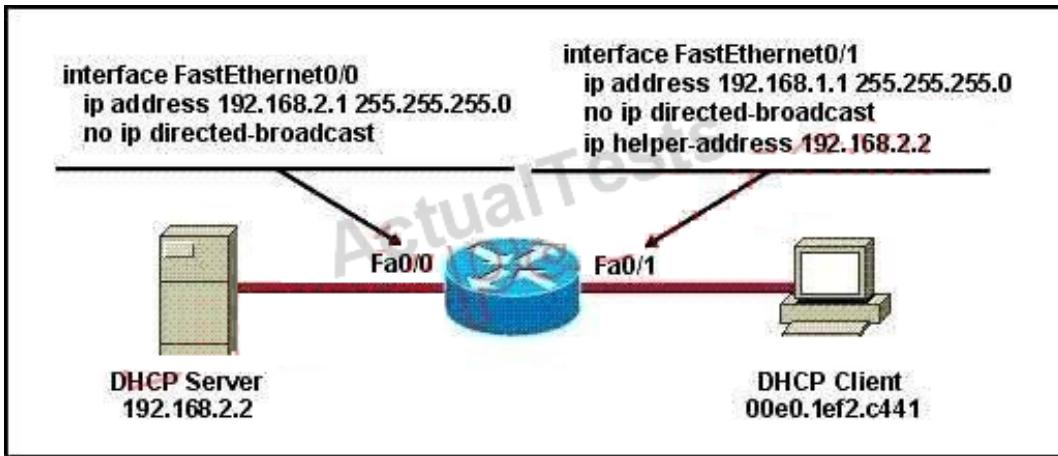
Answer: C

Explanation:

Here we see that Rtr3 is configured to use PPP encapsulation, but Rtr1 has not been configured for any kind of encapsulation. The default on Cisco router serial interfaces is HDLC, not PPP, so there is an encapsulation mismatch.

QUESTION NO: 190

Refer to the exhibit.



The DHCP settings have recently been changed on the DHCP server and the client is no longer able to reach network resources. What should be done to correct this situation?

- A. Verify that the DNS server address is correct in the DHCP pool.
- B. Ping the default gateway to populate the ARP cache.
- C. Use the tracert command on the DHCP client to first determine where the problem is located.
- D. Clear all DHCP leases on the router to prevent address conflicts.
- E. Issue the ipconfig command with the /release and /renew options in a command window.

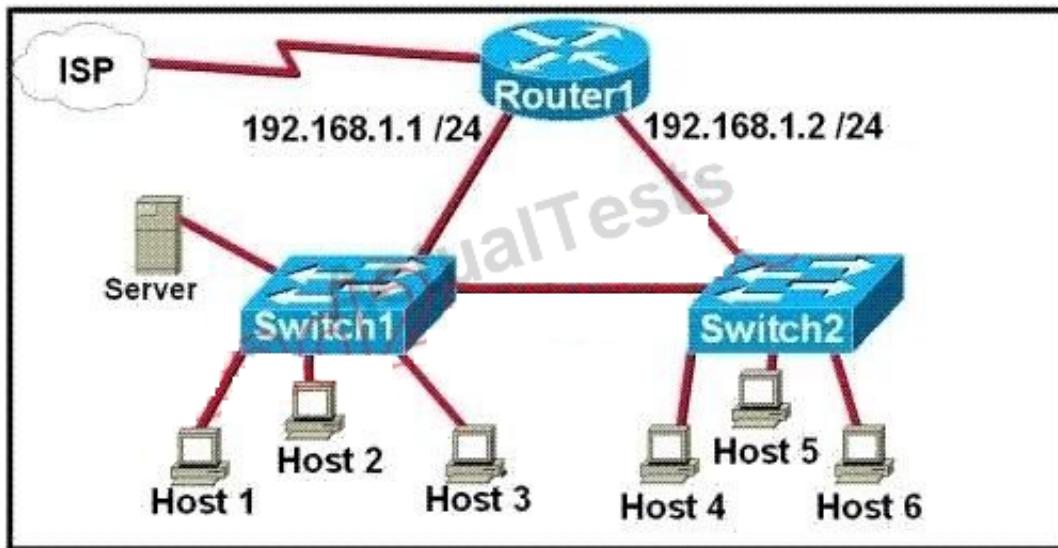
Answer: E

Explanation:

A PC will retain its DHCP assigned IP address until the lease time expires, which often times is 24 hours or more. When changes are made to the DHCP server, the client should issue the ipconfig/release and then ipconfig/renew commands to obtain a new IP address lease.

QUESTION NO: 191

Refer to the exhibit.



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

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

Answer: C

Explanation:

The proposed addressing scheme is on the same network. Cisco routers will not allow you to assign two different interfaces to be on the same IP subnet.

QUESTION NO: 192

Refer to the exhibit.

```

Finance# show interfaces fastEthernet 0/2
FastEthernet0/2 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 0017.596d.2a02
  Description: To Central Fa0/0
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:03, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
<output omitted>

```

An administrator replaced the 10/100 Mb NIC in a desktop PC with a 1 Gb NIC and now the PC will not connect to the network. The administrator began troubleshooting on the switch. Using the switch output shown, what is the cause of the problem?

- A. Speed is set to 100Mb/s.
- B. Input flow control is off.
- C. Encapsulation is set to ARPA.
- D. The port is administratively down.
- E. The counters have never been cleared.

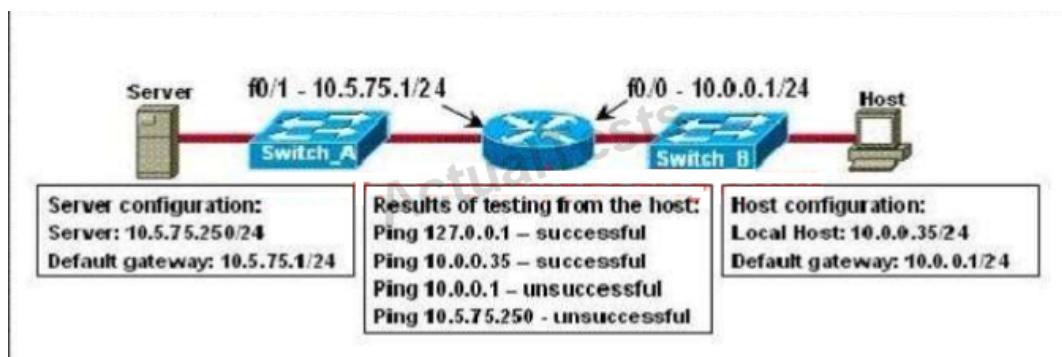
Answer: A

Explanation:

For PC to switch connectivity, the speed settings must match. In this case, the 1 Gb NIC will not be able to communicate with a 100Mb fast Ethernet interface, unless the 1Gb NIC can be configured to connect at 100Mb.

QUESTION NO: 193

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

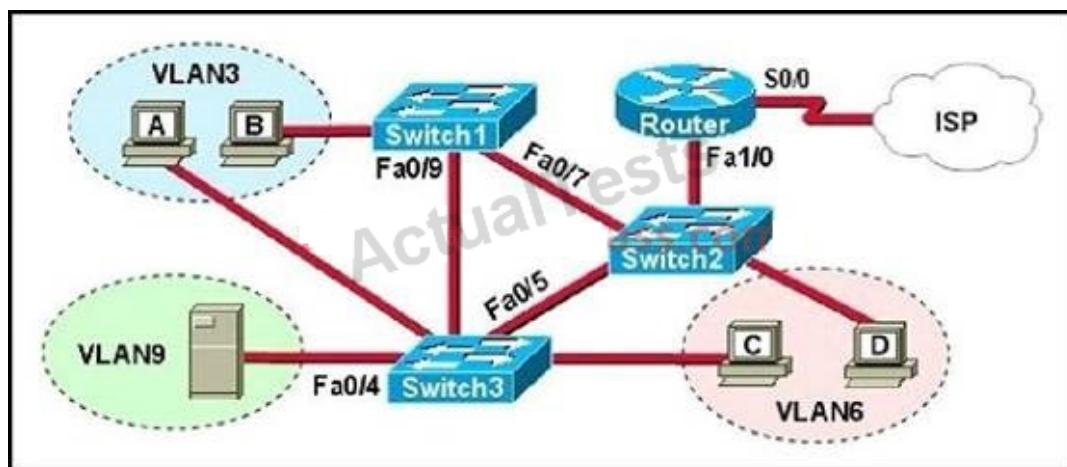
Answer: D

Explanation:

Here we see that the host is able to ping its own loopback IP address of 127.0.0.1 and its own IP address of 10.0.0.35, so we know that the NIC is functioning and that the host's TCP/IP stack is OK. However, it is not able to ping the IP address of its local default gateway, so we know that there is a local cabling problem between the switch and the router.

QUESTION NO: 194

Refer to the exhibit.



A problem with network connectivity has been observed. It is suspected that the cable connected to switch port Fa0/9 on Switch1 is disconnected. What would be an effect of this cable being disconnected?

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

network function would resume.

Answer: D

Explanation:

Because Switch1 has multiple redundant links in this network, traffic would not work for less than a minute, and then it would get rerouted along the longer path to the host. The 1 minute outage would be the length of time it takes STP to converge.

QUESTION NO: 195

A receiving host has failed to receive all of the segments that it should acknowledge. What can the host do to improve the reliability of this communication session?

- A. decrease the window size**
- B. use a different source port for the session**
- C. decrease the sequence number**
- D. obtain a new IP address from the DHCP server**
- E. start a new session using UDP**

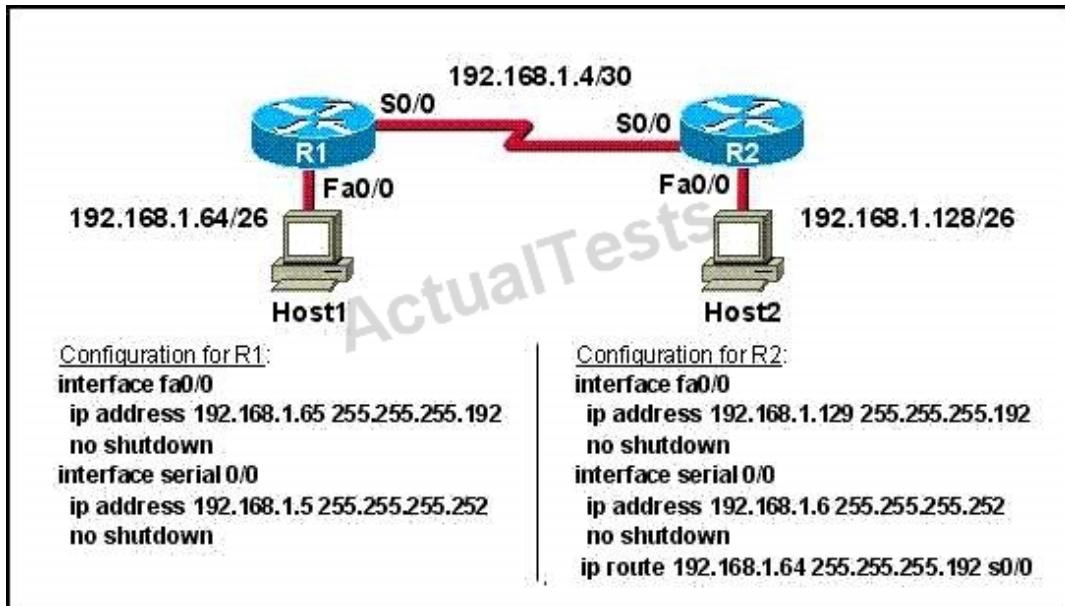
Answer: A

Explanation:

The Window bit in the header determines the number of segments that can be sent at a time. This is done to avoid overwhelming the destination. At the start of the session the window is small but it increases over time. The destination host can also decrease the window to slow down the flow. Hence the window is called the sliding window. When the source has sent the number of segments allowed by the window, it cannot send any further segments till an acknowledgement is received from the destination. On networks with high error rates or issues, decreasing the window size can result in more reliable transmission, as the receiver will need to acknowledge fewer segments. With a large window size, the sender will need to resend all the frames if a single one is not received by the receiver.

QUESTION NO: 196

Refer to the exhibit.



A technician pastes the configurations in the exhibit into the two new routers shown. Otherwise, the routers are configured with their default configurations.

A ping from Host1 to Host 2 fails, but the technician is able to ping the S0/0 interface of R2 from Host 1. The configurations of the hosts have been verified as correct. What could be the cause of the problem?

- A. The serial cable on R1 needs to be replaced.
- B. The interfaces on R2 are not configured properly
- C. R1 has no route to the 192.168.1.128 network.
- D. The IP addressing scheme has overlapping subnetworks.
- E. The ip subnet-zero command must be configured on both routers.

Answer: C

Explanation:

Without a static route pointing to the host 2 network the router R1 is unaware of the path to take to reach that network and reply traffic cannot be sent.

QUESTION NO: 197

Refer to the exhibit.

BHM# show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.16.1	YES	NVRAM	up	up
Serial0/0	192.168.15.2	YES	NVRAM	administratively down	down
FastEthernet0/1	192.168.17.1	YES	NVRAM	up	up
Serial0/1	unassigned	YES	NVRAM	administratively down	down

Serial 0/0 does not respond to a ping request from a host on the FastEthernet 0/0 LAN. How can this problem be corrected?

- A. Enable the Serial 0/0 interface.
- B. Correct the IP address for Serial 0/0.
- C. Correct the IP address for FastEthernet 0/0
- D. Change the encapsulation type on Serial 0/0
- E. Enable autoconfiguration on the Serial 0/0 interface

Answer: A

Explanation:

Serial 0/0 interface is administratively down therefore, you will have to run the "no shutdown" command to enable the interface for data.

QUESTION NO: 198

Refer to the exhibit.

```
WG1R2#telnet 10.3.1.2
Trying 10.3.1.2 ... Open

Password required, but none set

[Connection to 10.3.1.2 closed by foreign host]
WG1R2#_
```

Why was this message received?

- A. No VTY password has been set.
- B. No enable password has been set.
- C. No console password has been set.

- D. No enable secret password has been set.
- E. The login command has not been set on CON 0
- F. The login command has not been set on the VTY ports.

Answer: A

Explanation:

Your CCNA certification exam is likely going to contain questions about Telnet, an application-level protocol that allows remote communication between two networking devices. With Telnet use being as common as it is, you had better know the details of how to configure it in order to pass your CCNA exam and to work in real-world networks.

The basic concept is pretty simple - we want to configure R1, but we're at R2. If we telnet successfully to R1, we will be able to configure R1 if we've been given the proper permission levels. In this CCNA case study, R2 has an IP address of 172.12.123.2 and R1 an address of 172.12.123.1. Let's try to telnet from R2 to R1.

```
R2#telnet 172.12.123.1
Trying 172.12.123.1 ... Open
Password required, but none set
[Connection to 172.12.123.1 closed by foreign host]
```

This seems like a problem, but it's a problem we're happy to have. A Cisco router will not let any user telnet to it by default. That's a good thing, because we don't want just anyone connecting to our router! The "password required" message means that no password has been set on the VTY lines on R1. Let's do so now.

```
R1(config)#line vty 0 4
```

```
R1(config-line)#password baseball
```

A password of "baseball" has been set on the VTY lines, so we shouldn't have any trouble using Telnet to get from R2 to R1. Let's try that now.

```
R2#telnet 172.12.123.1
```

```
Trying 172.12.123.1 ... Open
```

User Access Verification

Password:

R1>

We're in, and placed into user exec mode.

Reference: http://www.mcmcse.com/cisco/guides/telnet_passwords_and_privilege_levels.shtml

QUESTION NO: 199

Refer to the exhibit.

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

After configuring two interfaces on the HQ router, the network administrator notices an error message. What must be done to fix this error?

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

Answer: D

Explanation:

The IP address 192.168.1.17 255.255.255.0 specifies that the address is part of the 192.168.1.0/24 subnet

24 mask bits = 255.255.255.0

28 mask bits = 255.255.255.240

192.168.1.0/24 subnet has a host range of 192.168.1.1 to 192.168.1.254 (0 being network and 255 being broadcast)

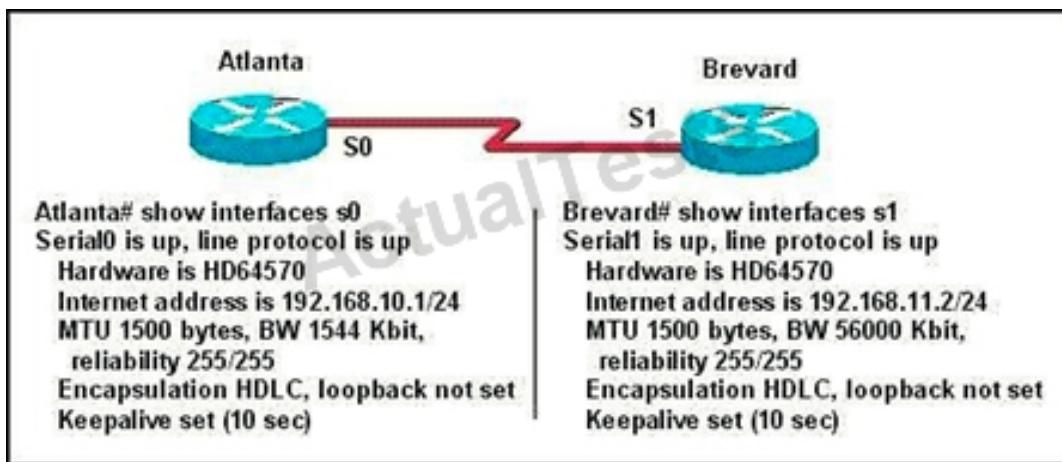
192.168.1.17/28 subnet has a host range of 192.168.1.17 to 192.168.1.30 (16 being network and 31 being broadcast)

192.168.1.65/28 subnet has a host range of 192.168.1.65 - 192.168.1.78 (64 being network and 79 being broadcast)

If fa0/0 was left as /24, you can see that the host range includes the host range of 192.168.1.64/28 which conflicts. Simply speaking, you can't overlap the subnets. By changing the subnet mask of fa0/0 to 255.255.255.240, these networks would no longer overlap.

QUESTION NO: 200

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. A loopback is not set.
- B. The IP address is incorrect.
- C. The subnet mask is incorrect.
- D. The serial line encapsulations are incompatible.
- E. The maximum transmission unit (MTU) size is too large.
- F. The bandwidth setting is incompatible with the connected interface.

Answer: B

Explanation:

The connection between two routers must have IP addresses that belong to the same subnet, but in this case Atlanta is using 192.168.10.1/24 and the other is in 192.168.11.1/24.

Topic 8, Simulation

QUESTION NO: 201 CORRECT TEXT

This screenshot shows a Cisco router configuration simulation. At the top, there is a network diagram with three routers labeled 'Tampa', 'Apopka', and 'Apopka LAN Switch'. Tampa has an interface 'Fa0/0' with IP '192.168.1.1/24'. Apopka has an interface 'Fa0/0' with IP '209.165.201.0/27'. A serial connection between Tampa and Apopka is labeled '5000N 192.0.2.128.028 Network'. A dashed line connects Apopka's Fa0/0 to a computer labeled 'Console'.

Task Instructions:

To configure the router (Apopka) click on the console host icon that is connected to a router by a serial console cable (shown in the diagram as a dashed black line).

You can click on the buttons below to view the different windows.

Each of the windows can be minimized by clicking on the []. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation. The help command does not display all commands of the help system.

Configuration Requirements:

Central Florida Widgets recently installed a new router in their Apopka office. Complete the network installation by performing the initial router configuration and configuring RIPv2 routing using the router command line interface (CLI) on the Apopka router.

Configure the router per the following requirements:

- Name of the router is Apopka
- Enable secret password (cisco10)
- The password to access user EXEC mode using the console is New2Rtr
- The password to allow telnet access to the router is scan90
- IPv4 addresses must be configured as follows:
 - Ethernet network 209.165.201.0/27 - router has second assignable host address in subnet
 - Serial network is 192.0.2.128/28 - router has last assignable host address in the subnet
- Interfaces should be enabled.
- Routing protocol is RIPv2.

Answer: Router>enable

Router#config terminal

Router(config)#hostname Apopka

2) Enable-secret password (cisco10):

Apopka(config)#enable secret cisco10

3) Set the console password to RouterPass:

Apopka(config)#line console 0

Apopka(config-line)#password RouterPass

Apopka(config-line)#login

Apopka(config-line)#exit

4) Set the Telnet password to scan90:

Apopka(config)#line vty 0 4

Apopka(config-line)#password scan90

Apopka(config-line)#login

Apopka(config-line)#exit

5) Configure Ethernet interface (on the right) of router Apopka:

The subnet mask of the Ethernet network 209.165.201.0 is 27. From this subnet mask, we can

find out the increment by converting it into binary form, that is /27 = 1111 1111.1111 1111.1111 1111.1110 0000. Pay more attention to the last bit 1 because it tells us the increment, using the formula:

Increment = 2^{place of the last bit 1 (starts counting from 0,from right to left)}, in this case increment = 2⁵ = 32. Therefore:

Increment: 32

Network address: 209.165.201.0

Broadcast address: 209.165.201.31 (because 209.165.201.32 is the second subnetwork, so the previous IP - 209.165.201.31 - is the broadcast address of the first subnet).

-> The second assignable host address of this subnetwork is 209.165.201.2/27

Assign the second assignable host address to Fa0/0 interface of Apopka router:

```
Apopka(config)#interface Fa0/0
```

```
Apopka(config-if)#ip address 209.165.201.2 255.255.255.224
```

```
Apopka(config-if)#no shutdown
```

```
Apopka(config-if)#exit
```

6) Configure Serial interface (on the left) of router Apopka:

Using the same method to find out the increment of the Serial network:

Serial network 192.0.2.128/28:

Increment: 16 (/28 = 1111 1111.1111 1111.1111 1111.1111 0000)

Network address: 192.0.2.128 (because 8 * 16 = 128 so 192.0.2.128 is also the network address of this subnet)

Broadcast address: 192.0.2.143

-> The last assignable host address in this subnet is 192.0.2.142/28.

Assign the last assignable host address to S0/0/0 interface of Apopka router:

```
Apopka(config)#interface S0/0/0 (or use interface S0/0 if not successful)
```

```
Apopka(config-if)#ip address 192.0.2.142 255.255.255.240
```

```
Apopka(config-if)#no shutdown
```

```
Apopka(config-if)#exit
```

7) Configure RIP v2 routing protocol:

```
Apopka(config)#router rip
```

```
Apopka(config-router)#version 2
```

```
Apopka(config-router)#network 209.165.201.0
```

```
Apopka(config-router)#network 192.0.2.128
```

```
Apopka(config-router)#end
```

Save the configuration:

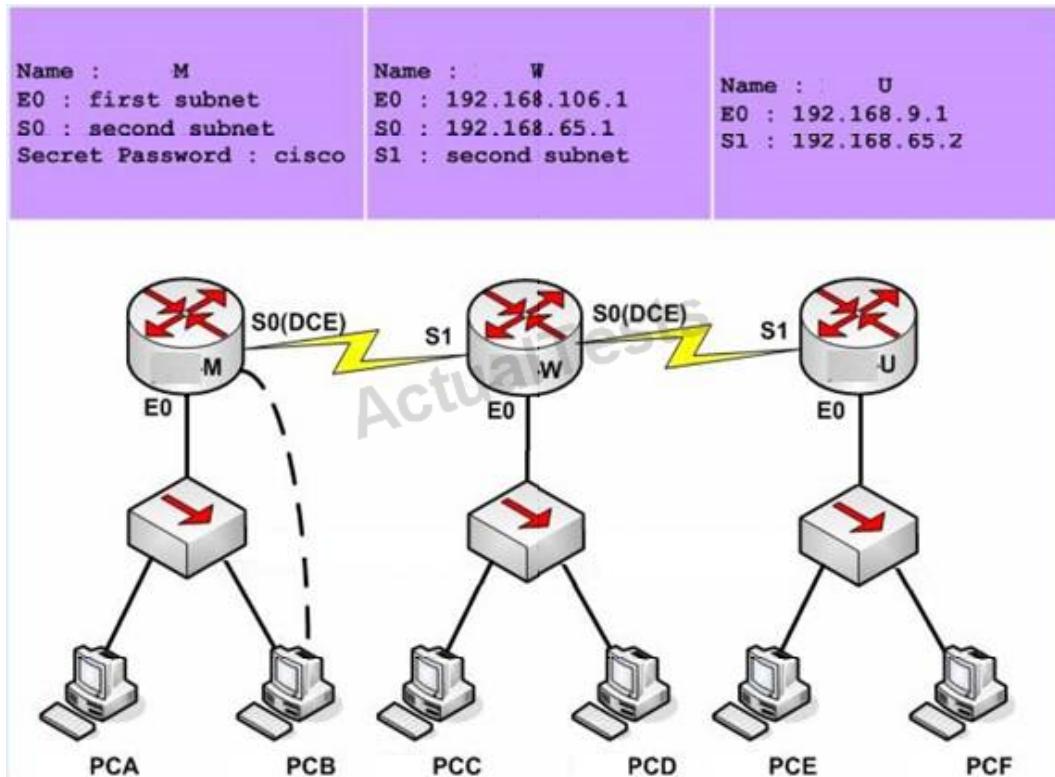
```
Apopka#copy running-config startup-config
```

Finally, you should use the ping command to verify all are working properly!

QUESTION NO: 202 CORRECT TEXT

There are three locations in a school district of a large city: ROUTER -M, ROUTER -W and

ROUTER -U. The network connection between two of these locations has already functioned. Configure the ROUTER -M router IP addresses on the E0 and S0 interfaces so that the E0 receives the first usable subnet while the S0 receives the second usable subnet from the network 192.168.160.0/28. Both interfaces would receive the last available ip address on the proper subnet.



Note. The OSPF process must be configured to allow interfaces in specific subnets to participate in the routing process.

Answer: ROUTER-M> enable

PassworD. Cisco

ROUTER-M# config t

ROUTER-M(config)# interface e0

ROUTER-M(config-if)# ip address 192.168.160.14 255.255.255.240

ROUTER-M(config-if)# no shutdown

ROUTER -M(config-if)# exit

ROUTER -M(config)# interface s0

ROUTER-M(config-if)# ip address 192.168.160.30 255.255.255.240

ROUTER-M(config-if)# no shutdown

ROUTER-M(config-if)# end

ROUTER-M# copy run start

QUESTION NO: 203 CORRECT TEXT

This topology contains 3 routers and 1 switch. Complete the topology.

Drag the appropriate device icons to the labeled Device

Drag the appropriate connections to the locations labeled Connections.

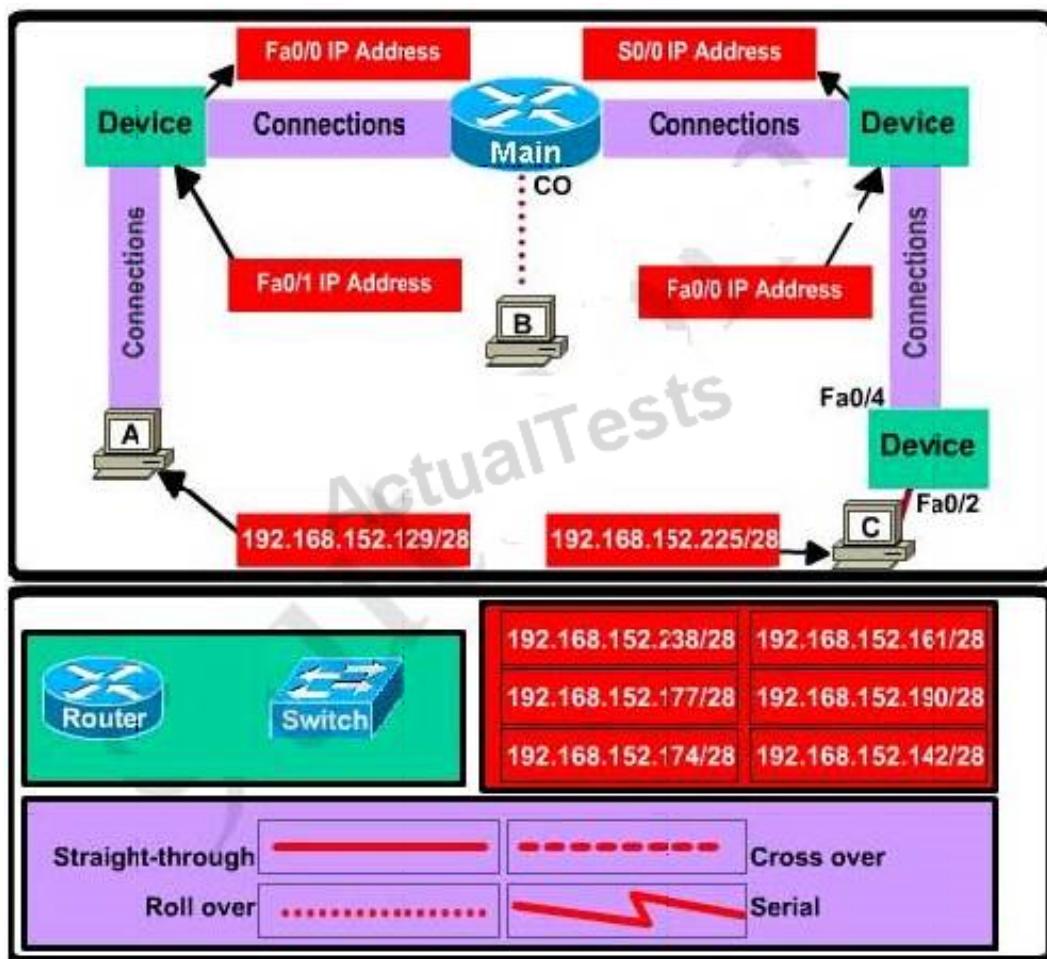
Drag the appropriate IP addresses to the locations labeled IP address

(Hint: use the given host addresses and Main router information)

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. The router does not require any configuration.



Configure each additional router with the following:

Configure the interfaces with the correct IP address and enable the interfaces.

Set the password to allow console access to consolepw

Set the password to allow telnet access to telnetpw

Set the password to allow privilege mode access to privpw

Not E: Because routes are not being added to the configurations, you will not be able to ping through the internetwork.

All devices have cable autosensing capabilities disabled.

All hosts are PC's

Answer: Specify appropriate devices and drag them on the "Device" boxes

For the device at the bottom-right box, we notice that it has 2 interfaces Fa0/2 and Fa0/4; moreover the link connects the PC on the right with the device on the bottom-right is a straight-through link -> it is a switch

The question stated that this topology contains 3 routers and 1 switch -> two other devices are routers

Place them on appropriate locations as following:

(Host D and host E will be automatically added after placing two routers. Click on them to access neighboring routers)

Specify appropriate connections between these devices:

+ The router on the left is connected with the Main router through FastEthernet interfaces: use a **crossover cable**

+ The router on the right is connected with the Main router through Serial interfaces: use a **serial cable**

+ The router on the right and the Switch: use a **straight-through cable**

+ The router on the left and the computer: use a **crossover cable**

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

- To connect **two serial interfaces** of 2 routers we use **serial cable**

- To specify when we use crossover cable or straight-through cable, we should remember:

Group 1: Router, Host, Server

Group 2: Hub, Switch

One device in group 1 + One device in group 2: use **straight-through cable**

Two devices in the same group: use **crossover cable**

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

Assign appropriate IP addresses for interfaces:

From Main router, use show running-config command.

(Notice that you may see different IP addresses in the real CCNA exam, the ones shown above are just used for demonstration)

From the output we learned that the ip address of Fa0/0 interface of the Main router is 192.168.152.177/28. This address belongs to a subnetwork which has:

Increment: 16 ($/28 = 255.255.255.240$ or 1111 1111.1111 1111.1111 1111.1111 0000)

Network address: 192.168.152.176 (because $176 = 16 * 11$ and $176 < 177$)

Broadcast address: 192.168.152.191 (because $191 = 176 + 16 - 1$)

And we can pick up an ip address from the list that belongs to this subnetwork: **192.168.152.190** and assign it to the Fa0/0 interface the router on the left

Use the same method for interface Serial0/0 with an ip address of 192.168.152.161

Increment: 16

Network address: 192.168.152.160 (because $160 = 16 * 10$ and $160 < 161$)

Broadcast address: 192.168.152.175 (because $176 = 160 + 16 - 1$)

-> and we choose **192.168.152.174** for Serial0/0 interface of the router on the right

Interface Fa0/1 of the router on the left

IP (of the computer on the left) : 192.168.152.129/28

Increment: 16

Network address: 192.168.152.128 (because $128 = 16 * 8$ and $128 < 129$)

Broadcast address: 192.168.152.143 (because $143 = 128 + 16 - 1$)

-> we choose **192.168.152.142** from the list

Interface Fa0/0 of the router on the right

IP (of the computer on the left) : 192.168.152.225/28

Increment: 16

Network address: 192.168.152.224 (because $224 = 16 * 14$ and $224 < 225$)

Broadcast address: 192.168.152.239 (because $239 = 224 + 16 - 1$)

-> we choose **192.168.152.238** from the list

Let's have a look at the picture below to summarize

Configure two routers on the left and right with these commands:

Router1 = router on the left

Assign appropriate IP addresses to Fa0/0 & Fa0/1 interfaces:

Router1>enable

Router1#configure terminal

Router1(config)#interface fa0/0

Router1(config-if)#ip address 192.168.152.190 255.255.255.240

Router1(config-if)#no shutdown

Router1(config-if)#interface fa0/1

Router1(config-if)#ip address 192.168.152.142 255.255.255.240

Router1(config-if)#no shutdown

Set passwords (configure on two routers)

+ Console password:

```
Router1(config-if)#exit
```

```
Router1(config)#line console 0
```

```
Router1(config-line)#password consolepw
```

```
Router1(config-line)#login
```

```
Router1(config-line)#exit
```

+ Telnet password:

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#password telnetpw
```

```
Router1(config-line)#login
```

```
Router1(config-line)#exit
```

+ Privilege mode password:

```
Router1(config)#enable password privpw
```

Save the configuration:

```
Router1(config)#exit
```

```
Router1#copy running-config startup-config
```

Configure IP addresses of Router2 (router on the right)

```
Router2>enable
```

```
Router2#configure terminal
```

```
Router2(config)#interface fa0/0
```

```
Router2(config-if)#ip address 192.168.152.238 255.255.255.240
```

```
Router2(config-if)#no shutdown
```

```
Router2(config-if)#interface serial0/0
```

```
Router2(config-if)#ip address 192.168.152.174 255.255.255.240
```

```
Router2(config-if)#no shutdown
```

Then set the console, telnet and privilege mode passwords for Router2 as we did for Router1, remember to save the configuration when you finished.