100-101 Cisco reworked with additional comments

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Cisco ICND1 100-101

VCEplus
VCE To PDF - Free Practice Exam

Number: 000-000 Passing Score: 800Time Limit: 120 min File Version: 1.0

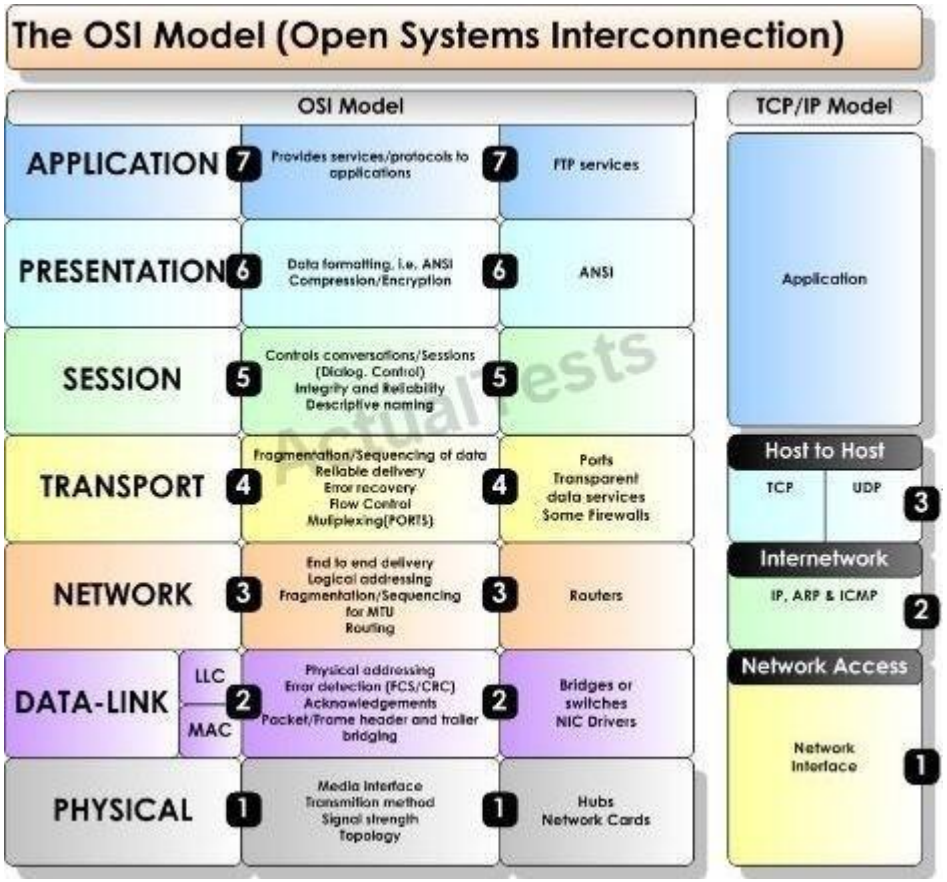
Exam A

QUESTION 1
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 then the OSI.
Below is a side by side comparison of the TCP/IP and OSI models.



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 then the OSI. Below is a side by side comparison of the TCP/IP and OSI models.
TCP/IP Model VS. OSI Model
Application Layer 7
Application Layer 6
Presentation Layer 5
Session Transport Layer 4
Transport Internet Layer 3
Network Network Access

Layer 2 Data Link
Layer 1 Physical

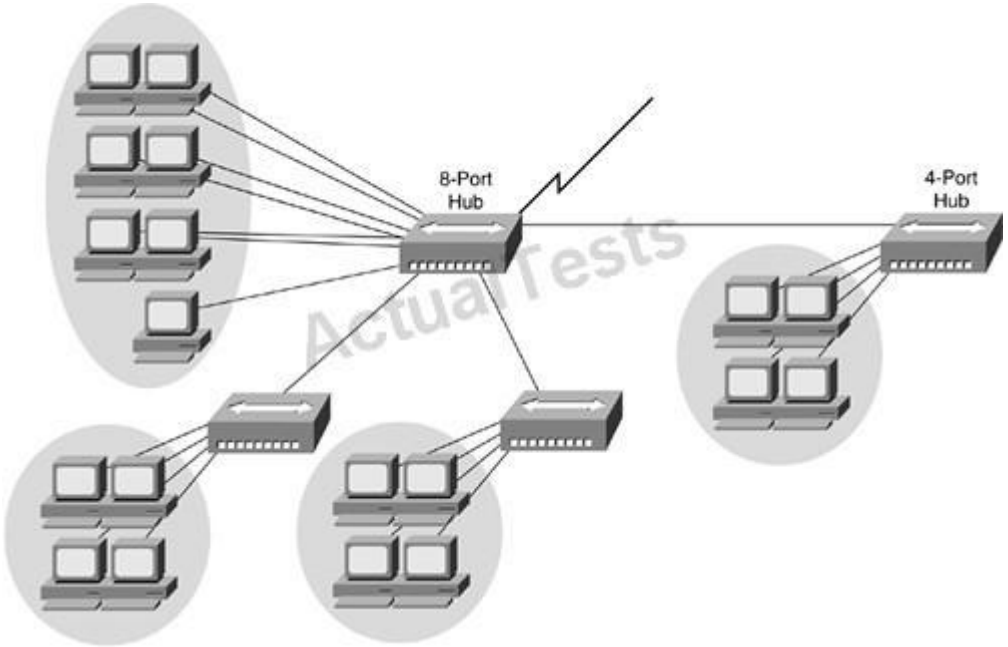
QUESTION 2
Which protocol uses a connection-oriented service to deliver files between end systems?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
FTP is an acronym for File Transfer Protocol. As the name suggests, FTP is used to transfer files between computers on a network. You can use FTP to exchange files between computer accounts, transfer files between an account and a desktop computer, or access online software archives

QUESTION 3
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

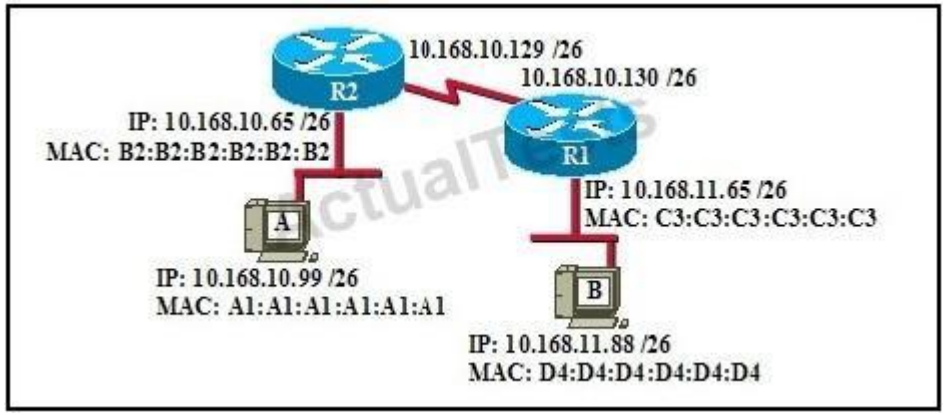
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Hubs do not separate collision domains so if hub is used in the topology above, we will have only 1 collision domain. Switches do separate collision domains so if hubs are replaced by switches, we would have 22 collision domains (19 collision domains for hosts and 3 collision domains among three

switches. Please notice that the WAN (serial) connection is not counted as a collision (or broadcast) domain.

QUESTION 4
Refer to the exhibit.



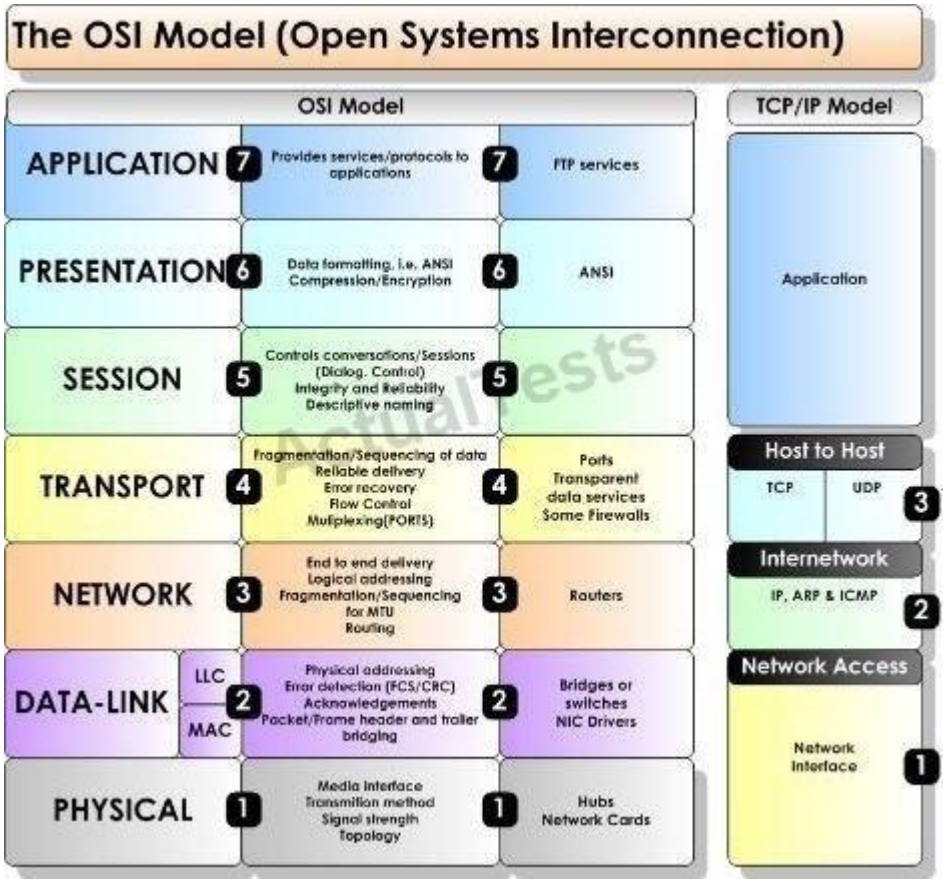
If host A sends an IP packet to host B, what will the source physical address be in the frame when it reaches host B?

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

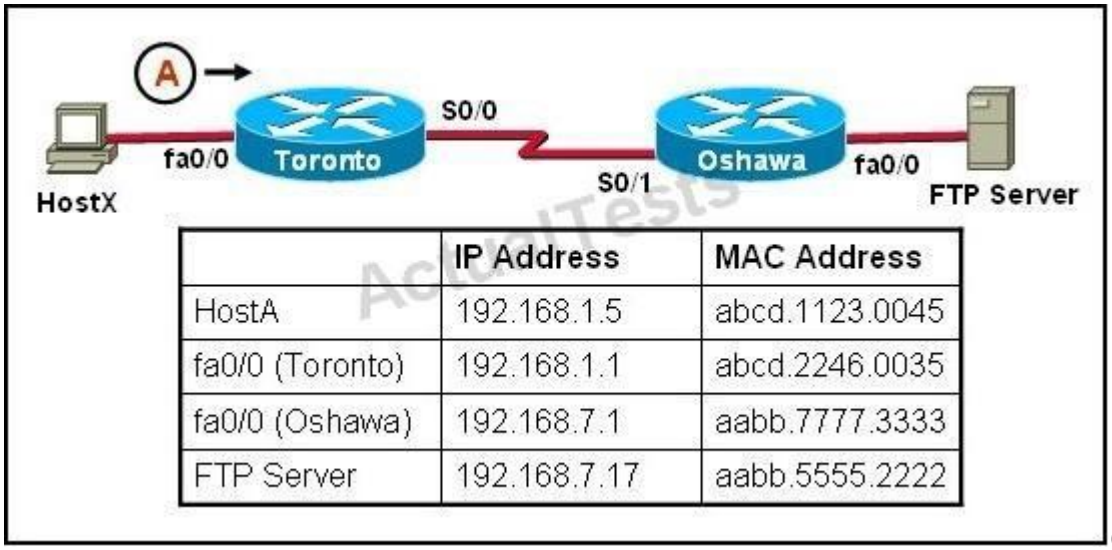
Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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.

Layer 2 ->Data Link -->MAC Address



QUESTION 5
Refer to the exhibit.



	IP Address	MAC Address
HostA	192.168.1.5	abcd.1123.0045
fa0/0 (Toronto)	192.168.1.1	abcd.2246.0035
fa0/0 (Oshawa)	192.168.7.1	aabb.7777.3333
FTP Server	192.168.7.17	aabb.5555.2222

d

Host X 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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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 6
Which network device functions only at Layer 1 of the OSI model?

A)

B)

C)

D)

E)

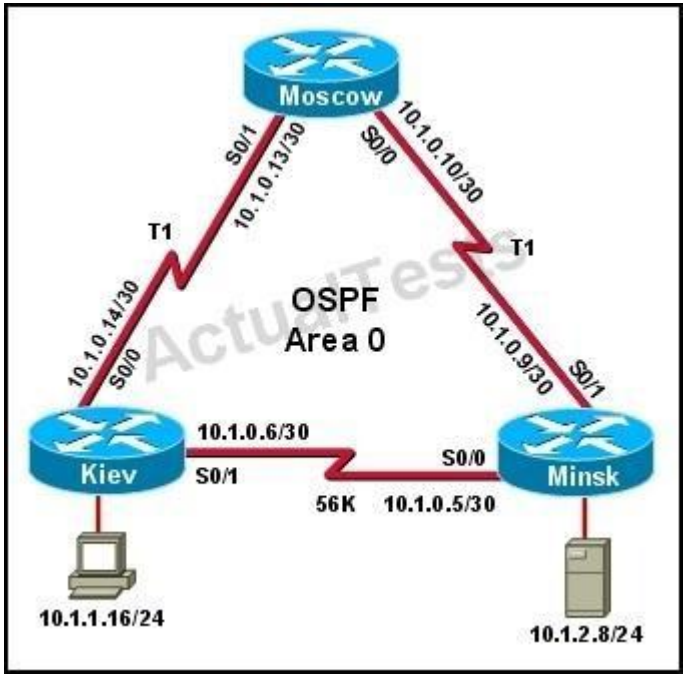
A. Option A
B. Option B
C. Option C
D. Option D

E. Option E

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 7
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?

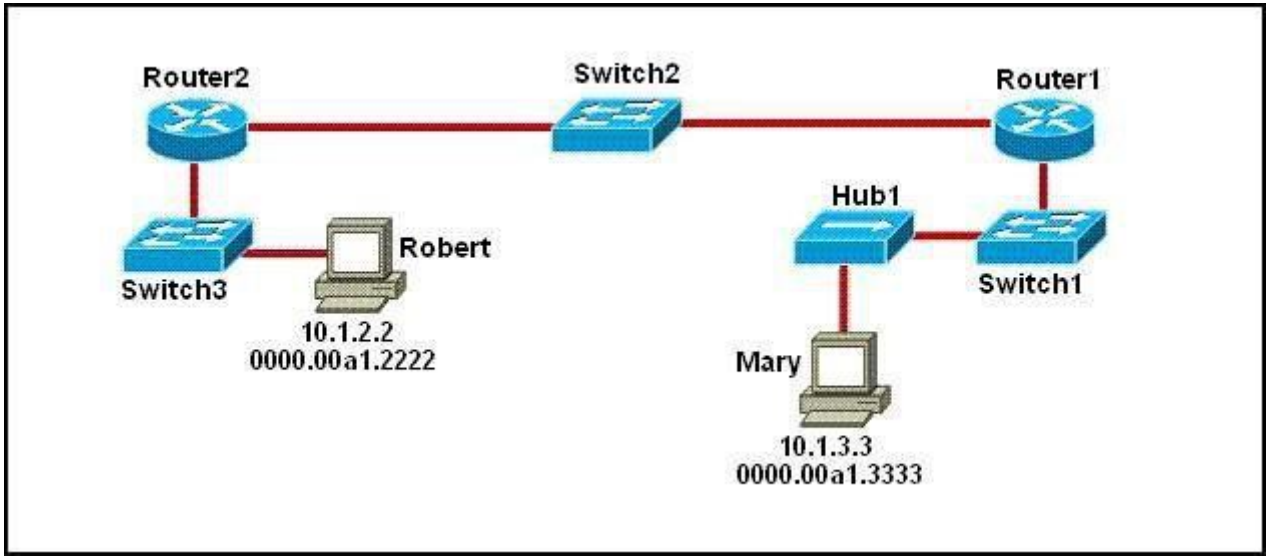
A. 10.1.0.1
B. 10.1.0.5
C. 10.1.0.6

D. 10.1.0.14
E. 10.1.1.16
F. 10.1.2.8

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Although the source and destination MAC address will change as a packet traverses a network, the source and destination IP address willnot unless network address translation (NAT) is being done, which is not the case here.

QUESTION 8
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.)

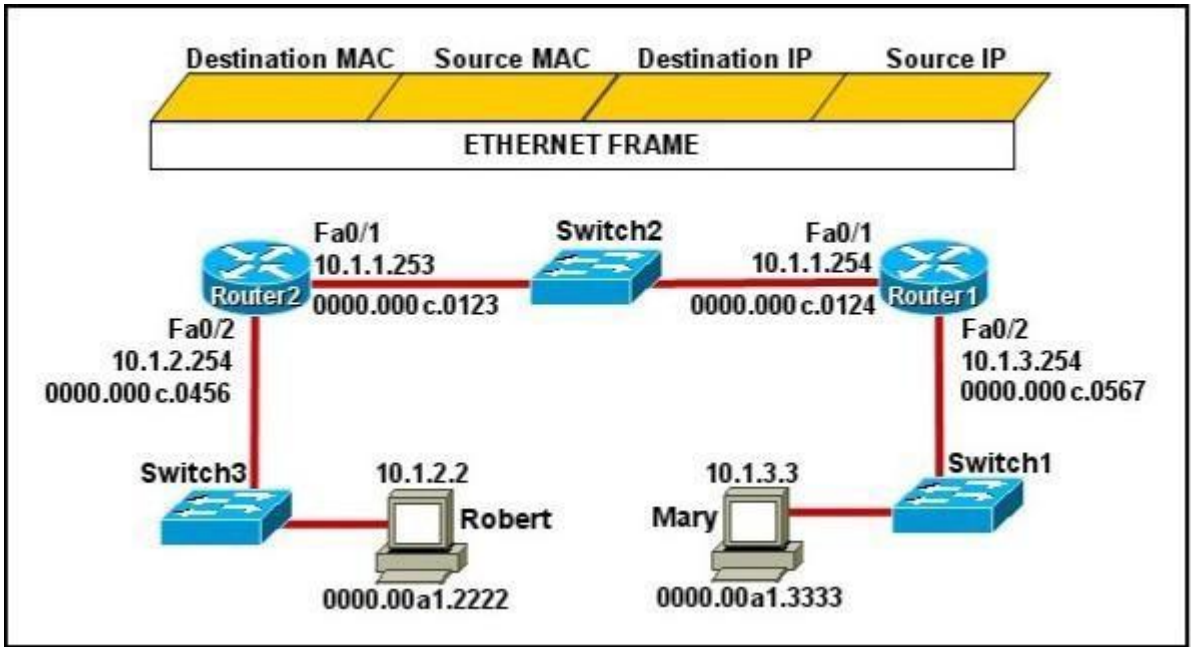
A. Hub1
B. Switch1
C. Router1
D. Switch2

E. Router2
F. Switch3

Correct Answer: BDF
Section: (none)
Explanation

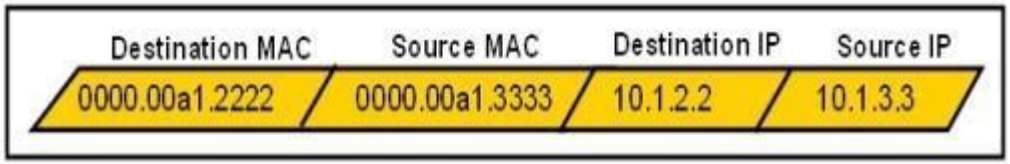
Explanation/Reference:
Switches use the destination MAC address information for forwarding traffic, while routers use the destination IP address information.
Local Area Networks employ Layer 2 Switches and Bridges to forward and filter network traffic.
Switches and Bridges operate at the Data Link Layer ofthe Open System Interconnect Model (OSI).
Since Switches and Bridges operate at the Layer 2 they operate more intelligently than hubs, which work atLayer 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 o 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 9
Refer to the exhibit.

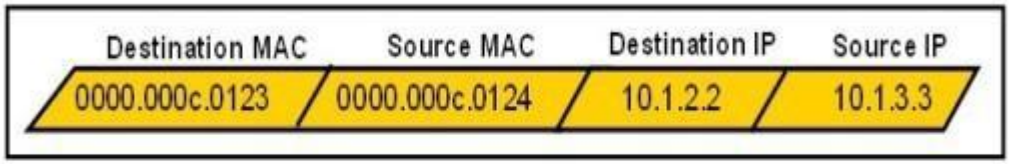


Mary is sending an instant message to Robert. The message will be broken into a series of packets that will traverse all network devices. What addresses will populate these packets as they are forwarded from Router1 to Router2?

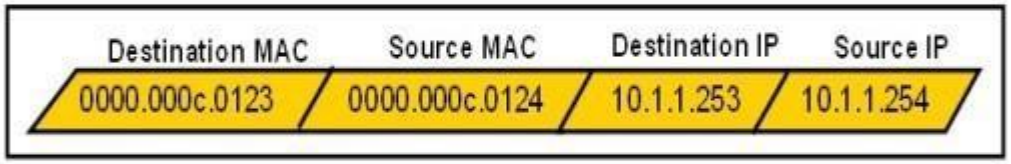
A.



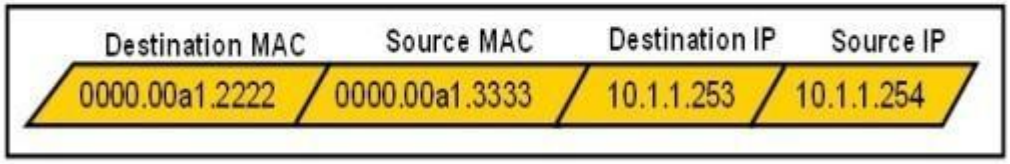
B.



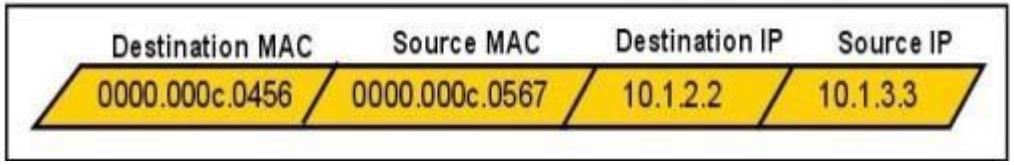
C.



D.



E.



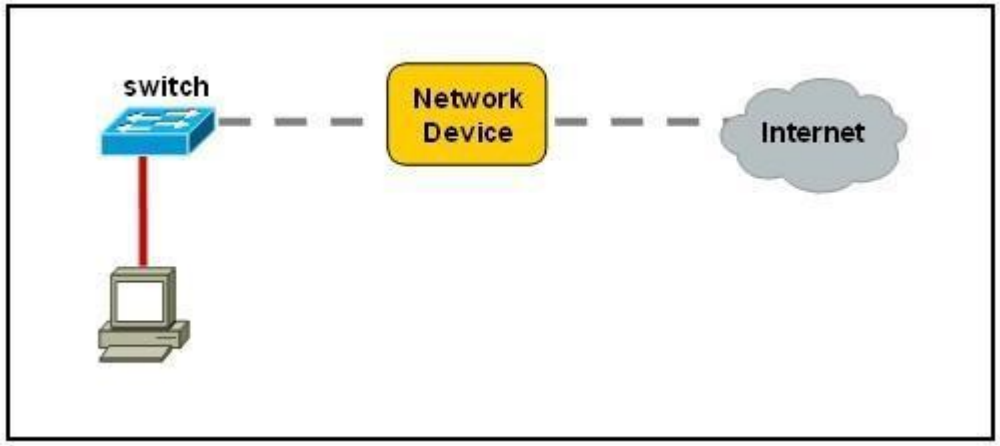
A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
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 hope 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 10
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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
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 11
Which transport layer protocol provides best-effort delivery service with no acknowledgment receipt required?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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 12
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
There are many services that can be optionally provided by a transport-layer protocol, and different protocols may or may not implement them.
Connection-oriented communication: It is normally easier for an application to interpret a connection as a data stream rather than having to deal with the underlying connection-less models, such as the datagram model of the User Datagram Protocol (UDP) and of the Internet Protocol (IP).

Byte orientation: Rather than processing the messages in the underlying communication system format, it is often easier for an application to process the data stream as a sequence of bytes.
This simplification helps applications work with various underlying message formats.
Same order delivery: The network layer doesn't generally guarantee that packets of data will arrive in the same order that they were sent, but often this is a desirable feature.
This is usually done through the use of segment numbering, with the receiver passing them to the application in order.
This can cause head-of-line blocking.
Reliability: Packets may be lost during transport due to network congestion and errors.
By means of an error detection code, such as a checksum, the transport protocol may check that the data is not corrupted, and verify correct receipt by sending an ACK or NACK message to the sender.
Automatic repeat request schemes may be used to retransmit lost or corrupted data.
Flow control: The rate of data transmission between two nodes must sometimes be managed to prevent a fast sender from transmitting more data than can be supported by the receiving data buffer, causing a buffer overrun.
This can also be used to improve efficiency by reducing buffer underrun.
Congestion avoidance: Congestion control can control traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets.
For example, automatic repeat requests may keep the network in a congested state; this situation can be avoided by adding congestion avoidance to the flow control, including slow-start.
This keeps the bandwidth consumption at a low level in the beginning of the transmission, or after packet retransmission.
Multiplexing: Ports can provide multiple endpoints on a single node.
For example, the name on a postal address is a kind of multiplexing, and distinguishes between different recipients of the same location.
Computer applications will each listen for information on their own ports, which enables the use of more than one network service at the same time.
It is part of the transport layer in the TCP/IP model, but of the session layer in the OSI model.

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 13
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
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, usualpacket-filtering rules for TCP/IP and UDP/IP are not applicable.

Fortunately, a special "signature" known as the packet's Message type is included fordenoting 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 receivingthe ICMP "echo request" packet from the source location, the destination

QUESTION 14
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.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
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 15
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.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
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 16
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
HTTP is based on TCP connection so a TCP connection must be established first between the workstation and the web server.
HTTP uses TCP port 80.
http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/

QUESTION 17
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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
TCP differs from UDP in the following ways:
- TCP provides best effort delivery.
- TCP provides synchronized communication.
- TCP segments are essentially datagrams.
- TCP provides sequence numbering of packets.
- TCP uses broadcast delivery

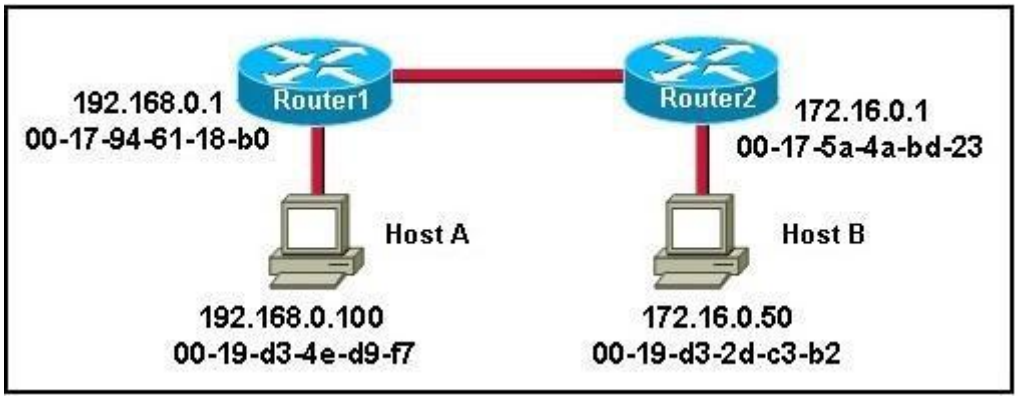
QUESTION 18
A workstation has just resolved a browser URL to the IP address of a server. What protocol will the workstation now use to determine the destination MAC address to be placed into frames directed toward the server?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
The RARP protocol is used to translate hardware interface addresses to protocol addresses.
The RARP message format is very similar to the ARPformat. 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 thebooting computer will know its IP address when it gets the message from the RARP server.

QUESTION 19
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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 legmen. The Ethernet header includes the source host MACaddress 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 20
What are two common TCP applications? (Choose two.)

A. TFTP
B. SMTP
C. SNMP

D. FTP
E. DNS

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
SMTP uses TCP port 25, while FTP uses TCP ports 20 and 21.
Reference: http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/

SMTP stands for Simple Mail Transfer Protocol. It's a set of communication guidelines that allow software to transmit email over the Internet while File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over TCP-based network.

Note: Simple Network Management Protocol (SNMP) uses UDP as the transport protocol for passing data between managers and agents. SNMP uses UDP to help reduce the impact on your network's performance. Although SNMP can be configured to run on TCP but we should only do it in special situations. SNMP uses the UDP port 161 for sending and receiving requests, and port 162 for receiving traps from managed devices.

DNS work on both the TCP and UDP protocols. DNS uses TCP for zone exchanges between servers and UDP when a client is trying to resolve a hostname to an IP address. Therefore in most cases we say "DNS uses UDP".

QUESTION 21
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?

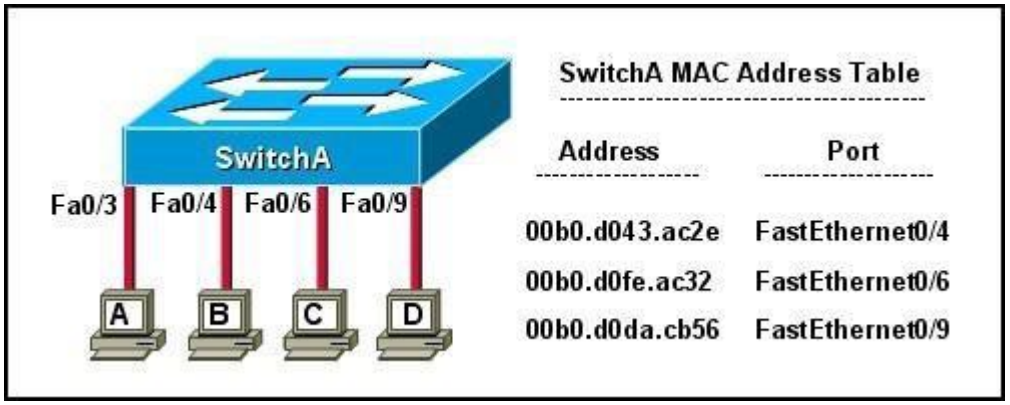
A. It will drop the frame.
B. It will forward the frame out port Fa0/6 only.
C. It will flood the frame out all ports.
D. It will flood the frame out all ports except Fa0/3.
E. It will forward the frame out port Fa0/3 only.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Switches learn the MAC addresses of PCs or workstations that are connected to their switch ports by examining the source address of frames that are received on that port.
Machines may have been removed from a port, turned off, or moved to another port on the same switch or a different switch. This could cause confusion in frame forwarding.
The MAC address entry is automatically discarded or aged out after 300 seconds.
If there is not MAC address of destination host in MAC table, switch sends broadcast to all ports except the source to find out the destination host.

In this specific case, the MAC address is known, therefore the switch will forward the frame out port Fa0/6 only.

QUESTION 22
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 23
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.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. In an Ethernet LAN, before transmitting, a computer first listens to the network media. If the media is idle, the computer sends its data. If the media is not idle (another station is talking), the computer must wait for some time.

When a station transmits, the signal is referred to as a carrier. Carrier Sense means that before a station can send data onto an Ethernet wire, it have to listen to see if another “carrier” (of another station) is present. If another station is talking, this station will wait until there is no carrier present.

Multiple Access means that stations can access the network at any time. It is opposed to Token-Ring network where a station must have the “token” so that it can send data.

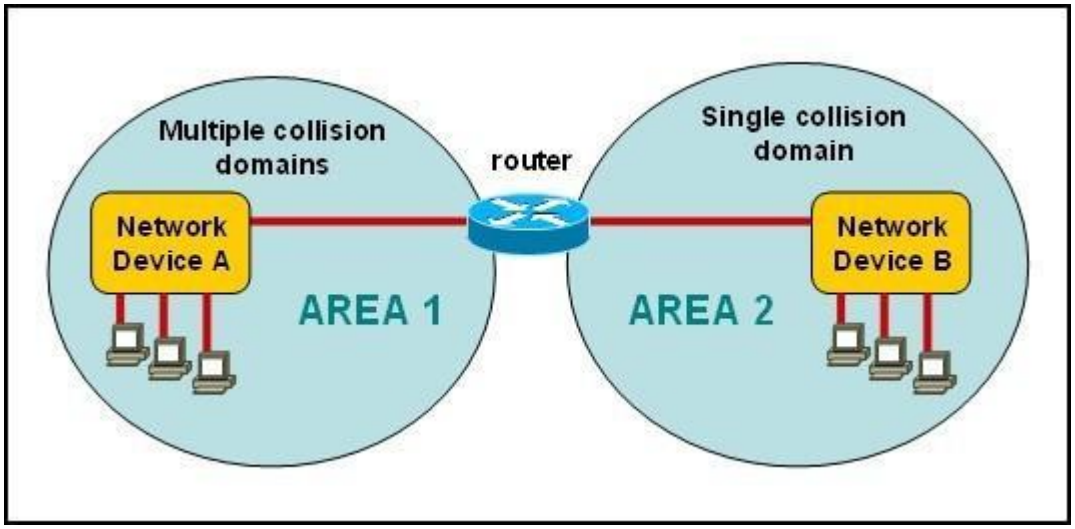
Although Carrier Sense help two stations not send data at the same time but sometimes two stations still send data at the same time! This is because two stations listen for network traffic, hear none, and transmit simultaneously -> a collision occurs and both stations must retransmit at some later time. Collision Detection is the ability of the media to detect collisions to know that they must retransmit.

Basically, the CSMA/CD algorithm can be summarized as follows:

+ A device that wants to send a frame must wait until the LAN is silent (no one is “talking”)
+ If a collision still occurs, the devices that caused the collision wait a random amount of time and then try to send data again.

Note: A switch separates each station into its own collision domain. It means that station can send data without worrying its data is collided with the data of other stations. It is as opposed to a hub which can cause collision between stations connected to it.

QUESTION 24
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.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
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 25
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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-discovery-protocol.html

QUESTION 26
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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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

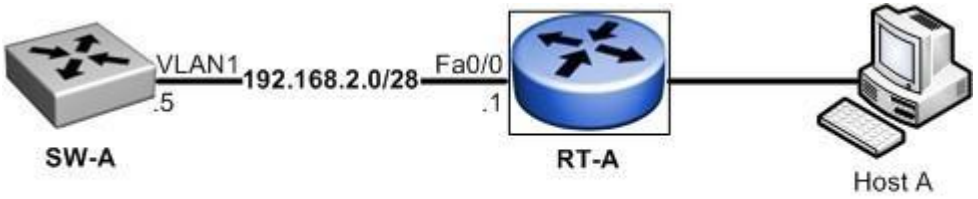
neighboring devices running lower-layer, transparent protocols.

- 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 showcdp neighbors to list out your directly connected Cisco neighboring devices.
Adding the detail parameter will display the layer-3 addressing configured onthe neighbor.

Reference: http://computernetworkingnotes.com/cisco-devices-administration-and-configuration/cisco-discovery-protocol.html

QUESTION 27
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 28
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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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 29
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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).

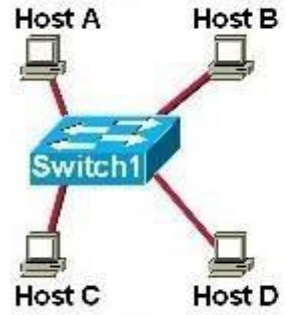
Switch features in the Access layer:
- Port security
- VLANs
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Link aggregation

- Quality of Service (QoS)

Benefits of a Hierarchical Network Scalability: The modularity of the design of hierarchical networks allows you to replicate design elements as the network grows including the use of layer 3 support on network switches.
Because each instance of the module is consistent, expansion is easy to plan and implement.
Redundancy: Redundancy at the core and distribution layers ensures path availability in case of any hardware failure in any of the devices on these layers.
Performance: Link aggregation between levels and high-performance core and distribution level switches allows for near wire speed throughout the network.
Properly designed hierarchical networks can achieve near wire speed between all devices.
Security: Port security at the access level, and policies at the distribution layer make the network more secure is important to keep the core layer free from any tasks that may compromise the speed of the link, all security should be handled at the access and distrubution layers.
Manageability: Consistency between switches at each level makes management more simple.
Each layer of the hierarchical design performs specific functions that are consistent throughout that layer.
Therefore, if you need to change the functionality of an access layer switch, you could repeat that change across all access layer switches in the network because they presumably perform the same functions at their layer.
Maintainability: Because hierarchical networks are modular in nature and scale very easily, they are easy to maintain.
With other network topology designs, manageability becomes increasingly complicated as the network grows.
In the hierarchical model, switch functions are different at each layer.
You can save money by using less expensive access layer switches at the lowest layer, and spend more on the distribution and core layer switches to achieve high performance on the network.

Reference:
http://www.ciscopath.com/content/61/
http://www.mcmcse.com/cisco/guides/hierarchical_model.shtml Access layer

QUESTION 30
Refer to the topology and switching table shown in the graphic.



Switch 1 switch table

Host	MAC Address	Port
A	00-0A-8A-47-E6-12	0/5
D	01-00-CD-22-03-14	0/9
B	01-1B-25-AB-32-E8	0/2

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
C. Send an ARP request for Host C
D. Send an ICMP Host Unreachable message to Host B
E. Record the destination MAC address in the switching table and send the frame directly to Host C

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Topic 2, LAN Switching Technologies

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 31
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The Enhanced Interior Gateway Routing Protocol (EIGRP) Stub Routing feature improves network stability, reduces resource utilization, and simplifies stub router configuration.

Stub routing is commonly used in a hub and spoke network topology. In a hub and spoke network, one or more end (stub) networks are connected to a remote router (the spoke) that is connected to one or more distribution routers (the hub). The remote router is adjacent only to one or more distribution routers. The only route for IP traffic to follow into the remote router is through a distribution router. This type of configuration is commonly used in WAN topologies where the distribution router is directly connected to a WAN. The distribution router can be connected to many more remote routers. Often, the distribution router will be connected to 100 or more remote routers. In a hub and spoke topology, the remote router must forward all nonlocal traffic to a distribution router, so it becomes unnecessary for the remote router to hold a complete routing table. Generally, the distribution router need not send anything more than a default route to the remote router.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/eigrpstb.html

CCNA question

QUESTION 32
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

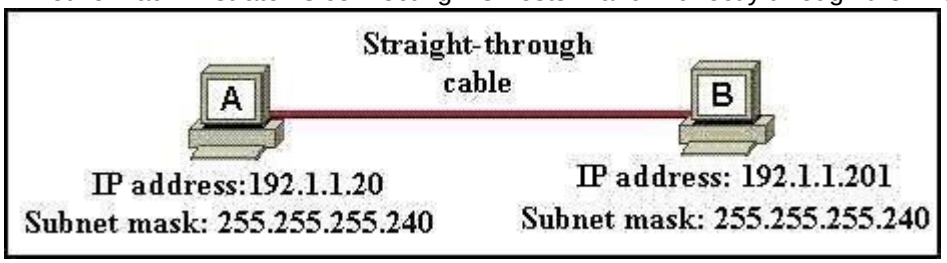
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 33
A network administrator is connecting PC hosts A and B directly through their Ethernet interfaces as shown in the graphic.



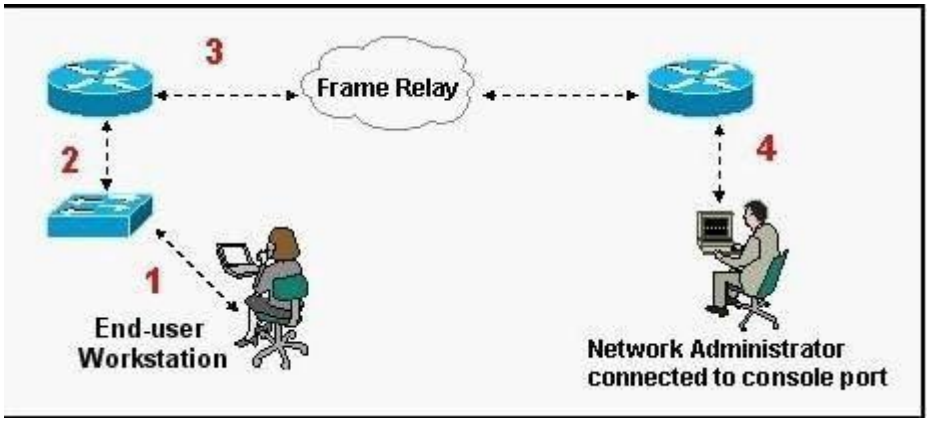
Ping attempts between the hosts are unsuccessful. What can be done to provide connectivity between the hosts? (Choose two.)

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following are types of flow control? (Choose three.)

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
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 increase it to say 5 for example.
Windowing is used only by TCP since UDP doesn't use or allow flow control.

Topic 2, LAN Switching Technologies

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

QUESTION 36
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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.

Definition - What does Broadcast Storm mean?

A broadcast storm occurs when a network system is overwhelmed by continuous multicast or broadcast traffic. When different nodes are sending/ broadcasting data over a network link, and the other network devices are rebroadcasting the data back to the network link in response, this eventually causes the whole network to melt down and lead to the failure of network communication.

There are many reasons a broadcast storm occurs, including poor technology, low port rate switches and improper network configurations.

A broadcast storm is also known as a network storm.

Techopedia explains Broadcast Storm

Although computer networks and network devices are very intelligent and efficient, networks and network devices sometimes fail to provide 100% efficiency. The broadcast storm is one of the major deficiencies in computer network systems.

For example, suppose there is a small LAN network consisting of three switches (Switch A, Switch B and Switch C), and three network segments (Segment A, Segment B and Segment C). Two nodes are attached within this network. Node A is attached to Segment B, while Node B is directly attached to Switch A. Now, if Node B wants to transmit a data packet to Node A, then traffic is broadcast from Switch A over to Segment C; if this fails, then Switch A also broadcasts traffic over Segment A. Because Node A neither attaches to Segment C, nor Segment A, these switches would further create a flood to Segment B. If neither device/switch has learned the Node A address, then traffic is sent back to Switch A. Hence, all devices/switches keep sending and resending the traffic, eventually resulting in a flood loop or broadcast loop. The final result is that the network melts down, causing failure in all network links, which is referred to as a broadcast storm.

The following elements play an active role in the creation of a broadcast storm:

- Poor network management
- Poor monitoring of the network
- The use of cheap devices, including hubs, switches, routers, cables, connectors, etc.
- Improperly maintained network configuration and inexperienced network engineers
- The lack of a network diagram design, which is needed for proper management and to provide guidelines for all network traffic routes. This can be done on paper and with the help of application software that creates an automated network diagram.

Reference: https://www.techopedia.com/definition/6270/broadcast-storm

QUESTION 37
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 it's table for the destination, it will forward the frame directly to the destination port.
If it was not already in it's MAC table, then they frame would have been flooded out all ports except for the port that it came from.

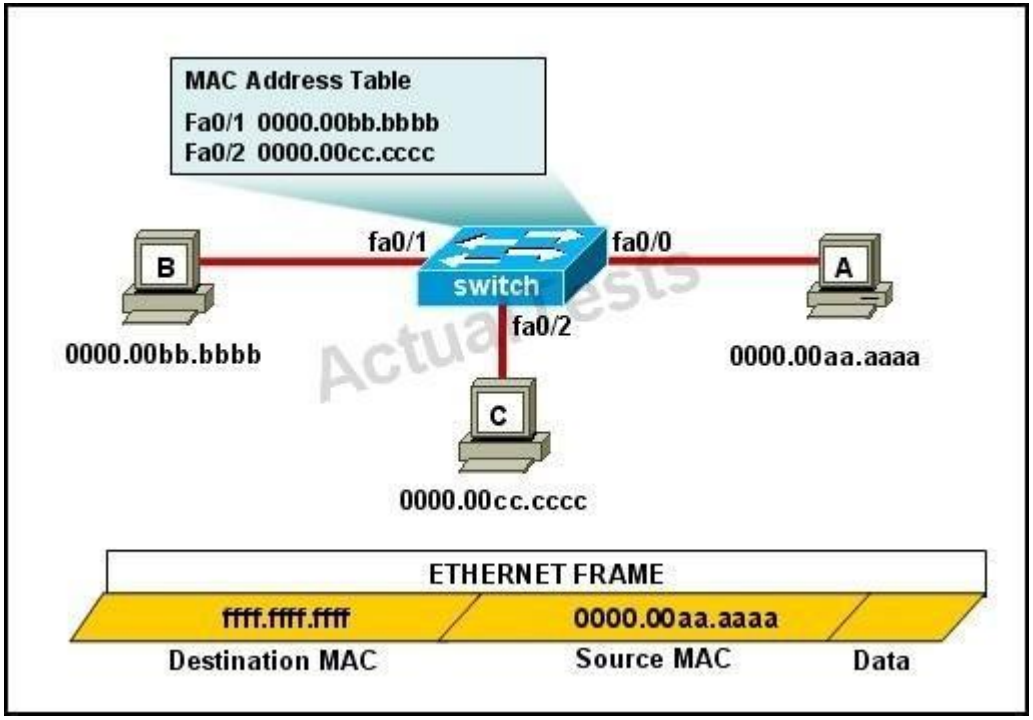
QUESTION 38
Which address type does a switch use to make selective forwarding decisions?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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 39
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 all active switch ports except for port fa0/0.
E. The frame will be forwarded out fa0/0 and fa0/1 only.
F. The frame will be forwarded out all the ports on the switch.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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 40
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

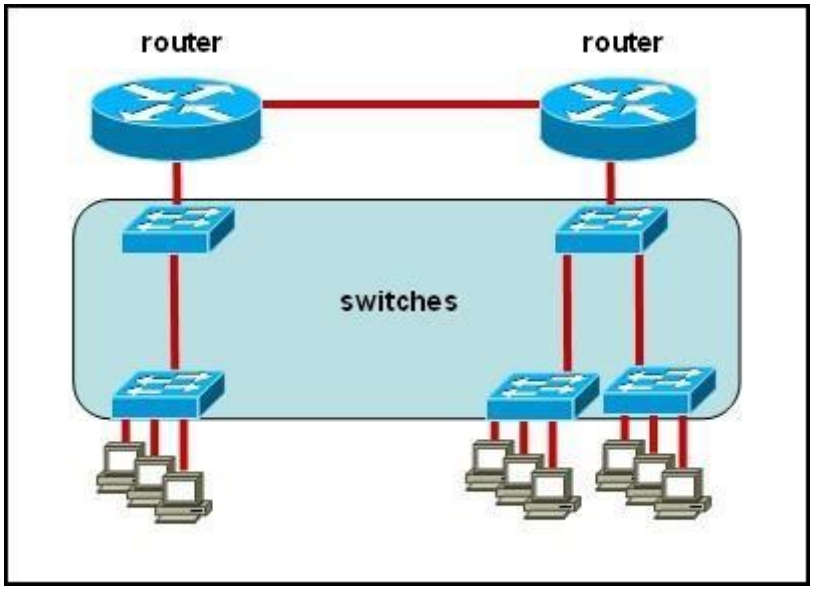
QUESTION 41
A switch has 48 ports and 4 VLANs. How many collision and broadcast domains exist on the switch (collision, broadcast)?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 42
All devices attached to the network are shown. How many collision domains are present in this network?

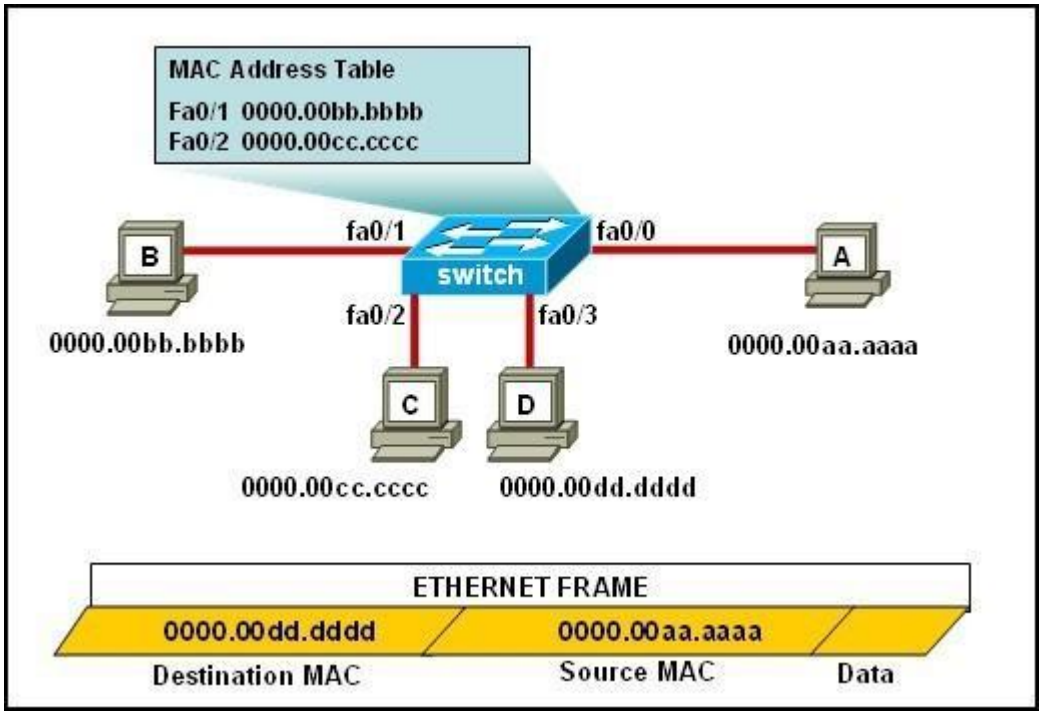


A. 2
B. 3
C. 6
D. 9
E. 15

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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 43
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 port fa0/3 only.
D. The frame will be forwarded out fa0/1, fa0/2, and fa0/3.
E. The frame will be forwarded out all the active ports.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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. It will also add the MAC address of the source

device to its MAC address table.

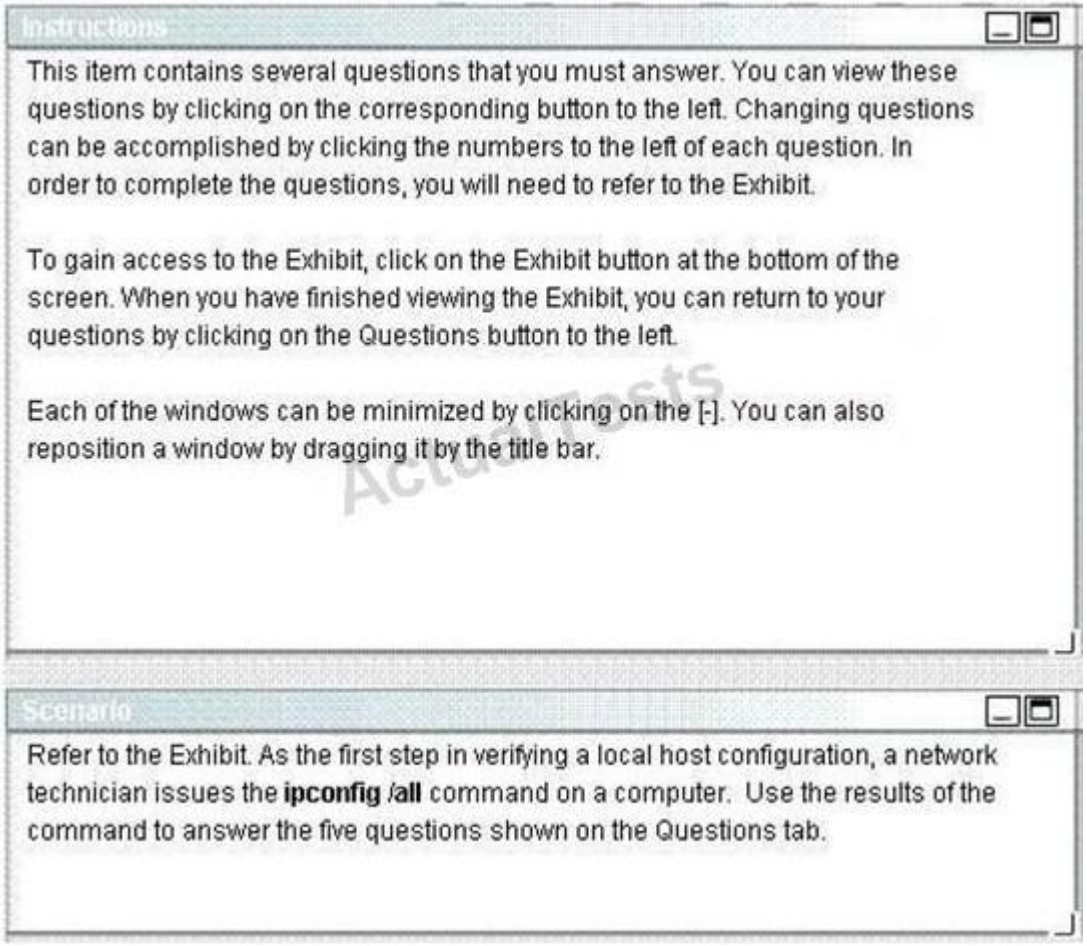
QUESTION 44
How many simultaneous Telnet sessions does a Cisco router support by default?

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

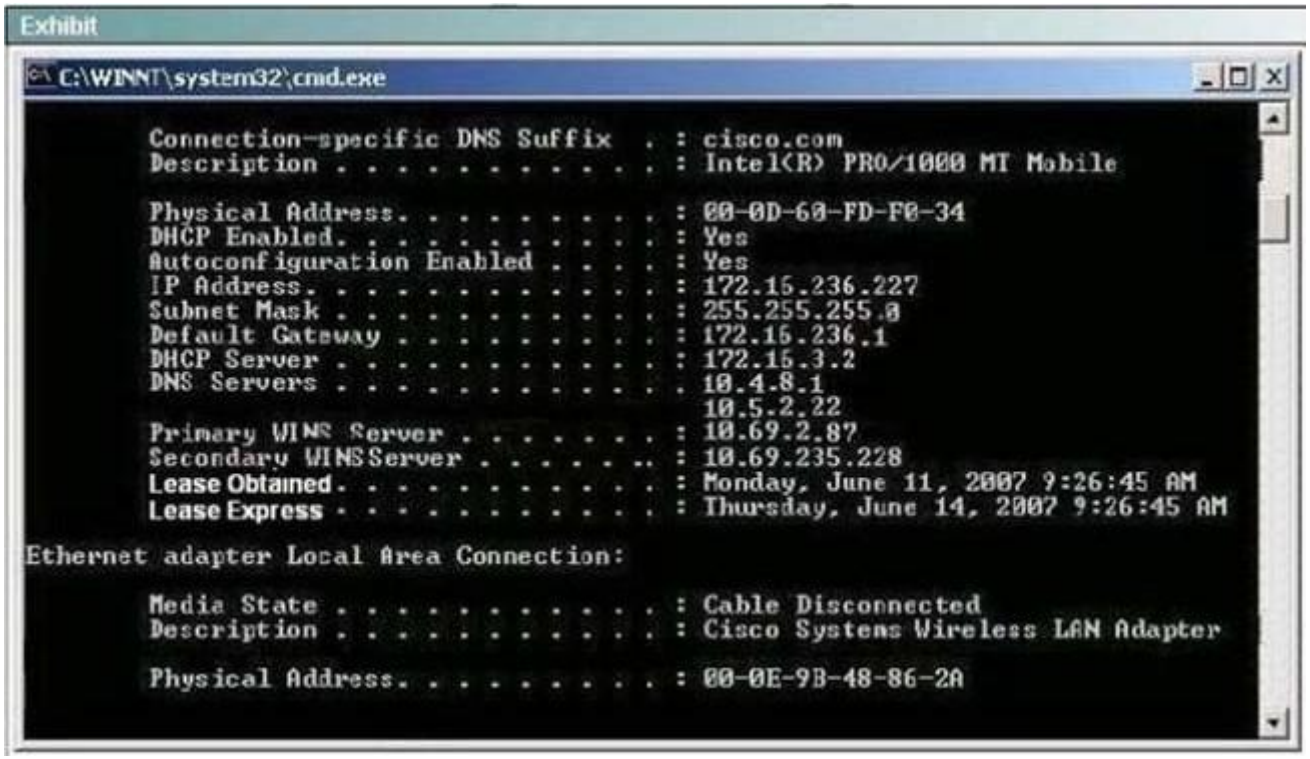
Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Refer to the exhibit.



Exhibit



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.

Correct Answer: AD
Section: (none)
Explanation

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

QUESTION 46

What is the purpose of flow control?

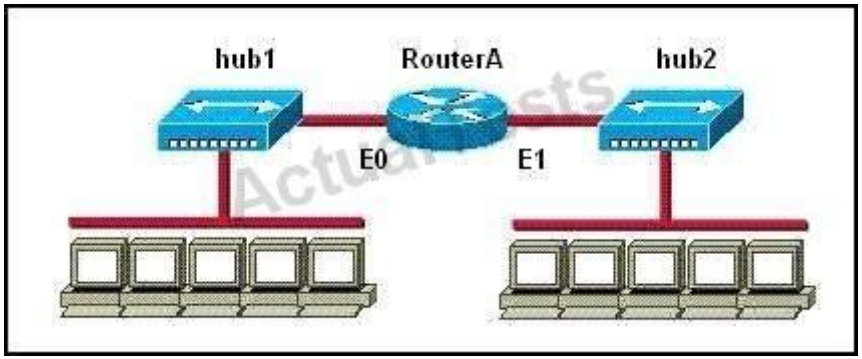
A. To ensure data is retransmitted if an acknowledgement is not received.
B. To reassemble segments in the correct order at the destination device.
C. To provide a means for the receiver to govern the amount of data sent by the sender.
D. To regulate the size of each segment.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 47
Refer to the exhibit.



How many collision domains are shown?

A. one
B. two
C. three

D. four
E. six
F. twelve

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Hubs create single collision and broadcast domains.
Topic 3, IP addressing (IPv4 / IPv6)

QUESTION 48
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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
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 00001010.00000001.10100000.00000000
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 49
Given an IP address of 192.168.1.42 255.255.255.248, what is the subnet address?

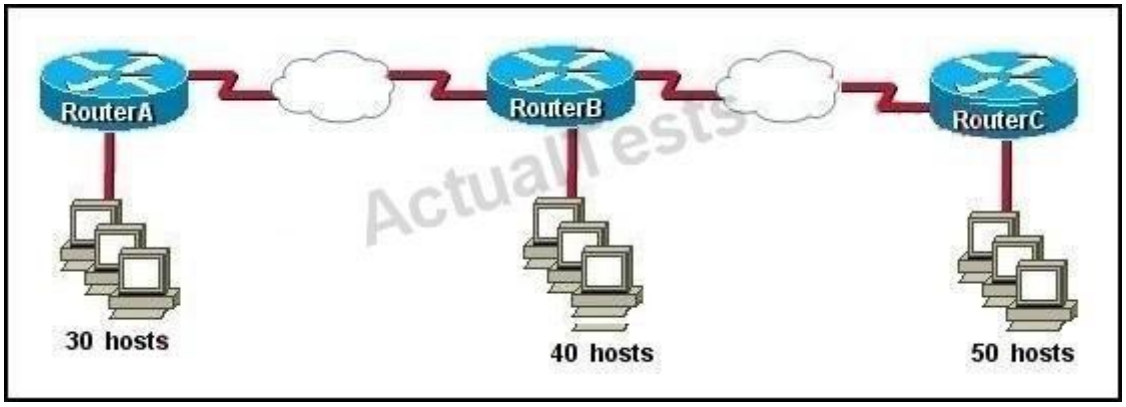
A. 192.168.1.8/29

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 50
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 51
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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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 52
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
/30 CIDR corresponds to mask 55.255.255.252 whose binary is 11111100 which means 6 subnet bits and 2 host bits which means 62 subnets and 2 hosts per subnet.

QUESTION 53
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 54
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

172.16.156.0

QUESTION 55
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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Using same logic as in question 57 we get this answer

Converting to binary format it comes to 11111111.11111111.11111111.11110000 or 255.255.255.240
Starting with 172.19.20.0 and having increment of 2 exp(4)=16 we get: 172.19.20.16

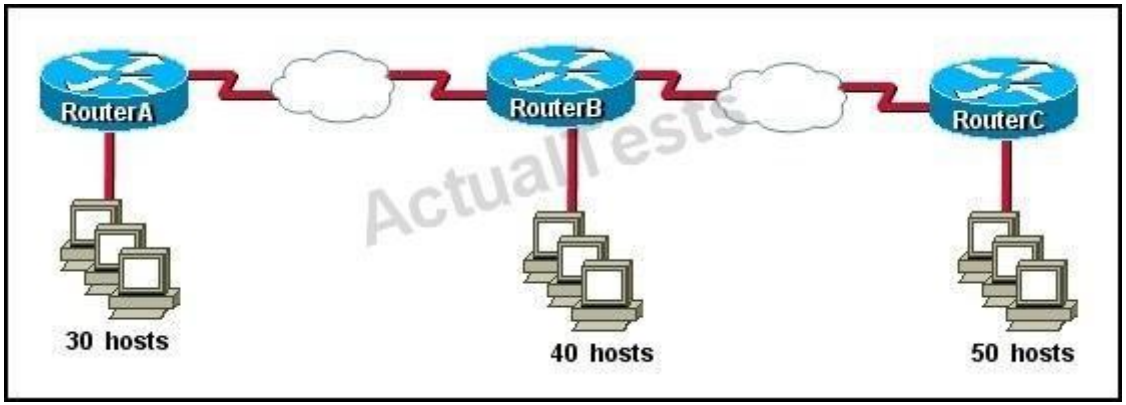
QUESTION 56
An administrator is working with the 192.168.4.0 network, which has been subnetted with a /26 mask. Which two addresses can be assigned to hostswithin the same subnet? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Only the values of host with 67 and 125 fall within the range of /26 CIDR subnet mask, all others lie beyond it.

QUESTION 57
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 sunbet '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 58
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

From the /28 we can find all information we need: Increment: 16 (/28 = 11111111.11111111.11111111.11110000) Network address: 192.168.23.48 (because 48 = 16 * 3 and 48 < 61)

QUESTION 59
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

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
To support 300 workstations in a single broadcast domain, we need to use a subnet mask which supports 512 hosts = 29 -> /23 or 255.255.254.0 in decimal form -> A is correct.
If we use 48-port switches we need 300/48 = 6.25 -> 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 60
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

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, 0:0:0:0:0:0:0:1, 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 0:0:0:0:0:0:0:0, 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 61
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.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8026003d.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 lengthx: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 62
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Each octet represents eight bits.
The bits, in turn, represent (from left to right): 128, 64, 32 , 16 , 8, 4, 2, 1Add 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 63
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.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
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 64
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 65
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
209.165.201.23 to 209.165.201.30 provides for 8 addresses.
Topic 4, IP Routing Technologies

QUESTION 66
What two things does a router do when it forwards a packet? (Choose two.)

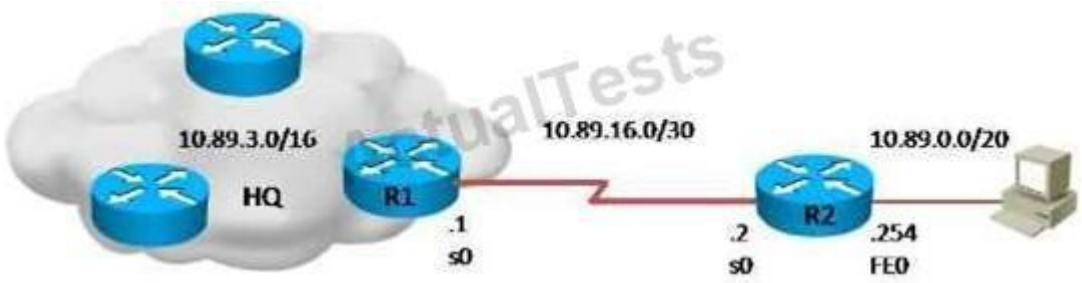
A. switches the packet to the appropriate outgoing interfaces

B. computes the destination host address
C. determines the next hop on the path
D. updates the destination IP address
E. forwards ARP requests

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Without following these two processes namely switching the packet to appropriate interface and telling the packet where to go by providing it with a destination IP address, the purpose of the same would not be solved.

QUESTION 67
Refer to the exhibit.



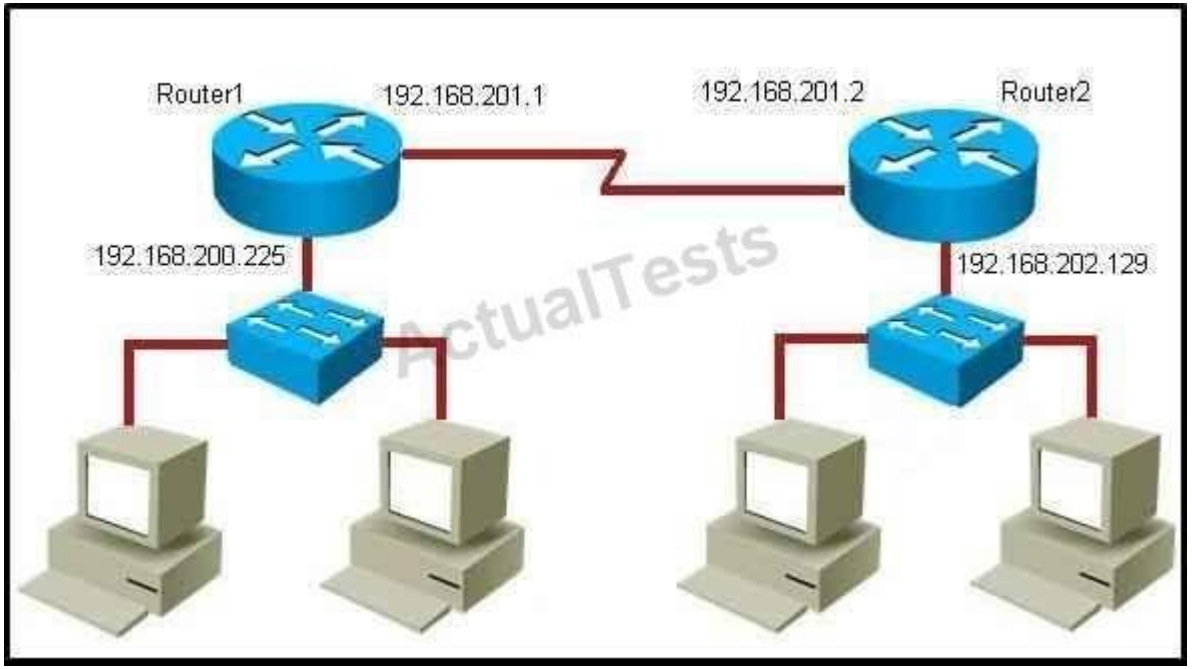
What is the simplest way to configure routing between the regional office network 10.89.0.0/20 and the corporate network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The fourth command makes it possible for all hosts beyond R2 and all hosts beyond R1 to interact with each other, hence it is the most simplest technique.

QUESTION 68
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Since it has /24 CIDR and it also has a non default administrative distance, the answer has to be option D.

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 69

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 70
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
VTY ports are telnet ports hence command B will initiate login to the telnet port.

QUESTION 71
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

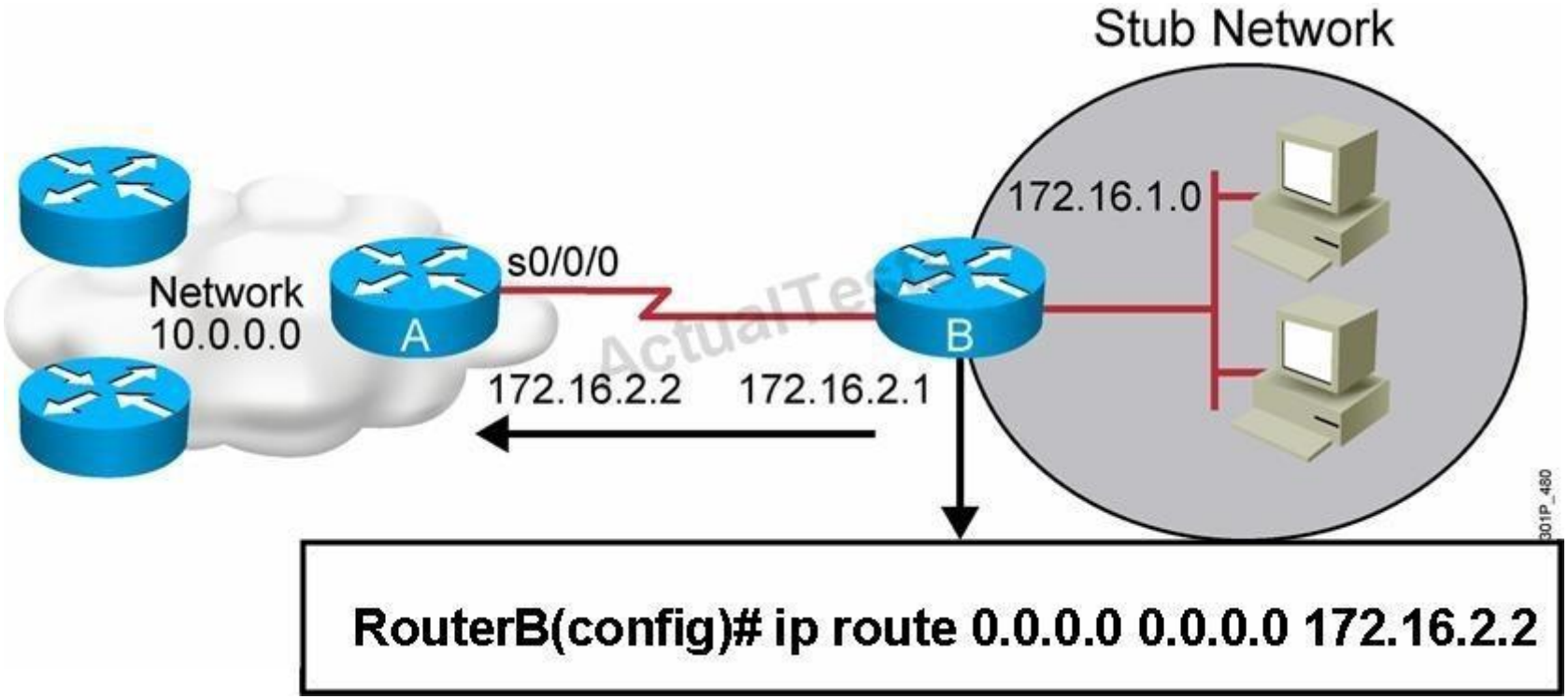
QUESTION 72
Which two of these functions do routers perform on packets? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
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 73
Refer to the exhibit.



Which two statements are correct? (Choose two.)

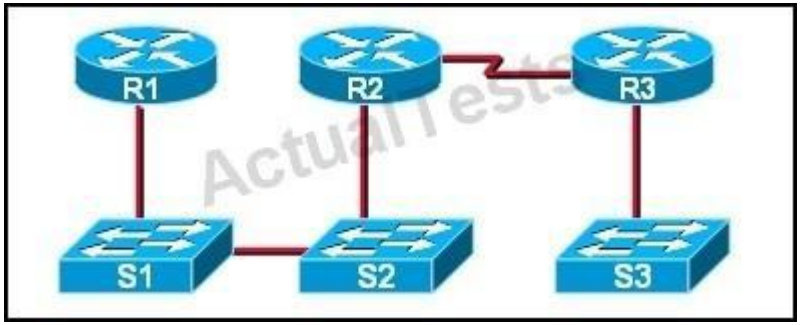
A. This is a default route.
B. Adding the subnet mask is optional for the ip route command.
C. This will allow any host on the 172.16.1.0 network to reach all known destinations beyond RouterA.
D. This command is incorrect, it needs to specify the interface, such as s0/0/0 rather than an IP address.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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
This is obviously the default value for the 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 74

Refer to the exhibit.



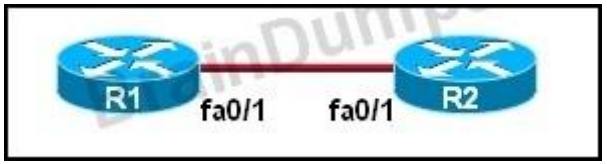
If CDP is enabled on all devices and interfaces, which devices will appear in the output of a show cdp neighbors command issued from R2?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 75
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 76
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

Correct Answer: BC
Section: (none)
Explanation

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

Global values:
Internet Protocol routing is enabled
Serial0/0 is up, line protocol is down
Internet address is 10.1.1.1/30
Serial0/1 is up, line protocol is down
Internet address is 209.65.200.225/30
Serial0/2 is up, line protocol is down
Serial0/3 is up, line protocol is down
NVI0 is up, line protocol is up
Interface is unnumbered. Using address of NVI0 (0.0.0.0)
Loopback0 is up, line protocol is up
Internet address is 10.1.10.1/32
Loopback1 is up, line protocol is up

Internet address is 10.1.2.1/27
Loopback6 is up, line protocol is up

Serial0/0 is up, line protocol is down
Internet address is 10.1.1.1/30
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is disabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Flow switching is disabled
IP CEF switching is disabled
IP Feature Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is enabled, interface in domain inside
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled

QUESTION 77
An administrator is in the process of changing the configuration of a router. What command will allow the administrator to check the changes that

havebeen 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The “show running-config” command displays active configuration in memory.
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 78
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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Both these commands will show the current status of the interfaces, either in show or debug mode both will display the information.

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

The outputs of two commands are shown below:

```
Router1#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.0.0.1/8
  MTU 1500 bytes, BW 512 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes);Total output drops: 0
```

City# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protcocol
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#

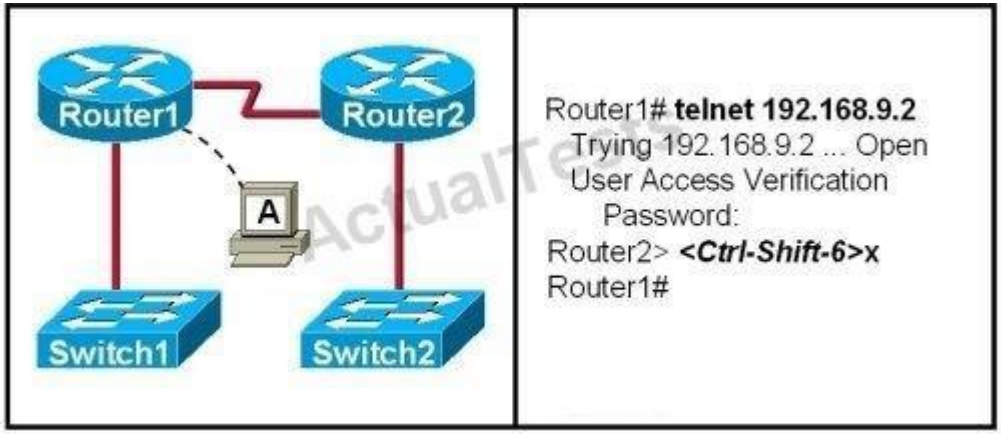
QUESTION 79
Which router command will configure an interface with the IP address 10.10.80.1/19?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
255.255.224 equal /19 in CIDR format hence the answer

QUESTION 80
Refer to the exhibit.



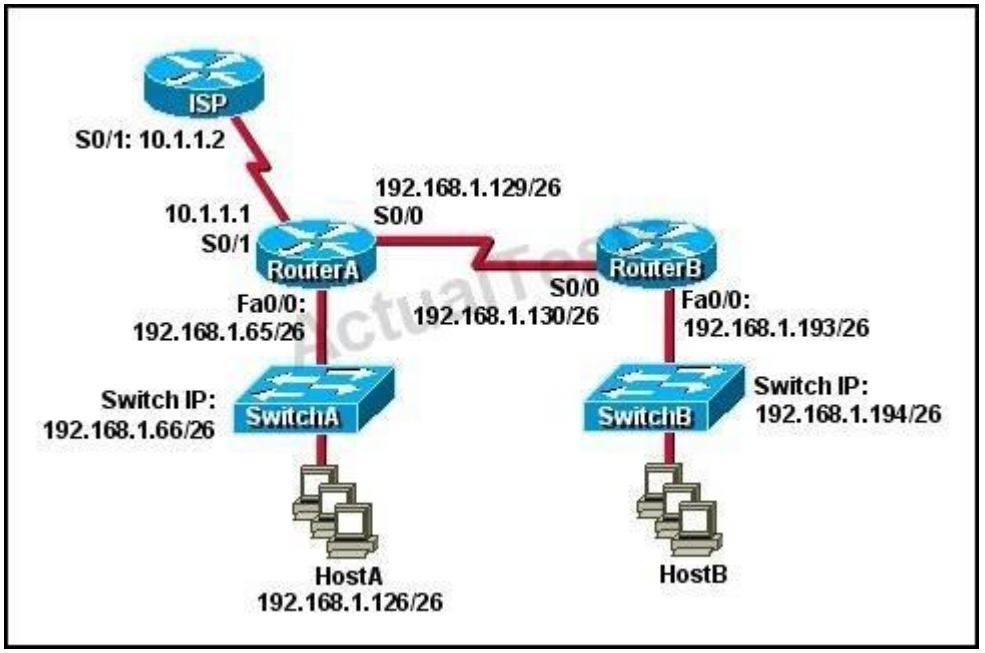
If the resume command is entered after the sequence that is shown in the exhibit, which router prompt will be displayed?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 81
Refer to the exhibit.



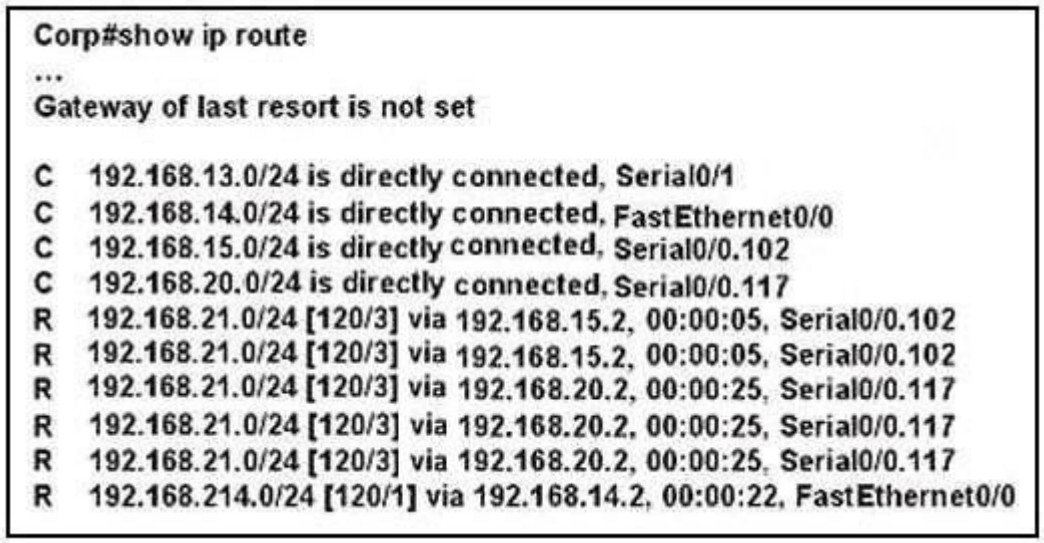
Which default gateway address should be assigned to HostA?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
It should be one less than the switch IP to which it is connected so it will be B.

QUESTION 82
Refer to the output of the corporate router routing table shown in the graphic.



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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 83
What is the default administrative distance of the OSPF routing protocol?

A. 90
B. 100
C. 110
D. 120
E. 130
F. 170

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Default Distance Value Table
This table lists the administrative distance default values of the protocols that Cisco supports:
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.

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

QUESTION 84

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.

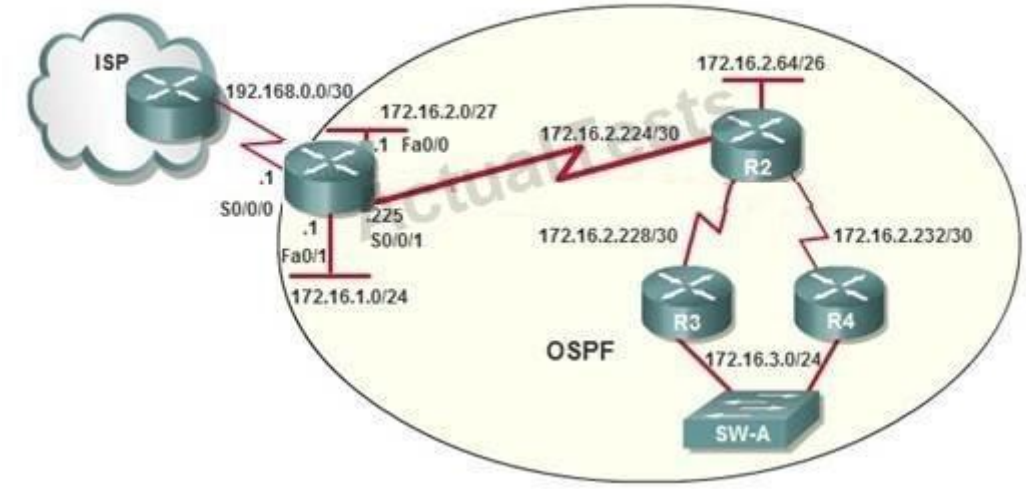
To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by clicking on the Questions button to the left.

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.

Topology



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.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml#t6
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:
Cost = 10000 0000/bandwidth in bps
For example, it will cost 10 EXP8/10 EXP7 = 10 to cross a 10M Ethernet line and will cost 10 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.

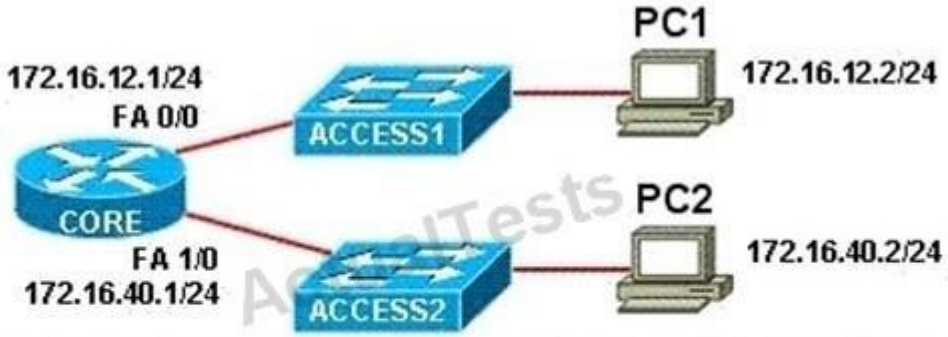
QUESTION 85
Some routers have been configured with default routes. What are some of the advantages of using default routes? (Choose two)

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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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 86
Refer to the exhibit.




```
CORE# show arp
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
CORE#
```

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.

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
The router will forward the frames out the interface toward the destination – B is correct. Since the router will has the end station already in it's MAC table as see 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 87
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 then RIP version 1.
E. It has the same maximum hop count as RIP version 1.
F. It does not send the subnet mask any updates.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
CCNA Question

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 88
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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 89
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
On broadcast multiacess and point-to-point links, the default is 10 seconds. On NBMA, the default is 30 seconds.

Note: non-broadcast multiple access network (NBMA)

QUESTION 90
What does the "Inside Global" address represent in the configuration of NAT?

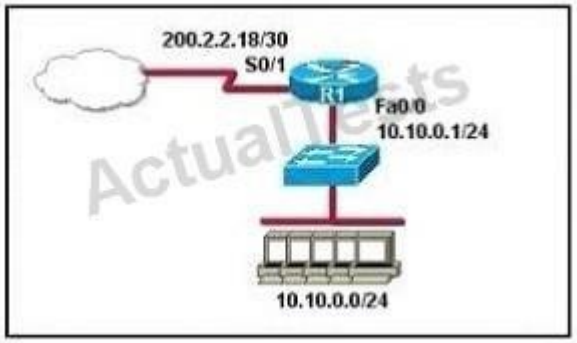
A. the summarized address for all of the internal subnetted addresses
B. the MAC address of the router used by inside hosts to connect to the Internet
C. a globally unique, private IP address assigned to a host on the inside network
D. a registered address that represents an inside host to an outside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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 91
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 serial0/1R1(config-if)# ip nat inside
B. R1(config)# interface serial0/1R1(config-if)# ip nat outside
C. R1(config)# interface fastethernet0/0R1(config-if)# ip nat inside
D. R1(config)# interface fastethernet0/0R1(config-if)# ip nat outside
E. R1(config)# interface serial0/1R1(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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Topic 5, IP Services

QUESTION 92
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Its best to use static addressing scheme where the number of systems is manageable rather than use dynamic protocol as it is easy to operate and manage.

QUESTION 93
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.)

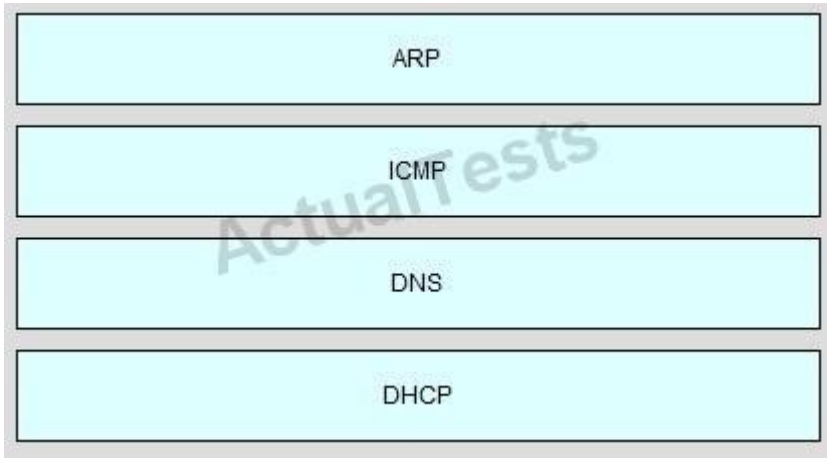
ICMP	A PC sends packets to the default gateway IP address the first time since the PC turned on.
DHCP	The network administrator is checking basic IP connectivity from a workstation to a server.
RARP	The TCP/IP protocol stack must find an IP address for packets destined for a URL.
UDP	A network device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

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

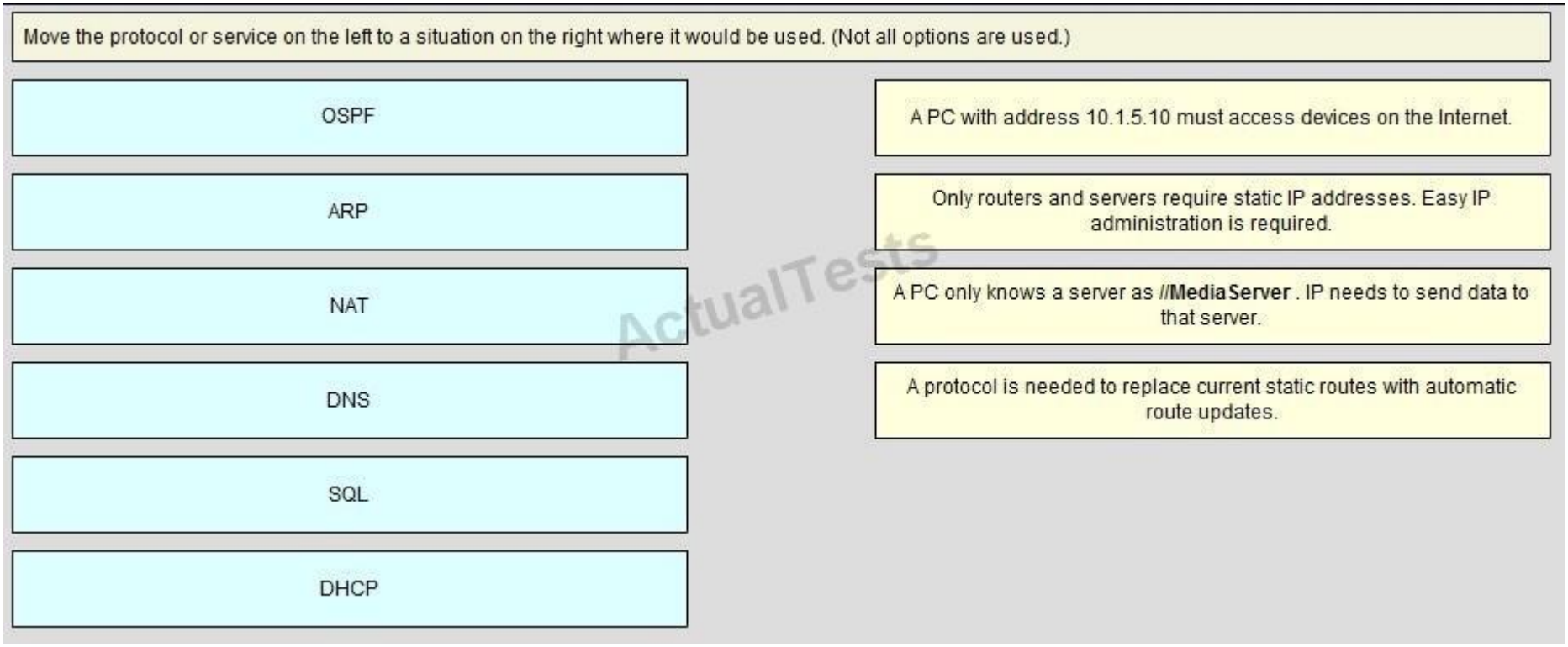
Explanation/Reference:

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.)



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

QUESTION 94
DRAG DROP

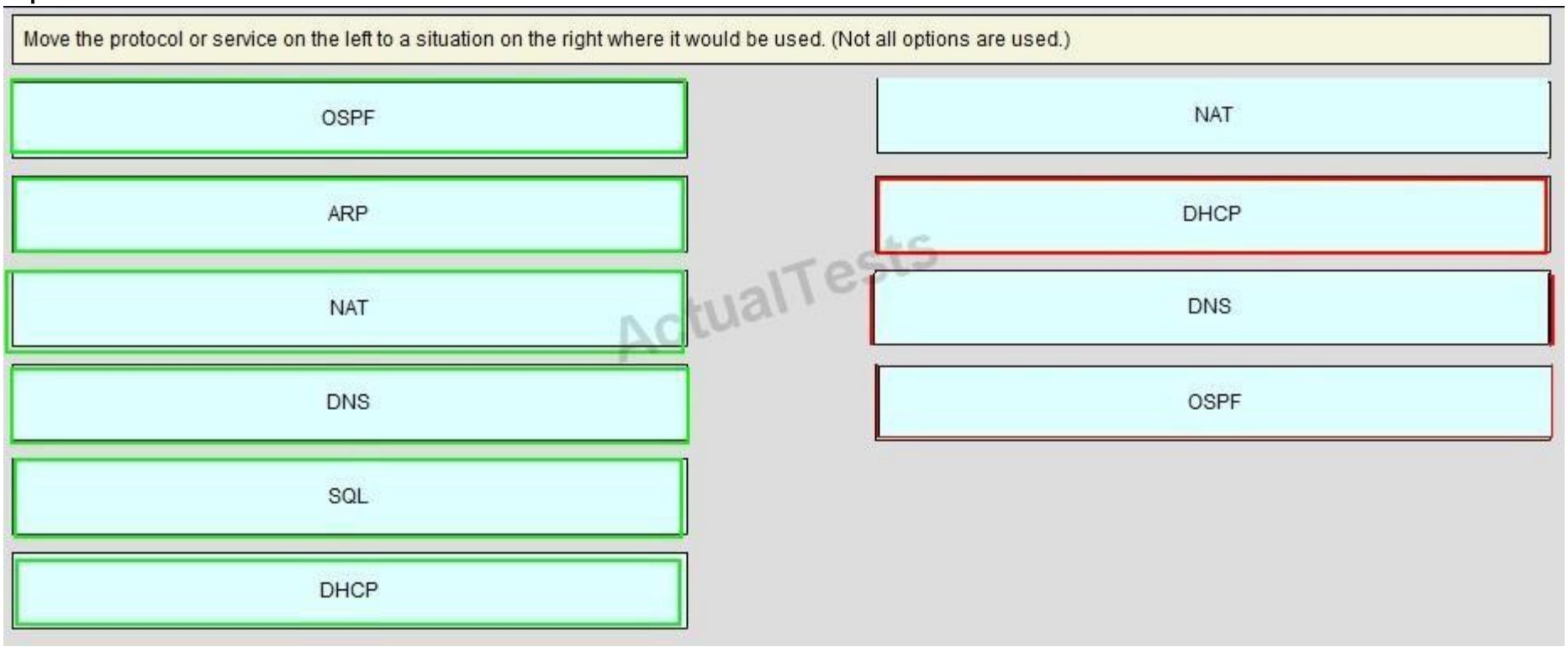


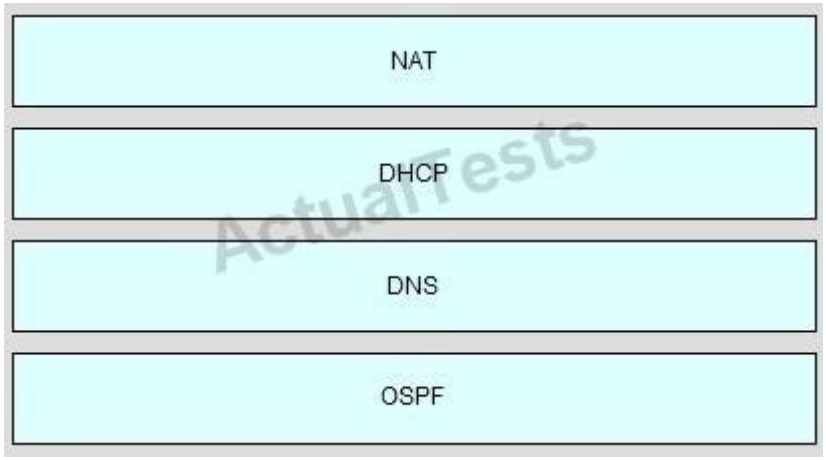
A.
B.
C.
D.

Correct Answer:
Section: (none)

Explanation

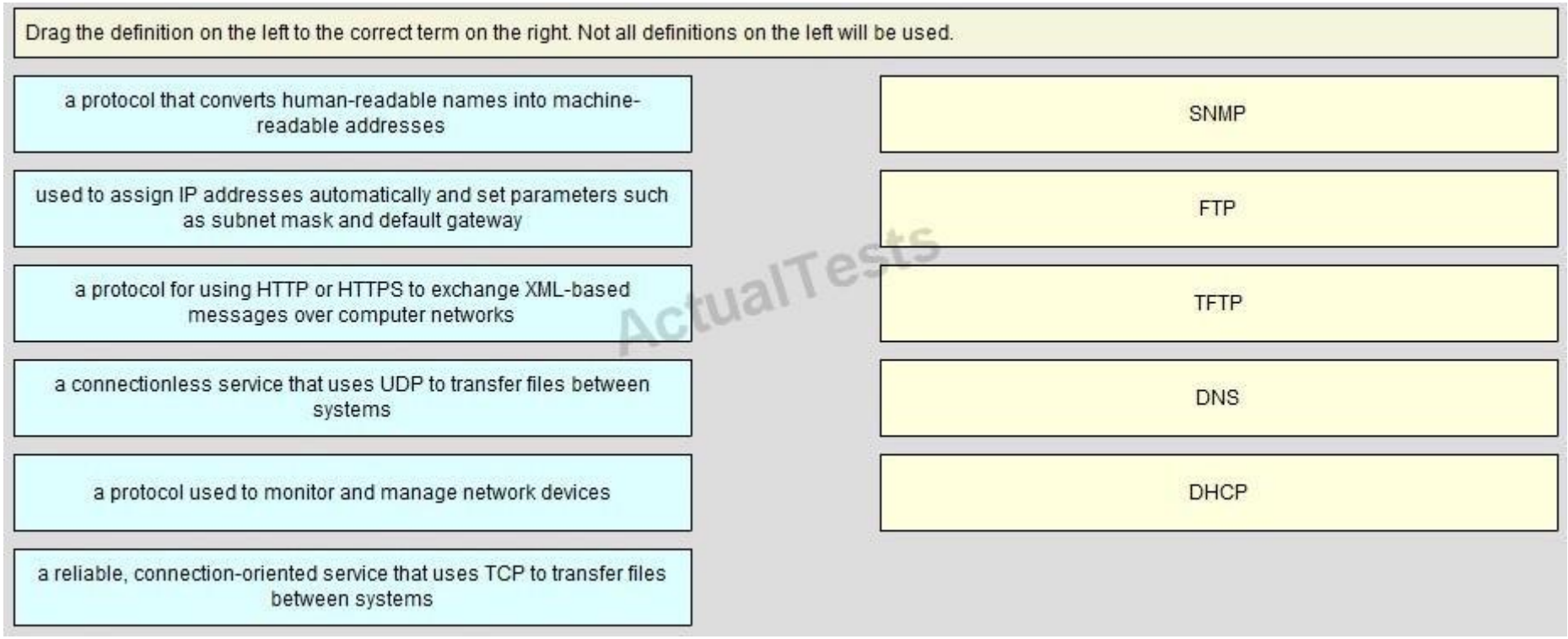
Explanation/Reference:





+ NAT: A PC with address 10.1.5.10 must access devices on the Internet.
+ DHCP: Only routers and servers require static IP addresses. Easy IP administration is required.
+ DNS: A PC only knows a server as MediaServer. IP needs to send data to that server.
+ OSPF: A protocol is needed to replace current static routes with automatic route updates.

QUESTION 95
DRAG DROP



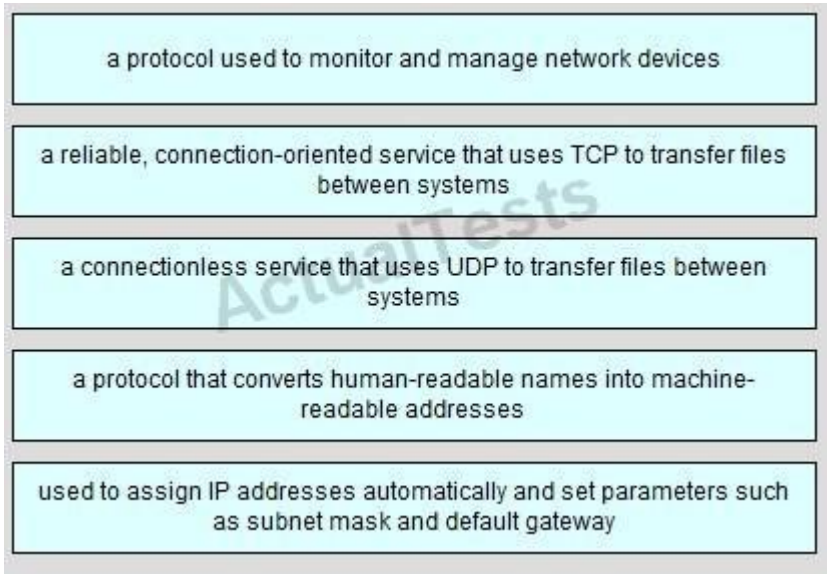
A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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	



+ SNMP: a protocol used to monitor and manage network devices
+ FTP: a reliable, connection-oriented service that uses TCP to transfer files between systems
+ TFTP: a connectionless service that uses UDP to transfer files between systems
+ DNS: a protocol that converts human-readable names into machine-readable addresses
+ DHCP: used to assign IP addresses automatically and set parameters such as subnet mask and default gateway

QUESTION 96
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
http://evilrouters.net/2009/07/09/configuring-basic-nat-with-overloading/
Overloading (having multiple clients all NAT'd to the same IP address) is probably the most common implementation (especially for those of us who run

NAT on a Cisco box at home!).

The keyword “overload” specifies we are using NAT Overload (PAT) in which multiple internal hosts will use only one IP address to access external network resources.

QUESTION 97
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Port Address Translation (PAT) can support thousands of users connect to the Internet using only one real global IP address. With PAT, each computer will be assigned a separate port number so that the router can identify which computer should receive the return traffic.

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 98
When configuring NAT, the Internet interface is considered to be what?

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Network address translation or NAT requires the Internet to be considered as an outside interface else it won't serve the purpose it intends to.

On the interface connecting to the Internet of the router we have to use the command "ip nat outside" for NAT to work. It identifies that interface as the outside interface.

QUESTION 99
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
http://cisconet.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.

QUESTION 100
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

Correct Answer: CE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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".
Hope this helps.

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 102
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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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

Topic 6, Network Device Security

QUESTION 103
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
Route r1(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

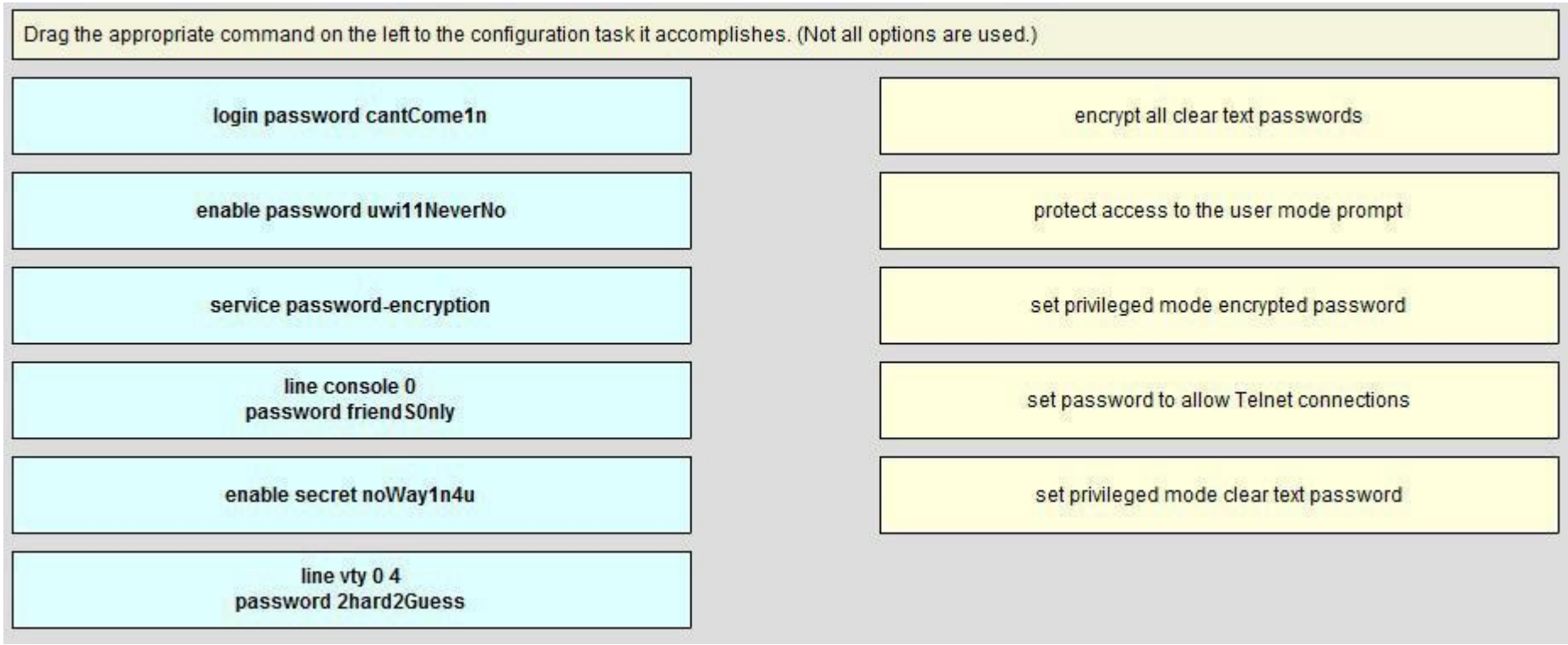
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The enable secret password takes precedence over the enable password, so sanfran will be used.

In the configuration above we have three passwords:
+ The "enable secret" password: sanfran
+ The "enable password" password: cisco
+ The VTY line password: sanjose
The two first "enable secret" and "enable password" are used to set password for entering privilege mode (an example of privilege mode: Router#). Both of them will be stored in the running configuration. But the password in "enable secret" command is always encrypted using MD5 hash while the password in "enable password" is in plain text.
Note: If you want to encrypt "enable password" you can use the command "service password- encryption" but it will be encrypted with a very basic form of encryption called vigenere cipher, which is very weak.
When you configure both an enable and a secret password, the secret password will be used -> B is correct.

QUESTION 104
DRAG DROP

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



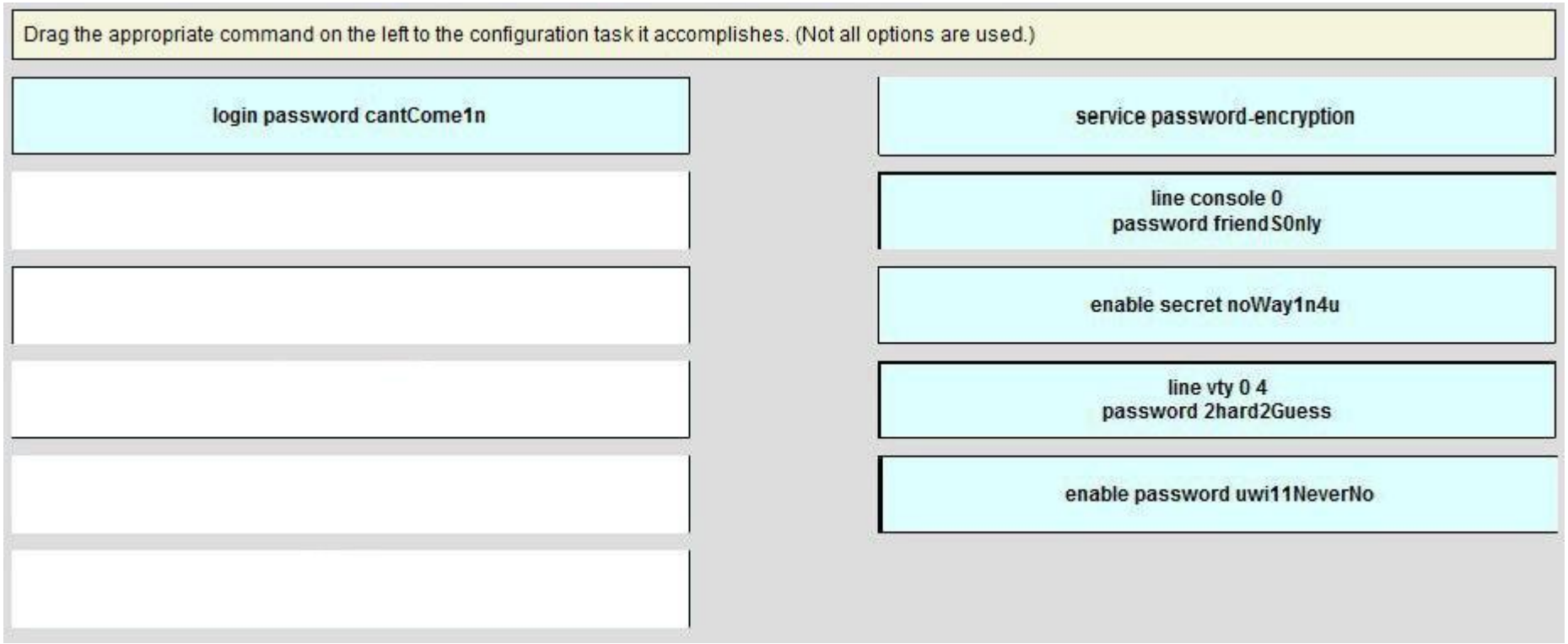
A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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

login password cantCome1n	service password-encryption
enable password uwi11NeverNo	line console 0 password friendS0nly
service password-encryption	enable secret noWay1n4u
line console 0 password friendS0nly	line vty 0 4 password 2hard2Guess
enable secret noWay1n4u	enable password uwi11NeverNo
line vty 0 4 password 2hard2Guess	



service password-encryption: encrypt all clear text passwords
line console 0 password friendS0nly: protect access to the user mode prompt
enable secret noWay1n4u set privileged mode encrypted password
line vty 0 4 password 2hard2Guess: Set password to allow Telnet connections
enable password uwi11NeverNo set privileged mode clear text password

QUESTION 105
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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 106
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.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
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 107
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

Port security with sticky MAC addresses provides many of the same benefits as port security with static MAC addresses, but sticky MAC addresses can be learned dynamically. Port security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down condition.

If you enter a write memory or copy running-config startup-config command, then port security with sticky MAC addresses saves dynamically learned MAC addresses in the startup-config file and the port does not have to learn addresses from ingress traffic after bootup or a restart.

QUESTION 108
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. Forthe 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.

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:
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.

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html

SUMMARY STEPS

1. config t
2. mac address-table static mac address vlan vlan-id {[drop | interface {type number | | port-channel number]}
3. exit
4. show mac address-table static
5. copy running-config startup-config

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/layer2/configuration/guide/nexus1000v_layer2/l2_2mac.html#wp1052857

QUESTION 109
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 110
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
When the MAC address is configured as static entry, no other address is allowed.

QUESTION 111
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

SUMMARY STEPS

1. config t
2. mac address-table static mac address vlan vlan-id {[drop | interface {type number | | port-channel number]}
3. exit
4. show mac address-table static
5. copy running-config startup-config

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/layer2/configuration/guide/nexus1000v_layer2/l2_2mac.html#wp1052857

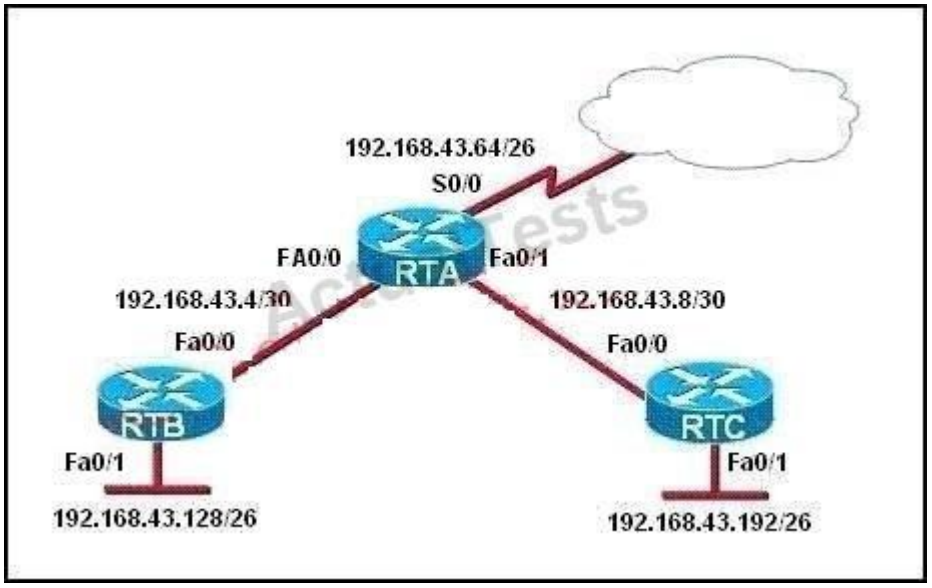
QUESTION 113
What are two recommended ways of protecting network device configuration files from outside network security threats? (Choose two.)

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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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 s0/0RTA(config-if)#no cdp run
D. RTA(config)#interface s0/0RTA(config-if)#no cdp enable

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/tech/tk962/technologies_tech_note09186a00801aa000.shtml#topicen ab
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   Holdtme    Capability   Platform   Port ID
R2-AGS       Ser 1             129          R         2500       Ser 0
R6-2500      Eth 0             144          R         4000       Eth 0
Router#
```

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 115
From which of the following attacks can Message Authentication Code (MAC) shield your network?

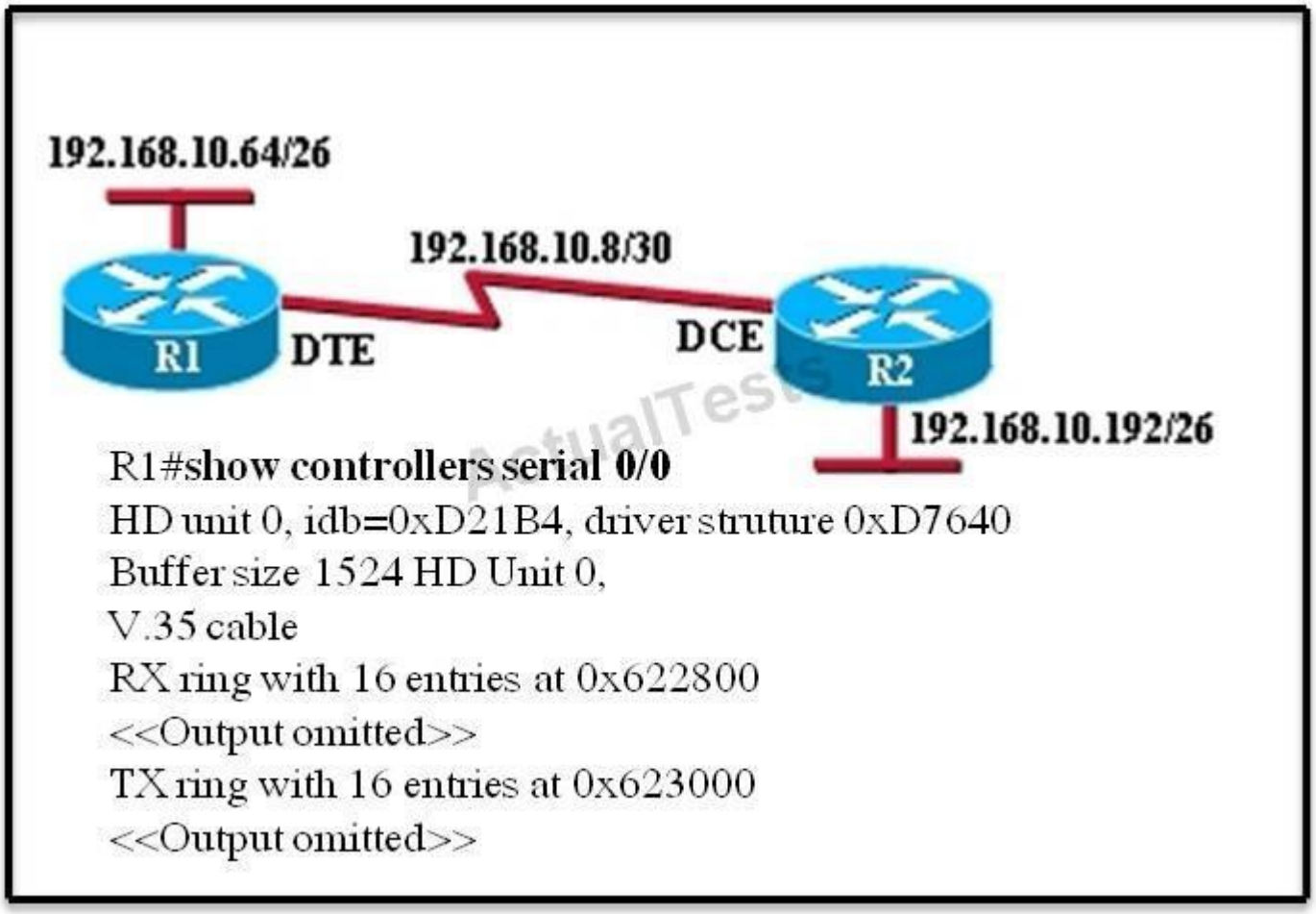
A. DoS
B. DDoS
C. spoofing
D. SYN floods

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Message Authentication Code (MAC) can shield your network from spoofing attacks.
Spoofing, also known as masquerading, is a popular trick in whichan 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 dataintegrity 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 generatesa flood of packets requesting a TCP connection with the target, tying up all resources and making the target unable to service other requests. MAC doesnot 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 thetarget 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 ofa 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 116
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
http://www.thebryantadvantage.com/CCNACertificationExamTutorialDirectlyConnectedSerialInterf aces.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.

The output above is unclear. Normally when we use this command we can see the type of serial connection on this interface, for example “V.35 DCE cable. Below is an example of the same command as above:

RouterA#show controllers serial 0
HD unit 0, idb = 0xECA4C, driver structure at 0xF1EC8
buffer size 1524 HD unit 0, V.35 DTE cable
cpb = 0x62, eda = 0x403C, cda = 0x4050
RX ring with 16 entries at 0x624000
00 bd_ptr=0x4000 pak=0x0F5704 ds=0x62FFB8 status=80 pak_size=22

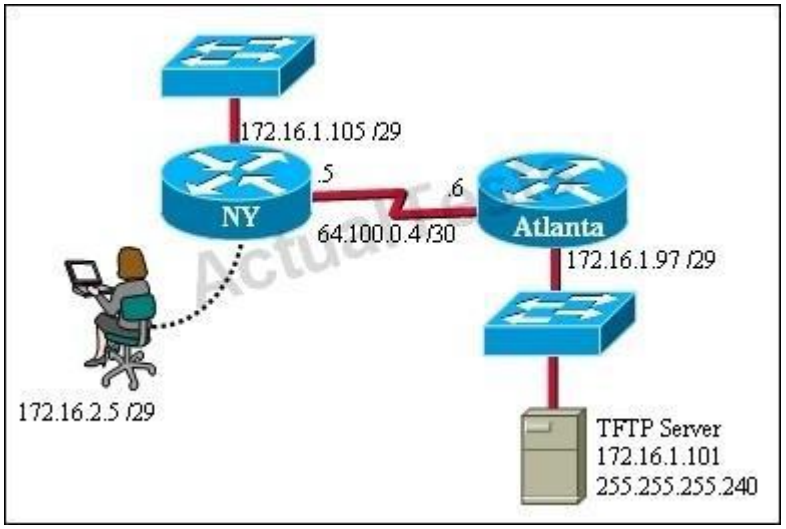
Or

RouterB#show controllers serial 0
buffer size 1524 HD unit 0, V.35 DCE cable, clockrate 64000
cpb = 0x62, eda = 0x408C, cda = 0x40A0
RX ring with 16 entries at 0x624000
00 bd_ptr=0x4000 pak=0x0F2F04 ds=0x627908 status=80 pak_size=22

but in this case we only get “V.35 cable”. So in fact we are not sure about the answer C. But the output above also does not have any information to confirm other answers are correct or not.

Just for your information, the V.35 male and V.35 female cable are shown below:

QUESTION 117
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The subnet mast of the TFTP server needs to be in tune with the other network requirements else it won't be possible.

QUESTION 118
If a host experiences intermittent issues that relate to congestion within a network while remaining connected, what could cause congestion on this LAN?

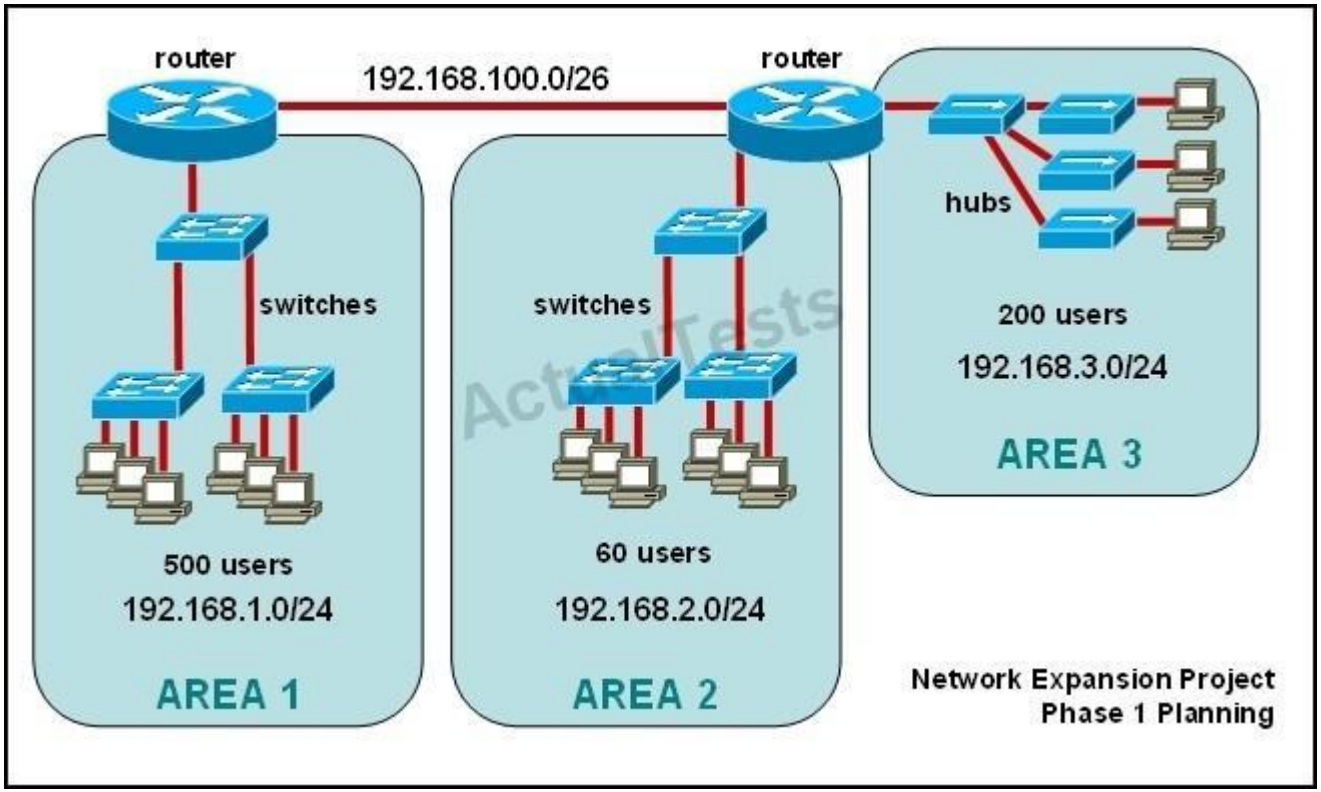
A. half-duplex operation
B. broadcast storms
C. network segmentation

D. multicasting

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 119
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

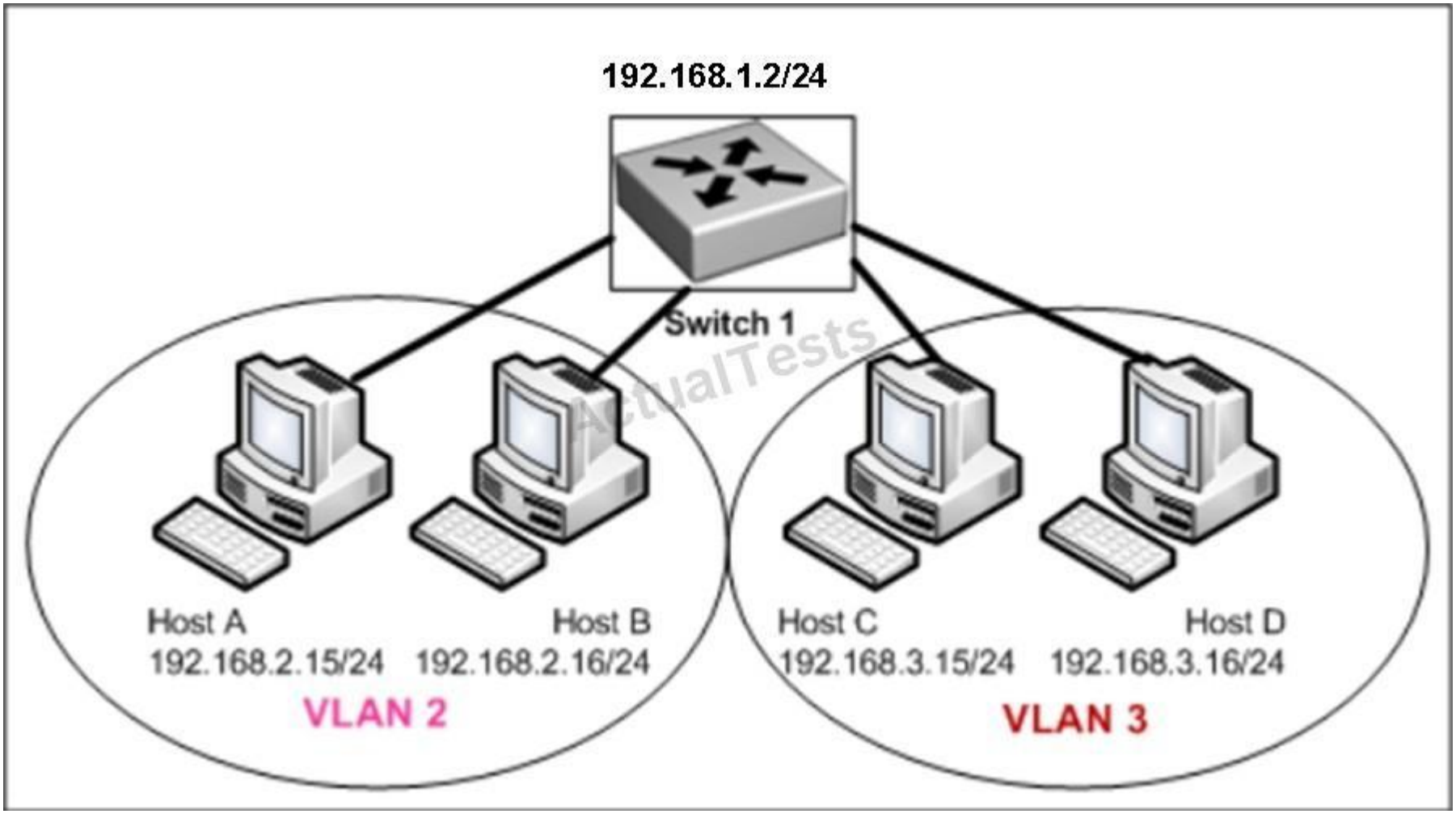
What are three problems with this design? (Choose three.)

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.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
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 120
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.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Two VLANs require a router in between otherwise they cannot communicate through a simple switch mechanism

QUESTION 121
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
```

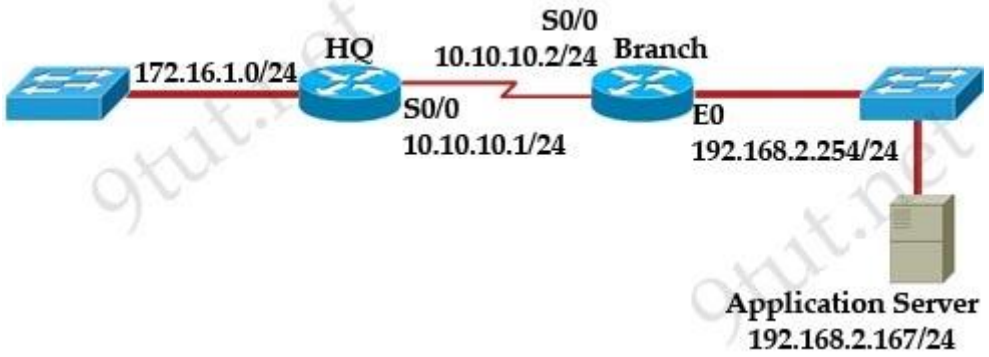
A network administrator has configured a Catalyst 2950 switch for remote management by pasting into the console the configuration commands that areshown in the exhibit. However, a Telnet session cannot be successfully established from a remote host. What should be done to fix this problem?

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The default gateway for remote session is 192.168.17.241 and not the one given in the exhibit.

QUESTION 122
Refer to the exhibit.



Branch# ping 192.168.2.167
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.167, timeout is 2 seconds: ..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/2/4 ms

Branch# ping 192.168.2.167
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.167, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Branch#

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Before a host can send ICMP (ping) packets to another device, it needs to learn the MAC address of the destination device so it first sends out an ARP Request. In fact, the first ping packet is dropped because the router cannot create a complete packet without learning the destination MAC address.

QUESTION 123

Instructions

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

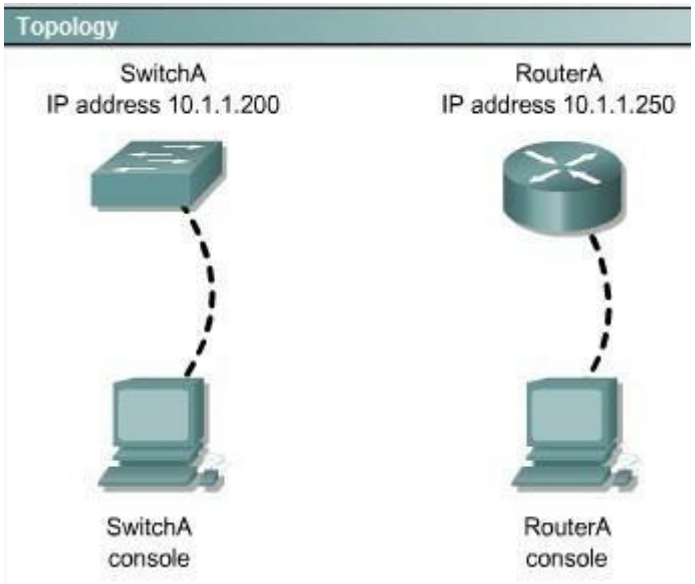
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

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.



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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
This answer can be done by simulation only, don't know user name password and banner message etc

QUESTION 124

Instructions

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

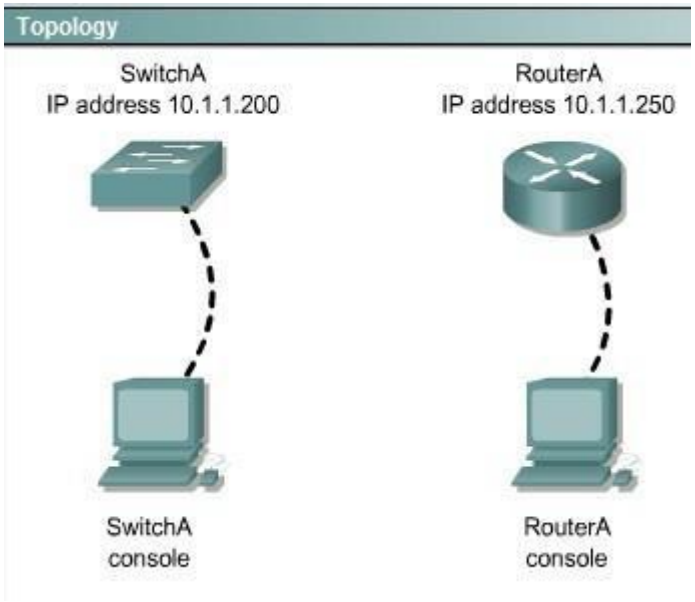
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

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.



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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
This answer can be done by simulation only, don't know user name password and banner message etc
Which two of the following are true regarding the configuration of RouterA? (Choose two.)

Instructions

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

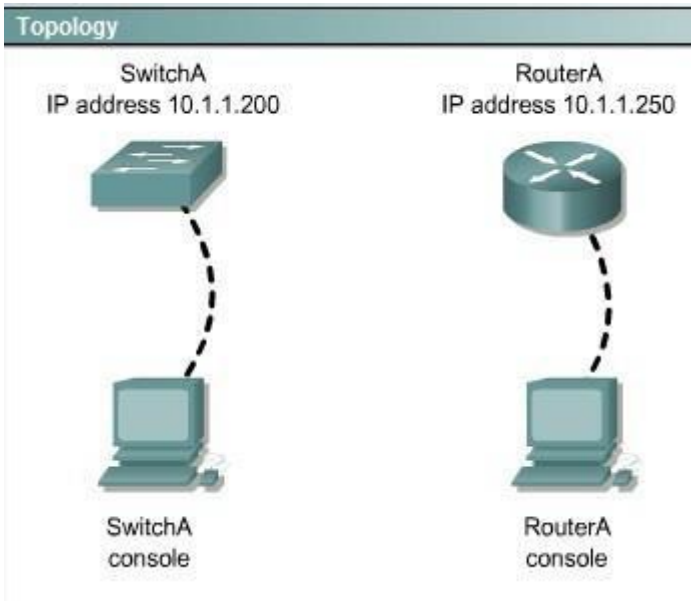
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

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.



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 nevertime out due to inactivity
E. Since DHCP is not used on Fa0/1 there is not a need to use the NAT protocol

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
The IP address can accommodate 5 hosts at least, telnet can be accessed on the router

QUESTION 126

Instructions

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

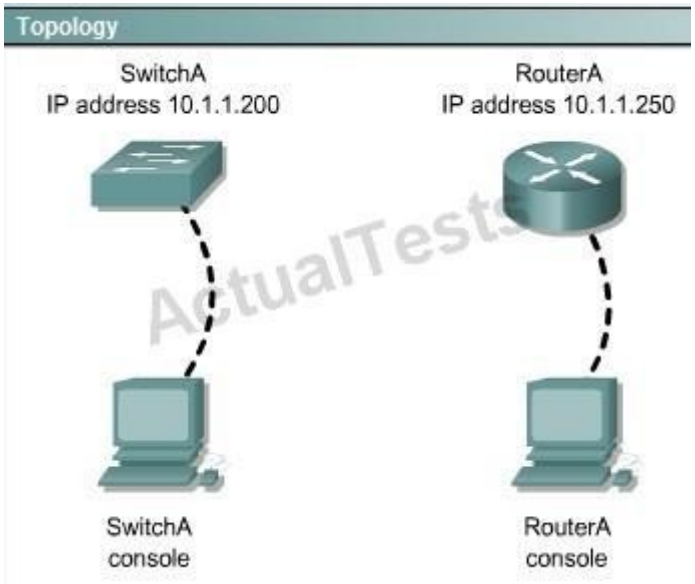
RouterA and SwitchA have been configured to operate in a private network which will connect to the Internet. You have been asked to review the configuration prior to cabling and implementation.

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.



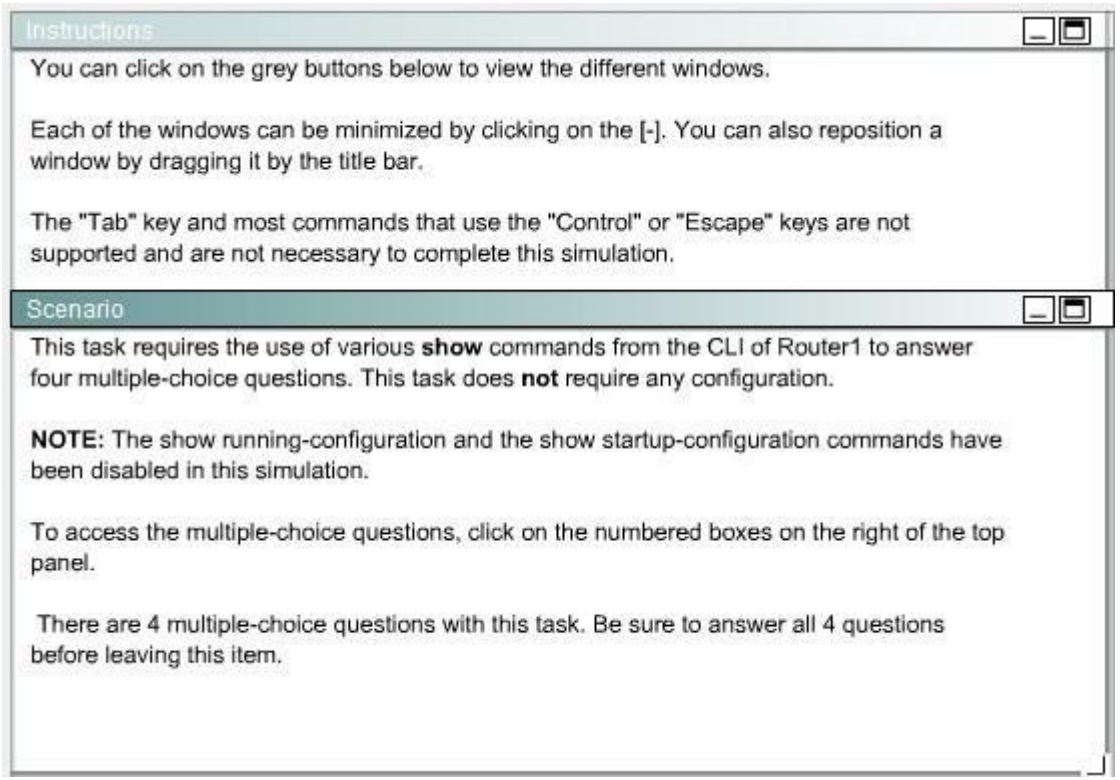
Which of the following is true regarding the configuration of SwitchA?

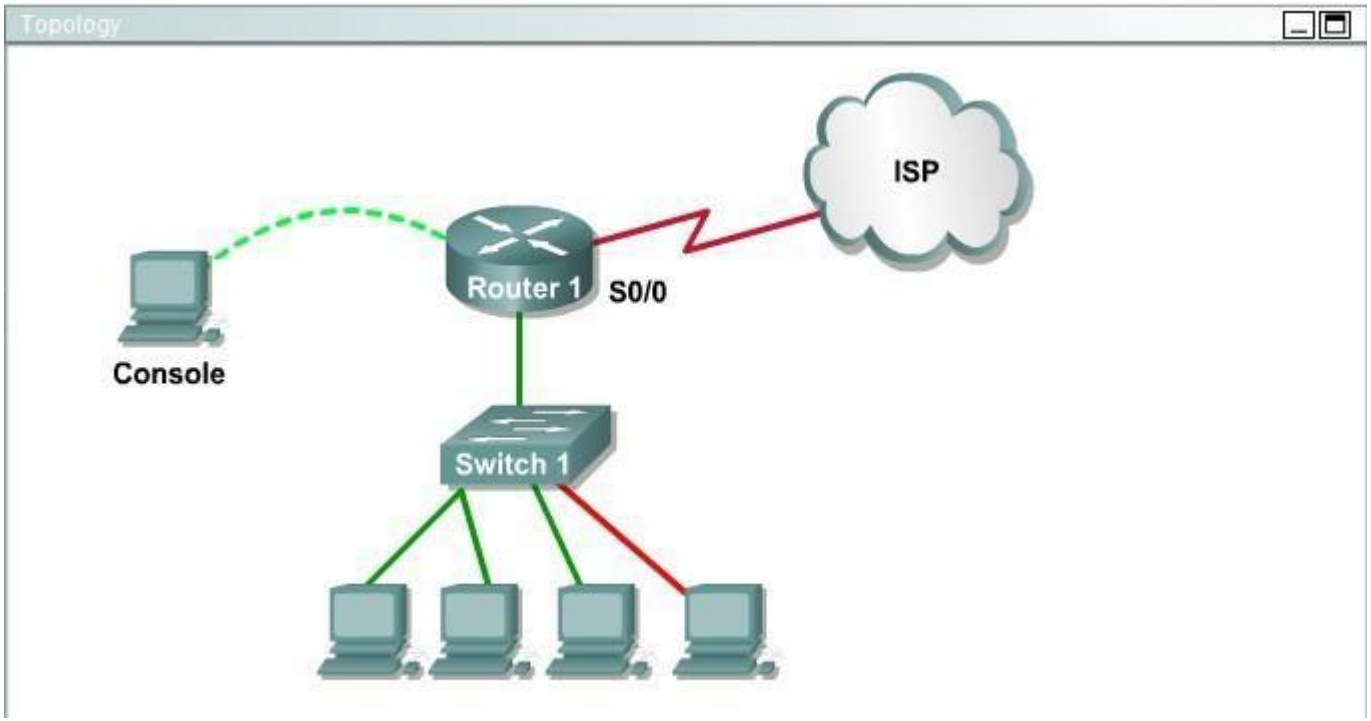
A. only 5 simultaneous remote connections are possible
B. remote connections using ssh will require a username and password
C. only connections from the local network will be possible
D. console access to SwitchA requires a password

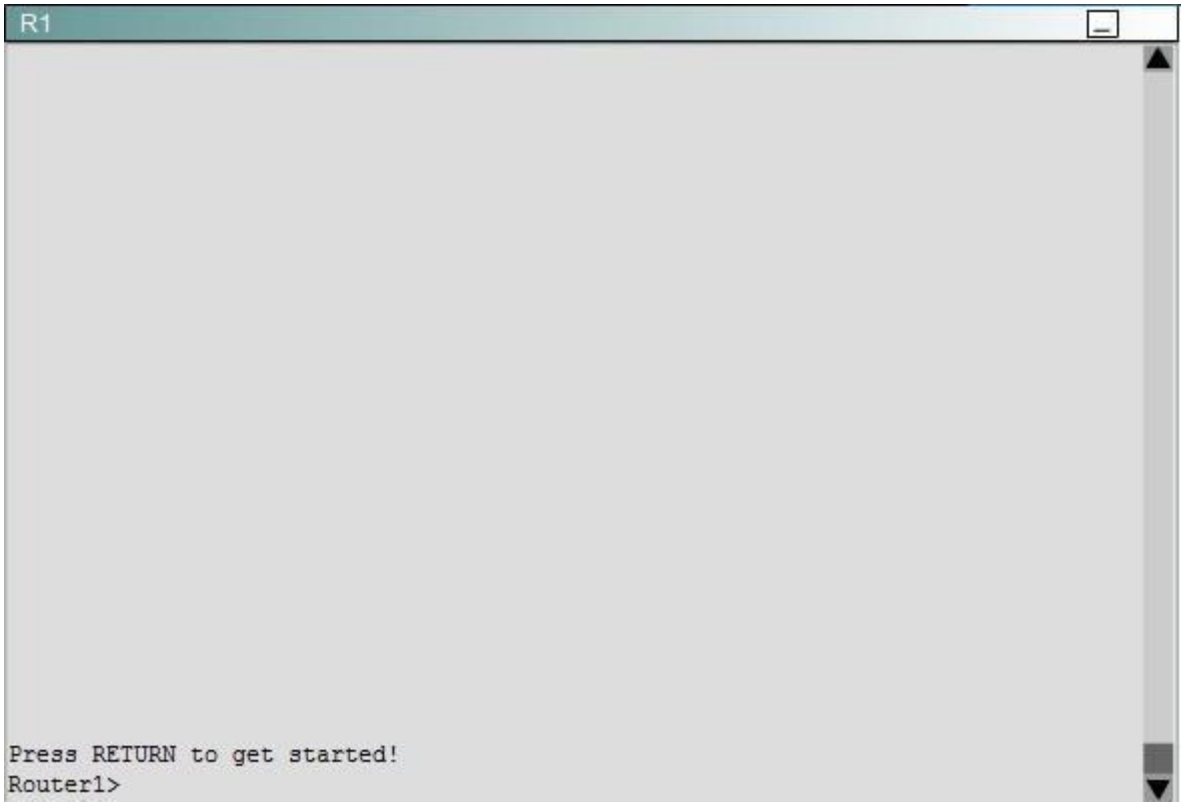
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Ssh login requires a user name and password always while other conditions may or may not be true.

QUESTION 127







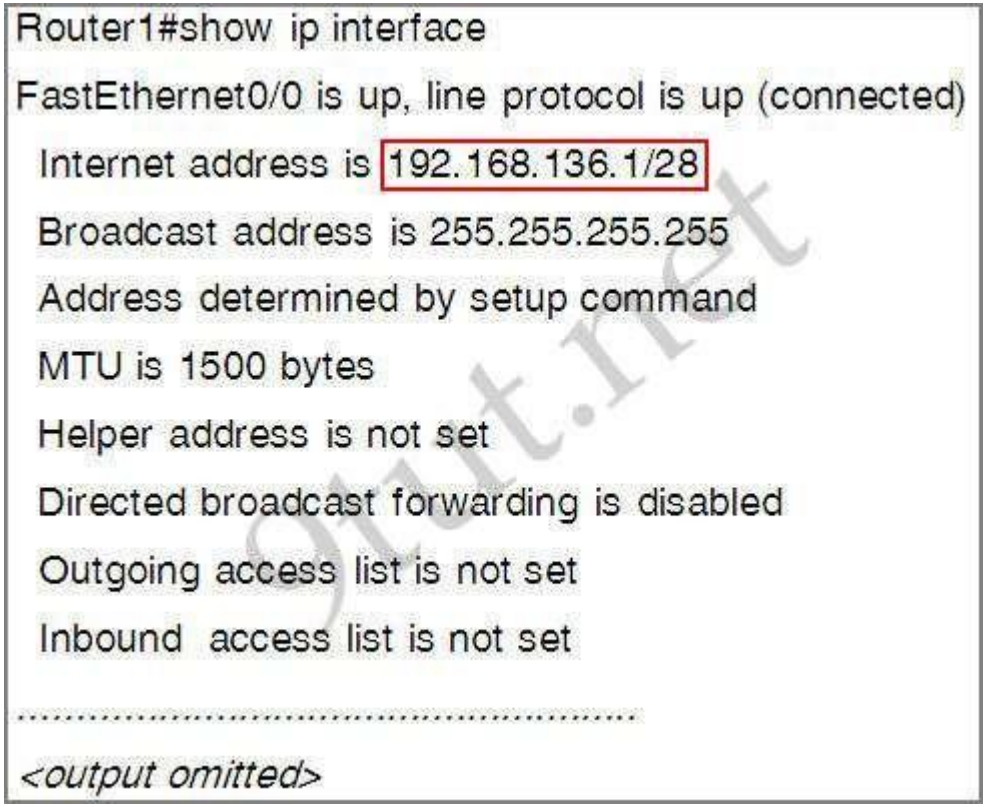
What is the subnet broadcast address of the LAN connected to Router1?

A. 192.168.136.15
B. 192.168.136.31
C. 192.168.136.63
D. 192.168.136.127

Correct Answer: A
Section: (none)
Explanation

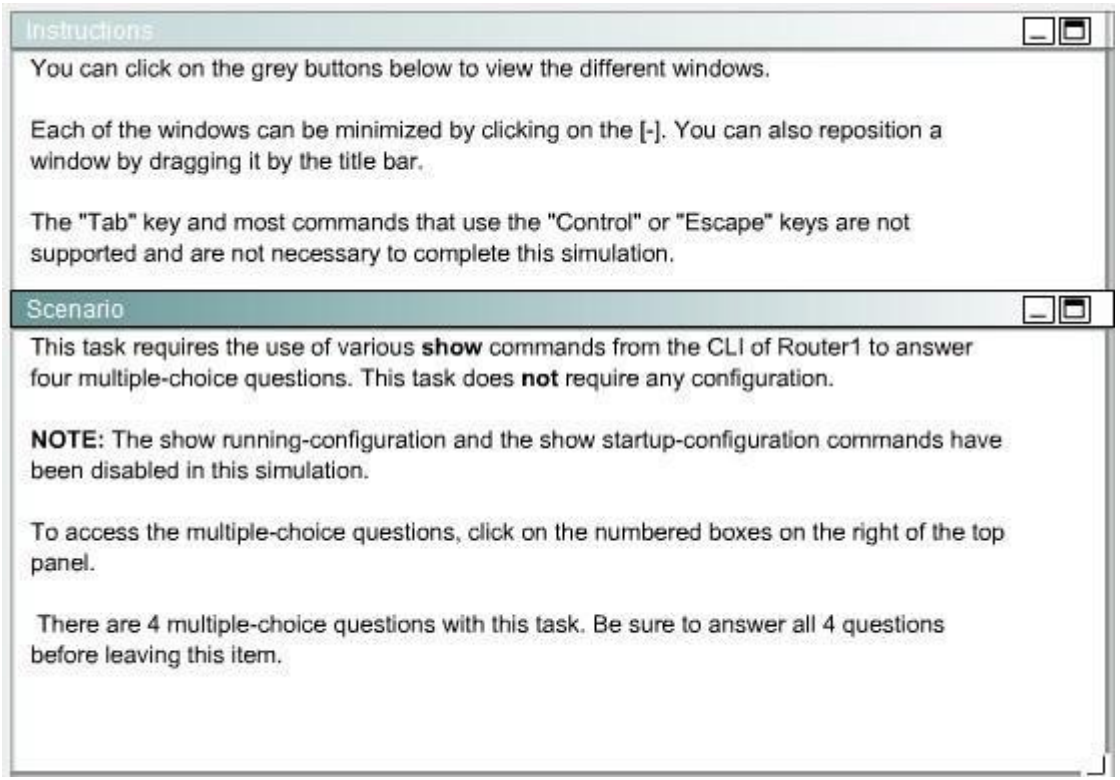
Explanation/Reference:
The "show running-configuration" and "show startup-configuration" have been disabled as stated above so we should use the **show ip interface** command to get information about the LAN network connected to Router1.

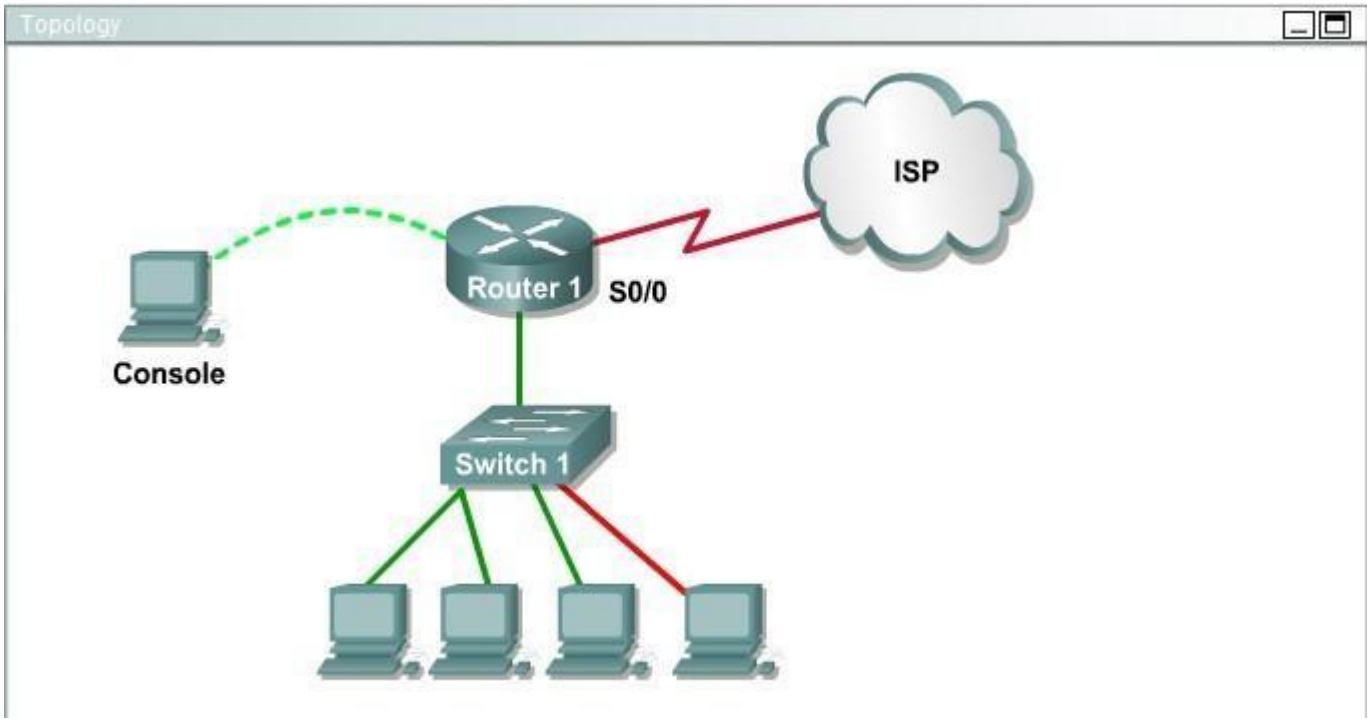
The IP address assigned to FA0/1 is 192.168.136.9/28, making 192.168.136.15 the broadcast address.

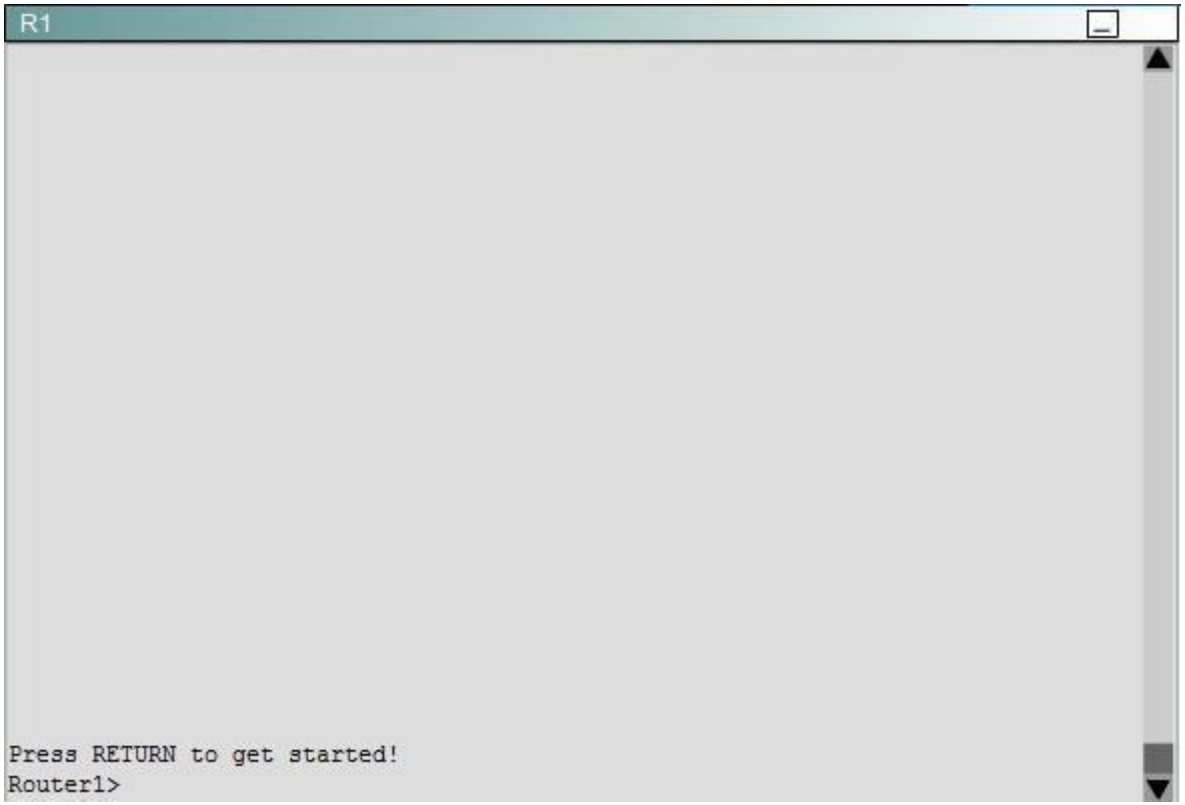


From the output we learn that the ip address of the FastEthernet interface of Router1 is 192.168.136.1 and the subnet mask is /28. Therefore:
Increment: 16 (/28=1111 1111.1111 1111.1111 1111.1111 0000) Network address: 192.168.136.0
Broadcast address: 192.168.136.15 (15 = 0 + 16 - 1)
-> The broadcast address of this subnetwork is 192.168.136.15

QUESTION 128







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

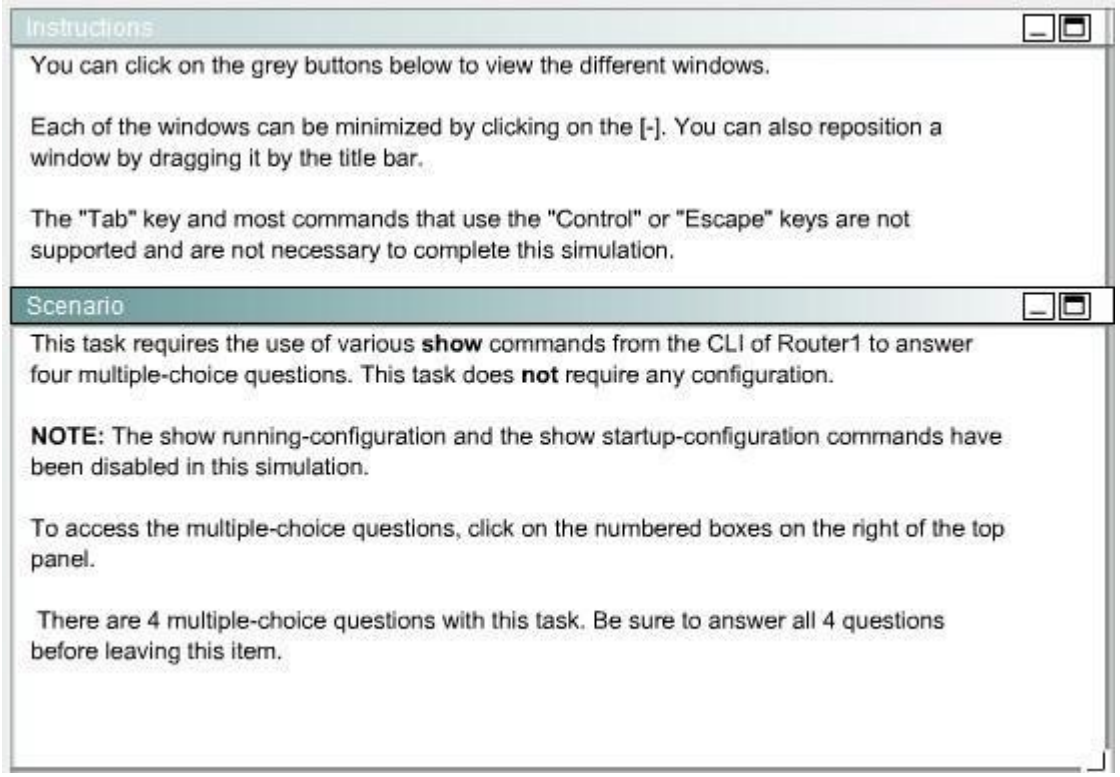
Correct Answer: A
Section: (none)
Explanation

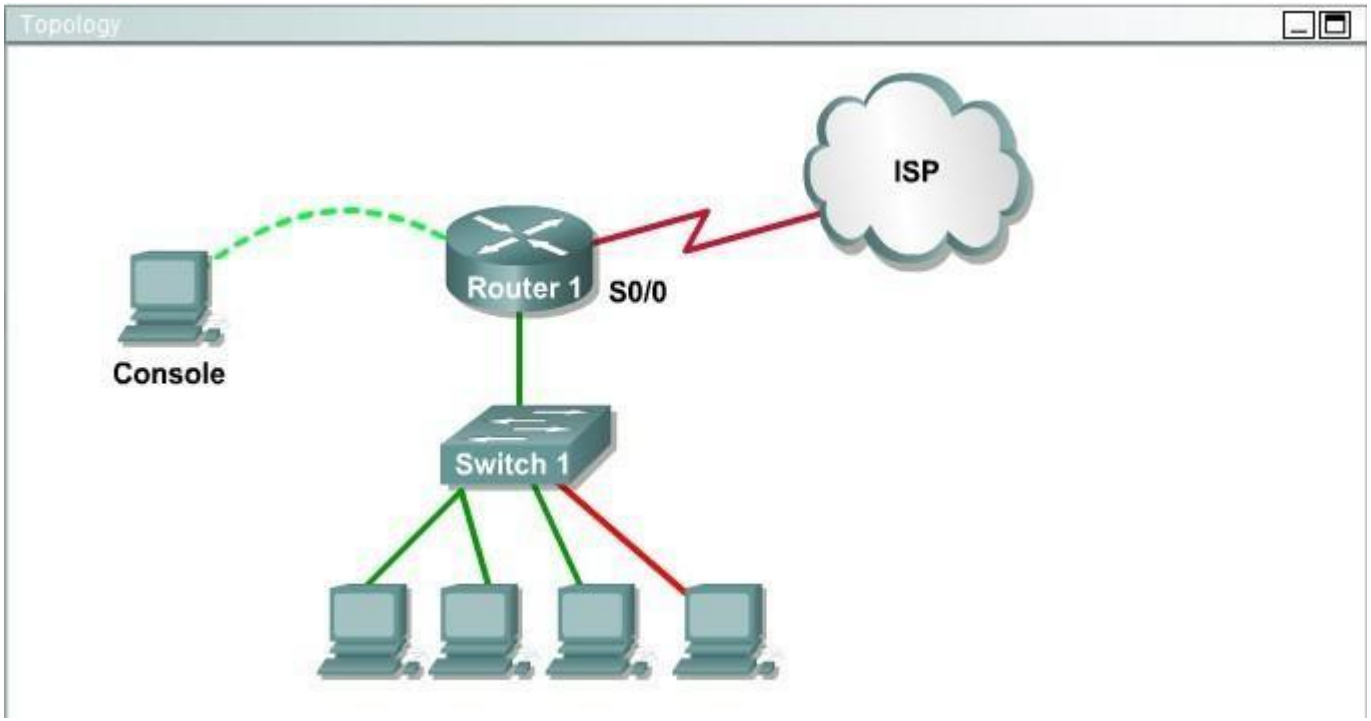
Explanation/Reference:

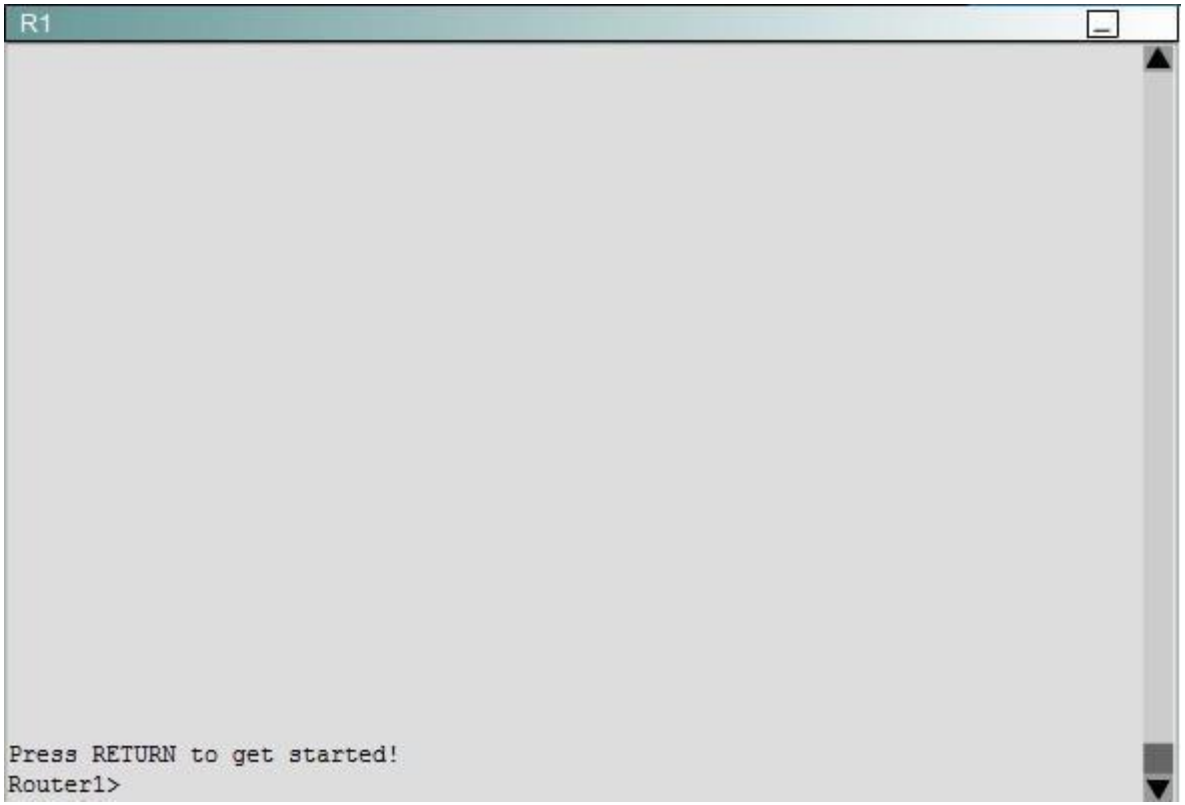
The "show running-configuration" and "show startup-configuration" have been disabled as stated above so we should use the show ip interface command to get information about the LAN network connected to Router1.

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 129







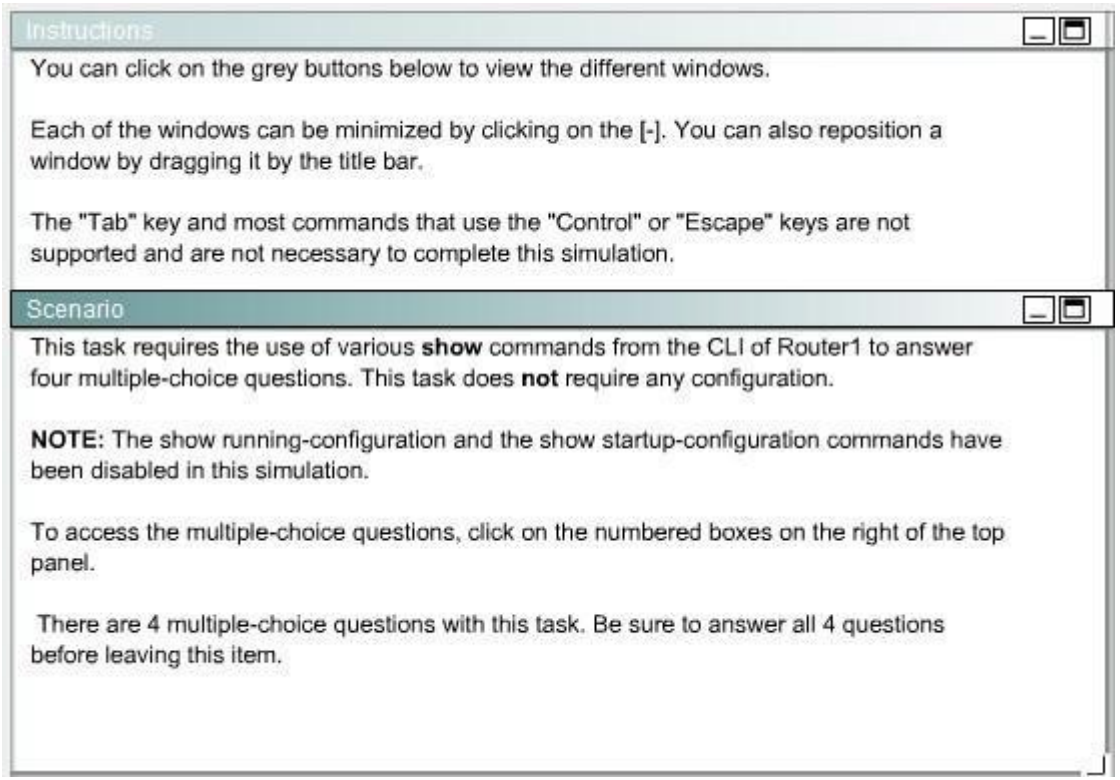
Including the address on the Routed Ethernet interface, how many hosts can have IP addresses on the LAN to which Routed is connected?

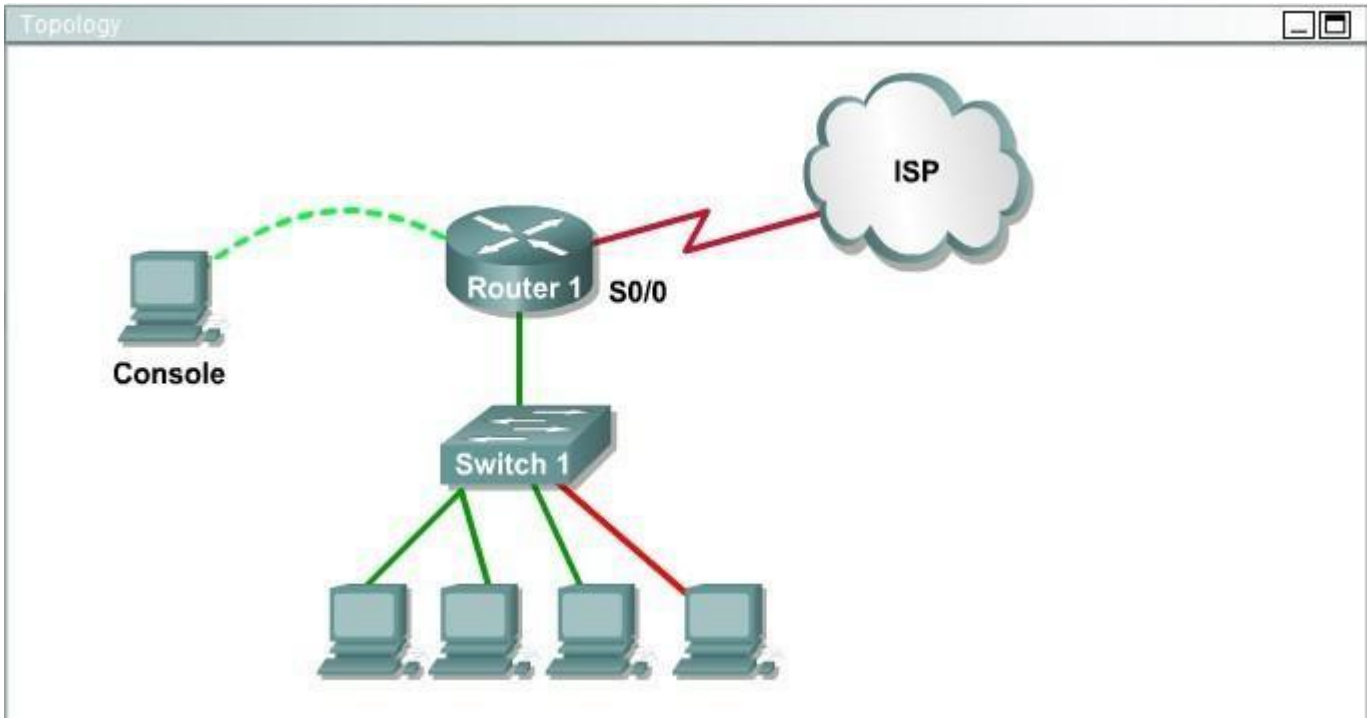
A. 6
B. 30
C. 62
D. 126

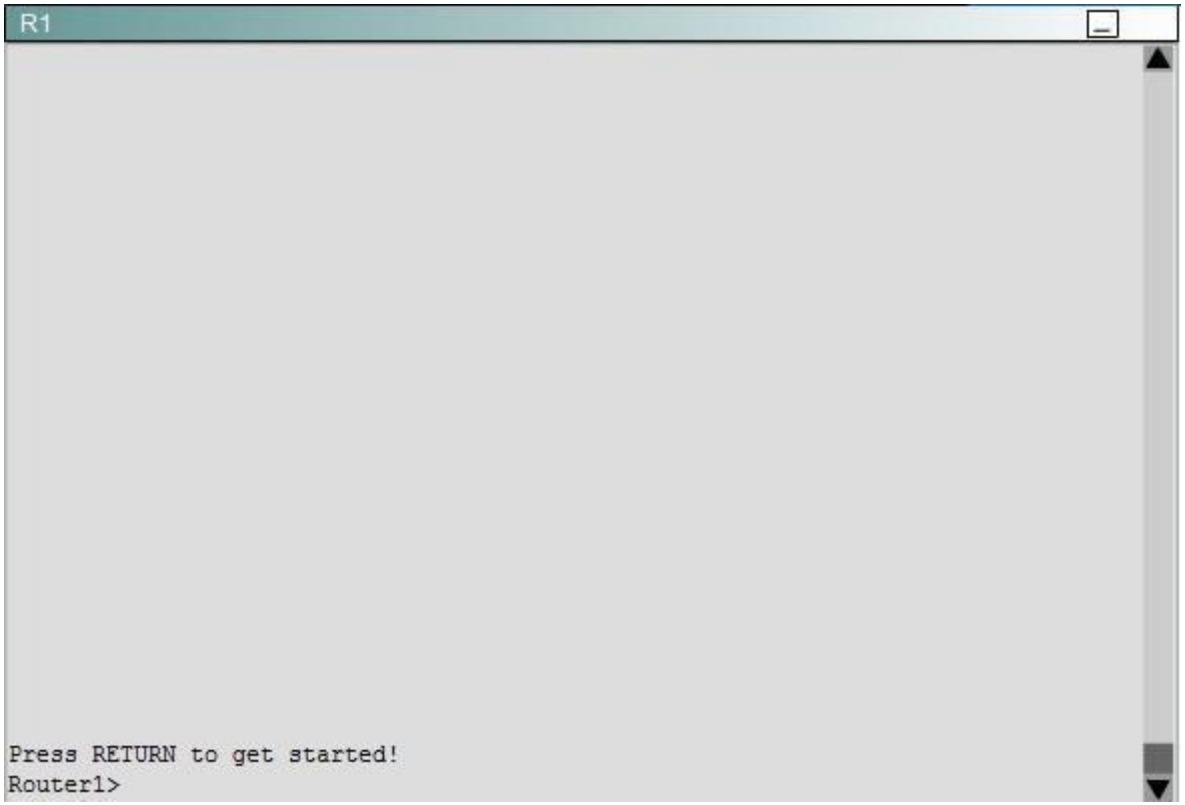
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
This is a /29 address, so there are 6 usable IP's on this subnet.

QUESTION 130







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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Do a "show ip int brief" and you will see that Fa0/1 has an IP address assigned, but it is shut down.

QUESTION 131
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
```

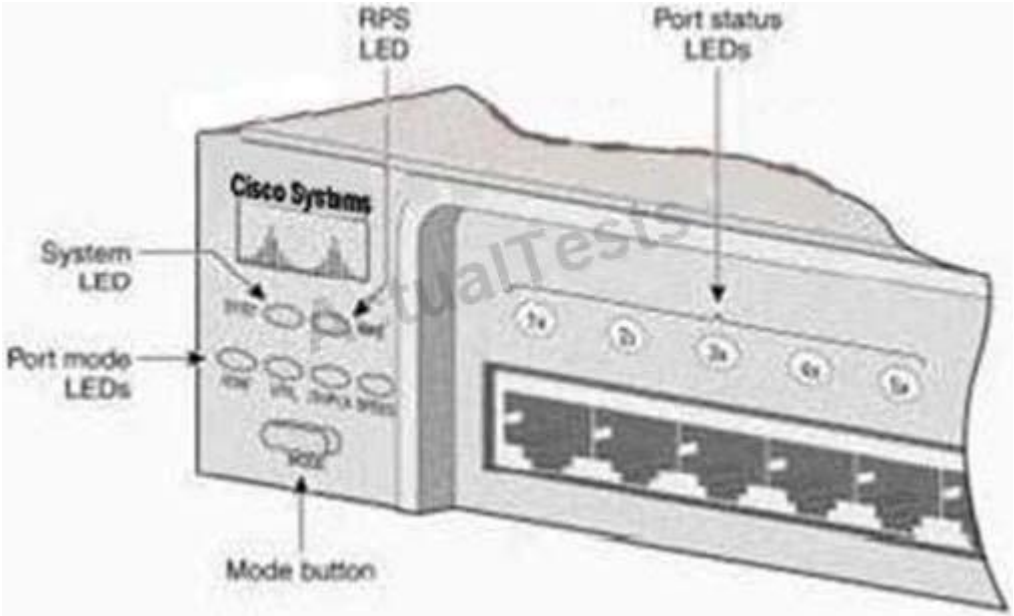
The remote networks 172.16.10.0, 172.16.20.0, and 172.16.30.0 are accessed through the Central router's serial 0/0 interface. No users are able to access 172.16.20.0. After reviewing the command output shown in the graphic, what is the most likely cause of the problem?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
Note. 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 133
Refer to the exhibit.

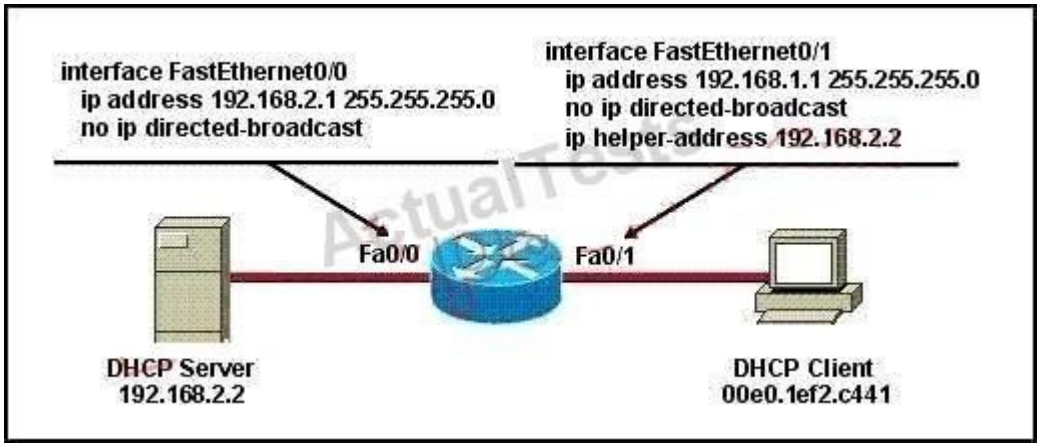
Why did the device return this message?

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer D is correct because when you type the incomplete command having more same more command same up to types characters it shows display the ambiguous command error.

QUESTION 134
Refer to the exhibit.



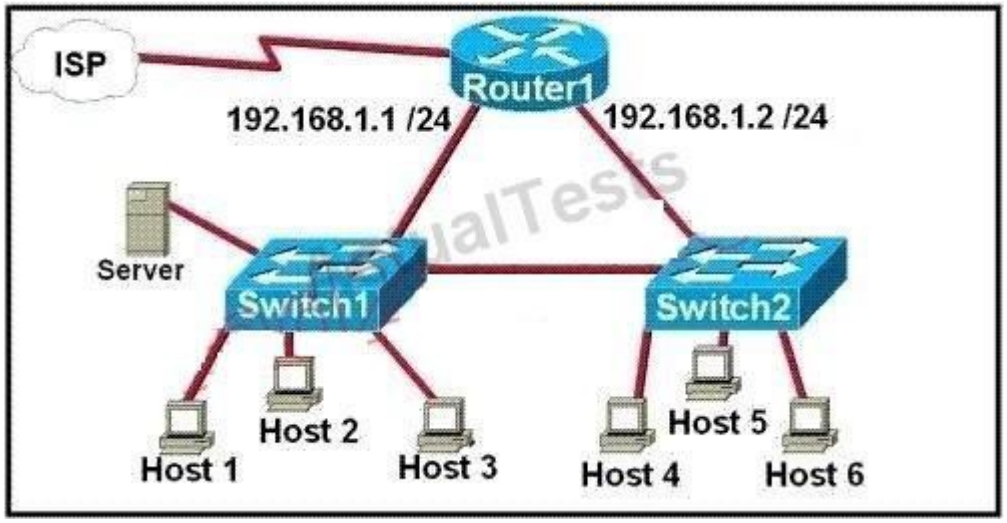
The DHCP settings have recently been changed on the DHCP server and the client is no longer able to reach network resources. What should be done to correct this situation?

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.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The proposed addressing scheme is on the same network.

QUESTION 136
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>
```

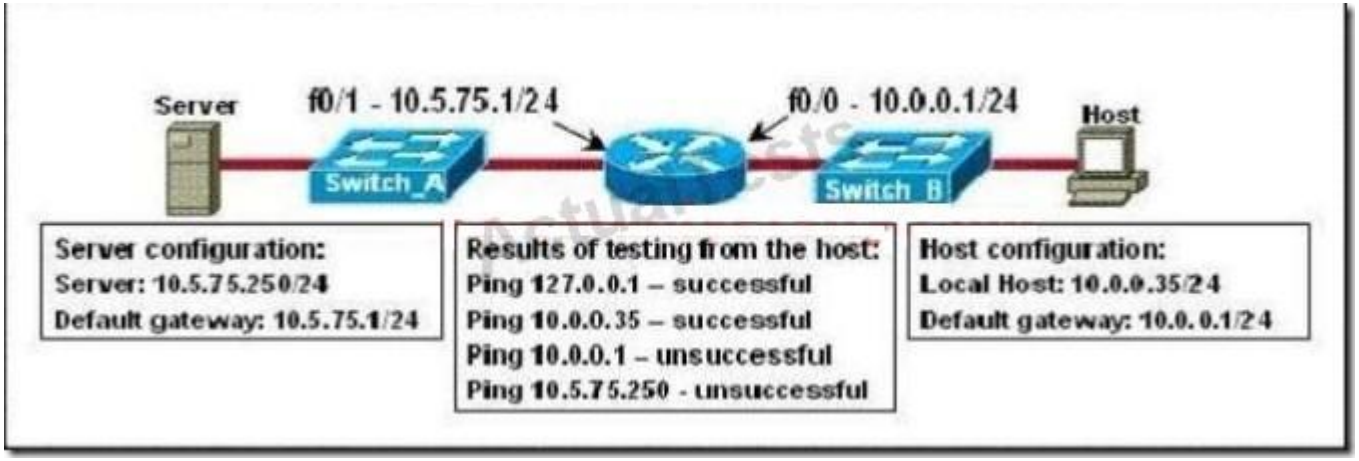
An administrator replaced the 10/100 Mb NIC in a desktop PC with a 1 Gb NIC and now the PC will not connect to the network. The administrator began troubleshooting on the switch. Using the switch output shown, what is the cause of the problem?

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Refer to the exhibit.



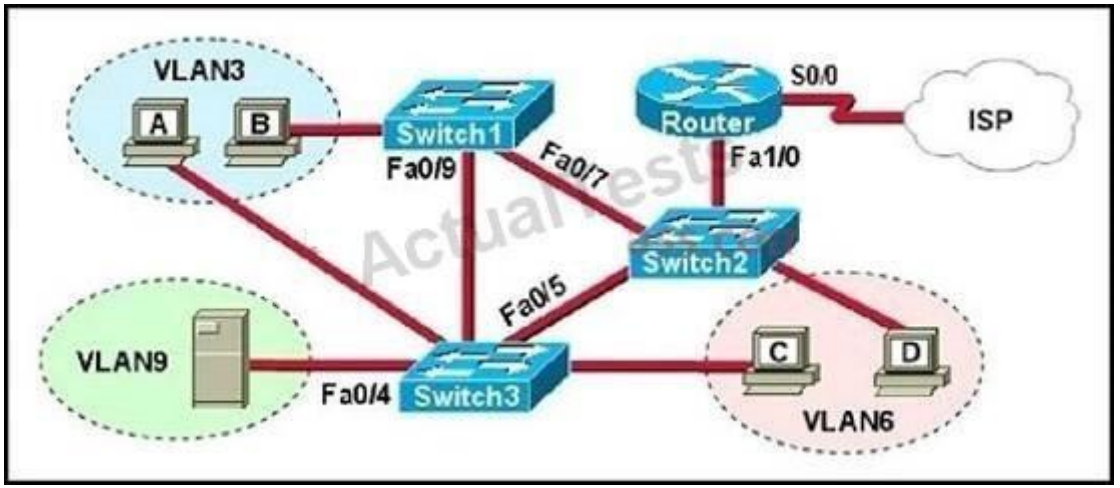
A technician is troubleshooting a host connectivity problem. The host is unable to ping a server connected to Switch_A. Based on the results of the testing, what could be the problem?

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

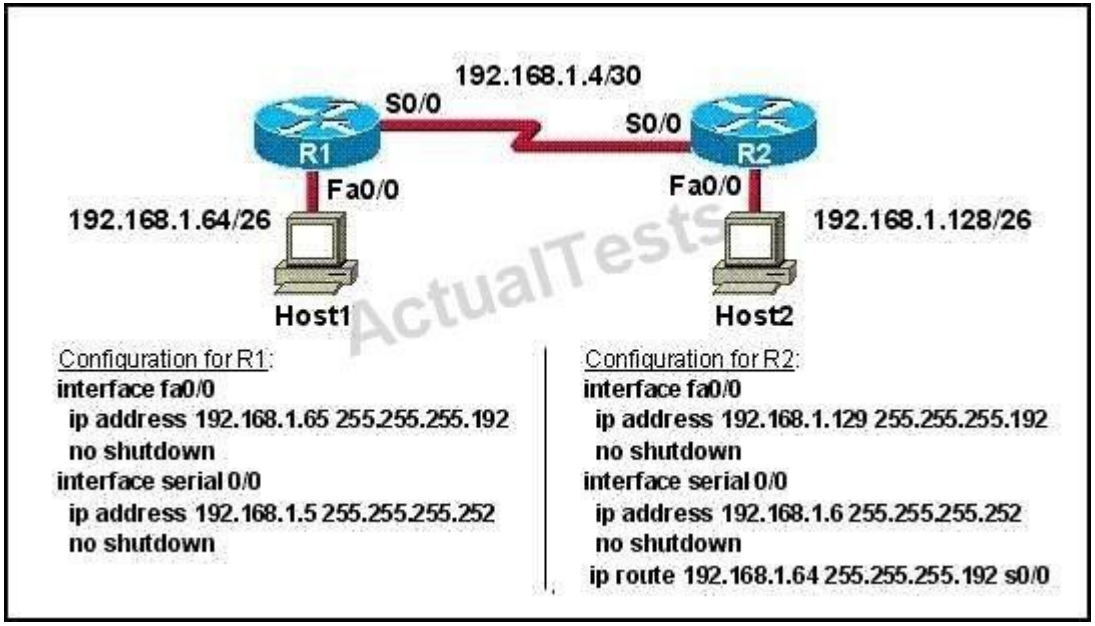
QUESTION 139
A receiving host has failed to receive all of the segments that it should acknowledge. What can the host do to improve the reliability of this communication session?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Without a static route pointing to host 2 network the router is unaware of the path to take to reach that network and reply traffic cannot be sent.

QUESTION 141
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Serial 0/0 interface is administratively down therefore, you will have to run the "no shutdown" command to enable the interface for data.

QUESTION 142
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
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
```

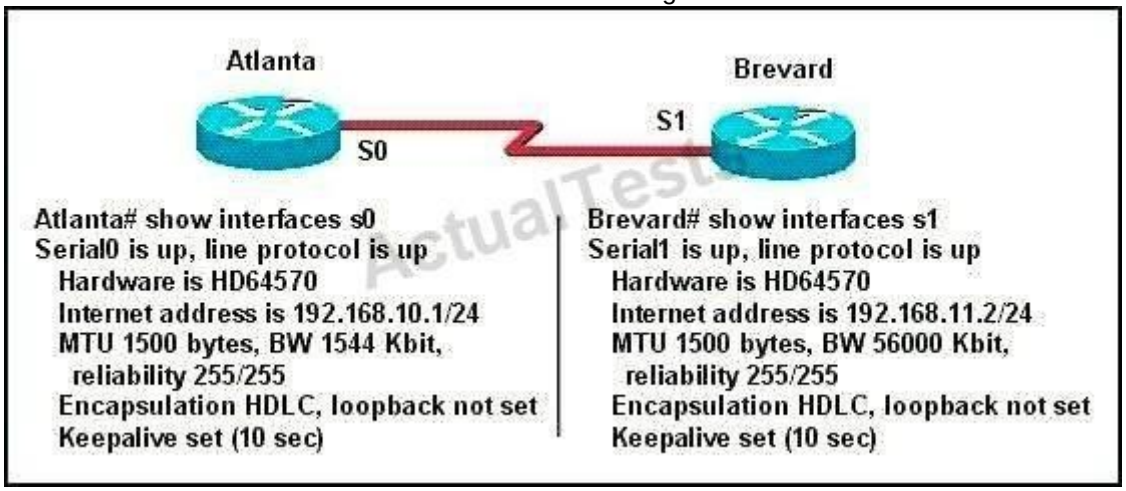
After configuring two interfaces on the HQ router, the network administrator notices an error message. What must be done to fix this error?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Topic 8, OSPF Questions

QUESTION 145
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

Correct Answer: A
Section: (none)
Explanation

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

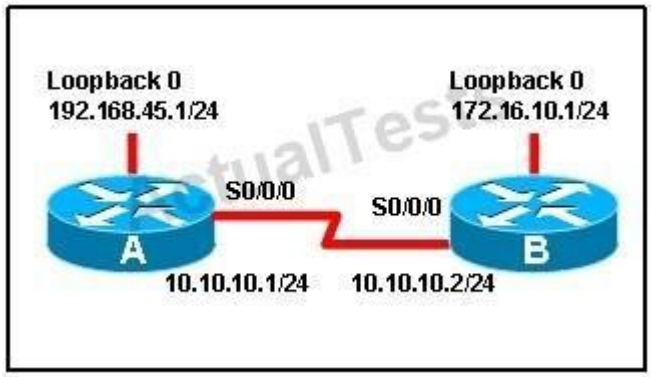
QUESTION 146
Why do large OSPF networks use a hierarchical design? (Choose three.)

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
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 147
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.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 148
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

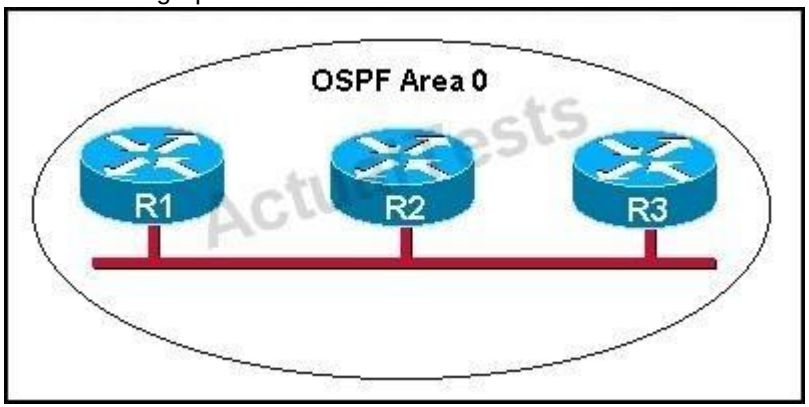
B. the EIGRP route
C. the RIPv2 route
D. all three routes
E. the OSPF and RIPv2 routes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 149
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.

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:
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 150
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The "show ip ospf database" command displays the link states. Here is an example:
Here is the lsa database on R2.
R2#show ip ospf database
OSPF Router with ID (2.2.2.2) (Process ID 1)
Router Link States (Area 0)
Link ID ADV Router Age Seq# Checksum Link count2.2.2.2 2.2.2.2 793 0x80000003 0x004F85 210.4.4.4 10.4.4.4 776 0x80000004 0x005643 1111.111.111.111 111.111.111.111 755 0x80000005 0x0059CA 2133.133.133.133 133.133.133.133 775 0x80000005 0x00B5B1 2 Net Link States (Area 0)
Link ID ADV Router Age Seq# Checksum10.1.1.1 111.111.111.111 794 0x80000001 0x001E8B10.2.2.3 133.133.133.133 812 0x80000001

0x004BA910.4.4.1 111.111.111.111 755 0x80000001 0x007F1610.4.4.3 133.133.133.133 775 0x80000001 0x00C31F

QUESTION 151
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 inthe 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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
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 152
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.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
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).

The OSPF protocol is based on link-state technology, which is a departure from the Bellman-Ford vector based algorithms used in traditional Internet routing protocols such as RIP. OSPF has introduced new concepts such as authentication of routing updates, Variable Length Subnet Masks (VLSM), route summarization, and so forth.
OSPF uses flooding to exchange link-state updates between routers. Any change in routing information is flooded to all routers in the network. Areas are introduced to put a boundary on the explosion of link-state updates. Flooding and calculation of the Dijkstra algorithm on a router is limited to changes within an area.

Reference: http://www.9tut.com/ospf-routing-protocol-tutorial

QUESTION 153
What is the default administrative distance of OSPF?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

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

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

QUESTION 154
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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 155
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
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 156
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
In the router ospf command, the ranges from 1 to 65535 so o is an invalid number -> but To configure OSPF, we need a wildcard in the "network" statement, not a subnet mask. We also need to assgin an area to this process -> .

Configuring OSPF is slightly different from configuring RIP. When configuring OSPF, use the following syntax:

Router(config)# router ospf process_ID
Router(config-router)# network IP_address wildcard_mask area area_#
Reference: http://computernetworkingnotes.com/routing-static-dynamics-rip-ospf-igrp-eigrp/ospf-routing-configurations.html
http://computernetworkingnotes.com/routing-static-dynamics-rip-ospf-igrp-eigrp/ospf-routing-configurations.html

OSPF Inter-Area Routing
Reference: http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/47864-ospfdb5.html

CCNA Question

QUESTION 157
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

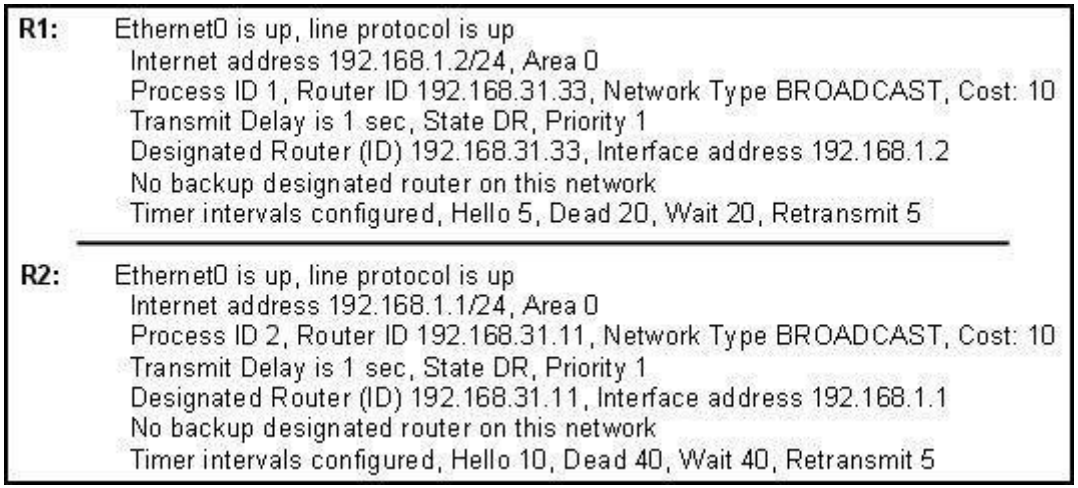
QUESTION 158
A network administrator is trying to add a new router into an established OSPF network. The networks attached to the new router do not appear in the routing tables of the other OSPF routers. Given the information in the partial configuration shown below, what configuration error is causing 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 159
A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common Ethernet link.



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

A. The 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

ip ospf hello-interval

Sets the number of seconds between hello packets sent on an interface.

Syntax: ip ospf hello-interval

no ip ospf hello-interval seconds

seconds: number of seconds to wait before sending another hello packet. Valid values are 1 to 65535.

Description: The hello interval is the number of seconds this router waits before sending out the next hello packet.

Use the ip ospf hello-interval seconds command to set the number of seconds this router waits before sending the next hello packet out this interface.

Use the no ospf hello-interval to set the hello-interval to the default value of 10 seconds.

Factory Default: 10 seconds.

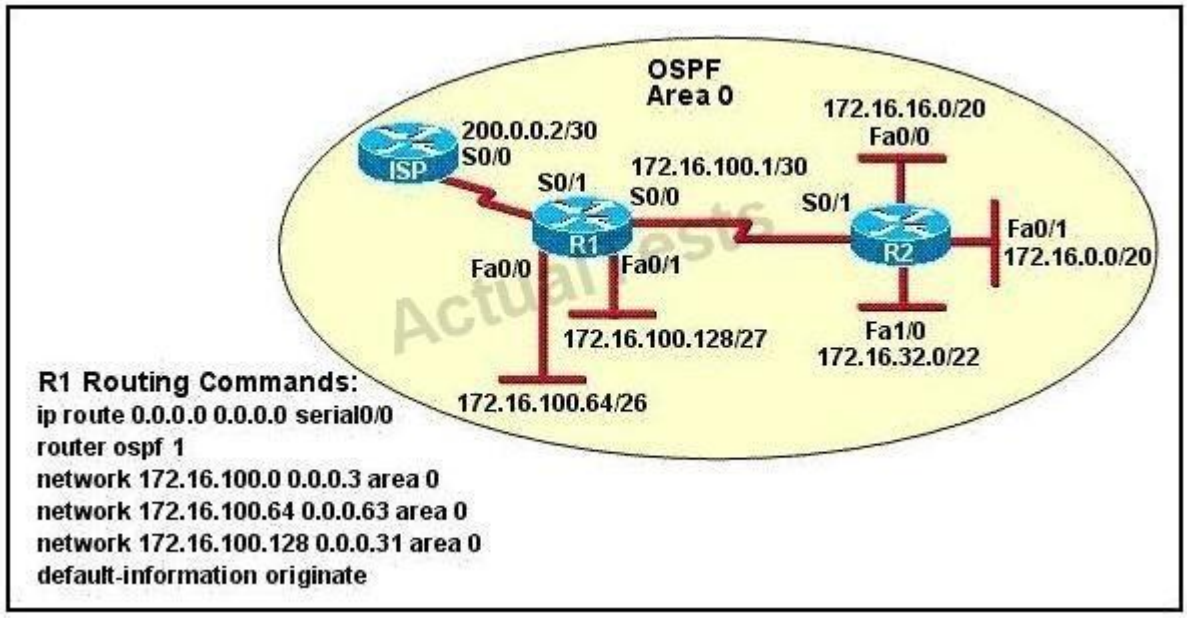
Command Mode: Interface configuration.

Example: In the following example, the ip ospf hello-interval seconds command sets the number of seconds between sending hello packets to 15 seconds, and the show ip ospf interface pos command displays the setting:

```
router(config)#router ospf 1
router(config-router)#network 10.1.1.0 0.0.0.255 area 0
router(config-router)#interface pos 1/1/1
router(config-if)#ip ospf hello-interval 15
router(config-if)#end
router#show ip ospf interface pos 1/1/1

Name: POS 1/1/1
Address: 201.1.1.10
Net type: PointToPoint
State: P To P
Area: 0.0.0.0
DR: 0.0.0.0
BDR: 0.0.0.0
Priority: 1
Cost: 10
Hello int: 15
Dead int:           40
Retrans int: 5
Transmit delay: 1
```

QUESTION 160
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 subnet works.
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.

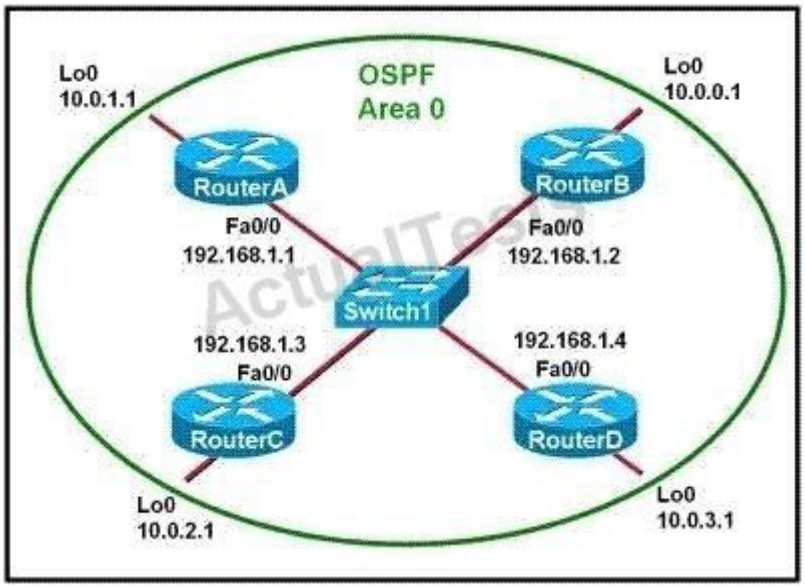
QUESTION 161
OSPF routing uses the concept of areas. What are the characteristics of OSPF areas? (Choose Three.)

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.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
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 162
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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
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'sphysical interfaces will be chosen. -> The loopback interface will be chosen as the router ID of RouterB