

100-105 Dumps

Cisco Interconnecting Cisco Networking Devices Part 1 (ICND1 v3.0)

<https://www.certleader.com/100-105-dumps.html>



NEW QUESTION 1

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



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

Answer: B

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

NEW QUESTION 2

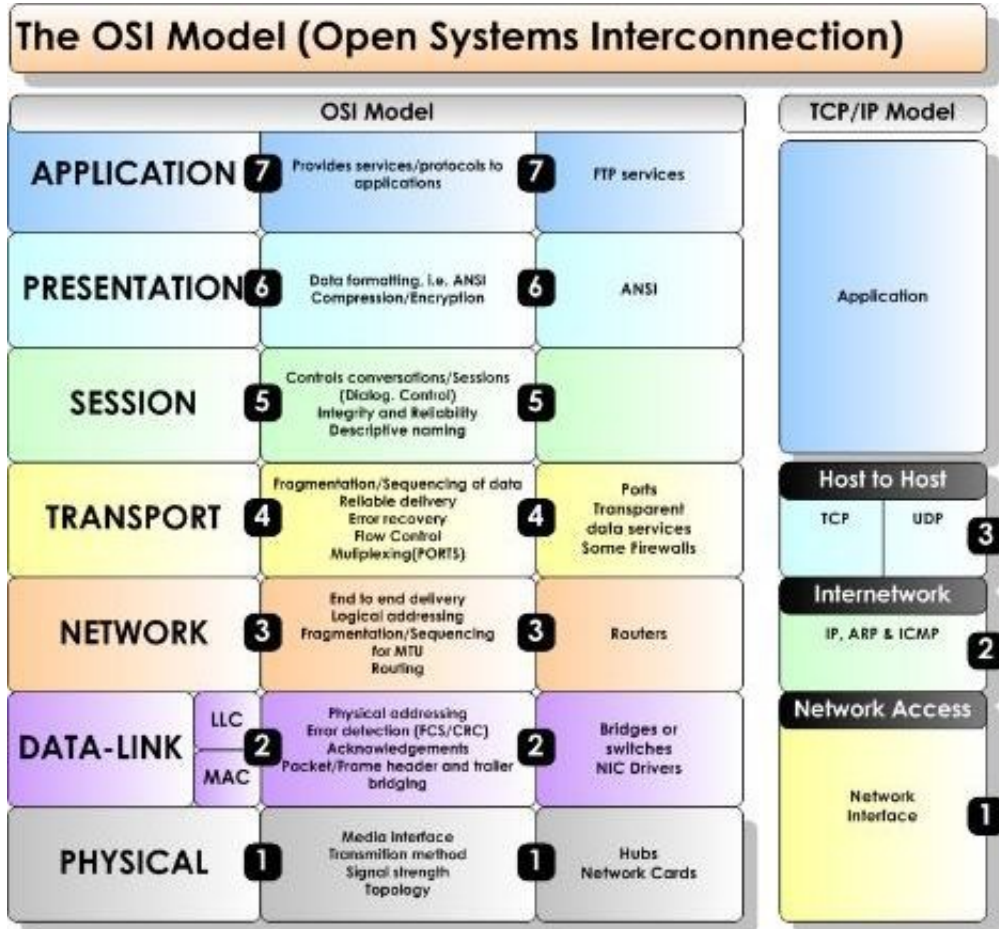
Which layer of the TCP/IP stack combines the OSI model physical and data link layers?

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

Answer: D

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

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



NEW QUESTION 3

Which statements accurately describe CDP? (Choose three.)

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

Answer: BCE

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

NEW QUESTION 4

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

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

Answer: C

NEW QUESTION 5

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

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

Answer: E

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

NEW QUESTION 6

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

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

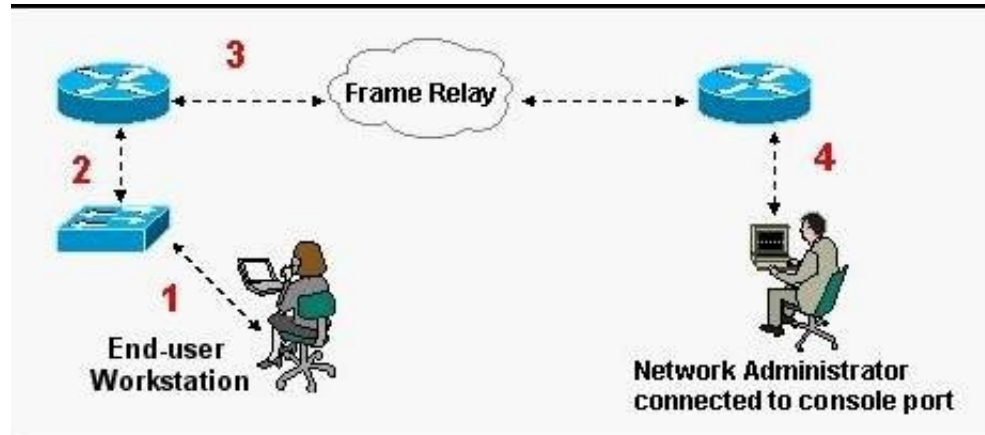
- E. An ICMP connection must be established between the workstation and its default gateway.
- F. An ICMP connection must be established between the workstation and the web server.

Answer: D

Explanation: HTTP uses TCP port 80, and a TCP port 80 connection must be established for HTTP communication to occur.
<http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/>

NEW QUESTION 7

Refer to the exhibit.



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

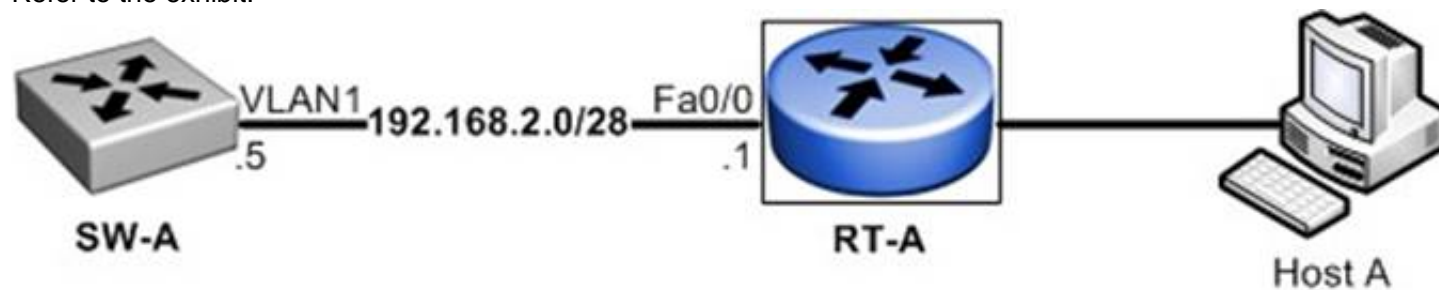
- A. 1 - Ethernet Crossover cable 2 - Ethernet straight-through cable 3 - Fiber Optic cable 4 - Rollover cable
- B. 1 - Ethernet straight-through cable 2 - Ethernet straight-through cable 3 - Serial cable 4 - Rollover cable
- C. 1 - Ethernet rollover cable 2 - Ethernet crossover cable 3 - Serial cable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

Answer: B

Explanation: When connecting a PC to a switch, a standard Ethernet straight through cable should be used. This same cable should also be used for switch to router connections. Generally speaking, crossover cables are only needed when connecting two like devices (PC-PC, switch-switch, router-router, etc). Routers connect to frame relay and other WAN networks using serial cables. Rollover cables are special cables used for connecting to the console ports of Cisco devices.

NEW QUESTION 8

Refer to the exhibit.



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

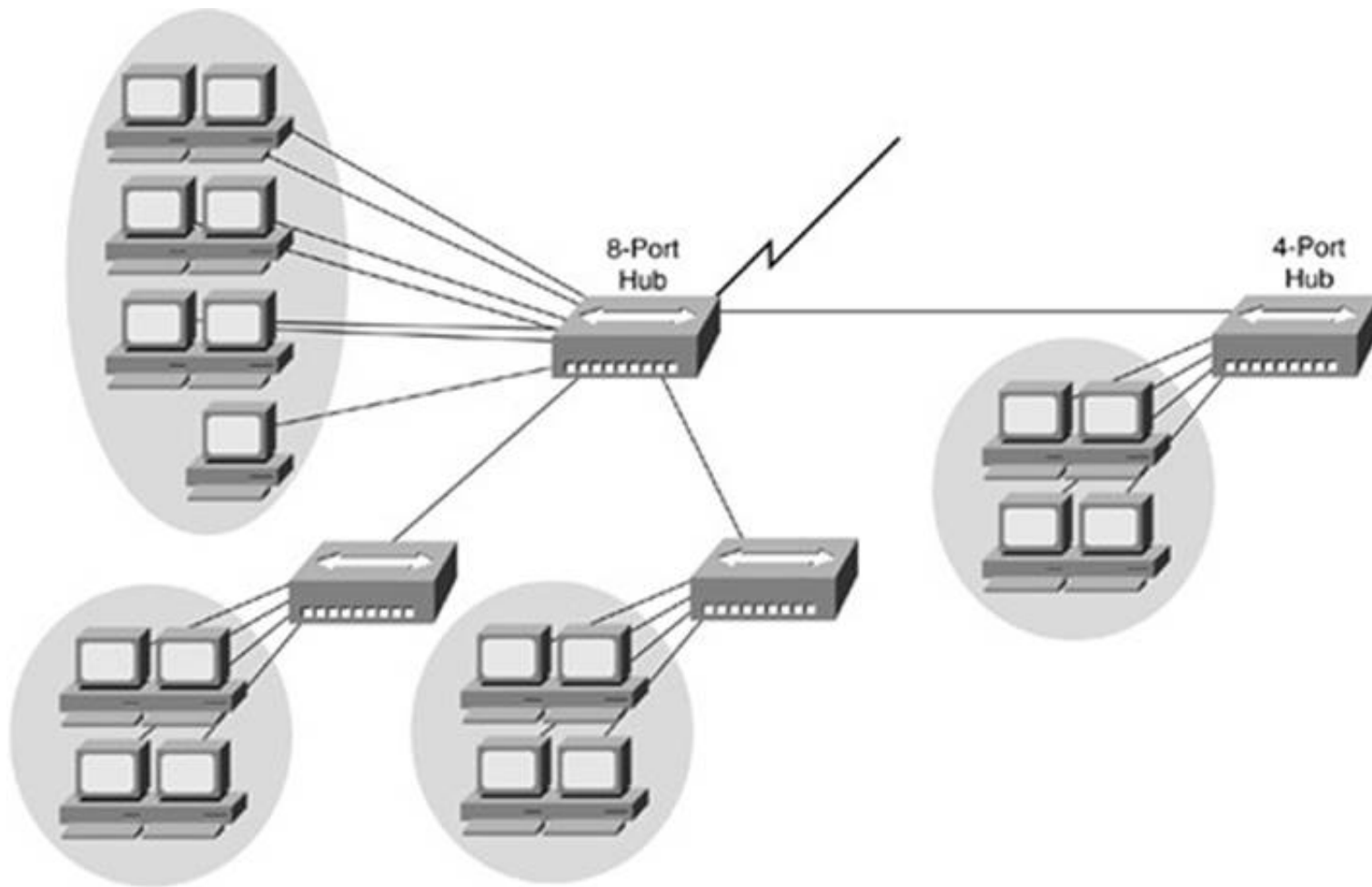
- A. VLAN 1 on RT-A
- B. IP routing on SW-A
- C. default gateway on SW-A
- D. crossover cable connecting SW-A and RT-A

Answer: C

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

NEW QUESTION 9

Refer to the exhibit.



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

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

Answer: C

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

NEW QUESTION 10

Refer to the exhibit.

SwitchA# show mac-address-table
< non-essential output omitted >

Destination Address	Address Type	VLAN	Destination Port
00b0.d056.fe4d	Dynamic	1	FastEthernet0/3
00b0.d043.ac2e	Dynamic	1	FastEthernet0/4
00b0.d0fe.ac32	Dynamic	1	FastEthernet0/5
00b0.d0da.cb56	Dynamic	1	FastEthernet0/6

Frame received by SwitchA:

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

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

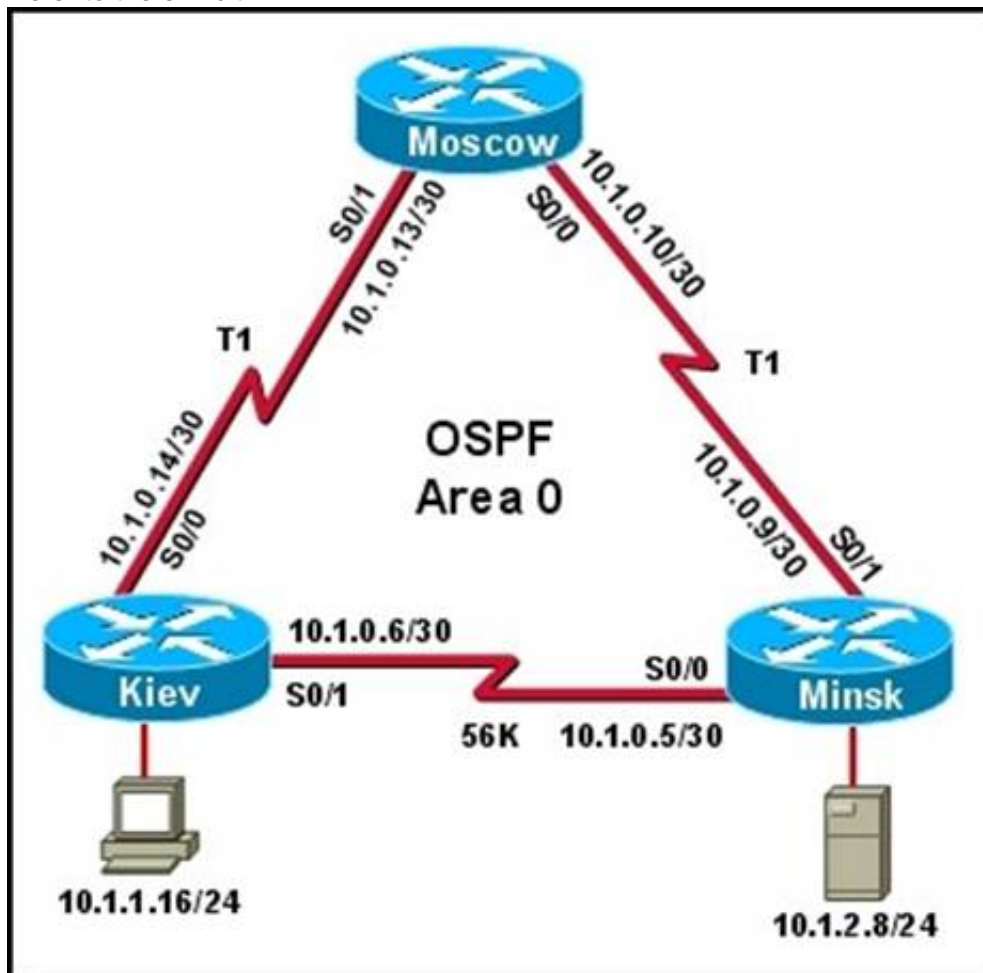
- A. It will drop the frame.
- B. It will forward the frame out port Fa0/6 only.
- C. It will flood the frame out all ports.
- D. It will flood the frame out all ports except Fa0/3.

Answer: B

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

NEW QUESTION 10

Refer to the exhibit.



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

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

Answer: E

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

NEW QUESTION 14

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. ACore router.
- B. The HQ Internet gateway router.
- C. The WAN router at the central site.

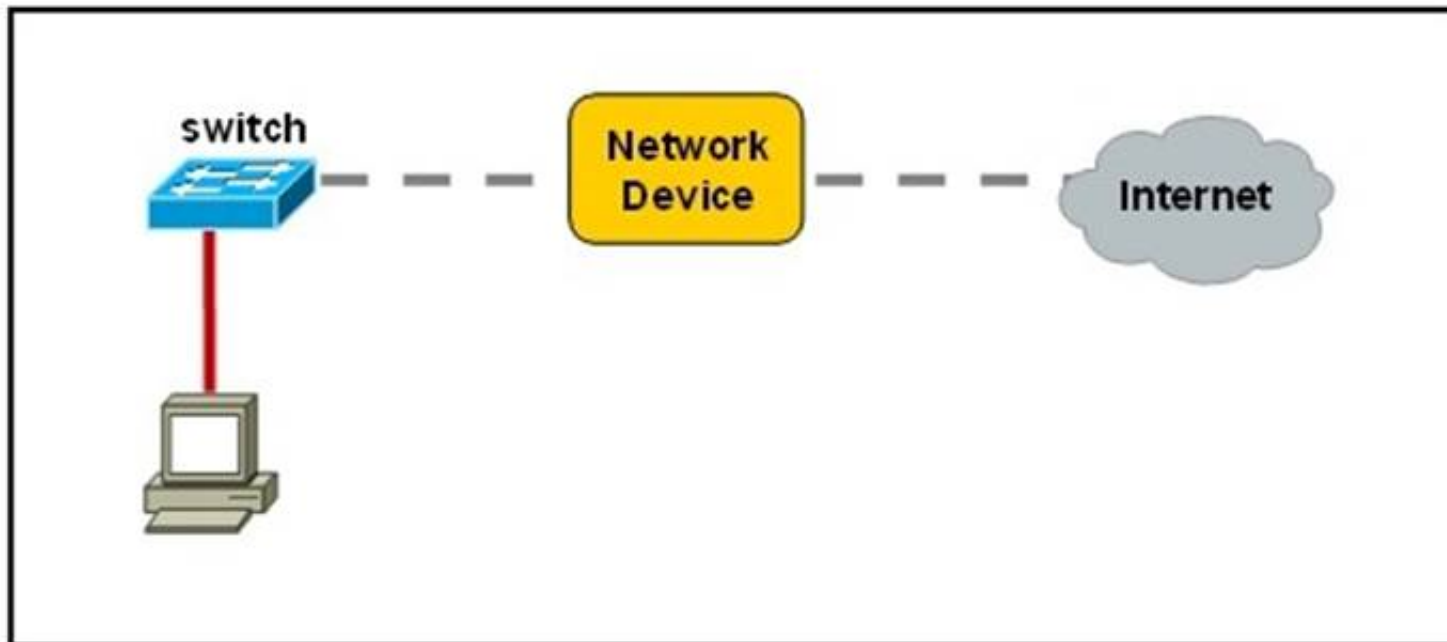
D. Remote stub router at a remote site.

Answer: D

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

NEW QUESTION 18

Refer to the exhibit.



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

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

Answer: C

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

NEW QUESTION 21

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

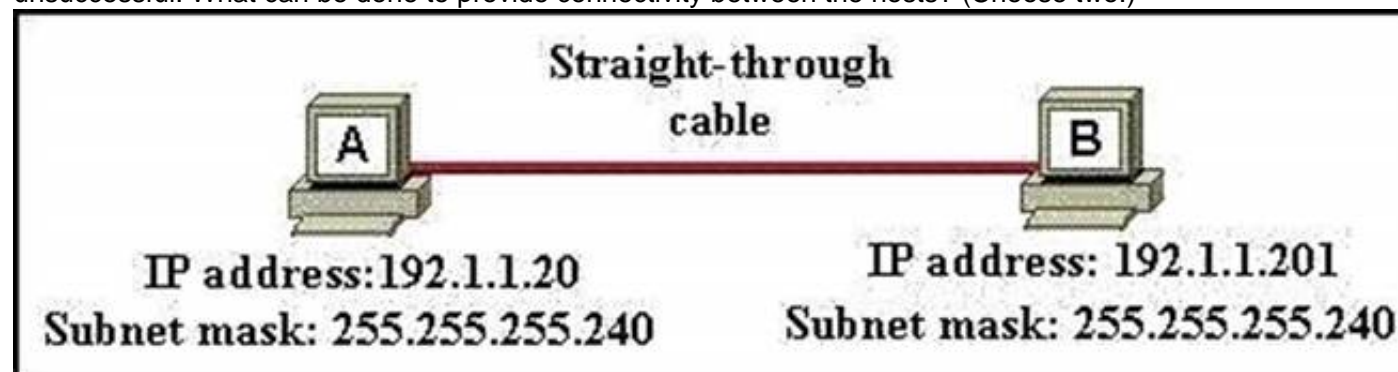
- A. HTTP
- B. DNS
- C. DHCP
- D. RARP
- E. ARP

Answer: E

Explanation: The RARP protocol is used to translate hardware interface addresses to protocol addresses. The RARP message format is very similar to the ARP format. When the booting computer sends the broadcast ARP request, it places its own hardware address in both the sending and receiving fields in the encapsulated ARP data packet. The RARP server will fill in the correct sending and receiving IP addresses in its response to the message. This way the booting computer will know its IP address when it gets the message from the RARP server

NEW QUESTION 24

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



A. A crossover cable should be used in place of the straight-through cable.

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

Answer: AF

Explanation: If you need to connect two computers but you don't have access to a network and can't set up an ad hoc network, you can use an Ethernet crossover cable to create a direct cable connection.
Generally speaking, a crossover cable is constructed by reversing (or crossing over) the order of the wires inside so that it can connect two computers directly. A crossover cable looks almost exactly like a regular Ethernet cable (a straight-through cable), so make sure you have a crossover cable before following these steps.
Both devices need to be on the same subnet, and since one PC is using 192.1.1.20 and the other is using 192.1.1.201, the subnet mask should be changed to 255.255.255.0.

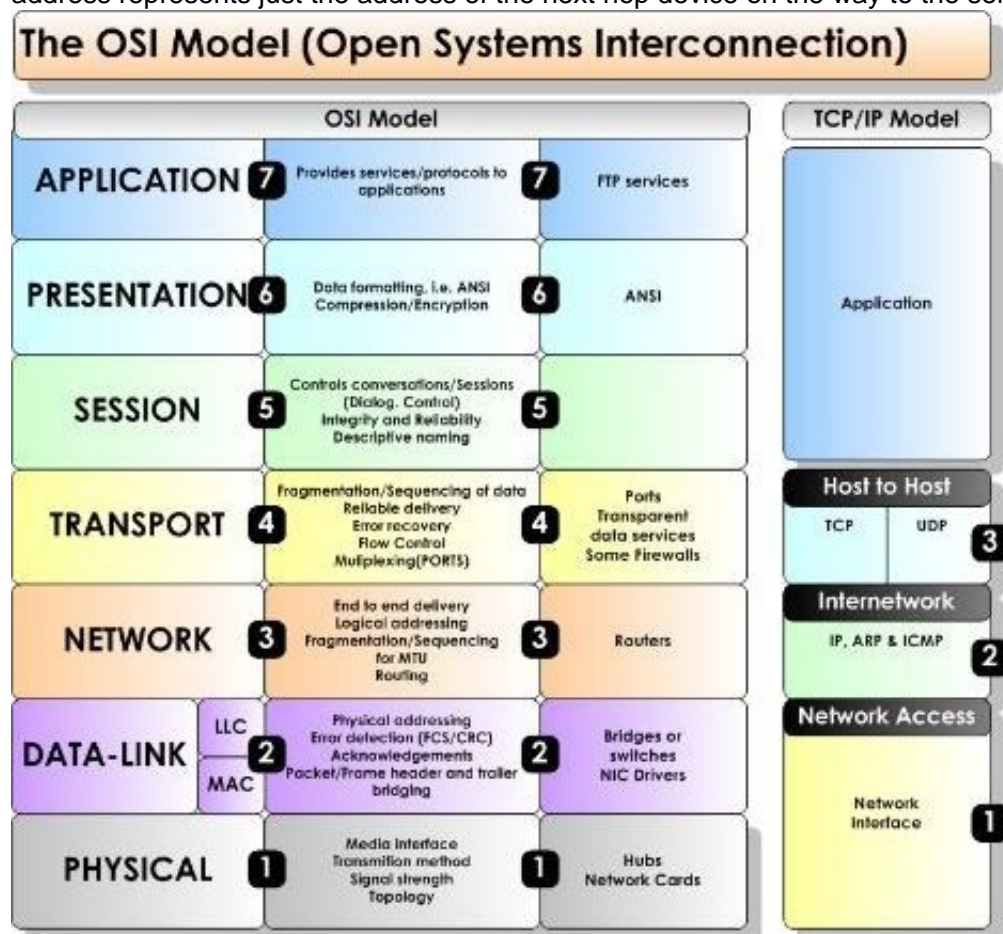
NEW QUESTION 27

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

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

Answer: D

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



NEW QUESTION 31

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

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

Answer: C

Explanation: TCP is an example of a connection-oriented protocol. It requires a logical connection to be established between the two processes before data is exchanged. The connection must be maintained during the entire time that communication is taking place, then released afterwards. The process is much like a telephone call, where a virtual circuit is established--the caller must know the person's telephone number and the phone must be answered-- before the message can be delivered.
TCP/IP is also a connection-oriented transport with orderly release. With orderly release, any data remaining in the buffer is sent before the connection is terminated. The release is accomplished in a three-way handshake between client and server processes. The connection-oriented protocols in the OSI protocol suite, on the other hand, do not support orderly release. Applications perform any handshake necessary for ensuring orderly release.
Examples of services that use connection-oriented transport services are telnet, rlogin, and ftp.

NEW QUESTION 36

How does a switch differ from a hub?

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

Answer: B

Explanation: Some of the features and functions of a switch include:

A switch is essentially a fast, multi-port bridge, which can contain dozens of ports. Rather than creating two collision domains, each port creates its own collision domain.

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

If an uplink port is included, one switch creates twenty-one single-node collision domains. A switch dynamically builds and maintains a Content-Addressable Memory (CAM) table, holding all of the necessary MAC information for each port.

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

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

NEW QUESTION 37

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

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

Answer: CD

Explanation: Ping may be used to find out whether the local machines are connected to the network or whether a remote site is reachable. This tool is a common network tool for determining the network connectivity, which uses ICMP protocol instead of TCP/IP and UDP/IP. This protocol is usually associated with the network management tools, which provide network information to network administrators, such as ping and traceroute (the later also uses the UDP/IP protocol). ICMP is quite different from the TCP/IP and UDP/IP protocols. No source and destination ports are included in its packets. Therefore, usual packet-filtering rules for TCP/IP and UDP/IP are not applicable. Fortunately, a special "signature" known as the packet's Message type is included for denoting the purposes of the ICMP packet. Most commonly used message types are namely, 0, 3, 4, 5, 8, 11, and 12 which represent echo reply, destination unreachable, source quench, redirect, echo request, time exceeded, and parameter problem respectively.

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

NEW QUESTION 42

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

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

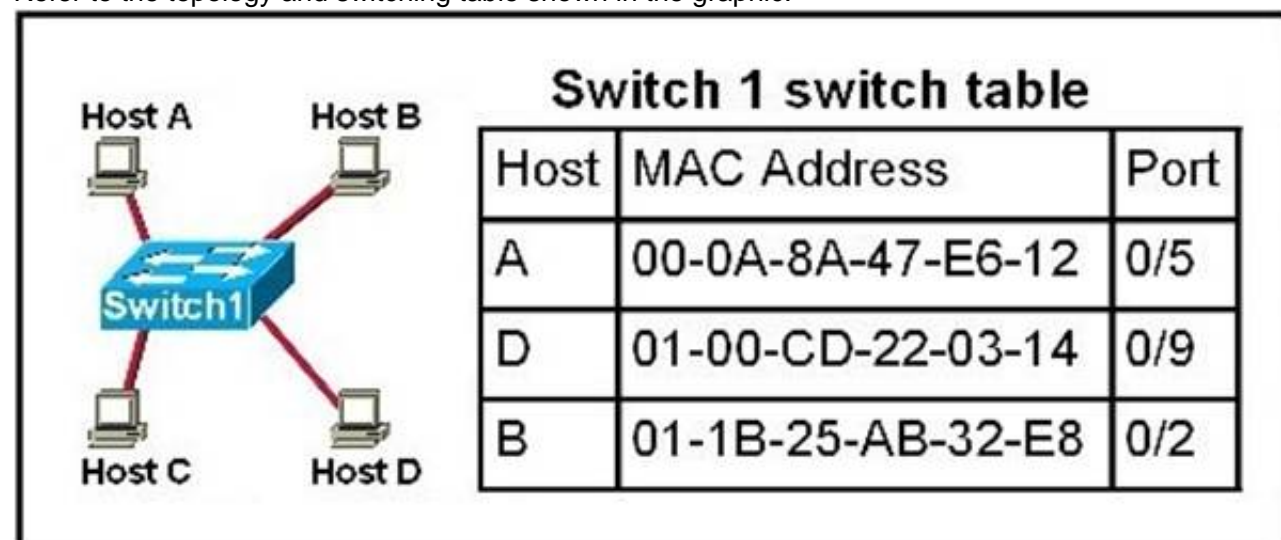
Answer: BD

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

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

NEW QUESTION 45

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



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

- A. Drop the frame
- B. Send the frame out all ports except port 0/2

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

Answer: B

NEW QUESTION 49

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
- F. When the backoff delay period has expired, all stations have equal priority to transmit data.
- G. After a collision, all stations involved run an identical backoff algorithm and then synchronize with each other prior to transmitting data.

Answer: BE

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

NEW QUESTION 52

Refer to the exhibit.

SwitchA# show mac-address-table			
< non-essential output omitted >			
Destination Address	Address Type	VLAN	Destination Port
-----	-----	---	-----
00b0.d056.fe4d	Dynamic	1	FastEthernet0/3
00b0.d043.ac2e	Dynamic	1	FastEthernet0/4
00b0.d0fe.ac32	Dynamic	1	FastEthernet0/5
00b0.d0da.cb56	Dynamic	1	FastEthernet0/6
Frame received by SwitchA:			
Source MAC	Destination MAC	Source IP	Destination IP
00b0.d056.fe4d	00b0.d0da.895a	192.168.40.5	192.168.40.6

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

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

Answer: E

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

NEW QUESTION 55

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

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

Answer: A

Explanation: Serial Connection



cl_3_dte_male



cl_2_dce

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.



cl_4_malefemale

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

NEW QUESTION 59

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

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

Answer: BD

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

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

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

NEW QUESTION 62

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

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

Answer: C

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

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

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

The information shared in a CDP packet about a Cisco device includes the following: Name of the device configured with the hostname command
IOS software version

Hardware capabilities, such as routing, switching, and/or bridging Hardware platform, such as 2600, 2950, or 1900

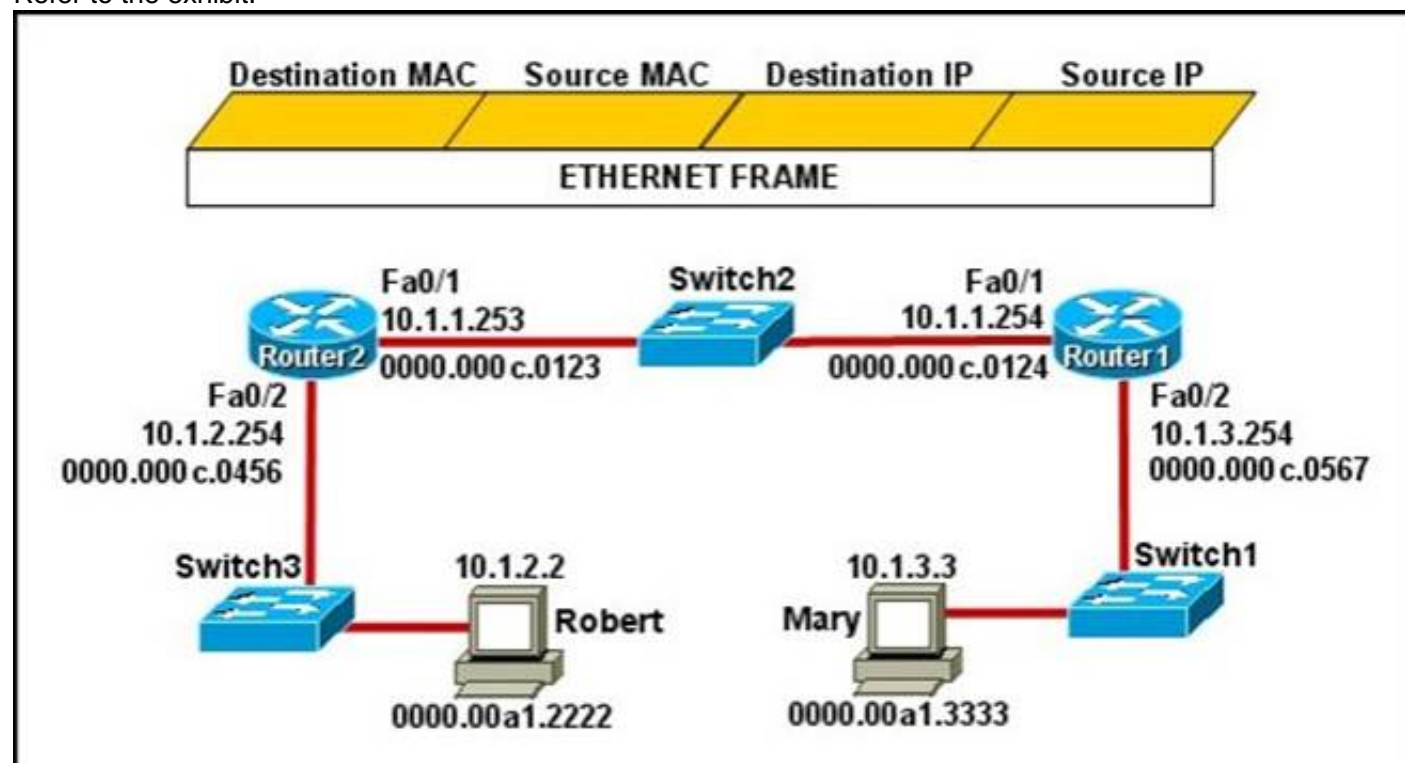
The layer-3 address(es) of the device

The interface the CDP update was generated on

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

NEW QUESTION 65

Refer to the exhibit.



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

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

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

Answer: B

Explanation:

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

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

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

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

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

Topic 2, LAN Switching Technologies

NEW QUESTION 68

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

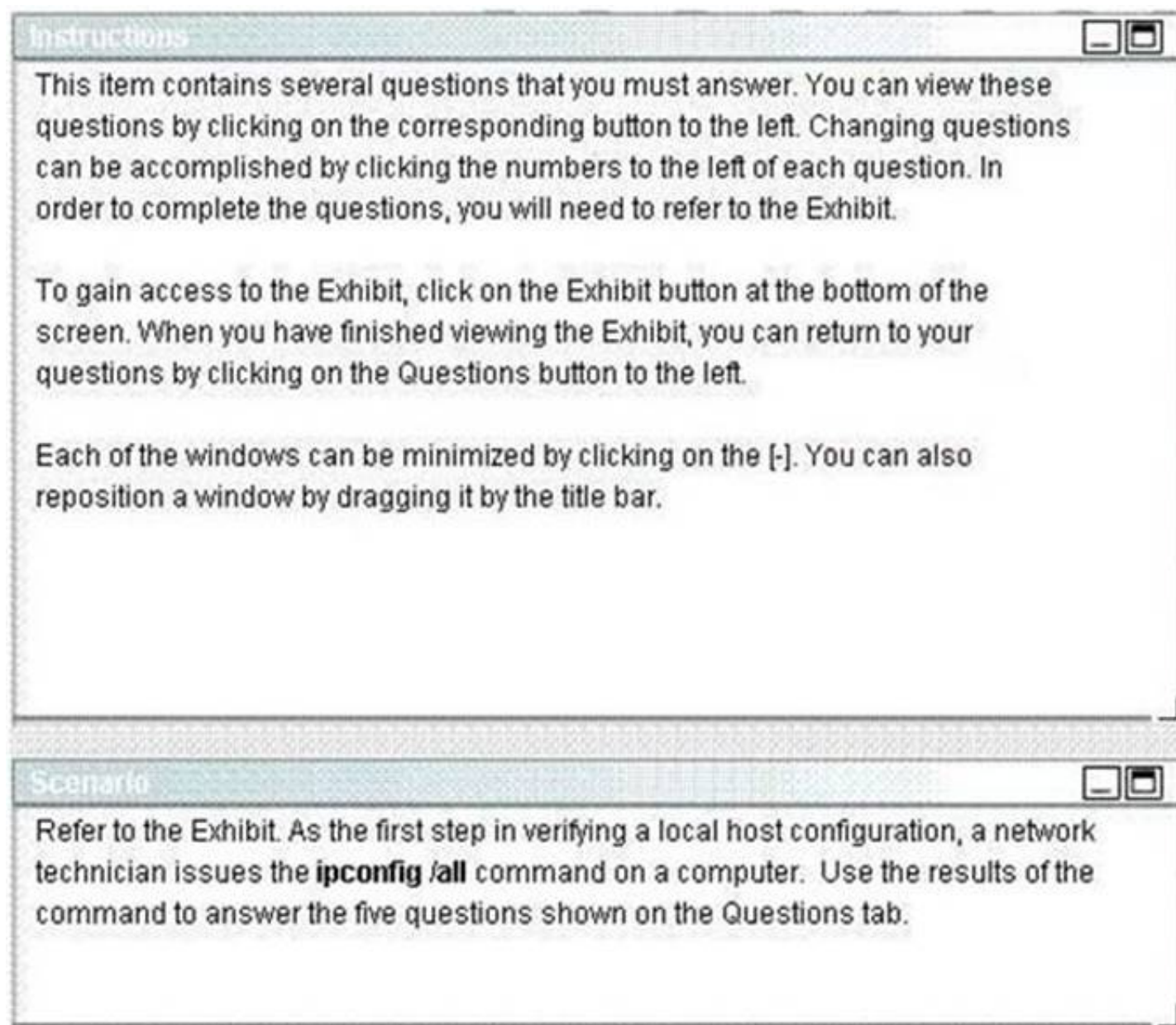
- A. drop the frame
- B. forward it out of all ports except the one that received it
- C. forward it out of all ports
- D. store it until it learns the correct port

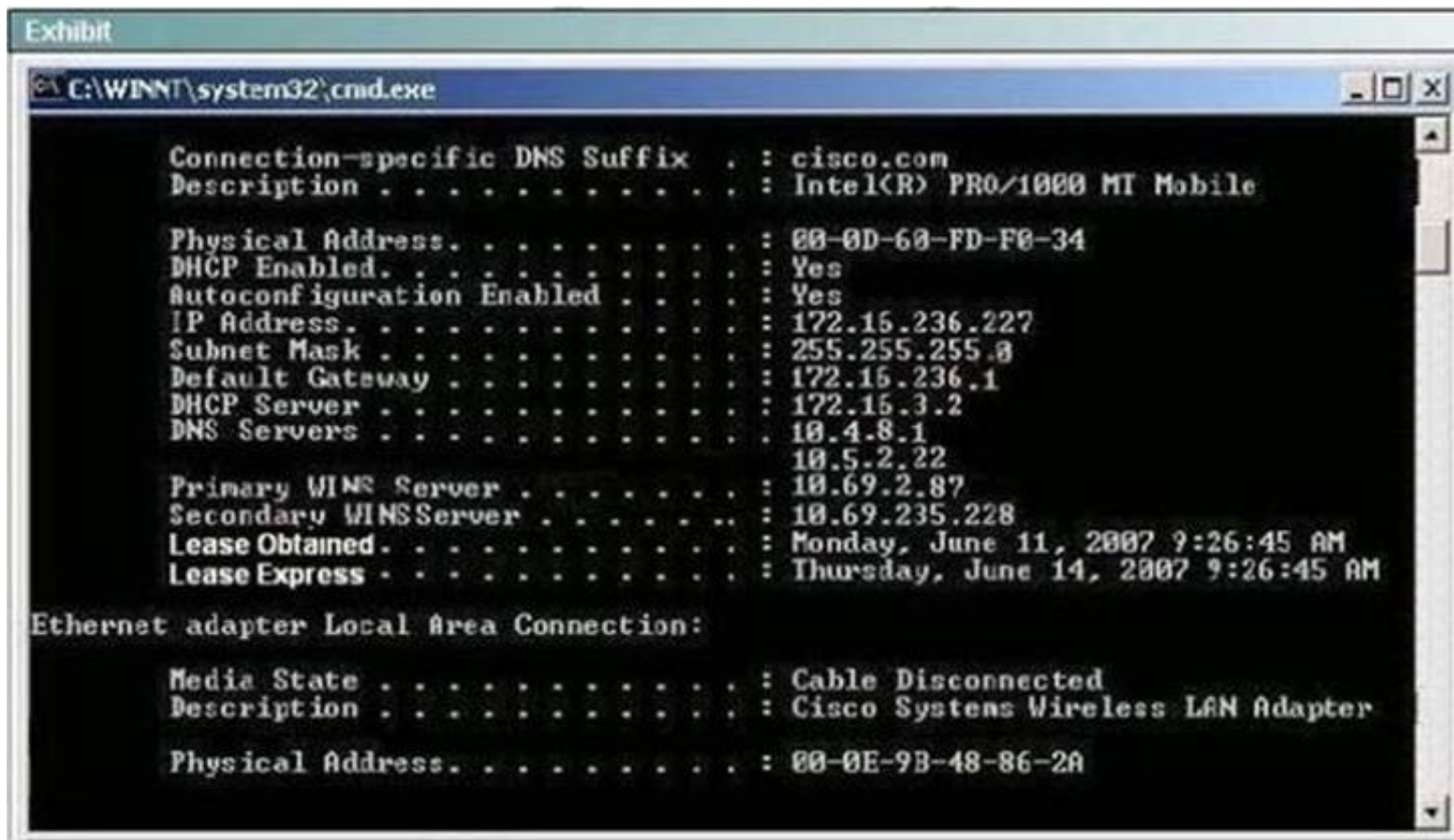
Answer: B

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

NEW QUESTION 73

Refer to the 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.

Answer: AD

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

NEW QUESTION 77

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

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

Answer: E

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

NEW QUESTION 79

What is the purpose of flow control?

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

Answer: C

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

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

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

NEW QUESTION 80

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

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

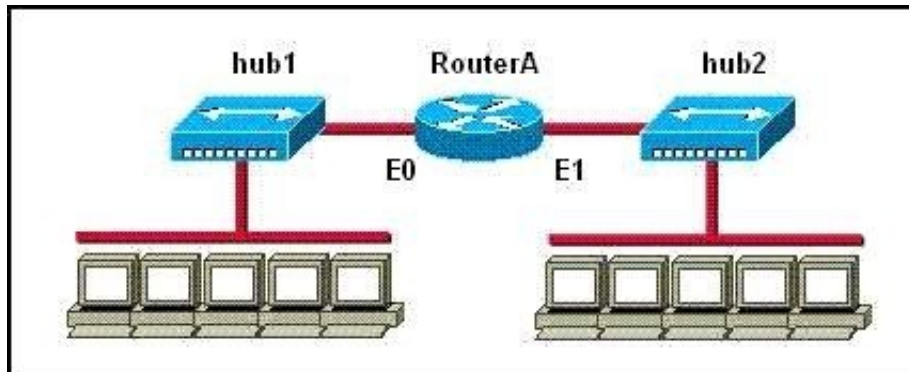
E. 5
F. 6

Answer: E

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

NEW QUESTION 83

Refer to the exhibit.



How many collision domains are shown?

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

Answer: B

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

NEW QUESTION 87

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

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

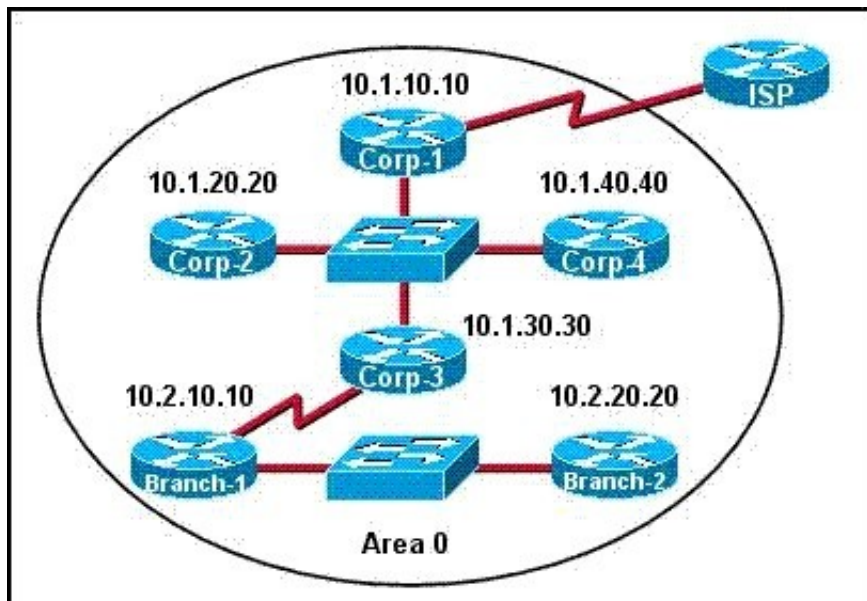
Answer: B

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

Topic 3, Routing Fundamentals

NEW QUESTION 90

The internetwork infrastructure of company XYZ consists of a single OSPF area as shown in the graphic. There is concern that a lack of router resources is impeding internetwork performance. As part of examining the router resources, the OSPF DRs need to be known. All the router OSPF priorities are at the default and the router IDs are shown with each router.



Which routers are likely to have been elected as DR? (Choose two.)

A. Corp-1
B. Corp-2
C. Corp-3
D. Corp-4
E. Branch-1
F. Branch-2

Answer: DF

Explanation: There are 2 segments on the topology above which are separated by Corp-3 router. Each segment will have a DR so we have 2 DRs. To select which router will become DR they will compare their router-IDs. The router with highest (best) router-ID will become DR. The router-ID is chosen in the order below:

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

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

NEW QUESTION 91

To allow or prevent load balancing to network 172.16.3.0/24, which of the following commands could be used in R2? (Choose two.)

Instructions

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

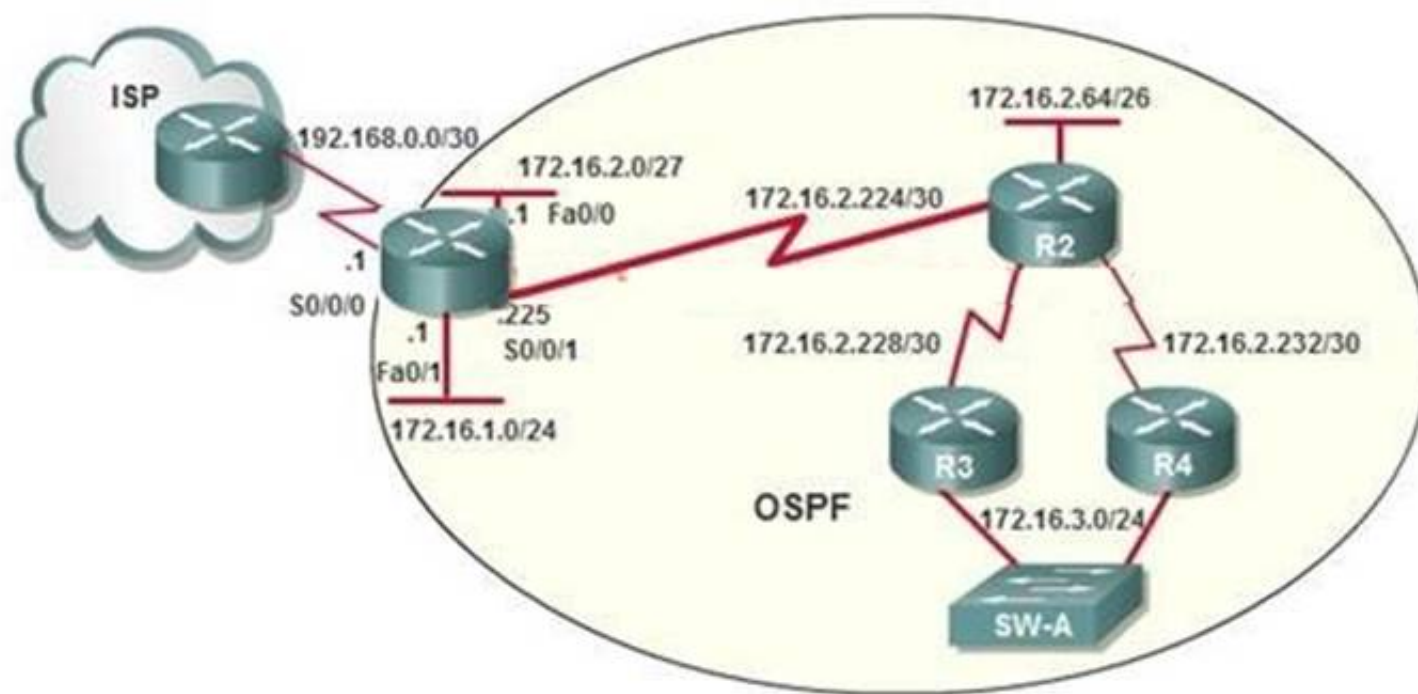
To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by **clicking on the Questions button to the left**.

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

Scenario

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

Topology



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

Answer: BC

Explanation: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.sht ml#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:

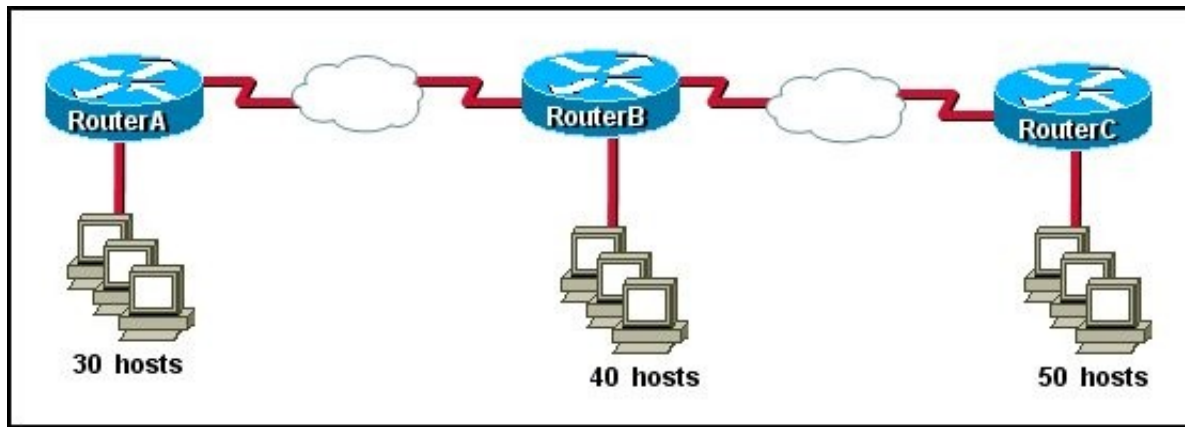
Cost = 10000 0000/bandwidth in bps

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.

NEW QUESTION 93

Refer to the exhibit.



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

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

Answer: D

Explanation: Subnet mask 255.255.255.224 with CIDR of /27 which results in 32 hosts per. 192.168.1.31 is the broadcast address for subnet '0' 192.168.1.64 is the network address for subnet '2' 192.168.1.127 is the broadcast address for subnet '3' 192.168.1.192 is the network address for subnet '6'

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

NEW QUESTION 95

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

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

Answer: B

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

NEW QUESTION 96

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

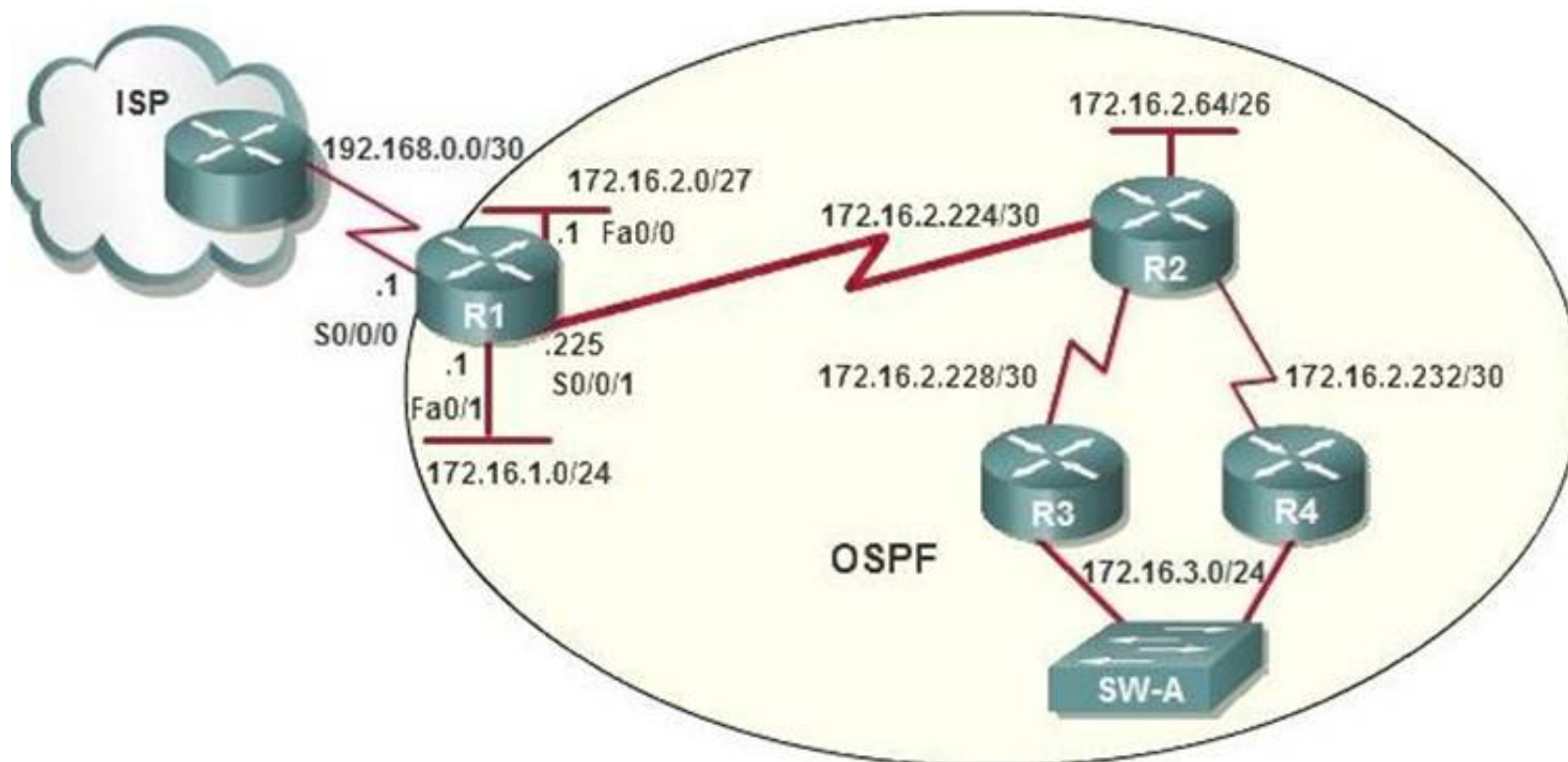
- A. It supports VLSM.
- B. It is used to route between autonomous systems.
- C. It confines network instability to one area of the network.
- D. It increases routing overhead on the network.
- E. It allows extensive control of routing updates.
- F. It is simpler to configure than RIP v2.

Answer: ACE

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

NEW QUESTION 97

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



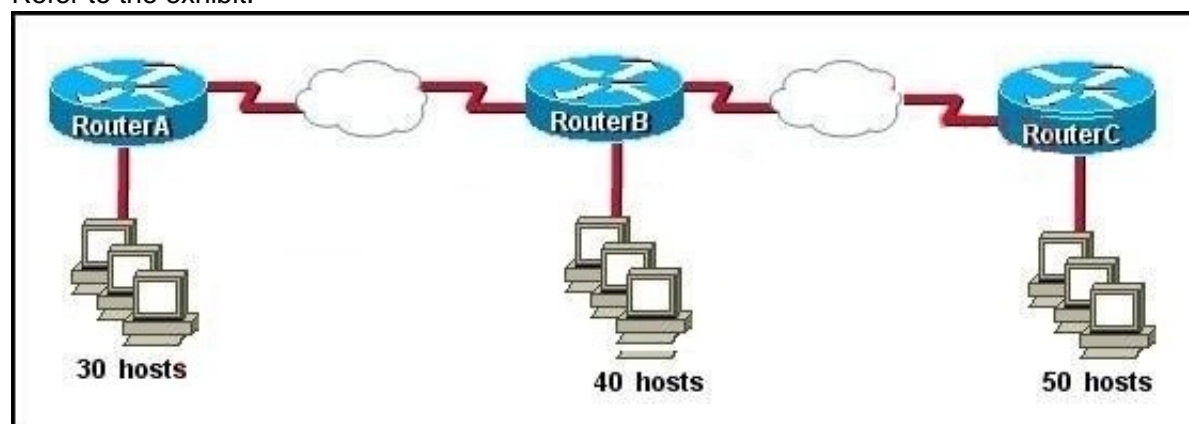
- A. No messages are exchanged
- B. Hellos are sent every 10 seconds.
- C. The full database from each router is sent every 30 seconds.
- D. The routing table from each router is sent every 60 seconds.

Answer: B

Explanation: HELLO messages are used to maintain adjacent neighbors so even when the network is converged, hellos are still exchanged. On broadcast and point-to-point links, the default is 10 seconds, on NBMA the default is 30 seconds. Although OSPF is a link-state protocol the full database from each router is sent every 30 minutes (not seconds) therefore, C and D are not correct.

NEW QUESTION 101

Refer to the exhibit.



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

- A. 255.255.255.192
- B. 255.255.255.224
- C. 255.255.255.240
- D. 255.255.255.248
- E. 255.255.255.252

Answer: A

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

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

NEW QUESTION 105

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

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

Answer: C

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

Add them up and you get 255. Add one for the all zeros option, and the total is 256. Now, take away one of these for the network address (all zeros) and another for the broadcast address (all ones). Each octet represents 254 possible hosts. Or 254 possible networks. Unless you have subnet zero set on your network gear, in which case you could conceivably have 255.

The CIDR addressing format (/20) tells us that 20 bits are used for the network portion, so the maximum number of networks are 2^{20} minus one if you have subnet zero enabled, or minus 2 if not.

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

NEW QUESTION 107

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

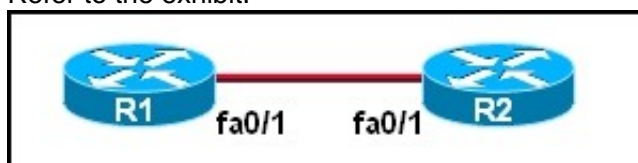
- A. Examine the Layer 2 headers of inbound packets and use that information to determine the next hops for the packets
- B. Update the Layer 2 headers of outbound packets with the MAC addresses of the next hops
- C. Examine the Layer 3 headers of inbound packets and use that information to determine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

Answer: BC

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

NEW QUESTION 108

Refer to the exhibit.



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

information between R1 and R2?

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

Answer: B

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

NEW QUESTION 113

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

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

Answer: A

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

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f11.shtml OSPF hello packets have a destination address of 224.0.0.5 (the all ospf routers multicast address).

NEW QUESTION 115

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

Router(config)# router ospf 1

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

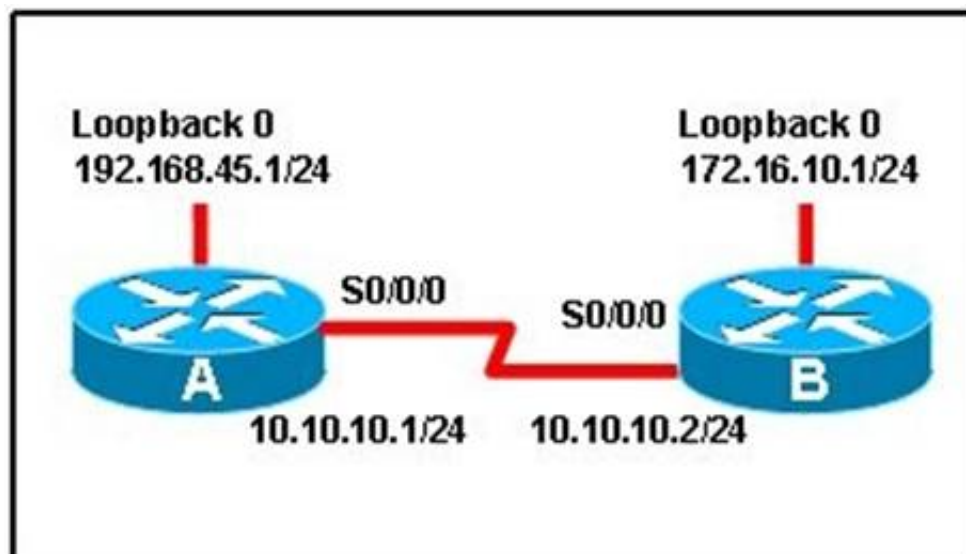
- A. The process id is configured improperly.
- B. The OSPF area is configured improperly.
- C. The network wildcard mask is configured improperly.
- D. The network number is configured improperly.
- E. The AS is configured improperly.
- F. The network subnet mask is configured improperly.

Answer: C

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

NEW QUESTION 119

Refer to the exhibit.



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

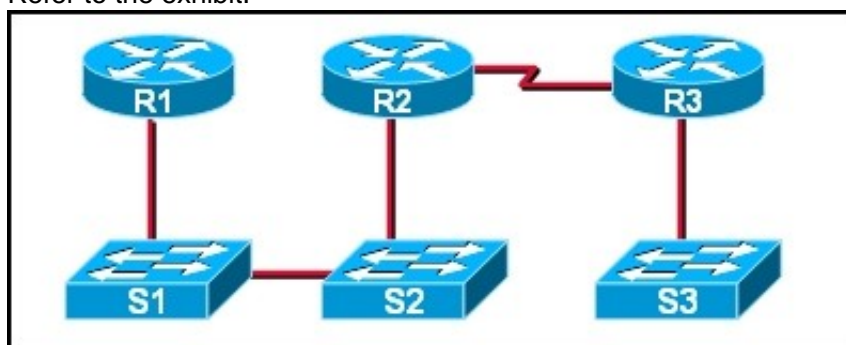
- A. The loopback addresses are on different subnets.
- B. The values of the dead timers on the routers are different.
- C. Route summarization is enabled on both routers.
- D. The process identifier on router A is different than the process identifier on router B.

Answer: B

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

NEW QUESTION 120

Refer to the exhibit.



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

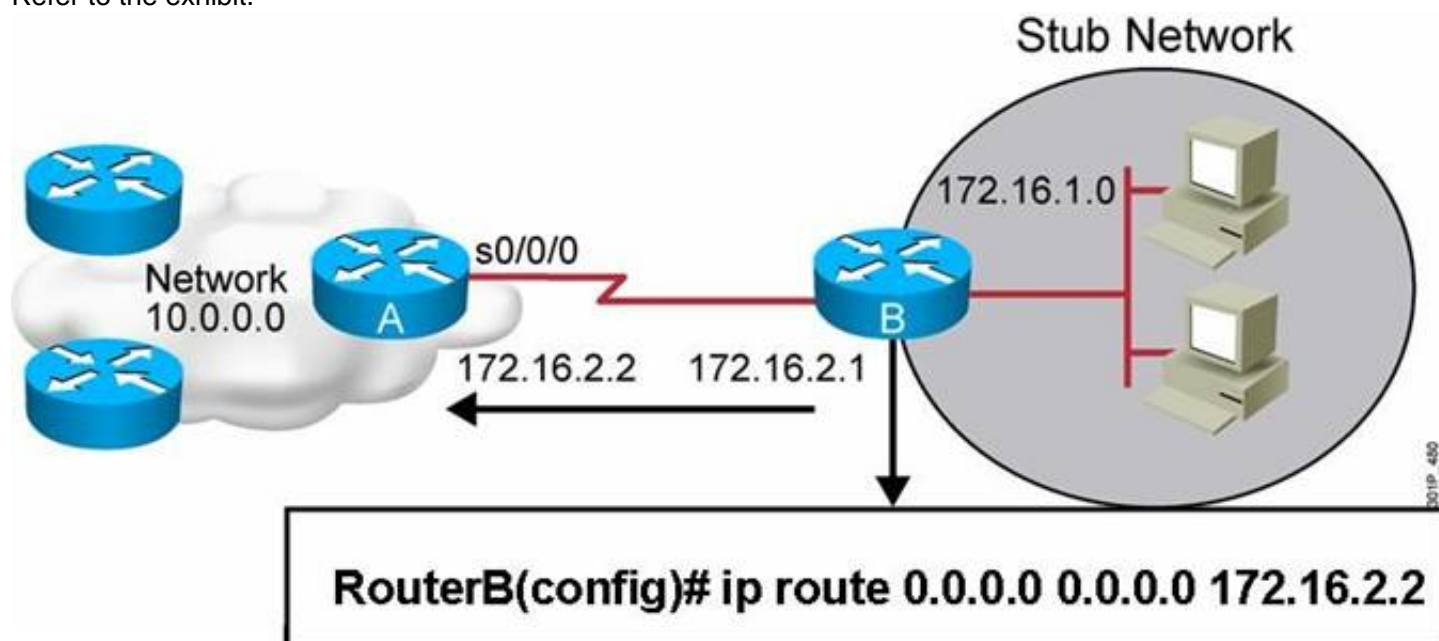
- A. R2 and R3
- B. R1 and R3
- C. R3 and S2
- D. R1, S1, S2, and R3
- E. R1, S1, S2, R3, and S3

Answer: C

Explanation: ACisco 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.

NEW QUESTION 124

Refer to the exhibit.



Which two statements are correct? (Choose two.)

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

Answer: AC

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

NEW QUESTION 125

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

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

Answer: A

Explanation: Example 3-1 displays OSPF with a process ID of 1 and places all interfaces configured with an IP address in area 0. The network command network 0.0.0.0 255.255.255.255 area 0

dictates that you do not care (255.255.255.255) what the IP address is, but if an IP address is enabled on any interface, place it in area 0.

Example 3-1 Configuring OSPF in a Single Area

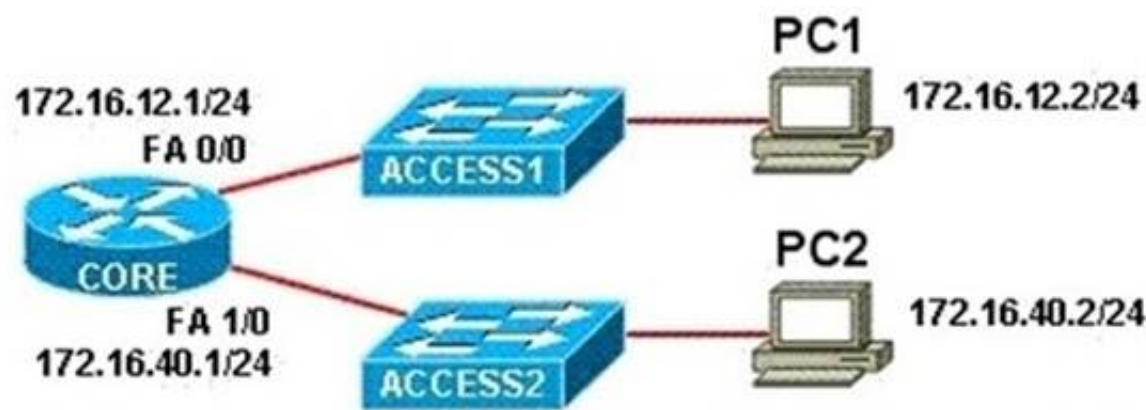
```
router ospf 1
```

```
network 0.0.0.0 255.255.255.255 area 0
```

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

NEW QUESTION 128

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          00E0.80B7.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.

Answer: BDF

Explanation: The router will forward the frames out the interface toward the destination – B is correct. Since the router will have the end station already in its MAC table as seen by the “show arp” command, it will replace the destination MAC address to that of PC2 – D is correct. The router will then replace the source IP address to 172.16.40.1 – E is correct.

NEW QUESTION 131

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

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

Answer: D

Explanation: One of the key advantages IPv6 brings is the exponentially larger address space. The following will outline the basic address architecture of IPv6. 128-bit-long addresses Represented in hexadecimal format:
Uses CIDR principles: prefix/prefix length x:x:x:x:x:x/x, where x is a 16-bit hex field The last 64 bits are used for the interface ID
http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd_8026003d.pdf

NEW QUESTION 134

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

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

Answer: AD

NEW QUESTION 139

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

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

Answer: B

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

NEW QUESTION 142

Which IP address is a private address?

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

Answer: C

NEW QUESTION 147

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

- A. 192.168.2.63
- B. 192.168.2.62
- C. 192.168.2.61
- D. 192.168.2.60
- E. 192.168.2.32

Answer: B

Explanation: With the 224 there are 8 networks with increments of 32
One of these is 32 33 62 63 where 63 is broadcast so 62 is last valid host out of given choices.

NEW QUESTION 151

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

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

Answer: C

Explanation: Default Distance Value Table

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

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

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

NEW QUESTION 153

What information can be used by a router running a link-state protocol to build and maintain its topological database? (Choose two.)

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

Answer: AC

Explanation: Reference 1:

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

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

Open Shortest Path First (OSPF) for IP

The ISO's Intermediate System to Intermediate System (IS-IS) for CLNS and IP DEC's DNA Phase V

Novell's NetWare Link Services Protocol (NLSP)

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

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

OSPF Tutorial

NEW QUESTION 156

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

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

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

Answer: C

Explanation: With network 192.168.20.24/29 we have:

Increment: 8 (/29 = 255.255.255.248 = 11111000 for the last octet) Network address: 192.168.20.24 (because 24 = 8 * 3)

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

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

NEW QUESTION 159

What does administrative distance refer to?

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

Answer: D

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

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

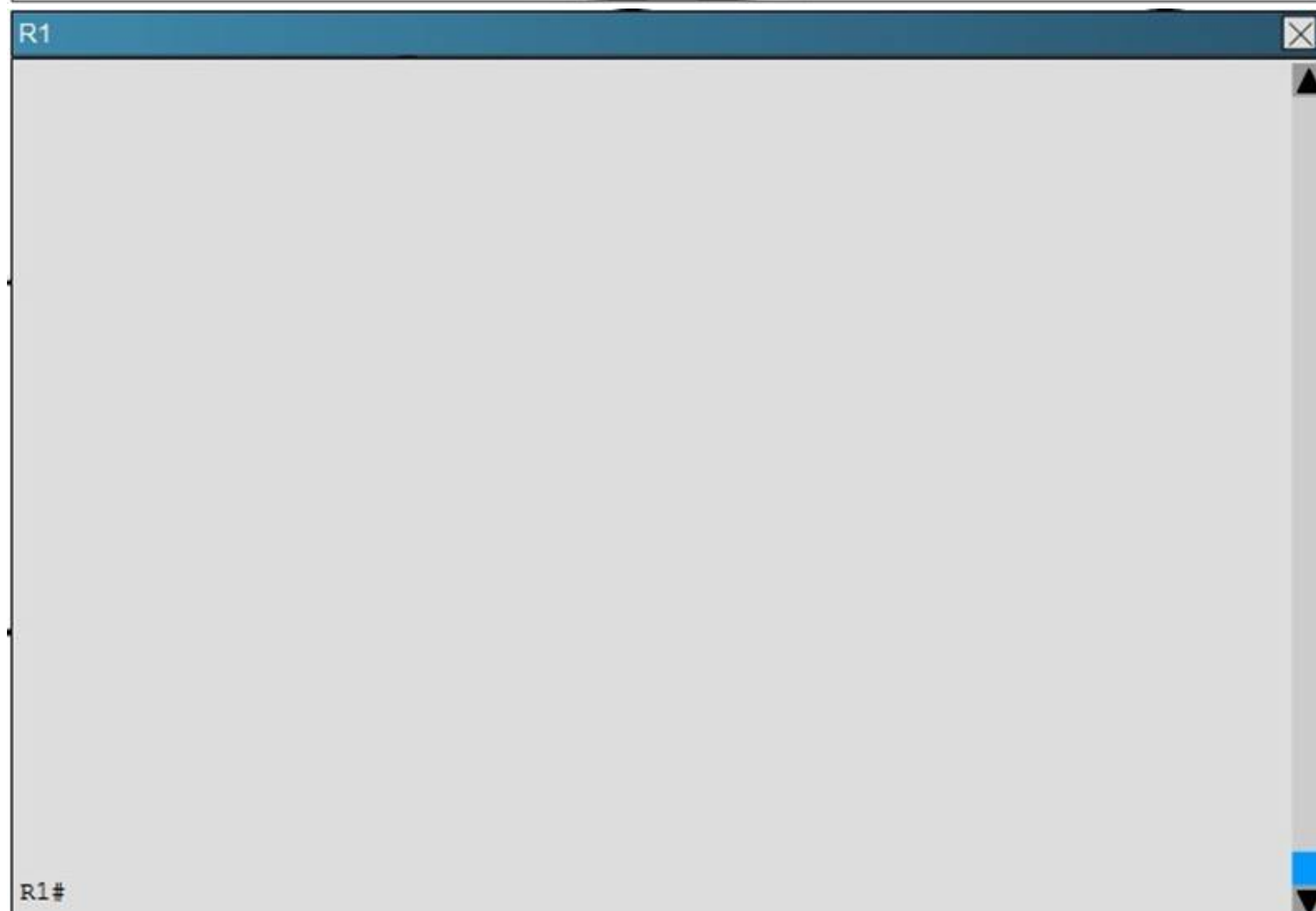
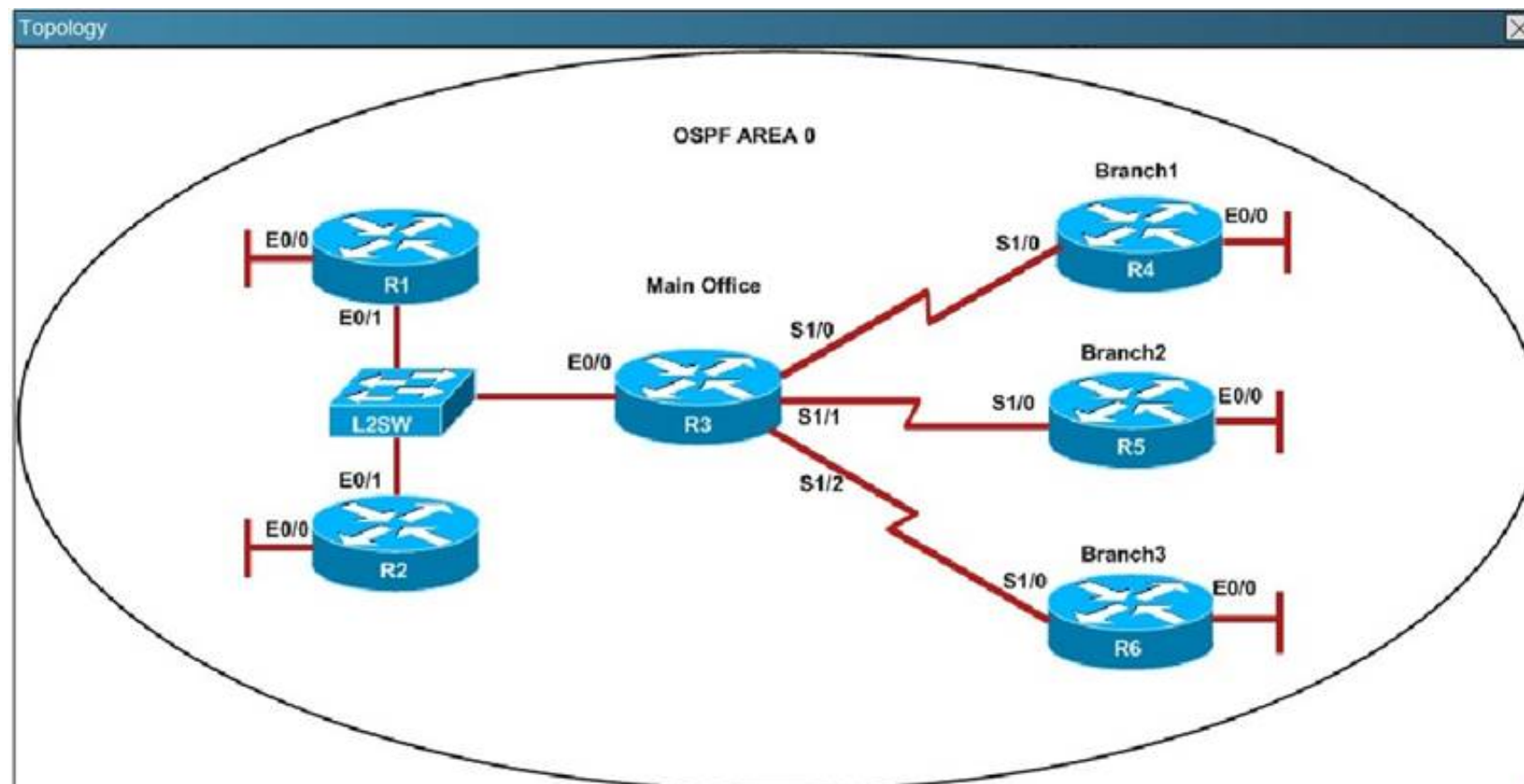
Administrative distance is the first criterion that a router uses to determine which routing protocol to use if two protocols provide route information for the same destination. Administrative distance is a measure of the trustworthiness of the source of the routing information. The smaller the administrative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

NEW QUESTION 160

Scenario

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

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



R2

R2#

R3

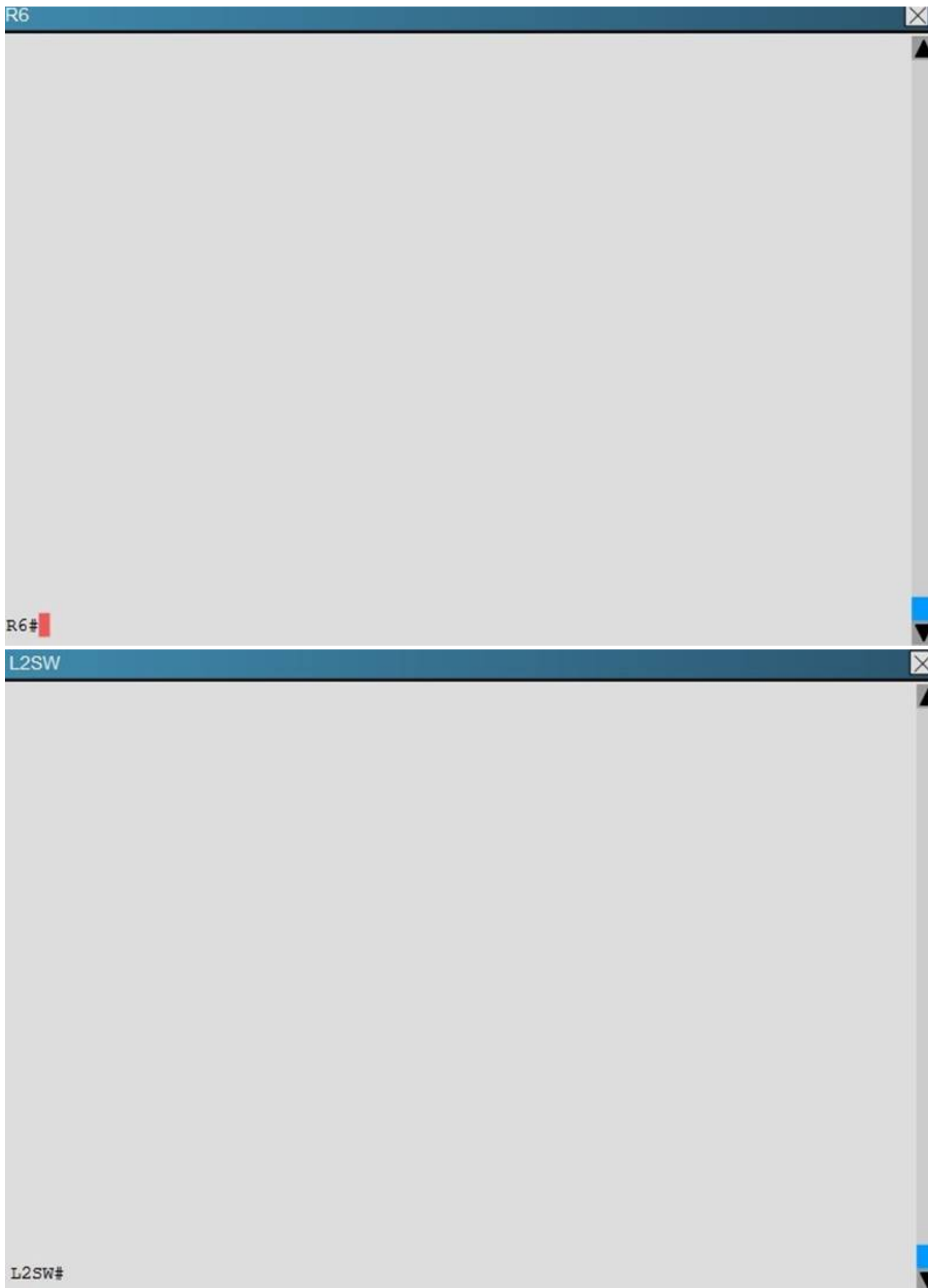
R3#

R4

R4#

R5

R5#



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

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

Answer: D

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

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

NEW QUESTION 163

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

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

Answer: D

Explanation: The “show ip ospf database” command displays the link states. Here is an example: Here is the lsa database on R2.

```

R2#show ip ospf database
OSPF Router with ID (2.2.2.2) (Process ID 1) Router Link States (Area 0)
Link ID ADV Router Age Seq# Checksum Link count 2.2.2.2 2.2.2.2 793 0x80000003 0x004F85 2
10.4.4.4 10.4.4.4 776 0x80000004 0x005643 1

```

NEW QUESTION 165

```

111.111.111 111.111.111.111 755 0x80000005 0x0059CA 2
133.133.133.133 133.133.133.133 775 0x80000005 0x00B5B1 2
Net Link States (Area 0)
Link ID ADV Router Age Seq# Checksum 10.1.1.1 111.111.111.111 794 0x80000001 0x001E8B
10.2.2.3 133.133.133.133 812 0x80000001 0x004BA9
10.4.4.1 111.111.111.111 755 0x80000001 0x007F16
10.4.4.3 133.133.133.133 775 0x80000001 0x00C31F

```

102.

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

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

Answer: B

Explanation: The 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

NEW QUESTION 168

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.

108.

Refer to the exhibit.

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

A network associate has configured OSPF with the command: City(config-router)# network 192.168.12.64 0.0.0.63 area 0

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

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

Answer: BCD

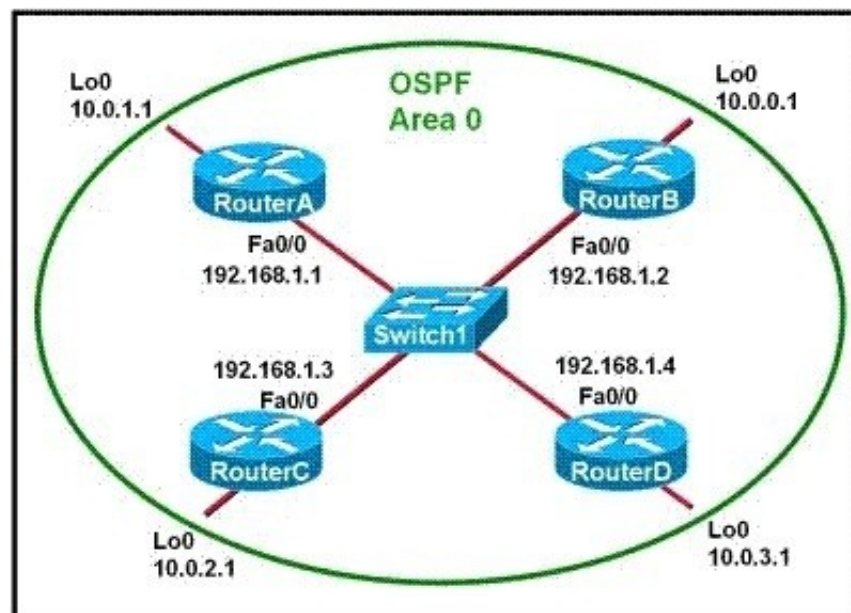
Explanation: This question is to examine the conditions for OSPF to create neighborhood.

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

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

NEW QUESTION 172

Refer to the exhibit.



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

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

Answer: BC

Explanation: A loopback interface never comes down even if the link is broken so it provides stability for the OSPF process (for example we use that loopback interface as the router-id) - The router-ID is chosen in the order below:
+ The highest IP address assigned to a loopback (logical) interface.
+ If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen.
-> The loopback interface will be chosen as the router ID of RouterB -

NEW QUESTION 173

Refer to the exhibit.

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

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

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

Answer: C

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

NEW QUESTION 175

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

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

Answer: BC

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

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

Optionally, every interface can have multiple unique local and global addresses. IPv6 host addresses can be assigned in multiple ways:

Static configuration Stateless autoconfiguration DHCPv6

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

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

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

NEW QUESTION 179

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

- A. Each OSPF area requires a loopback interface to be configured.
- B. Areas may be assigned any number from 0 to 65535.
- C. Area 0 is called the backbone area.
- D. Hierarchical OSPF networks do not require multiple areas.
- E. Multiple OSPF areas must connect to area 0.
- F. Single area OSPF networks must be configured in area 1.

Answer: BCE

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

See discussion following Cisco Learning discussion. <https://learningnetwork.cisco.com/message/90832>

NEW QUESTION 184

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

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

Answer: BCE

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

RIP version 1 updates are broadcasts, and RIP version 2 updates are multicast to

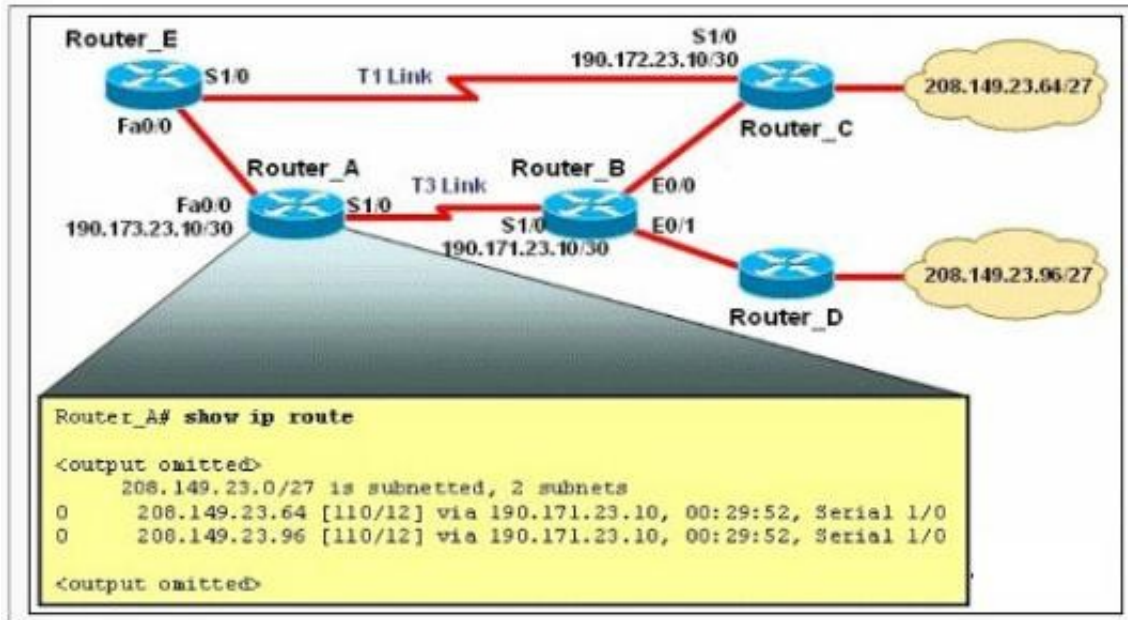
224.0.0.9 -> B is not correct.

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

RIPv1 and RIPv2 have the same default administrative distance of 120 -> D is not correct. RIPv2 is a classless routing protocol so it does send the subnet mask in updates -> F is not correct.

NEW QUESTION 187

Refer to the exhibit.



The network is converged. After link-state advertisements are received from Router_A, what information will Router_E contain in its routing table for the subnets 208.149.23.64 and 208.149.23.96?

- A. 208.149.23.64[110/13] via 190.173.23.10, 00:00:07, FastEthernet0/0 208.149.23.96[110/13] via 190.173.23.10, 00:00:16, FastEthernet0/0
- B. 208.149.23.64[110/1] via 190.172.23.10, 00:00:07, Serial1/0 208.149.23.96[110/3] via 190.173.23.10, 00:00:16, FastEthernet0/0
- C. 208.149.23.64[110/13] via 190.173.23.10, 00:00:07, Serial1/0 208.149.23.96[110/13] via 190.173.23.10, 00:00:16, Serial1/0 208.149.23.96[110/13] via 190.173.23.10, 00:00:16, FastEthernet0/0
- D. 208.149.23.64[110/3] via 190.172.23.10, 00:00:07, Serial1/0 208.149.23.96[110/3] via 190.173.23.10, 00:00:16, Serial1/0

Answer: A

Explanation: Router_E learns two subnets subnets 208.149.23.64 and 208.149.23.96 via Router_A through FastEthernet interface. The interface cost is calculated with the formula $108 / \text{Bandwidth}$. For FastEthernet it is $108 / 100 \text{ Mbps} = 108 / 100,000,000 = 1$. Therefore the cost is 12 (learned from Router_A) + 1 = 13 for both subnets ->

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

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

NEW QUESTION 192

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

- A. 2
- B. 8
- C. 16
- D. unlimited

Answer: B

Explanation: Maximum-paths (OSPF)

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

Syntax Description

maximum

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

Command Default

8 paths

NEW QUESTION 196

Which command enables IPv6 forwarding on a Cisco router?

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

Answer: B

Explanation: Enabling IPv6 on Cisco IOS Software Technology <http://www.ciscopress.com/articles/article.asp?p=31948&seqNum=4>

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

The ipv6 unicast-routing command is used to enable the forwarding of IPv6 packets between interfaces on the router. The syntax for this command is as follows:
Router(config)#ipv6 unicast-routing The ipv6 unicast-routing command is enabled on a global basis.

NEW QUESTION 197

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

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

Answer: CE

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

NEW QUESTION 201

DRAG DROP

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

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

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

Answer:

Explanation:

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

ICMP	ARP
DHCP	ICMP
RARP	DNS
UDP	DHCP
DNS	
ARP	

NEW QUESTION 202

DRAG DROP

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

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

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

Answer:

Explanation:

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

OSPF	NAT
ARP	DHCP
NAT	DNS
DNS	OSPF
SQL	
DHCP	

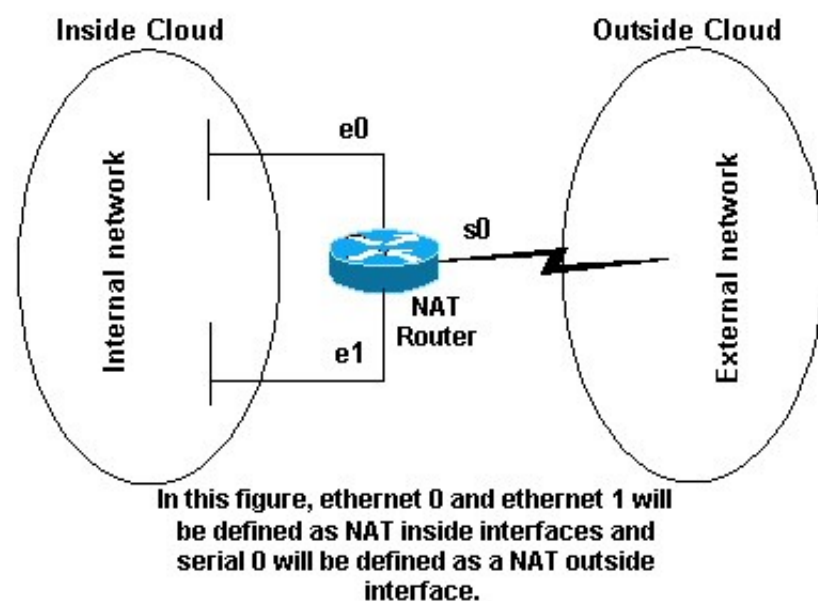
NEW QUESTION 205

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

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

Answer: D

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



Reference: <http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html#topic2>

NEW QUESTION 208

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

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

Answer: C

Explanation: The keyword overload used in theip nat inside source list 1 pool ovrlid overload example command allows NAT to translate multiple inside devices to the single address in the pool.

The types of NAT include:

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

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

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

NEW QUESTION 209

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

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

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

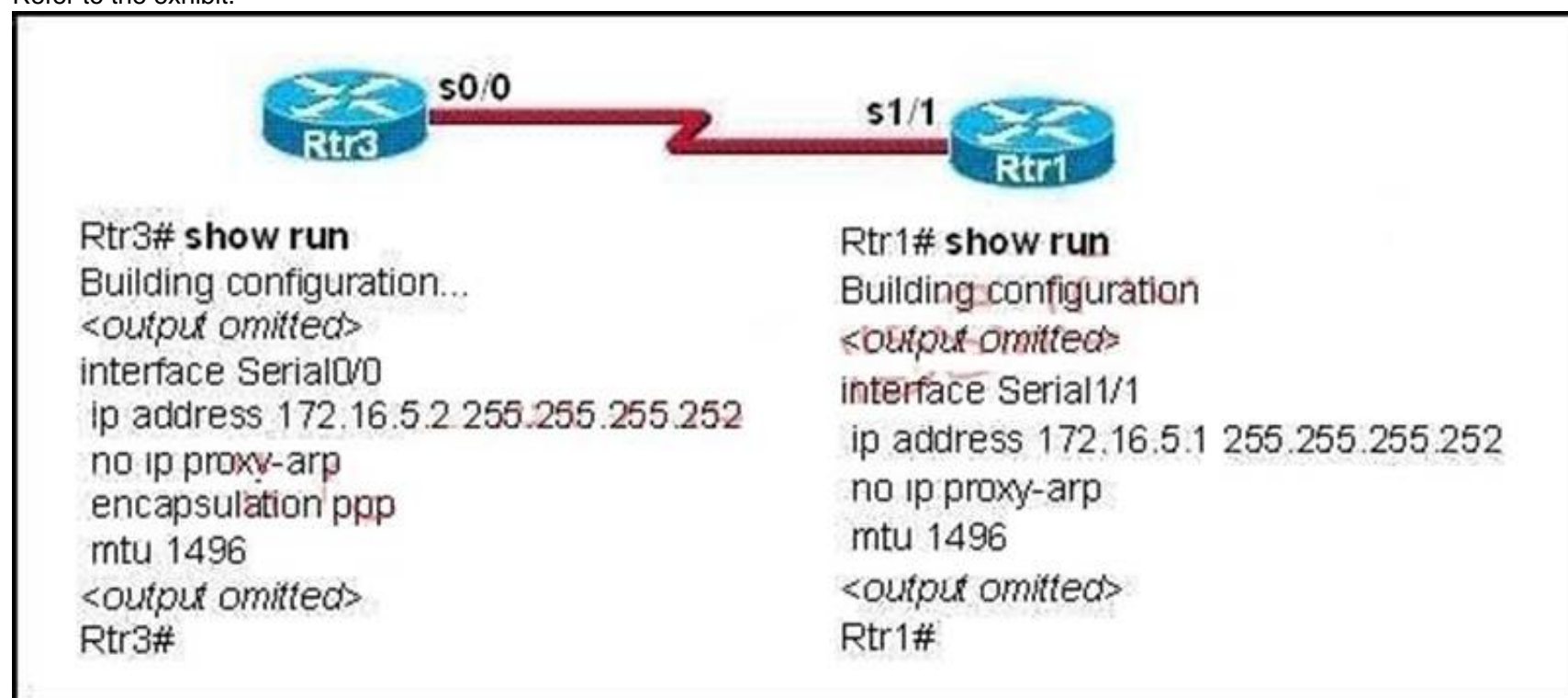
- A. 7
- B. 8
- C. 9
- D. 10
- E. 24
- F. 32

Answer: B

Explanation: 209.165.201.23 to 209.165.201.30 provides for 8 addresses.

NEW QUESTION 213

Refer to the exhibit.



A network administrator is troubleshooting a connectivity problem on the serial interfaces. The output from the show interfaces command on both routers shows that the serial interface is up, line protocol is down. Given the partial output for the show running-config in the exhibit, what is the most likely cause of this problem?

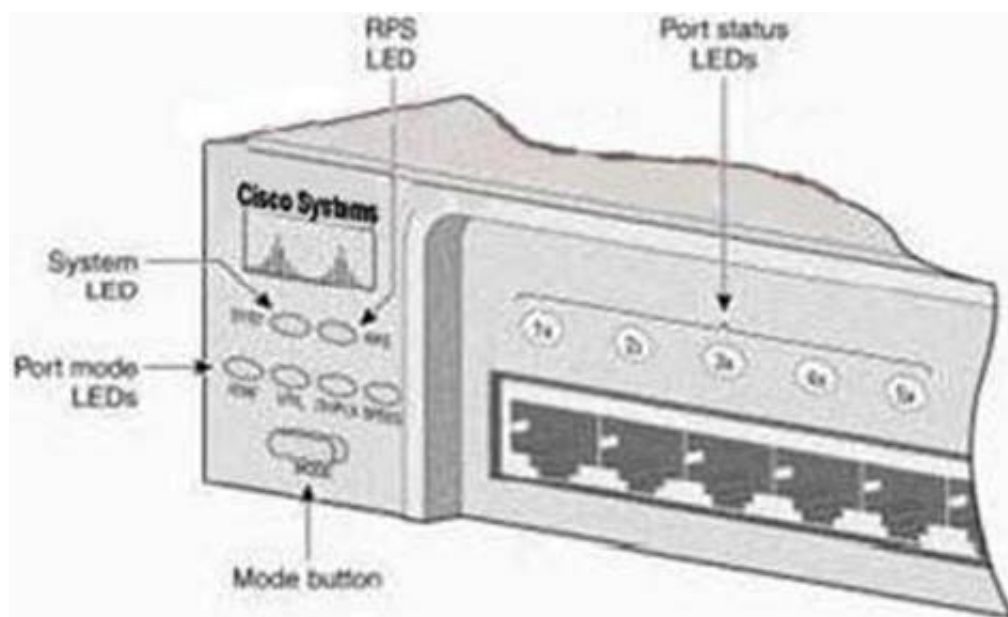
- A. The serial cable is bad.
- B. The MTU is incorrectly configured.
- C. The Layer 2 framing is misconfigured.
- D. The IP addresses are not in the same subnet.

Answer: C

Explanation: Here we see that Rtr3 is configured to use PPP encapsulation, but Rtr1 has not been configured for any kind of encapsulation. The default on Cisco router serial interfaces is HDLC, not PPP, so there is an encapsulation mismatch.

NEW QUESTION 216

Refer to the exhibit.



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

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

Answer: C

Explanation: http://www.cisco.com/en/US/products/hw/switches/ps607/products_tech_note09186a00801_25913.shtml

Each time you power up the switch, eight Power-On Self Tests (POSTs) run automatically. POSTs check the most important system components before the switch begins to forward packets. When the switch begins the POST, the port status LEDs display amber for two seconds, and then display green. As each test runs, the port status LEDs go out. 1x is the first to go out. The port status LEDs for ports 2x through 8x go out sequentially as the system completes a test. When the POST completes successfully, the port status LEDs go out. This indicates that the switch is operational. If a test fails, the port status LED associated with the test displays

amber. The system LED also displays amber.

Not E: From Cisco IOS Software Release 11.2(8.5) SA6 onwards, the port and system LEDs both remain amber after a POST failure. In the earlier Cisco IOS Software Releases, only the LEDs of failed linked ports remained amber.

NEW QUESTION 219

Refer to the exhibit.

```

Finance# show interfaces fastEthernet 0/2
FastEthernet0/2 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 0017.596d.2a02
  Description: To Central Fa0/0
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:03, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
<output omitted>
    
```

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

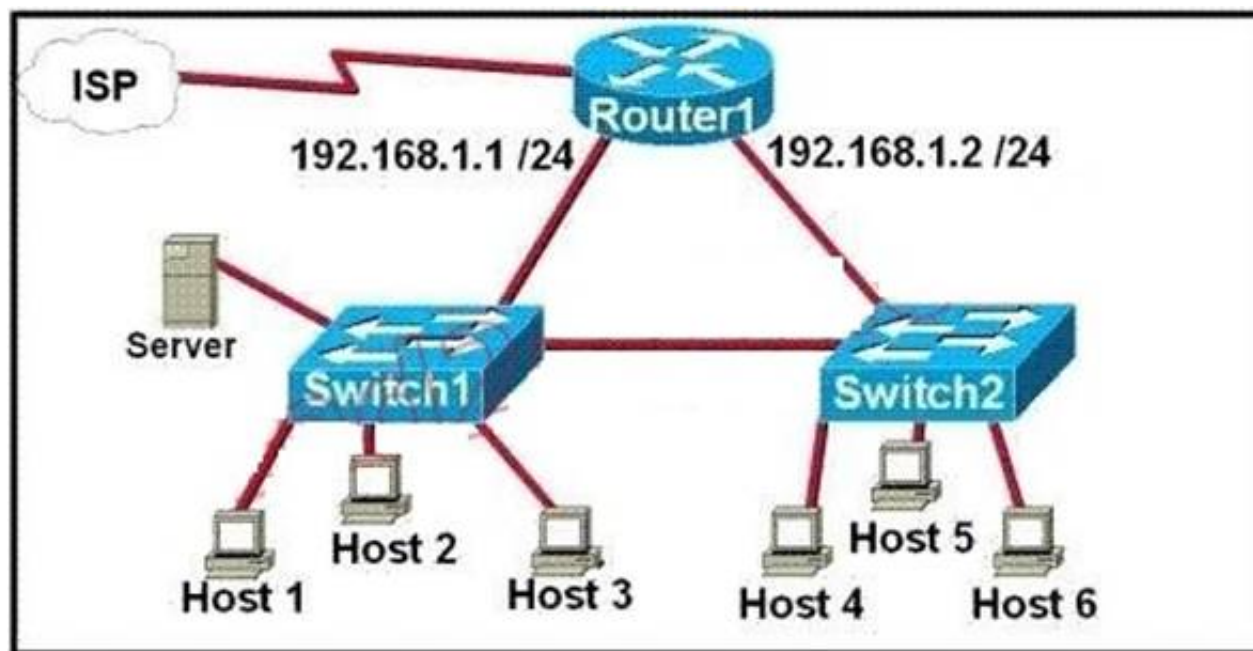
- A. Speed is set to 100Mb/s.
- B. Input flow control is off.
- C. Encapsulation is set to ARPA.
- D. The port is administratively down.
- E. The counters have never been cleared.

Answer: A

Explanation: For PC to switch connectivity, the speed settings must match. In this case, the 1 Gb NIC will not be able to communicate with a 100Mb fast Ethernet interface, unless the 1Gb NIC can be configured to connect at 100Mb.

NEW QUESTION 224

Refer to the exhibit.



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

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

Answer: C

Explanation: The proposed addressing scheme is on the same network. Cisco routers will not allow you to assign two different interfaces to be on the same IP subnet.

NEW QUESTION 227

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

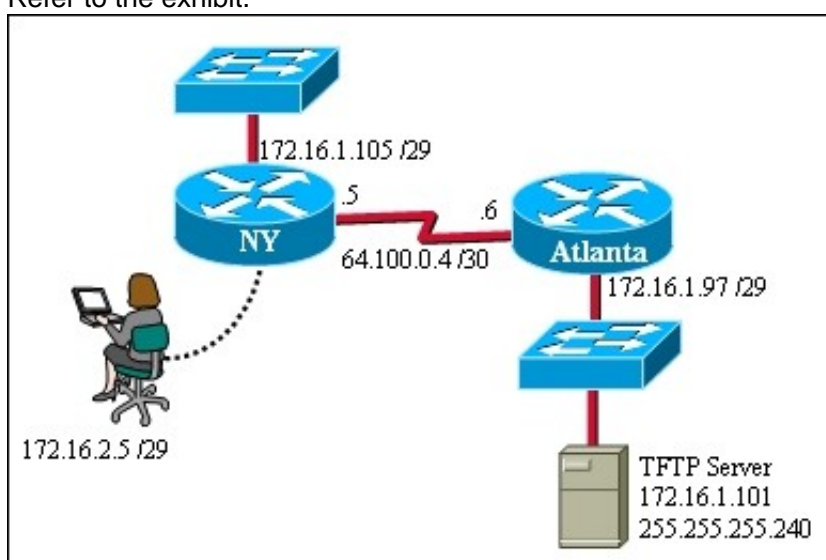
- A. Configure port Fa0/1 to accept connections only from the static IP address of the server.
- B. Configure the server MAC address as a static entry of port security.
- C. Use a proprietary connector type on Fa0/1 that is incompatible with other host connectors.
- D. Bind the IP address of the server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

Answer: B

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

NEW QUESTION 230

Refer to the exhibit.



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

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

Answer: C

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

NEW QUESTION 235

Instructions

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

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

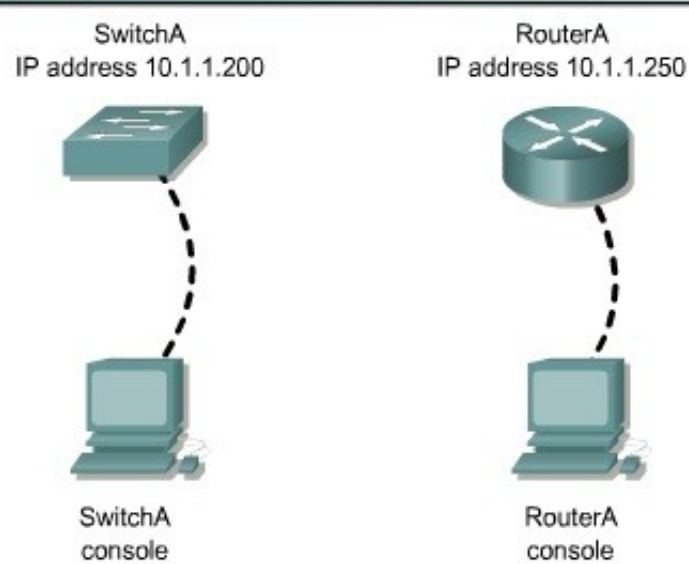
This task requires the use of various IOS commands to access and inspect the running configuration of RouterA and SwitchA. No configuration changes are necessary.

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

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

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

Topology



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

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

Answer: ABD

NEW QUESTION 240

The following commands are entered on the router:

```
Burbank(config)# enable secret fortress Burbank(config)# line con 0 Burbank(config-line)# login
```

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

```
Burbank(config)# service password-encryption
```

What is the purpose of the last command entered?

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

Answer: B

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

NEW QUESTION 242

Instructions

You can click on the grey buttons below to view the different windows.

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

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

Scenario

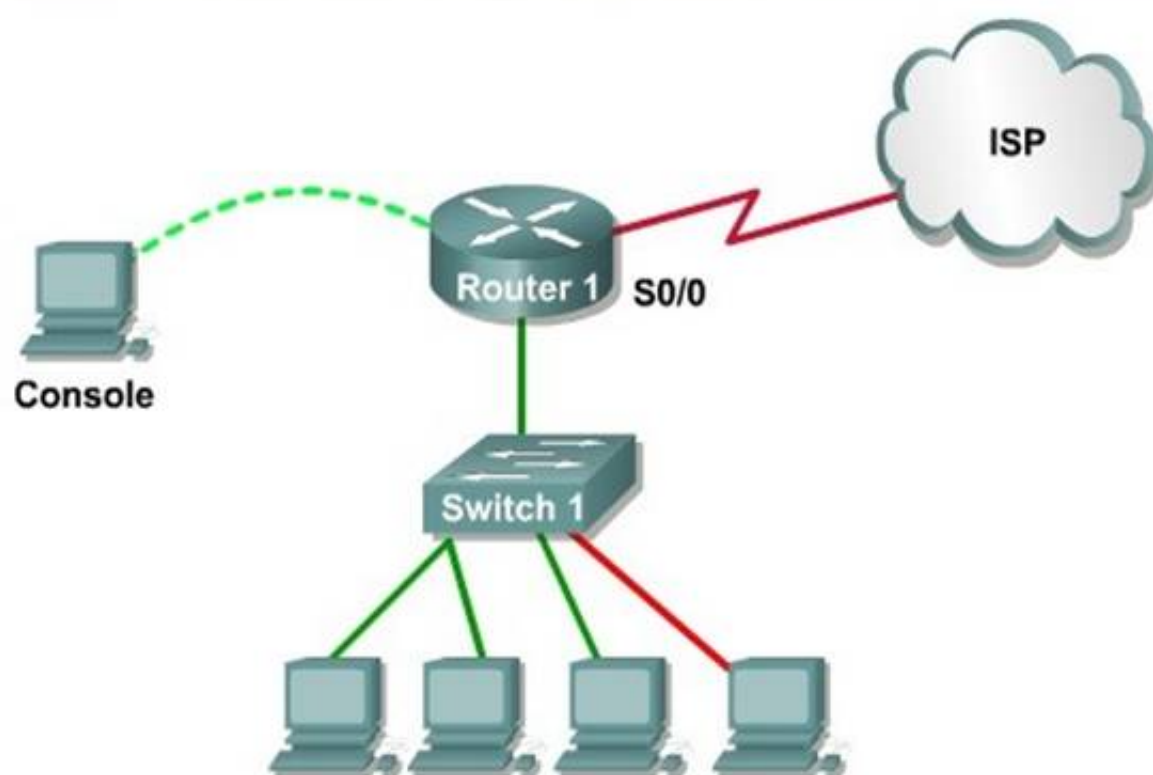
This task requires the use of various **show** commands from the CLI of Router1 to answer four multiple-choice questions. This task does **not** require any configuration.

NOTE: The show running-configuration and the show startup-configuration commands have been disabled in this simulation.

To access the multiple-choice questions, click on the numbered boxes on the right of the top panel.

There are 4 multiple-choice questions with this task. Be sure to answer all 4 questions before leaving this item.

Topology



R1

Press RETURN to get started!
Router1>

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

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

Answer: A

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

NEW QUESTION 246

DRAG DROP

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

Drag the appropriate command on the left to the configuration task it accomplishes. (Not all options are used.)	
login password cantCome1n	encrypt all clear text passwords
enable password uwi11NeverNo	protect access to the user mode prompt
service password-encryption	set privileged mode encrypted password
line console 0 password friendS0nly	set password to allow Telnet connections
enable secret noWay1n4u	set privileged mode clear text password
line vty 0 4 password 2hard2Guess	

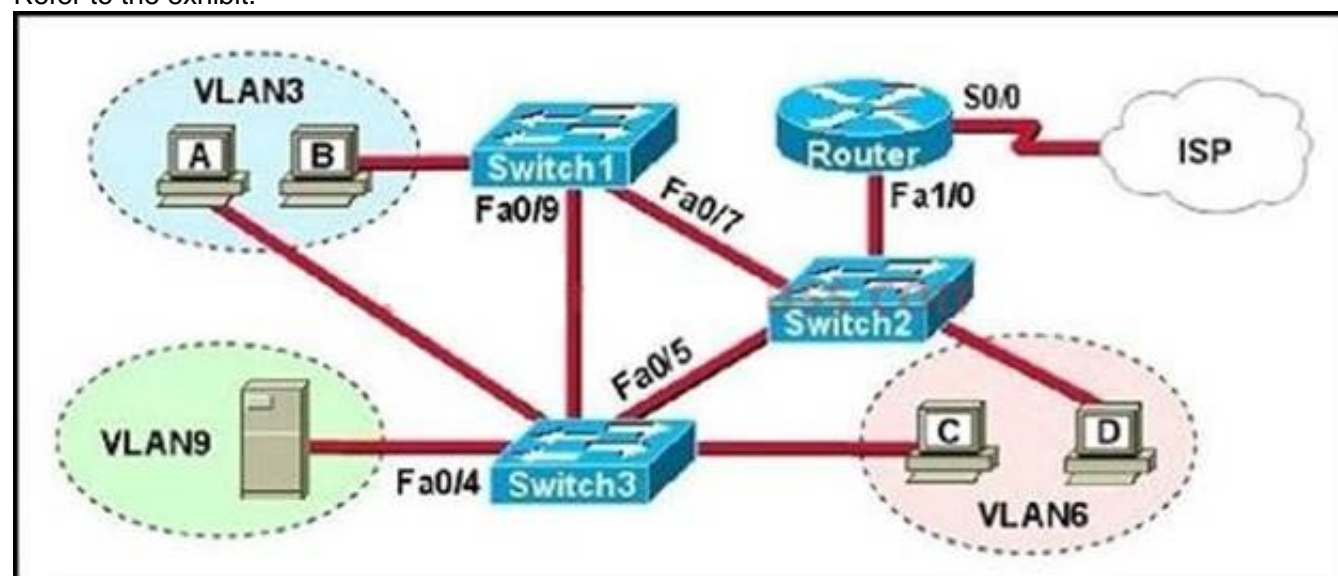
Answer:

Explanation:

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	

NEW QUESTION 248

Refer to the exhibit.



A problem with network connectivity has been observed. It is suspected that the cable connected to switch port Fa0/9 on Switch1 is disconnected. What would be

an effect of this cable being disconnected?

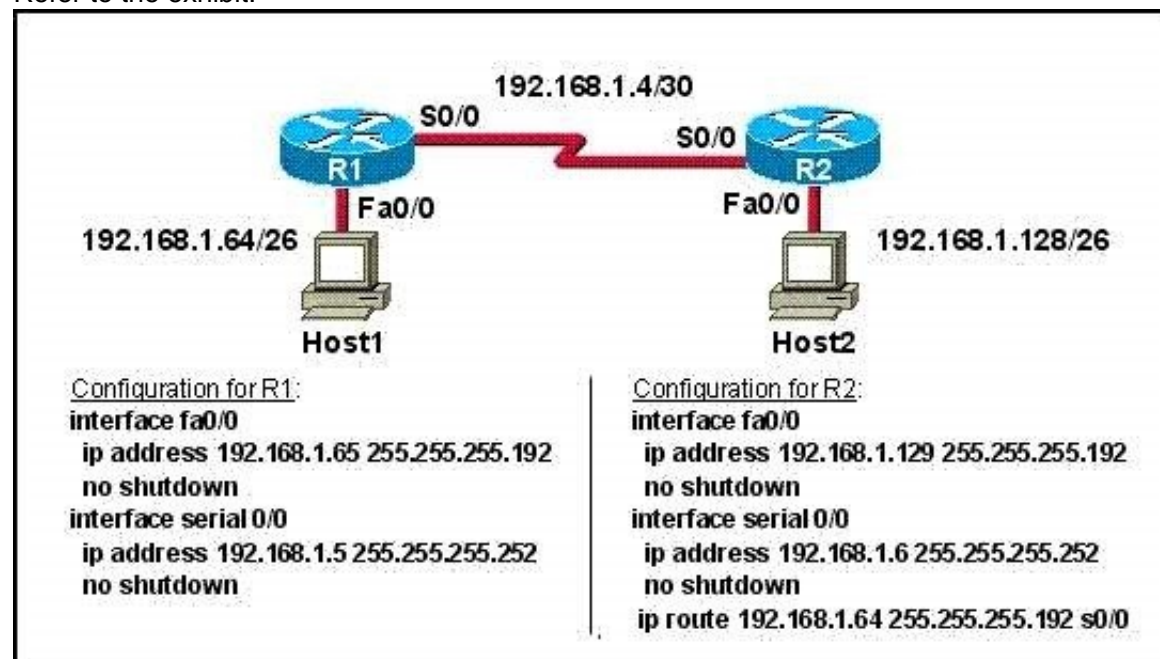
- A. Host B would not be able to access the server in VLAN9 until the cable is reconnected.
- B. Communication between VLAN3 and the other VLANs would be disabled.
- C. The transfer of files from Host B to the server in VLAN9 would be significantly slower.
- D. For less than a minute, Host B would not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

Answer: D

Explanation: Because Switch1 has multiple redundant links in this network, traffic would not work for less than a minute, and then it would get rerouted along the longer path to the host. The 1 minute outage would be the length of time it takes STP to converge.

NEW QUESTION 250

Refer to the exhibit.



A technician pastes the configurations in the exhibit into the two new routers shown. Otherwise, the routers are configured with their default configurations. A ping from Host1 to Host 2 fails, but the technician is able to ping the S0/0 interface of R2 from Host 1. The configurations of the hosts have been verified as correct. What could be the cause of the problem?

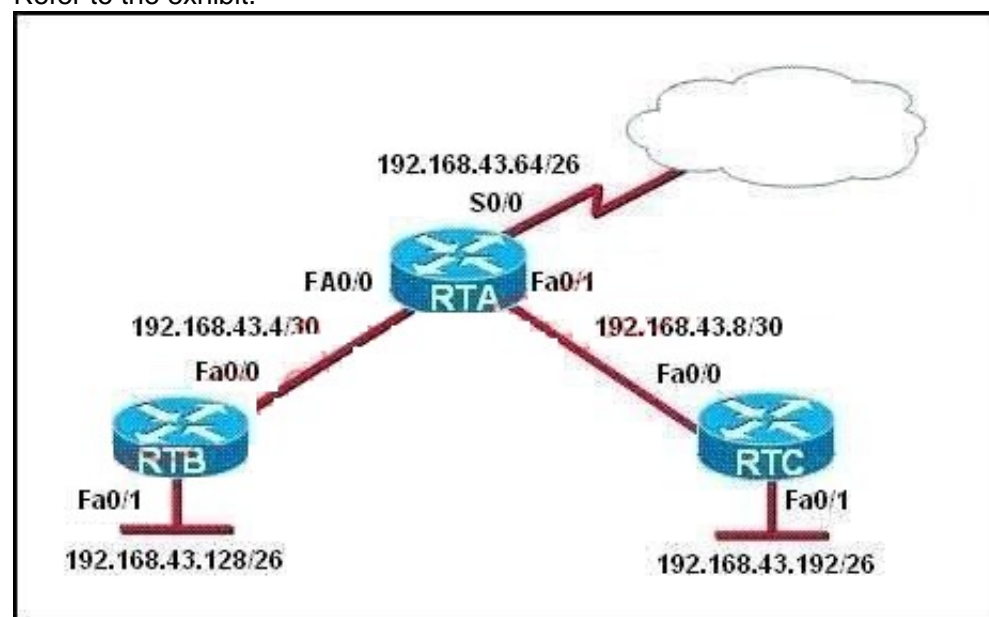
- A. The serial cable on R1 needs to be replaced.
- B. The interfaces on R2 are not configured properly
- C. R1 has no route to the 192.168.1.128 network.
- D. The IP addressing scheme has overlapping subnetworks.
- E. The ip subnet-zero command must be configured on both routers.

Answer: C

Explanation: Without a static route pointing to the host 2 network the router R1 is unaware of the path to take to reach that network and reply traffic cannot be sent.

NEW QUESTION 253

Refer to the exhibit.



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

Which command or series of commands will accomplish these objectives?

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

Answer: D

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

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

Router#show cdp neighbors

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

Device ID	Local Intrfce	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

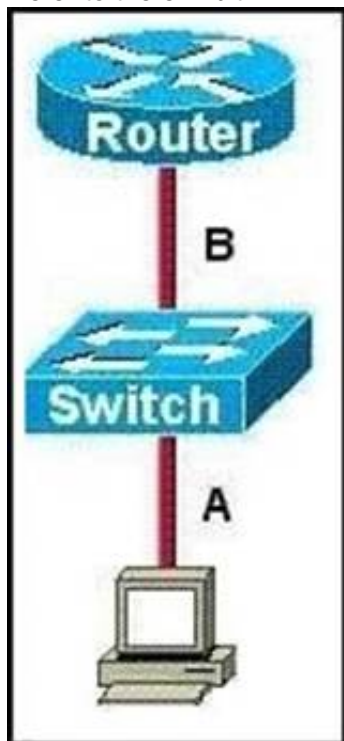
Enter configuration commands, one per line. End with CNTL/Z. Router(config)#interface s1

Router(config-if)#no cdp enable Router(config-if)# Z

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

NEW QUESTION 257

Refer to the exhibit.



The two connected ports on the switch are not turning orange or green. What would be the most effective steps to troubleshoot this physical layer problem? (Choose three.)

- A. Ensure that the Ethernet encapsulations match on the interconnected router and switch ports.
- B. Ensure that cables A and B are straight-through cables.
- C. Ensure cable A is plugged into a trunk port.
- D. Ensure the switch has power.
- E. Reboot all of the devices.
- F. Reseat all cables.

Answer: BDF

Explanation: The ports on the switch are not up indicating it is a layer 1 (physical) problem so we should check cable type, power and how they are plugged in.

NEW QUESTION 261

The network administrator has found the following problem.

Central# debug ip rip

<some output text omitted>

Central#debug ip rip

1d00h: RIP: received v1 update from 172.16.100.2 on Serial0/0

1d00h: 172.16.10.0 in 1 hops

1d00h: 172.16.20.0 in 1 hops

1d00h: 172.16.30.0 in 1 hops

Central# show ip route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 8 subnets

C 172.16.150.0 is directly connected, FastEthernet0/0

C 172.16.220.0 is directly connected, Loopback2

C 172.16.210.0 is directly connected, Loopback1

C 172.16.200.0 is directly connected, Loopback0

R 172.16.30.0 [120/1] via 172.16.100.2, 00:00:07, Serial0/0

S 172.16.20.0 [1/0] via 172.16.150.15

R 172.16.10.0 [120/1] via 172.16.100.2, 00:00:07, Serial0/0

C 172.16.100.0 is directly connected, Serial0/0

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

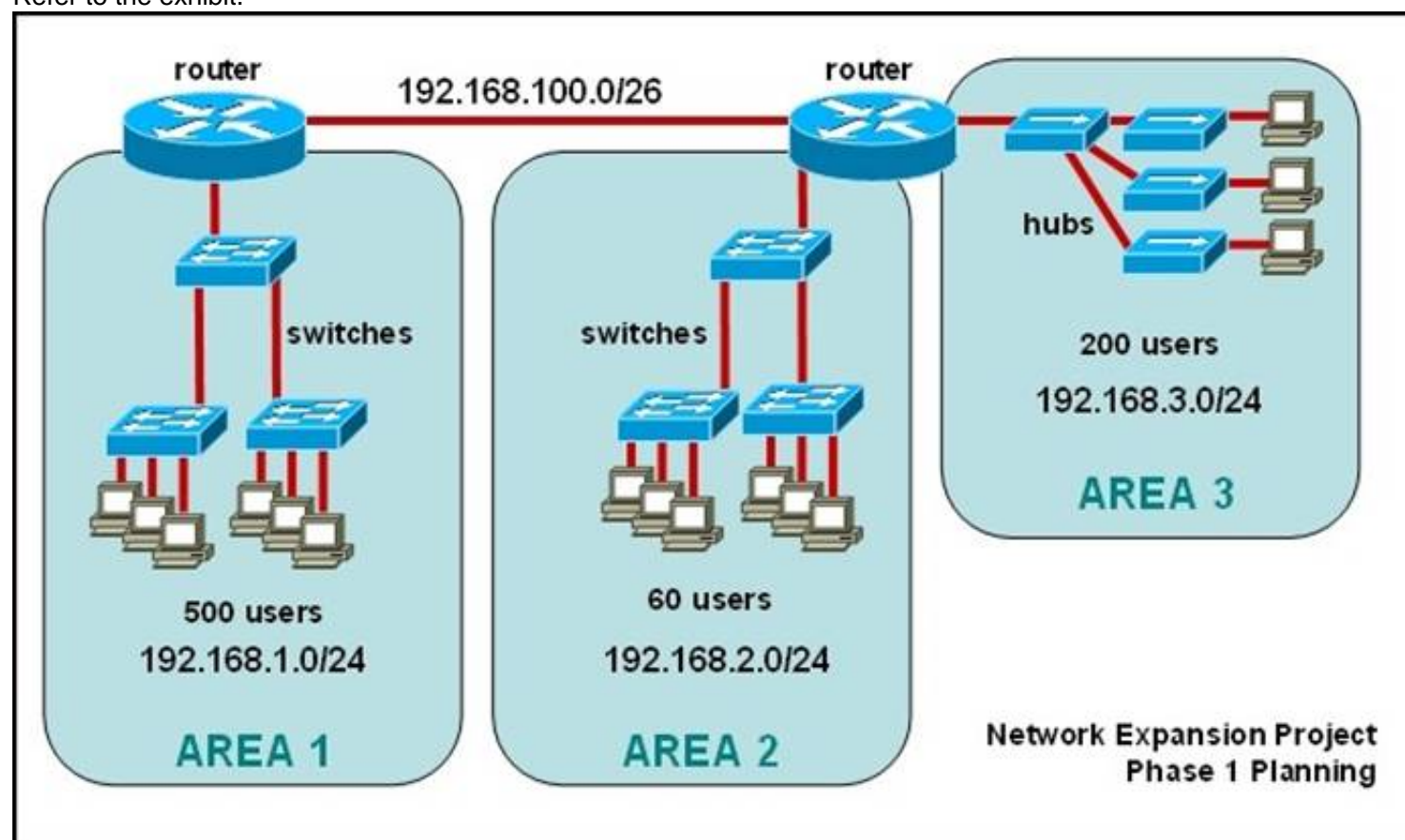
- A. no gateway of last resort on Central
- B. Central router's not receiving 172.16.20.0 update
- C. incorrect static route for 172.16.20.0
- D. 172.16.20.0 not located in Central's routing table

Answer: C

Explanation: If we use 172.16.20.0 to route to 172.16.150.15, then the packet will route back. To clear this error we have to use #no ip route 172.16.20.0 255.255.255.0 172.16.150.15 command in configuration mode.

NEW QUESTION 266

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.

Answer:

NEW QUESTION 267

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

- A. Allow unrestricted access to the console or VTY ports.
- B. Use a firewall to restrict access from the outside to the network devices.
- C. Always use Telnet to access the device command line because its data is automatically encrypted.
- D. Use SSH or another encrypted and authenticated transport to access device configurations.

E. Prevent the loss of passwords by disabling password encryption.

Answer: BD

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

NEW QUESTION 272

What is the purpose of the switchport command?

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

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

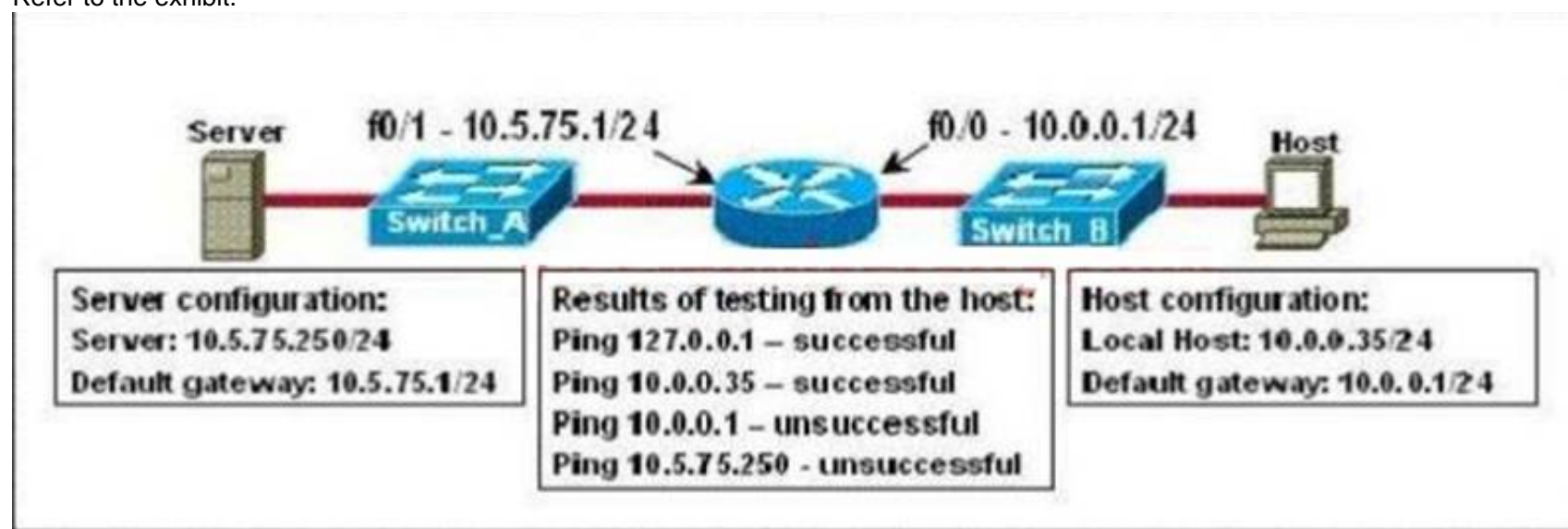
- A. It ensures that only the device with the MAC address 0018.DE8B.4BF8 will be able to connect to the port that is being configured.
- B. It informs the switch that traffic destined for MAC address 0018.DE8B.4BF8 should only be sent to the port that is being configured.
- C. It will act like an access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

Answer: A

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

NEW QUESTION 275

Refer to the exhibit.



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

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

Answer: D

Explanation: Here we see that the host is able to ping its own loopback IP address of 127.0.0.1 and its own IP address of 10.0.0.35, so we know that the NIC is functioning and that the host's TCP/IP stack is OK. However, it is not able to ping the IP address of its local default gateway, so we know that there is a local cabling problem between the switch and the router.

NEW QUESTION 278

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

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

Answer: C

Explanation: Message Authentication Code (MAC) can shield your network from spoofing attacks. Spoofing, also known as masquerading, is a popular trick in which an attacker intercepts a network packet, replaces the source address of the packets header with the address of the authorized host, and reinserts fake information which is sent to the receiver. This type of attack involves modifying packet contents. MAC can prevent this type of attack and ensure data integrity by ensuring that no data has changed. MAC also protects against frequency analysis, sequence manipulation, and ciphertext-only attacks. MAC is a secure message digest that requires a secret key shared by the sender and receiver, making it impossible for sniffers to change both the data and the MAC as the receiver can detect the changes.

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

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

attacks.

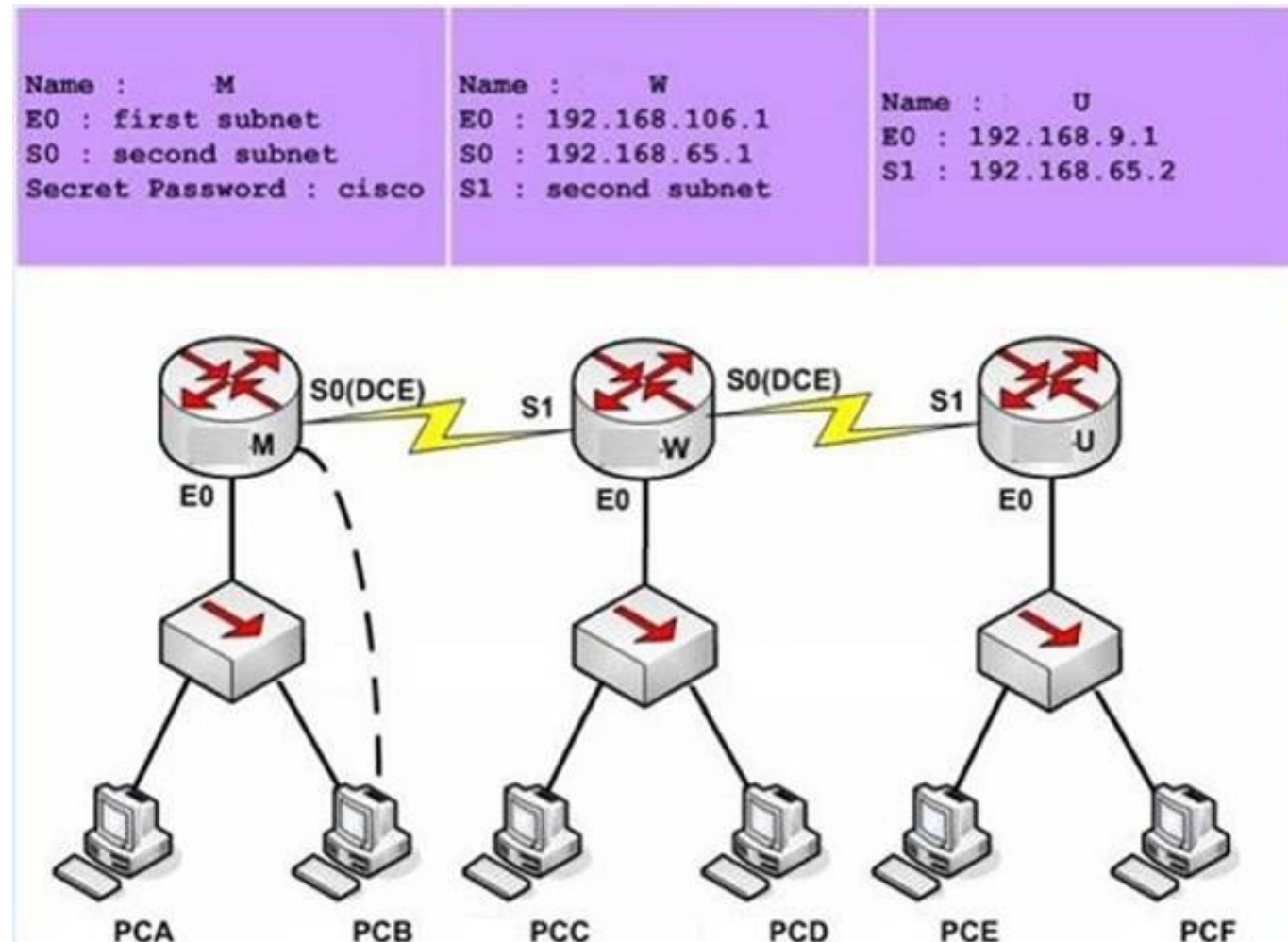
In a SYN flood attack, the attacker floods the target with spoofed IP packets and causes it to either freeze or crash. A SYN flood attack is a type of denial of service attack that exploits the buffers of a device that accept incoming connections and therefore cannot be prevented by MAC. Common defenses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

Topic 6, Simulation

NEW QUESTION 279

CORRECT TEXT

There are three locations in a school district of a large city: ROUTER -M, ROUTER -W and ROUTER -U. The network connection between two of these locations has already functioned. Configure the ROUTER -M router IP addresses on the E0 and S0 interfaces so that the E0 receives the first usable subnet while the S0 receives the second usable subnet from the network 192.168.160.0/28. Both interfaces would receive the last available ip address on the proper subnet.



NotE. The OSPF process must be configured to allow interfaces in specific subnets to participate in the routing process.

Answer:

Explanation: ROUTER-M> enable Password. Cisco

```
ROUTER-M# config t
ROUTER-M(config)# interface e0
ROUTER-M(config-if)# ip address 192.168.160.14 255.255.255.240
ROUTER-M(config-if)# no shutdown
ROUTER-M(config-if)# exit
ROUTER-M(config)# interface s0
ROUTER-M(config-if)# ip address 192.168.160.30 255.255.255.240
ROUTER-M(config-if)# no shutdown
ROUTER-M(config-if)# end
ROUTER-M# copy run start
```

NEW QUESTION 284

CORRECT TEXT

Topology

Instructions

To configure the router (Apopka) click on the console host icon that is connected to a router by a serial console cable (shown in the diagram as a dashed black line).

You can click on the buttons below to view the different windows.

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

The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation. The **help** command does not display all commands of the help system.

Scenario

Central Florida Widgets recently installed a new router in their Apopka office. Complete the network installation by performing the initial router configurations and configuring RIP v2 routing using the router command line interface (CLI) on the Apopka router.

Configure the router per the following requirements:

- Name of the router is **Apopka**
- Enable-secret password is **ish555ana**
- The password to access user EXEC mode using the console is **New2Rtr**
- The password to allow telnet access to the router is **str8R0us**
- IPv4 addresses must be configured as follows:
 - Ethernet network **209.165.201.0 /27** - router has **second** assignable host address in subnet.
 - Serial network is **192.0.2.128 /28** - router has **last** assignable host address in the subnet.
- Interfaces should be enabled.
- Routing protocol is **RIP v2**.

Answer:

Explanation: Router>enable

Router#config terminal

Router(config)#hostname Apopka

2) Enable-secret password (cisco10):

Apopka(config)#enable secret cisco10

3) Set the console password to RouterPass:

Apopka(config)#line console 0

Apopka(config-line)#password RouterPass

Apopka(config-line)#login

Apopka(config-line)#exit

4) Set the Telnet password to scan90:

Apopka(config)#line vty 0 4

Apopka(config-line)#password scan90

Apopka(config-line)#login

Apopka(config-line)#exit

5) Configure Ethernet interface (on the right) of router Apopka:

The subnet mask of the Ethernet network 209.165.201.0 is 27. From this subnet mask, we can find out the increment by converting it into binary form, that is /27 = 1111 1111.1111 1111.1111 1110 0000. Pay more attention to the last bit 1 because it tells us the increment, using the formula:

Increment = 2^{place of the last bit 1} (starts counting from 0, from right to left), in this case increment = 25 = 32. Therefore:

Increment: 32

Network address: 209.165.201.0

Broadcast address: 209.165.201.31 (because 209.165.201.32 is the second subnetwork, so the previous IP - 209.165.201.31 - is the broadcast address of the first subnet).

-> The second assignable host address of this subnetwork is 209.165.201.2/27 Assign the second assignable host address to Fa0/0 interface of Apopka router:

Apopka(config)#interface Fa0/0

Apopka(config-if)#ip address 209.165.201.2 255.255.255.224 Apopka(config-if)#no shutdown

Apopka(config-if)#exit

6) Configure Serial interface (on the left) of router Apopka:

Using the same method to find out the increment of the Serial network: Serial network 192.0.2.128/28:

Increment: 16 (/28 = 1111 1111.1111 1111.1111 1111 0000)

Network address: 192.0.2.128 (because 8 * 16 = 128 so 192.0.2.128 is also the network address of this subnet)

Broadcast address: 192.0.2.143

-> The last assignable host address in this subnet is 192.0.2.142/28.

Assign the last assignable host address to S0/0/0 interface of Apopka router: Apopka(config)#interface S0/0/0 (or use interface S0/0 if not successful)

Apopka(config-if)#ip address 192.0.2.142 255.255.255.240

Apopka(config-if)#no shutdown Apopka(config-if)#exit

7) Configure RIP v2 routing protocol: Apopka(config)#router rip Apopka(config-router)#version 2

Apopka(config-router)#network 209.165.201.0

Apopka(config-router)#network 192.0.2.128 Apopka(config-router)#end

Save the configuration:

Apopka#copy running-config startup-config

Finally, you should use the ping command to verify all are working properly!

NEW QUESTION 287

CORRECT TEXT

This topology contains 3 routers and 1 switch. Complete the topology.

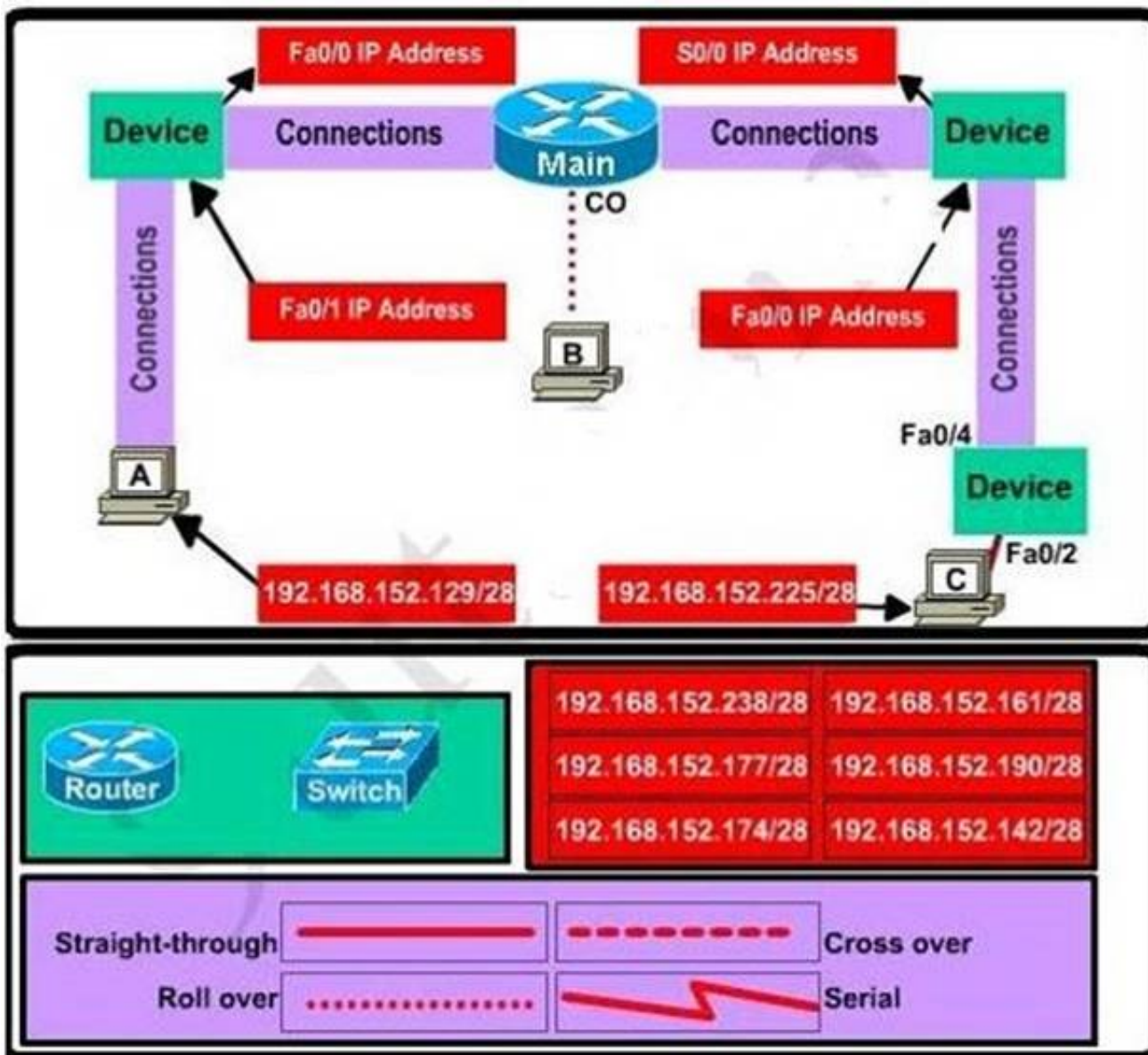
Drag the appropriate device icons to the labeled Device

Drag the appropriate connections to the locations labeled Connections. Drag the appropriate IP addresses to the locations labeled IP address

(Hint: use the given host addresses and Main router information) To remove a device or connection, drag it away from the topology.

Use information gathered from the Main router to complete the configuration of any additional routers.

No passwords are required to access the Main router. The config terminal command has been disabled for the HQ router. The router does not require any configuration.



Configure each additional router with the following:

Configure the interfaces with the correct IP address and enable the interfaces. Set the password to allow console access to consolepw

Set the password to allow telnet access to telnetpw

Set the password to allow privilege mode access to privpw

Not E: Because routes are not being added to the configurations, you will not be able to ping through the internetwork.

All devices have cable autosensing capabilities disabled. All hosts are PC's

Answer:

Explanation: Specify appropriate devices and drag them on the "Device" boxes

For the device at the bottom-right box, we notice that it has 2 interfaces Fa0/2 and Fa0/4; moreover the link connects the PC on the right with the device on the bottom-right is a straight-through link -> it is a switch

The question stated that this topology contains 3 routers and 1 switch -> two other devices are routers

Place them on appropriate locations as following:

(Host D and host E will be automatically added after placing two routers. Click on them to access neighboring routers)

Specify appropriate connections between these devices:

+ The router on the left is connected with the Main router through FastEthernet interfaces: use a crossover cable

+ The router on the right is connected with the Main router through Serial interfaces: use a serial cable

+ The router on the right and the Switch: use a straight-through cable

+ The router on the left and the computer: use a crossover cable

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

- To connect two serial interfaces of 2 routers we use serial cable

- To specify when we use crossover cable or straight-through cable, we should remember:

Group 1: Router, Host, Server

Group 2: Hub, Switch

One device in group 1 + One device in group 2: use straight-through cable

Two devices in the same group: use crossover cable

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

Assign appropriate IP addresses for interfaces:

From Main router, use show running-config command.

(Notice that you may see different IP addresses in the real CCNA exam, the ones shown above are just used for demonstration)

From the output we learned that the ip address of Fa0/0 interface of the Main router is 192.168.152.177/28. This address belongs to a subnetwork which has:

Increment: 16 (/28 = 255.255.255.240 or 1111 1111.1111 1111.1111 1111.1111 0000)

Network address: 192.168.152.176 (because 176 = 16 * 11 and 176 < 177)

Broadcast address: 192.168.152.191 (because 191 = 176 + 16 - 1)

And we can pick up an ip address from the list that belongs to this subnetwork:

192.168.152.190 and assign it to the Fa0/0 interface the router on the left

Use the same method for interface Serial0/0 with an ip address of 192.168.152.161 Increment: 16

Network address: 192.168.152.160 (because 160 = 16 * 10 and 160 < 161)

Broadcast address: 192.168.152.175 (because 176 = 160 + 16 - 1)

-> and we choose 192.168.152.174 for Serial0/0 interface of the router on the right Interface Fa0/1 of the router on the left

IP (of the computer on the left) : 192.168.152.129/28 Increment: 16

Network address: 192.168.152.128 (because 128 = 16 * 8 and 128 < 129)

Broadcast address: 192.168.152.143 (because 143 = 128 + 16 - 1)

-> we choose 192.168.152.142 from the list Interface Fa0/0 of the router on the right
IP (of the computer on the left) : 192.168.152.225/28 Increment: 16
Network address: 192.168.152.224 (because $224 = 16 * 14$ and $224 < 225$)
Broadcast address: 192.168.152.239 (because $239 = 224 + 16 - 1$)
-> we choose 192.168.152.238 from the list
Let's have a look at the picture below to summarize
Configure two routers on the left and right with these commands: Router1 = router on the left
Assign appropriate IP addresses to Fa0/0 & Fa0/1 interfaces: Router1>enable
Router1#configure terminal Router1(config)#interface fa0/0
Router1(config-if)#ip address 192.168.152.190 255.255.255.240 Router1(config-if)#no shutdown
Router1(config-if)#interface fa0/1
Router1(config-if)#ip address 192.168.152.142 255.255.255.240 Router1(config-if)#no shutdown
Set passwords (configure on two routers)
+ Console password: Router1(config-if)#exit Router1(config)#line console 0
Router1(config-line)#password consolepw Router1(config-line)#login
Router1(config-line)#exit
+ Telnet password: Router1(config)#line vty 0 4 Router1(config-line)#password telnetpw Router1(config-line)#login Router1(config-line)#exit
+ Privilege mode password: Router1(config)#enable password privpw Save the configuration: Router1(config)#exit
Router1#copy running-config startup-config
Configure IP addresses of Router2 (router on the right) Router2>enable
Router2#configure terminal Router2(config)#interface fa0/0
Router2(config-if)#ip address 192.168.152.238 255.255.255.240 Router2(config-if)#no shutdown
Router2(config-if)#interface serial0/0
Router2(config-if)#ip address 192.168.152.174 255.255.255.240 Router2(config-if)#no shutdown
Then set the console, telnet and privilege mode passwords for Router2 as we did for Router1, remember to save the configuration when you finished.

Topic 7, Mix Questions A

NEW QUESTION 290

Configuration of which option is required on a Cisco switch for the Cisco IP phone to work?

- A. PortFast on the interface
- B. the interface as an access port to allow the voice VLAN ID
- C. a voice VLAN ID in interface and global configuration mode
- D. Cisco Discovery Protocol in global configuration mode

Answer: B

Explanation: When you connect an IP phone to a switch using a trunk link, it can cause high CPU utilization in the switches. As all the VLANs for a particular interface are trunked to the phone, it increases the number of STP instances the switch has to manage. This increases the CPU utilization. Trunking also causes unnecessary broadcast / multicast / unknown unicast traffic to hit the phone link.

In order to avoid this, remove the trunk configuration and keep the voice and access VLAN configured along with Quality of Service (QoS). Technically, it is still a trunk, but it is called a Multi-VLAN Access Port (MVAP). Because voice and data traffic can travel through the same port, you should specify a different VLAN for each type of traffic. You can configure a switch port to forward voice and data traffic on different VLANs. Configure IP phone ports with a voice VLAN configuration. This configuration creates a pseudo trunk, but does not require you to manually prune the unnecessary VLANs.

The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. You can configure a voice VLAN with the “switchport voice vlan ...” command under interface mode. The full configuration is shown below:

```
Switch(config)#interface fastethernet0/1 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#switchport voice vlan 20
```

Reference:

<http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4500-series-switches/69632-configuring-cat-ip-ph>

Configure the Switch Port to Carry Both Voice and Data Traffic

When you connect an IP phone to a switch using a trunk link, it can cause high CPU utilization in the switches. As all the VLANs for a particular interface are trunked to the phone, it increases the number of STP instances the switch has to manage. This increases the CPU utilization. Trunking also causes unnecessary broadcast / multicast / unknown unicast traffic to hit the phone link.

In order to avoid this, remove the trunk configuration and keep the voice and access VLAN configured along with Quality of Service (QoS). Technically, it is still a trunk, but it is called a Multi-VLAN Access Port (MVAP). Because voice and data traffic can travel through the same port, you should specify a different VLAN for each type of traffic. You can configure a switch port to forward voice and data traffic on different VLANs. Configure IP phone ports with a voice VLAN configuration. This configuration creates a pseudo trunk, but does not require you to manually prune the unnecessary VLANs.

The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. The voice VLAN feature is disabled by default. The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

NEW QUESTION 291

Which dynamic routing protocol uses only the hop count to determine the best path to a destination?

- A. IGRP
- B. RIP
- C. EIGRP
- D. OSPF

Answer: B

NEW QUESTION 292

Which statement about a router on a stick is true?

- A. Its data plane router traffic for a single VLAN over two or more switches.
- B. It uses multiple subinterfaces of a single interface to encapsulate traffic for different VLANs on the same subnet.
- C. It requires the native VLAN to be disabled.
- D. It uses multiple subinterfaces of a single interface to encapsulate traffic for different VLANs.

Answer: D

Explanation: <https://www.freeccnaworkbook.com/workbooks/ccna/configuring-inter-vlan-routing-router-on-a-stick>

NEW QUESTION 293

Which statement about the inside interface configuration in a NAT deployment is true?

- A. It is defined globally
- B. It identifies the location of source addresses for outgoing packets to be translated using access or route maps.
- C. It must be configured if static NAT is used
- D. It identifies the public IP address that traffic will use to reach the internet.

Answer: B

Explanation: This module describes how to configure Network Address Translation (NAT) for IP address conservation and how to configure inside and outside source addresses. This module also provides information about the benefits of configuring NAT for IP address conservation.

NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise to the outside world only one address for the entire network. This ability provides additional security by effectively hiding the entire internal network behind that one address.

NAT is also used at the enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

NEW QUESTION 298

Which function enables an administrator to route multiple VLANs on a router?

- A. IEEE 802 1X
- B. HSRP
- C. port channel
- D. router on a stick

Answer: D

NEW QUESTION 302

Scenario:

You are a junior network engineer for a financial company, and the main office network is experiencing network issues. Troubleshoot the network issues.

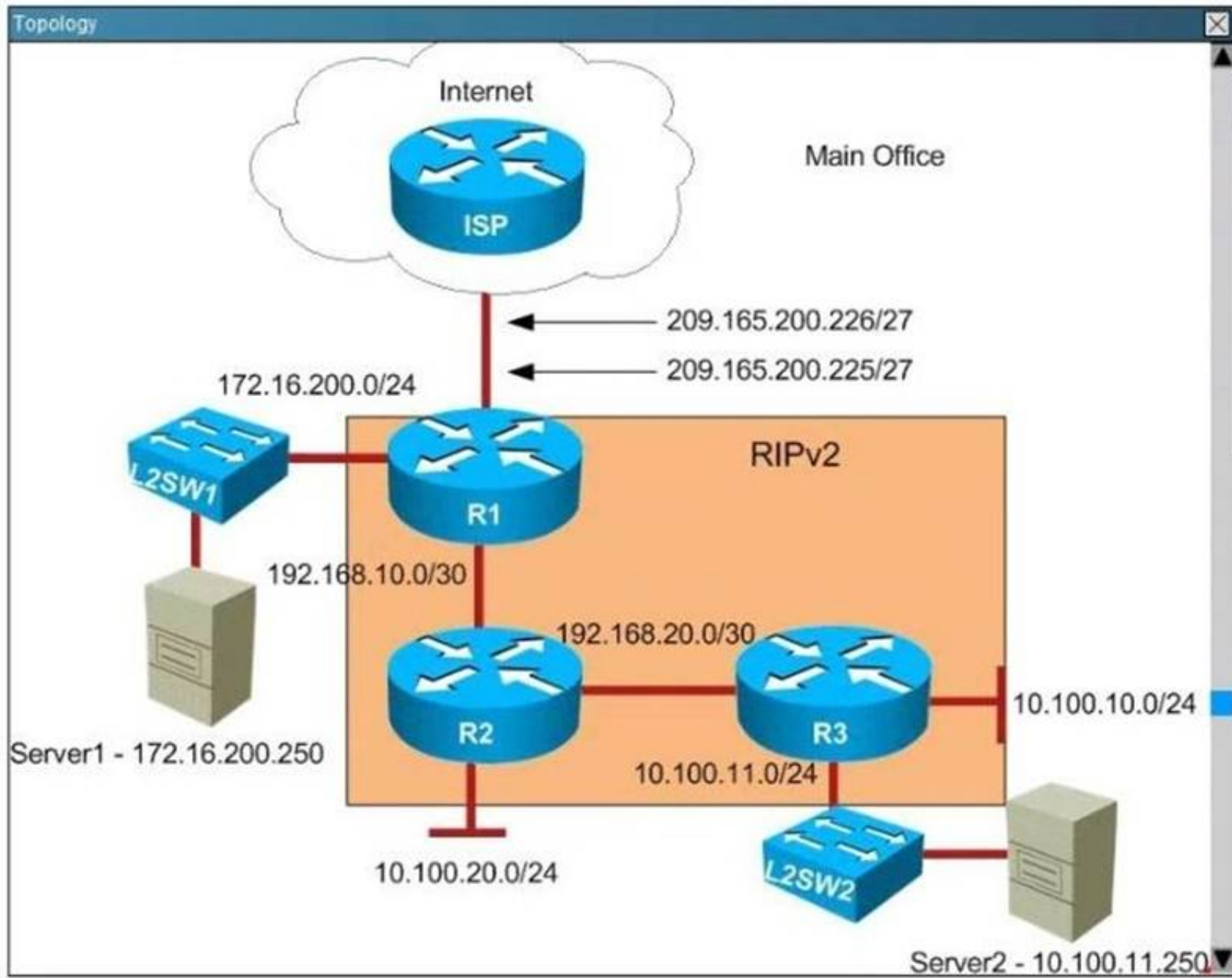
Router R1 connects the main office to the internet, and routers R2 and R3 are internal routers.

NAT is enabled on router R1.

The routing protocol that is enabled between routers R1, R2 and R3 is RIPv2.

R1 sends the default route into RIPv2 for the internal routers to forward internet traffic to R1.

You have console access on R1, R2 and R3 devices. Use only show commands to troubleshoot the issues.



R1

```

Current configuration : 1651 bytes
!
! No configuration change since last restart
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
--- More (105) ---
  
```

```
R1
ip nat inside source list LOCAL interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard R2LANBLOCK
deny 10.100.20.0 0.0.0.255
permit any
!
ip access-list extended LOCAL
permit ip host 127.0.0.1 any
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
logging synchronous
line aux 0
--- More (7) ---
```



```
R1
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
ntp server 209.165.200.226
!
end
R1#
```

```
R2
Building configuration...

Current configuration : 1243 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
--- More (92) ---
```

```
R2
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
```

```
R3
!
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
--- More (60) ---
```

```
R3
!
!
interface Loopback0
 ip address 192.168.250.3 255.255.255.255
!
interface Ethernet0/0
 description ***Link to LAN***
 ip address 10.100.10.1 255.255.255.0
!
interface Ethernet0/1
 description ***Link to R2***
 ip address dhcp
!
interface Ethernet0/2
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
```

```
R3
 description ***Link to Server2 Segment***
 ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
```

```
R3
 network 192.168.250.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 --- More (5) ---
```



```

R3
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  login
  transport input all
!
!
end
R3#
  
```

Examine the DHCP configuration between R2 and R3; R2 is configured as the DHCP server and R3 as the client. What is the reason R3 is not receiving the IP address via DHCP?

- A. On R2. The network statement in the DHCP pool configuration is incorrectly configured.
- B. On R3. DHCP is not enabled on the interface that is connected to R2.
- C. On R2, the interface that is connected to R3 is in shutdown condition.
- D. On R3, the interface that is connected to R2 is in shutdown condition.

Answer: B

Explanation: Please check the below:

Explanation/show commands:

R2 no mmi pvc mmi snmp-timeout 180 ! ! ip dhcp excluded-address 192.168.20.1 ! ip dhcp pool DHCPASSIGNR3 network 192.168.20.0 255.255.255.252 ! ip cef no ipv6 cef ! multilink bundle-name authenticated ! 	R3 ! ! interface Loopback0 ip address 192.168.250.3 255.255.255.255 ! interface Ethernet0/0 description ***Link to LAN*** ip address 10.100.10.1 255.255.255.0 ! interface Ethernet0/1 description ***Link to R2*** no ip address ! interface Ethernet0/2 description ***Link to Server2 Segment*** ip address 10.100.11.1 255.255.255.0 ! interface Ethernet0/3 no ip address
---	---

NEW QUESTION 303

Scenario:

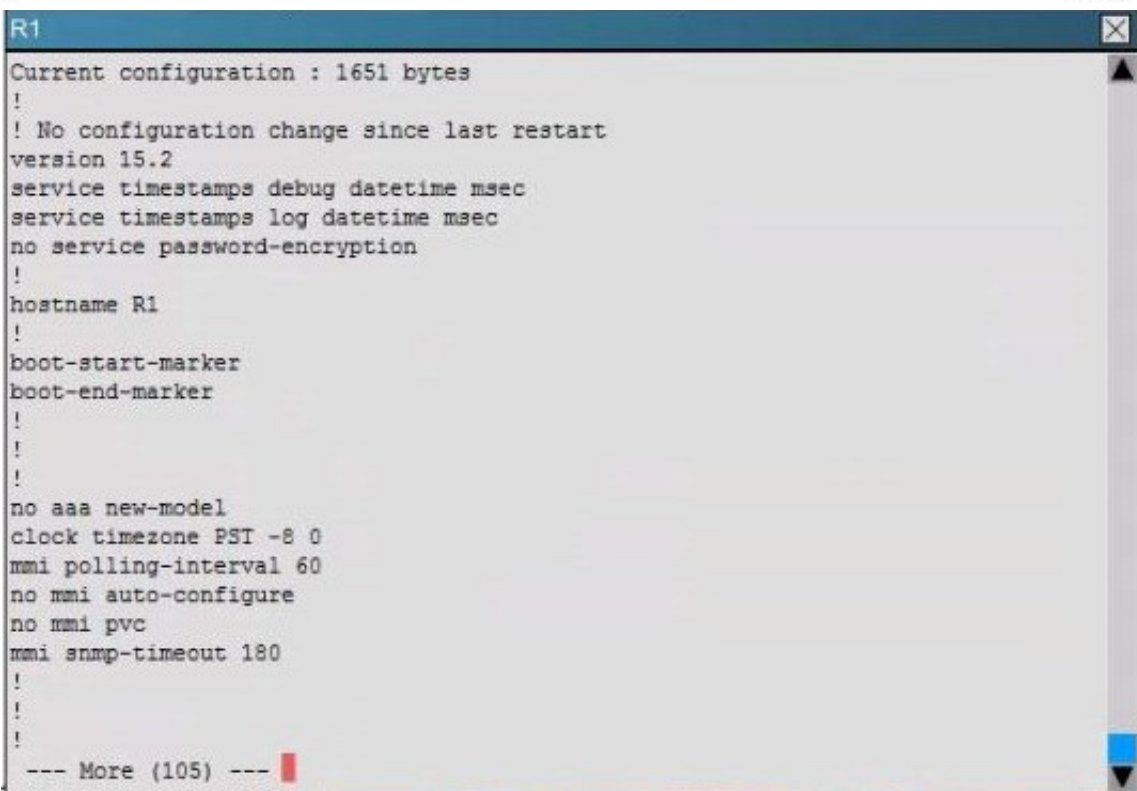
You are a junior network engineer for a financial company, and the main office network is experiencing network issues. Troubleshoot the network issues.

Router R1 connects the main office to the internet, and routers R2 and R3 are internal routers. NAT is enabled on router R1.

The routing protocol that is enabled between routers R1, R2 and R3 is RIPv2.

R1 sends the default route into RIPv2 for the internal routers to forward internet traffic to R1.

You have console access on R1, R2 and R3 devices. Use only show commands to troubleshoot the issues.



```
R1
!
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
redundancy
!
!
!
!
!
!
--- More (79) ---
```

```
R1
ip access-list extended LOCAL
 permit ip host 127.0.0.1 any
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
!
ntp server 209.165.200.226
!
end
R1#
```



```
R2
Building configuration...

Current configuration : 1243 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
--- More (92) ---
```

```
R2
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
```

```
R2
!
!

!
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool DHCPASSIGNR3
 network 10.10.10.0 255.255.255.252
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
R2#
```

```
R3
!  
!  
interface Loopback0  
  ip address 192.168.250.3 255.255.255.255  
!  
interface Ethernet0/0  
  description ***Link to LAN***  
  ip address 10.100.10.1 255.255.255.0  
!  
interface Ethernet0/1  
  description ***Link to R2***  
  ip address dhcp  
!  
interface Ethernet0/2  
  description ***Link to Server2 Segment***  
  ip address 10.100.11.1 255.255.255.0  
!  
interface Ethernet0/3  
  no ip address  
  shutdown  
!  
router rip  
  version 2  
  network 10.0.0.0  
  network 192.168.20.0
```

```

R3
description ***Link to Server2 Segment***
ip address 10.100.11.1 255.255.255.0
!
interface Ethernet0/3
no ip address
shutdown
!
router rip
version 2
network 10.0.0.0
network 192.168.20.0
network 192.168.250.0
no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!

R3
network 192.168.250.0
no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
--- More (5) ---

R3
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input all
!
!
end
R3#

```

Users complain that they are unable to reach internet sites. You are troubleshooting internet connectivity problem at main office. Which statement correctly identifies the problem on Router R1?

- A. Interesting traffic for NAT ACL is incorrectly configured.
- B. NAT configurations on the interfaces are incorrectly configured
- C. NAT translation statement incorrectly configured.
- D. Only static NAT translation configured for the server, missing Dynamic NAT or Dynamic NAT overloading for internal networks.

Answer: B

Explanation:


```
R1
!
!
!
!
interface Loopback0
ip address 192.168.250.1 255.255.255.255
!
interface Ethernet0/0
description ***Link to ISP***
ip address 209.165.200.225 255.255.255.224
ip nat inside
ip virtual-reassembly in
!
interface Ethernet0/1
description ***Link to Server1 segment***
ip address 172.16.200.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
!
interface Ethernet0/2
description ***Link to R2***
ip address 192.168.10.1 255.255.255.252
ip nat outside
ip virtual-reassembly in
!
```

NEW QUESTION 305

Which MTU size can cause a baby giant error?

- A. 1500
- B. 9216
- C. 1600
- D. 1518

Answer: D

Explanation: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/29805-175.html>

NEW QUESTION 306

Which component of the routing table ranks routing protocols according to their preferences?

- A. administrative distance
- B. next hop
- C. metric
- D. routing protocol code

Answer: A

Explanation: Administrative distance - This is the measure of trustworthiness of the source of the route. If a router learns about a destination from more than one routing protocol, administrative distance is compared and the preference is given to the routes with lower administrative distance. In other words, it is the believability of the source of the route.

NEW QUESTION 308

Which option is the default switch port port-security violation mode?

- A. shutdown
- B. protect
- C. shutdown vlan
- D. restrict

Answer: A

Explanation: Shutdown—This mode is the default violation mode; when in this mode, the switch will automatically force the switchport into an error disabled (err-disable) state when a violation occurs. While in this state, the switchport forwards no traffic. The switchport can be brought out of this error disabled state by issuing the errdisable recovery cause CLI command or by disabling and reenabling the switchport.

Shutdown VLAN—This mode mimics the behavior of the shutdown mode but limits the error disabled state the specific violating VLAN.

NEW QUESTION 313

Which route source code represents the routing protocol with a default administrative distance of 90 in the routing table?

- A. S
- B. E
- C. D
- D. R
- E. O

Answer: C

Explanation: SStatic EEGP DEIGRP RRIP OOSPF

Default Administrative distance of EIGRP protocol is 90 then answer is C

```
Router# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Default Distance Value Table

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

Route Source

Default Distance Values

Connected interface 0

Static route 1

Enhanced Interior Gateway Routing Protocol (EIGRP) summary route 5

External Border Gateway Protocol (BGP) 20

Internal EIGRP 90

IGRP 100 OSPF 110

Intermediate System-to-Intermediate System (IS-IS) 115

Routing Information Protocol (RIP) 120

Exterior Gateway Protocol (EGP) 140

On Demand Routing (ODR) 160

External EIGRP 170

Internal BGP 200

Unknown* 255

NEW QUESTION 317

Which component of a routing table entry represents the subnet mask?

- A. routing protocol code
- B. prefix
- C. metric
- D. network mask

Answer: D

Explanation: IP Routing Table Entry Types

An entry in the IP routing table contains the following information in the order presented:

Network ID. The network ID or destination corresponding to the route. The network ID can be class-based, subnet, or supernet network ID, or an IP address for a host route.

Network Mask. The mask that is used to match a destination IP address to the network ID.

Next Hop. The IP address of the next hop.

Interface. An indication of which network interface is used to forward the IP packet.

Metric. A number used to indicate the cost of the route so the best route among possible multiple routes to the same destination can be selected. A common use of the metric is to indicate the number of hops (routers crossed) to the network ID.

Routing table entries can be used to store the following types of routes:

Directly Attached Network IDs. Routes for network IDs that are directly attached. For directly attached networks, the Next Hop field can be blank or contain the IP address of the interface on that network.

Remote Network IDs. Routes for network IDs that are not directly attached but are available across other routers. For remote networks, the Next Hop field is the IP address of a local router in between the forwarding node and the remote network.

Host Routes. A route to a specific IP address. Host routes allow routing to occur on a per-IP address basis. For host routes, the network ID is the IP address of the specified host and the network mask is 255.255.255.255.

Default Route. The default route is designed to be used when a more specific network ID or host route is not found. The default route network ID is 0.0.0.0 with the network mask of 0.0.0.0.

NEW QUESTION 321

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 100-105 Exam with Our Prep Materials Via below:

<https://www.certleader.com/100-105-dumps.html>