640-802

Exam: 640-802
Title: Cisco Certified Network Associate
Version: Demo

QUESTION NO: 1
Refer to the exhibit. What is the effect of the configuration that is shown?

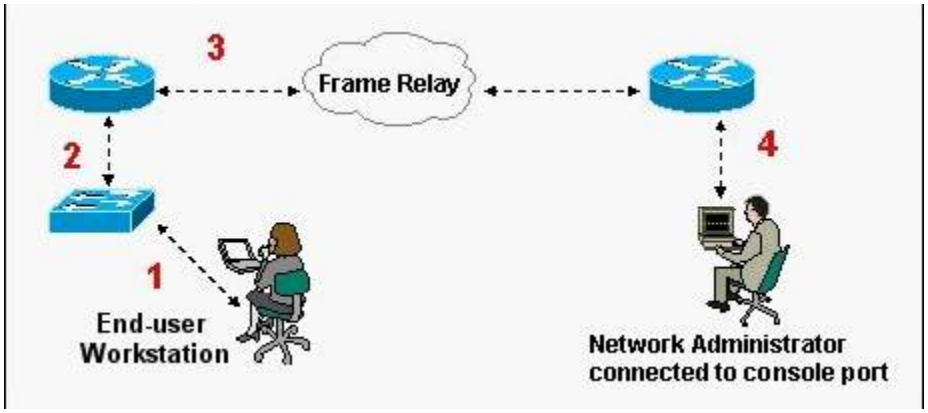
```
line vty 0 4
 password 7 030752180500
 login
 transport input ssh
```

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

Answer: B

Explanation:
Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. Communication between the client and server is encrypted in both SSH version 1 and SSH version 2. If you want to prevent non-SSH connections, add the "transport input ssh" command under the lines to limit the router to SSH connections only. Straight (non-SSH) Telnets are refused.
Reference: www.cisco.com/warp/public/707/ssh.shtml

QUESTION NO: 2
Refer to the exhibit. What kind of cable should be used to make each connection that is identified by the numbers shown?



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

Answer: E

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

QUESTION NO: 3
You work as a network technician in a Company. Please study the exhibit carefully.

```
00:34:43: RIP: recevied v1 update from 192.168.11.2 on Serial0/0
00:34:43:      192.168.12.0 in 1 hops
00:34:43: RIP: update contains 1 routers
00:34:50: Serial0/0: HDLC myseq 179, mineseen 179*, yourseen 180, line up
00:35:00: Serial0/0: HDLC myseq 180, mineseen 180*, yourseen 181, line up
00:35:00: IP: s= 192.168.11.1 (local), d= 192.168.11.2 (Serial0/0), len 40, rcvd 3
00:35:00: IP: s= 192.168.11.2 (Serial0/0), d= 192.168.11.1 (Serial0/0), len 40, rcvd 3
00:35:00: tcp2: I ESTAB 192.168.11.2: 11] 03 192.168.11.1: 23 seq 4063973782
      ACK 4061200175 WIN 4049
```

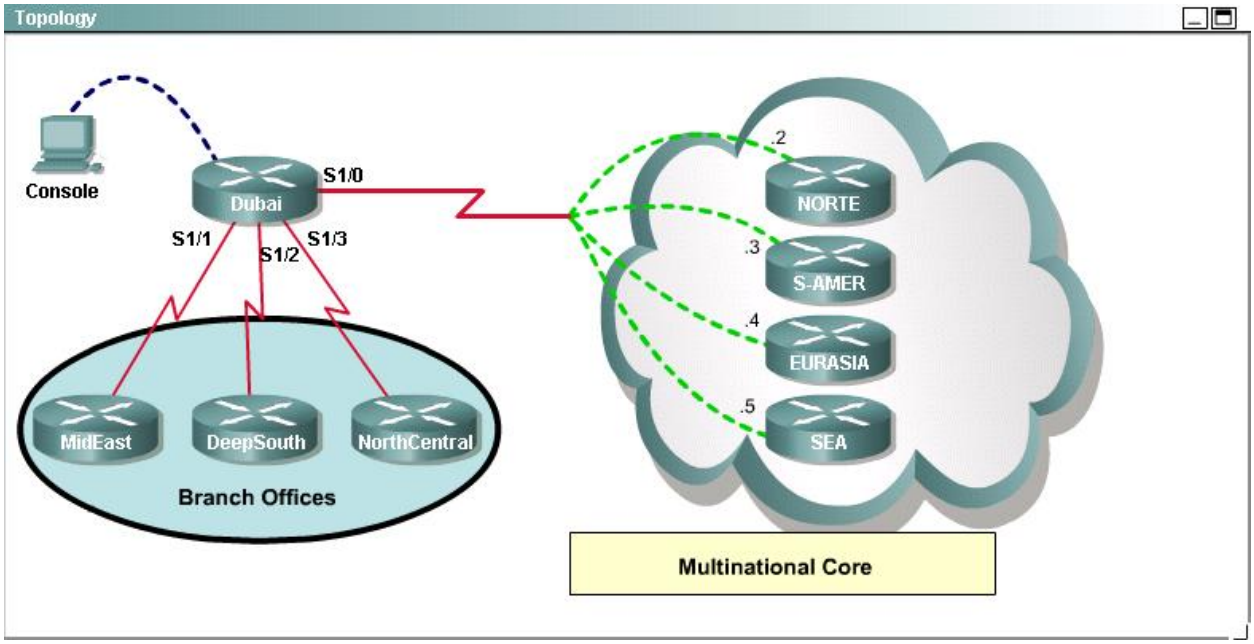
The router console screen is rapidly displaying line after line of output similar to what is shown in the exhibit. The help desk has called to say that users are reporting a slowdown in the network. What will solve this problem while not interrupting network operation?

A. Press the CTRL+C keys.
B. Save the configuration and reboot the router.
C. Enter the no debug all command.
D. Use the show processes command.

Answer: C

Explanation:
The output shown in this example is a result of one or more debug commands that have been used to troubleshoot an issue. Using **debug** commands might slow down traffic on busy networks. To see the current debug command settings, enter the show debug command. To stop the debug output, enter the no debug command. To stop all debug messages from being displayed, enter the no debug all command.

QUESTION NO: 4



```
Dubai#sh frame-relay map
Serial1/0 (up): ip 172.30.0.2 dlci 704 (0x7B,0x1CB0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.3 dlci 196 (0xEA,0x38A0), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.4 dlci 702 (0x159,0x5490), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 172.30.0.5 dlci 344 (0x1C8,0x7080), dynamic,
                broadcast,, status defined, active
Dubai#
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial1/0
 ip address 172.30.0.1 255.255.255.240
 encapsulation frame-relay
 no fair-queue
!
interface Serial1/1
 ip address 192.168.0.1 255.255.255.252
!
interface Serial1/2
 ip address 192.168.0.5 255.255.255.252
 encapsulation ppp
!
interface Serial1/3
 ip address 192.168.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.0.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password Tlnet
 login
!
end
```

Please study the exhibit shown above carefully, and answer the following questions.

A static map to the S-AMER location is required. Which command should be used to create this map?

A. frame-relay map ip 172.30.0.3 702 broadcast
B. frame-relay map ip 172.30.0.3 196 broadcast
C. frame-relay map ip 172.30.0.3 344 broadcast
D. frame-relay map ip 172.30.0.3 704 broadcast

Answer: B
Explanation:

Based on the output of the command "show frame-relay map", we know that DLCI mapped to the router S-AMER is 196. (.3 In the above network topology, the complete layer3 IP address is172.30.0.3)
Frame-relay map: The mapping command "Frame-relay map" can statically create a mapping reaching the remote protocol address.
The format is :

frame-relay map protocol protocol-address dlci [broadcast][ietf | cisco]

Configuring a static Frame Relay map is optional unless you are using subinterfaces. The Frame Relay map will map a Layer 3 address to a local DLCI. This step is optional because inverse-arp will automatically perform this map for you.
Syntax for frame-relay map is:

frame-relay map protocol address dlci [broadcast] [cisco | ietf]

The broadcast option allows packets, such as RIP updates to be forwarded across the PVC. If you are not using the broadcast option, you need to specify the neighbor to forward unicast packet using neighbor command.

neighbor a.b.c.d
Specify RIP neighbor. When a neighbor doesn't understand multicast, this command is used to specify neighbors. In some cases, not all routers will be able to understand multicasting, where packets are sent to a network or a group of addresses. In a situation where a neighbor cannot process multicast packets, it is necessary to establish a direct link between routers. The neighbor command allows the network administrator to specify a router as a RIP neighbor. The no neighbor a.b.c.d command will disable the RIP neighbor.

QUESTION NO: 5
You have finished physically installing an access point on the ceiling at your office. At a minimum, which parameter must be configured on the access point in order to allow a wireless client to operate on it?

A. SSID
B. AES
C. TKIP
D. PSK

Answer: A
Explanation:
SSID (Service Set Identifier) can also be written as ESSID, which is used to distinguish different networks. It has 32 characters at most, WLAN cards set up different SSID to enter different networks. SSID is usually broadcast by AP or wireless routers , you can view SSID of the present area through XP built-in scanning feature .Taking security into consideration, SSID can be not broadcast, meanwhile users need to set up SSID manually to enter the appropriate

network. Simply speaking, SSID is the name of a local area network, only those computers that set up the same SSID value can communicate with each other.

QUESTION NO: 6
Which is the correct fallback sequence for loading the Cisco IOS?

A. Flash, TFTP server, ROM
B. ROM, Flash, NVRAM
C. Flash, NVRAM, RAM
D. ROM, TFTP server, Flash

Answer: A
Explanation:
By default, a Cisco IOS router will normally boot up from flash where the IOS is stored. If the IOS in not found or has become corrupted, the router will then send an all hosts broadcast (255.255.255.255) to find a TFTP server to download the IOS from. Should that fail, the router will boot up in ROM Monitor mode as a last resort.

QUESTION NO: 7
Which tables of EIGRP route information are held in RAM and maintained through the use of hello and update packets? (Choose two.)

A. RTP table
B. SPF table
C. query table
D. neighbor table
E. DUAL table
F. topology table

Answer: D,F
Explanation:
Only the neighbor table and the topology table of EIGRP route information are held in RAM and maintained through the use of hello and update packets.

QUESTION NO: 8
A receiving host computes the checksum on a frame and determines that the frame is damaged. The frame is then discarded. At which OSI layer did this happen?

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

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

QUESTION NO: 9
Refer to the exhibit. Why are two OSPF designated routers identified on Core_Router?

```
Core_Router# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
208.149.23.194    1   FULL/DR         00:00:33    190.172.32.10   Ethernet1
208.149.23.66     1   FULL/BDR        00:00:32    190.171.23.13   Ethernet0
208.149.23.130    1   FULL/DR         00:00:39    190.171.23.10   Ethernet0

Core_Router#
```

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

Answer: C

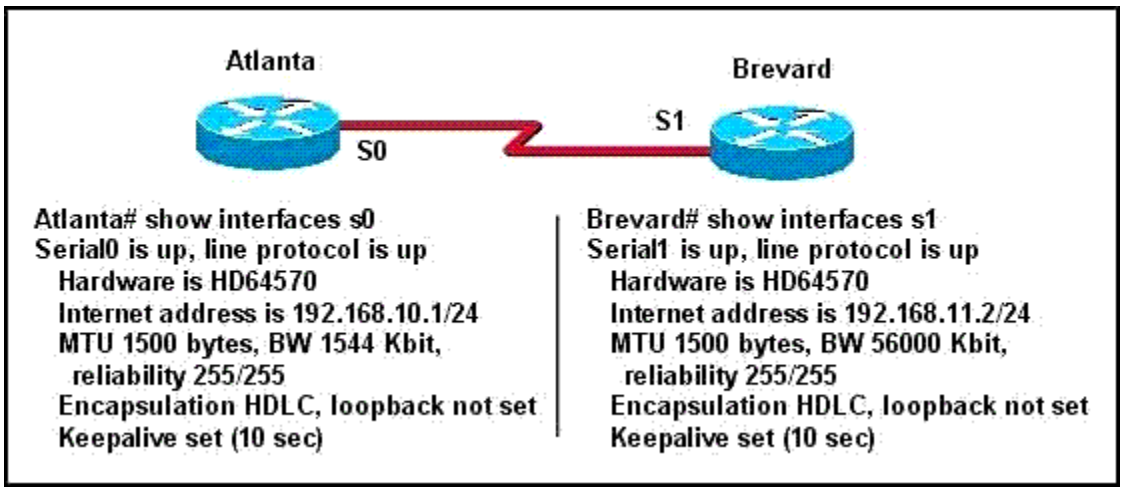
Explanation:
OSPF neighbors process multicast hello packets upon multicast address 224.0.0.5 to find neighbors dynamically. Default hello packets sending interval is 10 seconds, and dead interval is 40 seconds. In multi-access broadcasting network (such as Ethernet Net and Token Ring), DR/BDR elections are needed. When electing DR/BDR, hello packets priority is considered, the highest priority is DR, then BDR. Default priority is 1. In the circumstances when Priority is the same, RID will be considered, the highest rating RID is DR, and then BDR. When you set the priority 0, OSPF router can not become DR/BDR, it will only turn into DROTHER. From the above OSPF neighbors table, we learn that Ethernet1 and Ethernet0 select DR correspondingly, and Core_Router is connected two multi-access networks.

QUESTION NO: 10
As a CCNA candidate, you will be expected to know the POST process very well. A Cisco router is booting and has just completed the POST process. It is now ready to find and load an IOS image. What function does the router perform next?

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

Answer: D
Explanation:
This question tests how a Cisco router is started.
Step 1 The router is booting.
Step 2 The router completes the POST process.
Step 3 The router finds and loads an IOS image.
Step 4 The router checks the configuration register and decides how to load start configuration based on the value of the configuration register.

QUESTION NO: 11
Two routers named Atlanta and Brevard are connected by their serial interfaces as shown in the exhibit, but there is no data connectivity between them. The Atlanta router is known to have a correct configuration. Given the partial configurations shown in the exhibit, what is the problem on the Brevard router that is causing the lack of connectivity?

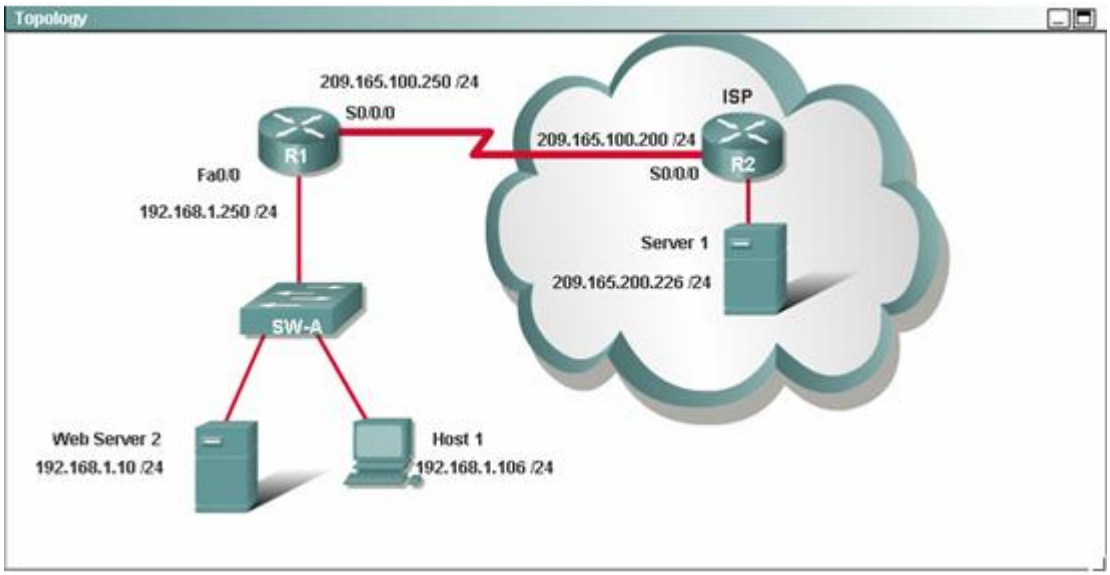


A. The serial line encapsulations are incompatible.
B. The subnet mask is incorrect.
C. The bandwidth setting is incompatible with the connected interface.
D. The maximum transmission unit (MTU) size is too large.
E. The IP address is incorrect.
F. A loopback is not set.

Answer: E
Explanation:

The IP address of the S0 interface of Atlanta is 192.168.10.0/24, and the IP address of the S1 interface of Breavard is 192.168.11.0/24. Change the IP address of the S1 interface to 192.168.10.0/24, the same as that of the S0 interface.

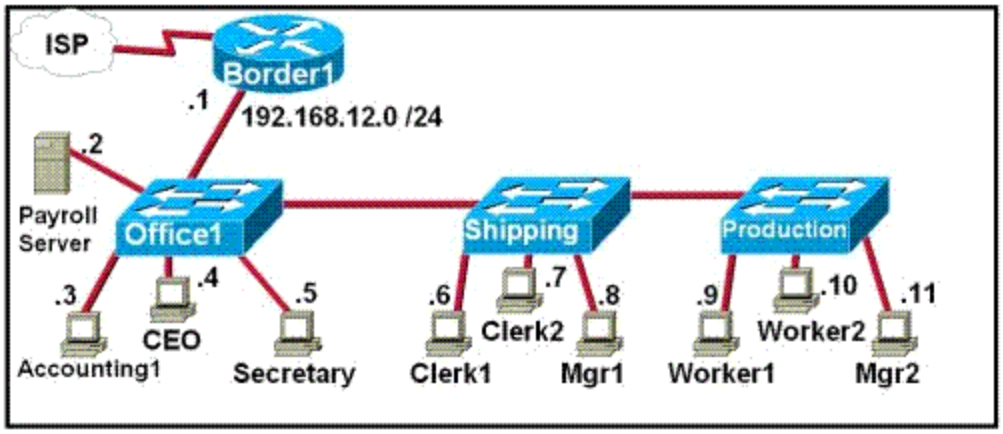
QUESTION NO: 12
R1 forwards a packet from Host 1 to remote Server 1. Which statement describes the use of a MAC as the frame carrying this packet leaves the s0/0/0 interface of R1?



A. The frame does not have MAC addresses.
B. The destination MAC address in the frame is the MAC address of the s0/0/0 interface of R2
C. The source MAC address in the frame is the MAC address of the s0/0/0 interface of R1.
D. The destination MAC address in the frame is the MAC address of the NIC of server 1.
E. The source MAC address in the frame is the MAC address of the NIC of Host 1.

Answer: A
Explanation:
The frame relay network does not have hardware addresses.

QUESTION NO: 13
Refer to the exhibit. The FMJ manufacturing company is concerned about unauthorized access to the Payroll Server. The Accounting1, CEO, Mgr1, and Mgr2 workstations should be the only computers with access to the Payroll Server. What two technologies should be implemented to help prevent unauthorized access to the server? (Choose two.)



A. STP
B. access lists
C. VTP
D. VLANs
E. wireless LANs
F. encrypted router passwords

Answer: B,D
Explanation:
Group these workstations into the same VLAN and use access control lists to set the access authority of the VLAN.

QUESTION NO: 14
Which PPP authentication methods will you use when configuring PPP on an interface of a Cisco router?(Choose two)

A. PAP
B. SSL
C. CHAP
D. SLIP

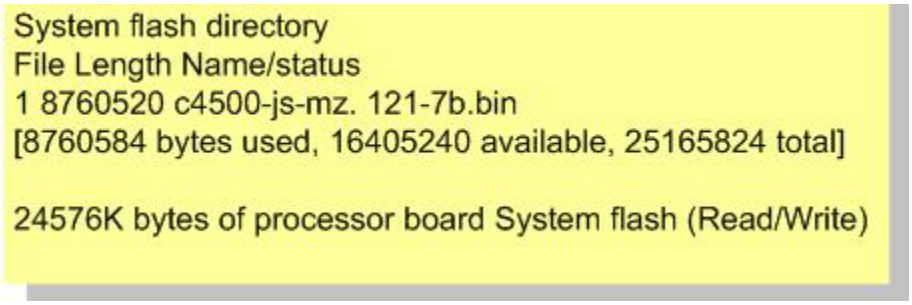
Answer: A,C

Explanation:
Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authenticate the endpoints on either end of a point-to-point serial link. Chap is the preferred method today because the identifying codes flowing over the link are created using a MD5 one-way hash, which is more secure that the clear-text passwords sent by PAP.
Reference:
CCNA Self-Study CCNA ICND exam certification Guide (Cisco Press, ISBN 1-58720-083-X) Page 314

PPP has two ways to authenticate : one is PAP, the other is CHAP. PAP is less secure than CHAP. PAP transmits the password in the form of plaintext, while the transmission process of

CHAP does not contain password, using hash to replace password. The PAP authentication can be achieved by two-way handshake ,while the CHAP authentication can be achieved by three-way handshake. The PAP authentication is that the dialed sends the request and the dial reply, while the CHAP authentication is that the dial send request and the dialed sends back a data packet which contains the random hash value sent by the dial, after confirming the database has no error, the dial will send a successfully connected packet to connect.

QUESTION NO: 15
Refer to the graphic. A network associate is planning to copy a new IOS image into the router. This new image requires 8 MB of flash memory and 32 MB of RAM. How will the IOS proceed with the copy process?
Exhibit #sow flash:



A. The new IOS will be copied into flash memory and the current image will remain.
B. IOS will issue an error message because flash memory is not large enough to hold the new image.
C. The current IOS image must be manually erased before IOS will allow the new image to be copied.
D. During the copy process, the current IOS image will be erased.

Answer: A
Explanation:
According to the output shown above, the existing IOS is 8760520 bytes (8M) and the total size of the flash on this device is 24567K (24M). The new IOS only requires an additional 8 MB, so it will be copied on to the flash directly and both images will reside on the flash. The existing IOS is only overwritten it there is insufficient space to hold both.

Through the above chart we can see that the total space of current flash is 25 M, available space being 16 M, so 8M new image will be copied into the flash, while the original image will be preserved.

QUESTION NO: 16
Which two statements best describe the wireless security standard that is defined by WPA? (Choose two.)

A. It specifies the use of dynamic encryption keys that change each time a client establishes a connection.
B. It specifies use of a static encryption key that must be changed frequently to enhance security.

C. It includes authentication by PSK.
D. It requires that all access points and wireless devices use the same encryption key.
E. It requires use of an open authentication method.

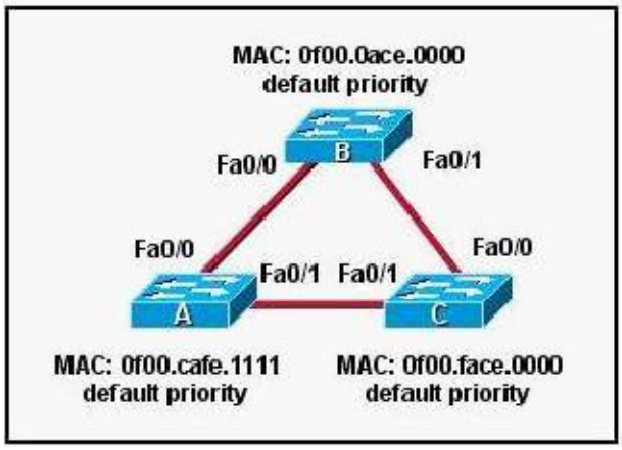
Answer: A,C

Explanation:
WPA is a more powerful security technology for Wi-Fi networks than WEP. It provides strong data protection by using encryption as well as strong access controls and user authentication. WPA utilizes 128-bit encryption keys and dynamic session keys to ensure your wireless network's privacy and enterprise security.
There are two basic forms of WPA:
• WPA Enterprise (requires a Radius server)
• WPA Personal (also known as WPA-PSK)

Either can use TKIP or AES for encryption. Not all WPA hardware supports AES.
WPA-PSK is basically an authentication mechanism in which users provide some form of credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN. Encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is in WPA-PSK, authentication is reduced to a simple common password, instead of user-specific credentials.
The Pre-Shared Key (PSK) mode of WPA is considered vulnerable to the same risks as any other shared password system - dictionary attacks for example. Another issue may be key management difficulties such as removing a user once access has been granted where the key is shared among multiple users, not likely in a home environment.
Reference: http://www.dslreports.com/faq/wifisecurity/2.2_WPA

WPA is a standard-based interoperable solution designed to enhance the security of WLAN, which greatly improves the present and future level of data protection and access control of WLAN. WPA is evolved from the being developed IEEE802.11i standards and keeps compatible with its former. WPA can protect WLAN users data with proper deployment , and only the authorized network users can access the WLAN network.
WPA provides users with a temporary solution. The encryption of this standard adopts TKIP (Temporary Key Integrity Protocol). There are two authentication modes to choose :one mode uses 802.1 x protocol to authenticate, the other is known as PSK (Pre-Shared Key) Mode.

QUESTION NO: 17
Refer to the topology shown in the exhibit. Which ports will be STP designated ports if all the links are operating at the same bandwidth? (Choose three.)



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

Explanation:

1) Switch B will become the ROOT BRIDGE because it has the lowest MAC address as you can see in the picture.Its both ports will become STP designated ports so choice **C and D are right**.

2) Next Election will be of Designated Ports on the segment connecting A and C.**Switch A has lower MAC address so, its port FA0/1 will become designated port** and FA0/1 of switch C will be placed in a BLOCKING state to avoid switching LOOPS.**This makes option B right.**.So,ultimately B,C & D are correct.

QUESTION NO: 18
The Company WAN is migrating from RIPv1 to RIPv2. Which three statements are correct about RIP version 2? (Choose three)

A. It is a classless routing protocol.
B. It supports authentication.
C. It has a lower default administrative distance than RIP version 1.
D. It uses broadcasts for its routing updates.
E. It has the same maximum hop count as version 1.

Answer: A,B,E
Explanation:
RIPV2 has the maximum hop count as RIPV1(15).
RIPV2 uses multicast for its routing updates while RIPV1 uses broadcast for its routing updates.

RIPV2 has a higher security than RIPV1 because RIPV2 supports authentication.
RIPV2, rather than RIPV1, sends the subnet mask in updates.

RIPV1 is a classful routing protocol , it sends update packets which does not contain subnet mask information every 30 seconds , it does not support VLSM and performs border automatic route summary by default, it can't be shut down, so it does not support non-consecutive networks and authentication, it uses hop counts as metric, the administrative distance is 120. Each packet contains 25 routing information at most , and routing update is broadcast.
RIPV2 is a classless routing protocol, whose transmitted packets contain subnet mask information , it supports VLSM and enables the function of auto-summary . So , it is needed to manually shut down the function of auto-summary in order to send subnet information to the main network . RIPV2 only supports summarizing routing to the main network instead of summarizing different main networks. So it does not support CIDR. RIPV2 updates routing by use of the multicast address 224.0.0.9, only the corresponding multicast MAC address can reply to packets. Whether reply to packets and support authentication or not can be distinguished at the MAC layer.
Note : Refer to the classful routing protocol, when the subnet of the interface sending routing packets is in the same main network as the subnet associated with the packets, the router can transmit subnet information through this interface assuming that the interface and the subnet of packets use the same subnet mask.
What is the consecutive subnet:
Consecutive subnets belong to the same main network and use the same subnet mask, otherwise it is not. Using the manual summary command on the interface: ip summary-address rip to summarize subnet and subnet mask . RIP uses UDP(User Datagram Protocol)520 port to transmit routing update packets .

QUESTION NO: 19
Some of the company routers have been configured with default routes. What are some of the advantages of using default routes?(Choose two.)

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

Answer: A,C

Explanation:
Routers use default routing as a last resort when all other methods (directly connected, static, or dynamic) have been exhausted. For stub networks, a single default static route could be used to provide connectivity to the entire network. This is desirable for stub networks where only a single link connects the remote location to the rest of the networks. Because all of the traffic only has one link to use, a single default route will make the routing table as small as possible, while providing for connectivity to networks not in the routing table, since as traffic destined for the Internet.

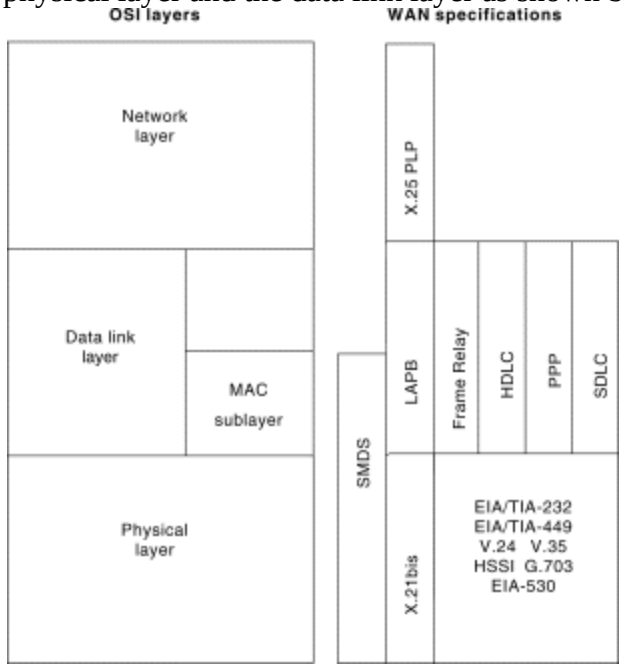
Incorrect Answers:
E. Although default routes are normally statically assigned, these routes can still go down. If the interface used as the default route should go down, or the next hop IP address of the default route become unreachable, the static default route will go down.
D. Using static routes, including default routes, is the least CPU-intensive method of routing.
B. To influence the way incoming traffic from the Internet gets to a corporation, BGP routing would be used, not default routing.

QUESTION NO: 20
It is known that the OSI model has seven layers. Can you tell me at which layers of the OSI model WANs operate? (Choose two.)

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

Answer: B,D

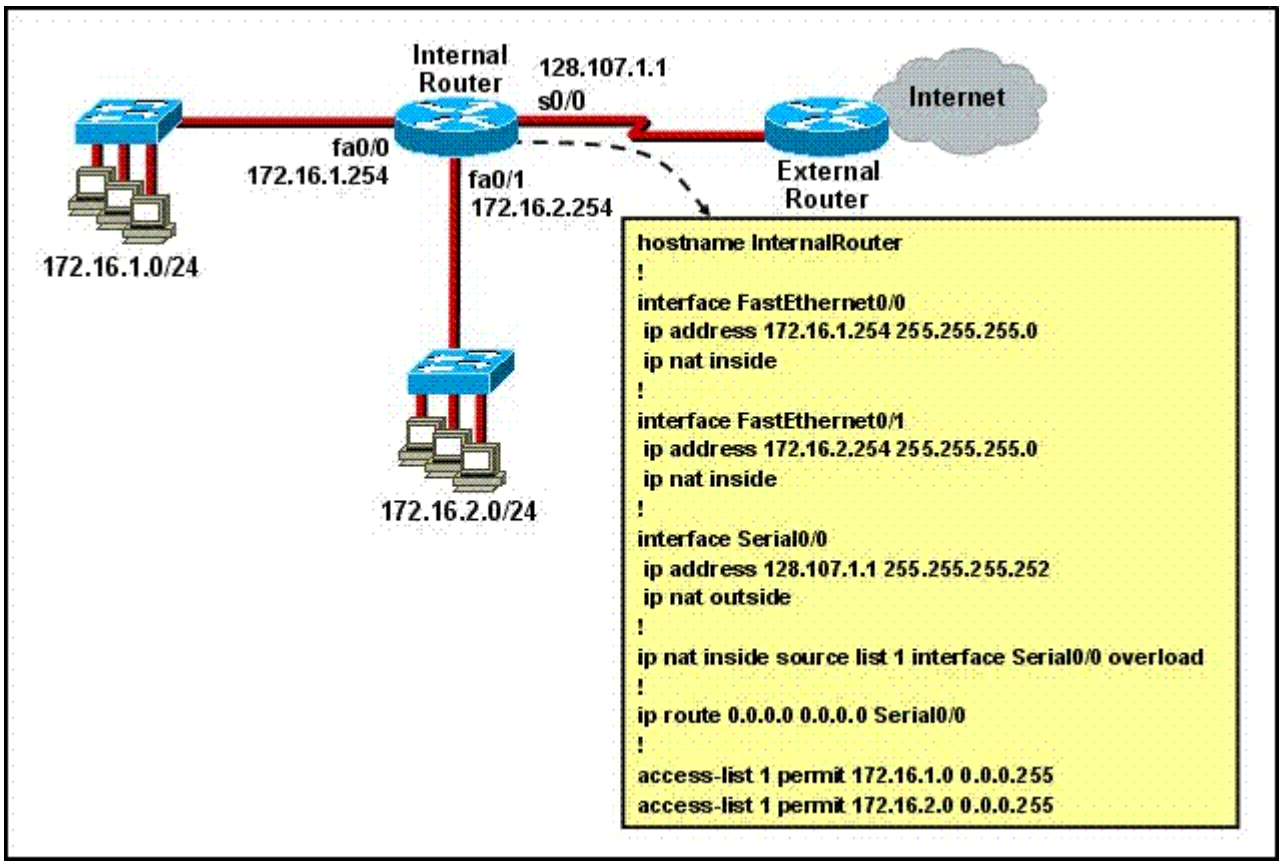
Explanation:
A *WAN* is a data communications network that covers a relatively broad geographic area and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower two layers of the OSI reference model: the physical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



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

QUESTION NO: 21

Refer to the exhibit. What is the purpose of the configuration that is shown?

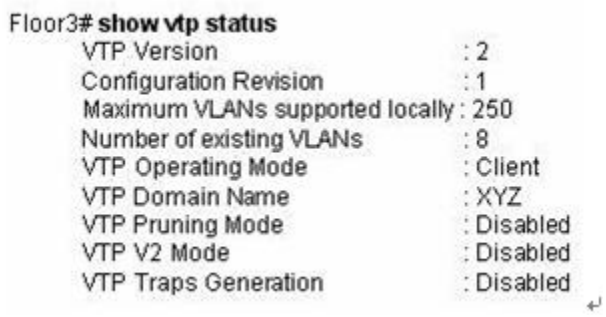


A. to translate addresses of hosts on the fa0/0 and fa0/1 networks to a single public IP address for Internet access
B. to allow IP hosts on the Internet to initiate TCP/IP connections to hosts on fa0/0 and fa0/1
C. to provide security on fa0/0 and fa0/1 through the application of an access list
D. to translate the internal address of each host on fa0/0 and fa0/1 to a unique external IP address for Internet acces

Answer: A

Explanation:
The internal network, which is connected by the internal router, uses private IP addresses. These IP addresses cannot be routed in a public network, so NAT is used. Two ACLs are defined on the internal router to allow the fa0/0 and fa0/1 networks to invoke the NAT pool for address translation. All devices with an IP address in the 172.16.1.0/24 and 172.16.20./24 subnets will be translated to the single IP address of the S0/0 interface, which is 28.107.1.1. This configuration is an example of many-to-1 NAT or NAT overload

QUESTION NO: 22
Given the output of the Floor3 switch shown above, which statement best describes the operation of this switch?



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

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

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

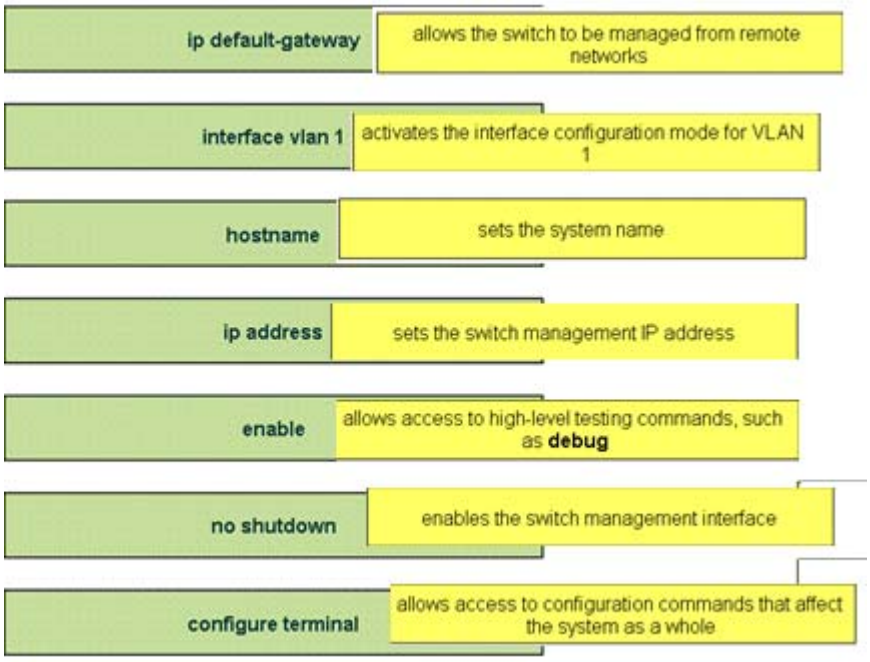
QUESTION NO: 23 DRAG DROP
Drag and drop question. Drag the items to the proper locations.

640-802

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

ip default-gateway	allows access to high-level testing commands, such as **debug**
interface vlan 1	allows access to configuration commands that affect the system as a whole
hostname	sets the system name
ip address	activates the interface configuration mode for VLAN 1
enable	enables the switch management interface
no shutdown	sets the switch management IP address
configure terminal	allows the switch to be managed from remote networks

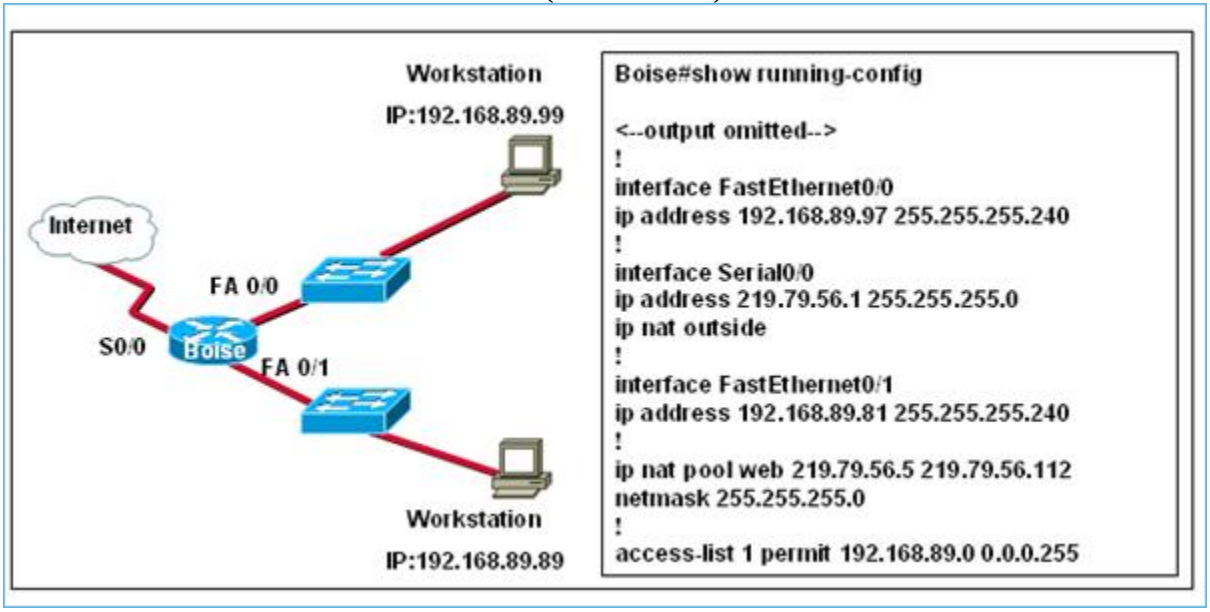
Answer:



enable : This command is used to enter into User Privileges Mode
configure terminal: This command is used to enter into global configuration mode
hostname : This command is used to set the hostname of switch
ip default-gateway : This command should enter should enter on global configuration mode to set default gateway of switch.

Interface vlan 1 : Enters into the vlan 1 SVI (Switched Virtual Interface) configuration mode, where you can enter vlan 1 SVI interface specific configuration
ip add x.x.x.x y.y.y.y : Use to assign the ip address on interface
no shutdown: Brings the interface on up state from administratively down state

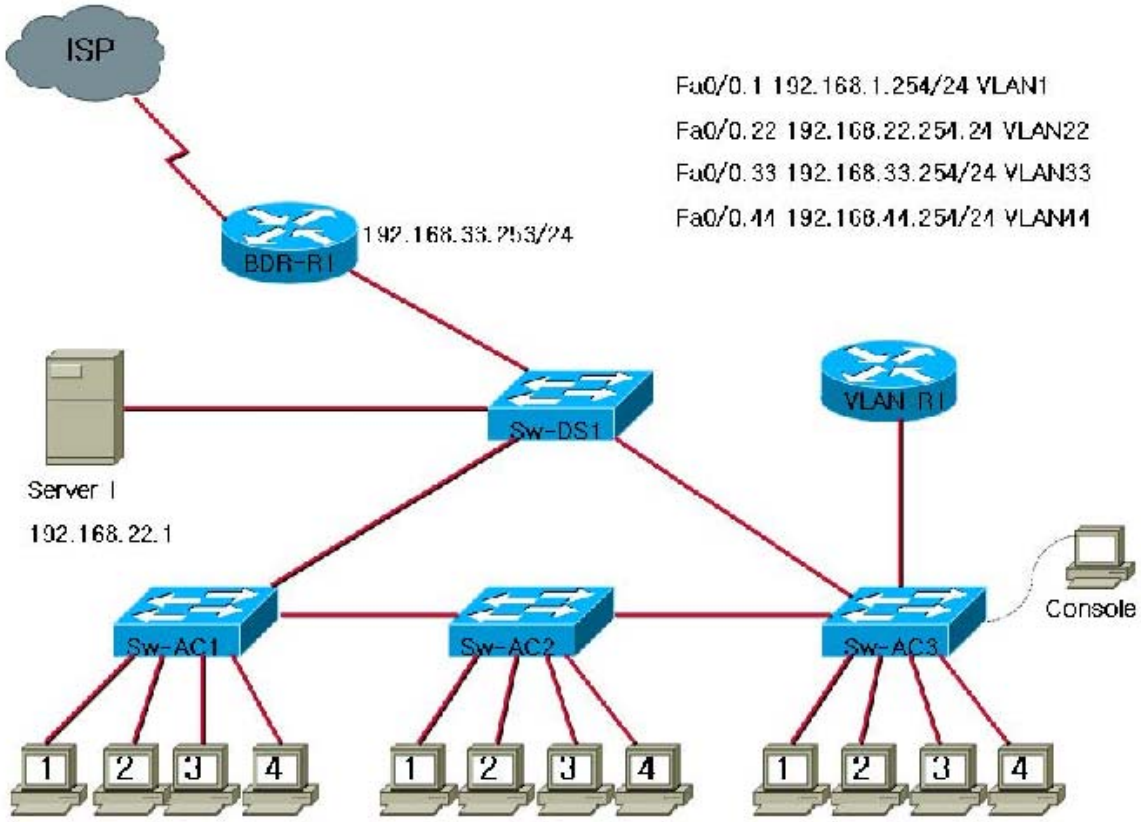
QUESTION NO: 24
Refer to the exhibit. Which statements describe why the workstation with the IP address 192.168.89.99 cannot access the Internet? (Choose two.)



A. The NAT pool is not properly configured to use routable outside addresses.
B. The NAT outside interface is not configured properly.
C. The router is not properly configured to use the access control list for NAT.
D. The NAT inside interfaces are not configured properly.

Answer: C,D

QUESTION NO: 25
What address should be configured as the default-gateway for the host connected to interface Fa0/4 of Sw-AC3?



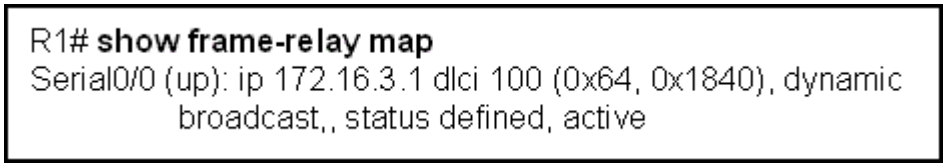
Sw-AC3#show vlan

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

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

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

QUESTION NO: 26
Refer to the exhibit. What is the meaning of the term dynamic as displayed in the output of the show frame-relay map command shown?

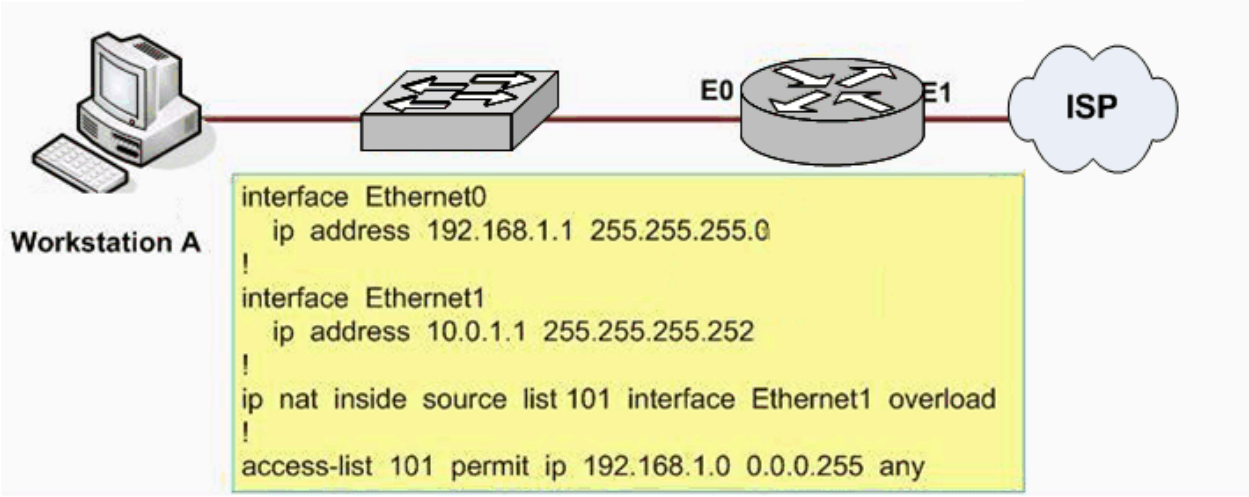


A. The mapping between DLCI 100 and the end station IP address 172.16.3.1 was learned through Inverse ARP.
B. The Serial0/0 interface is passing traffic.
C. The DLCI 100 will be dynamically changed as required to adapt to changes in the Frame Relay cloud.
D. The DLCI 100 was dynamically allocated by the router.
E. The Serial0/0 interface acquired the IP address of 172.16.3.1 from a DHCP server.

Answer: A

Explanation:
Inverse Address Resolution Protocol (Inverse ARP) was developed to provide a mechanism for dynamic DLCI to Layer 3 address maps. Inverse ARP works much the same way Address Resolution Protocol (ARP) works on a LAN. However, with ARP, the device knows the Layer 3 IP address and needs to know the remote data link MAC address. With Inverse ARP, the router knows the Layer 2 address which is the DLCI, but needs to know the remote Layer 3 IP address. When using dynamic address mapping, Inverse ARP requests a next-hop protocol address for each active PVC. Once the requesting router receives an Inverse ARP response, it updates its DLCI-to-Layer 3 address mapping table. Dynamic address mapping is enabled by default for all protocols enabled on a physical interface. If the Frame Relay environment supports LMI autosensing and Inverse ARP, dynamic address mapping takes place automatically. Therefore, no static address mapping is required.

QUESTION NO: 27
Refer to the exhibit. Given the partial configuration shown in the exhibit, why do internal workstations on the 192.168.1.0 network fail to access the Internet?



A. A NAT pool has not been defined.
B. NAT has not been applied to the inside and outside interfaces.
C. The access list has not been applied to the proper interface to allow traffic out of the internal network.
D. The wrong interface is overloaded.

Answer: B
Explanation:
Two basic configurations are needed when configuring NAT in CISCO IOS: 1, the definition of address translation types (global configuration mode command); 2, the definition of devices location (interface sub-configuration mode command). Inside and outside parameters designate the transmission direction. Designate inside on interface that is connected to internal network, and designate outside on interface that is connected to external network. The configuration in the figure above does not apply NAT to interface, so address can not be translated.

QUESTION NO: 28
A single 802.11g access point has been configured and installed in the center of a square office. A few wireless users are experiencing slow performance and drops while most users are operating at peak efficiency. What are three likely causes of this problem? (Choose three.)

A. antenna type or direction
B. metal file cabinets
C. mismatched SSID
D. cordless phones

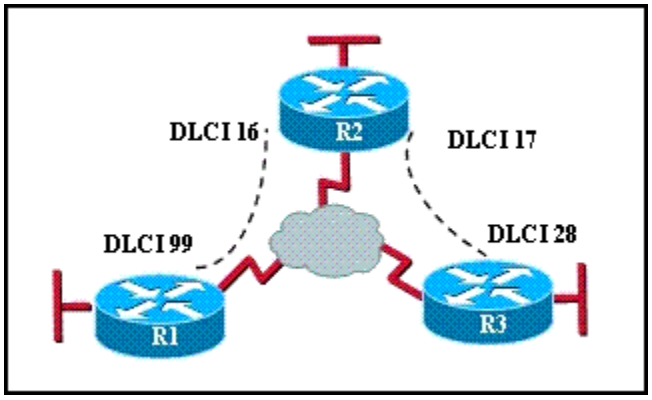
Answer: A,B,D

Explanation:

D: If you have cordless phones or other wireless electronics in your home or office, your computer might not be able to "hear" your router over the noise from the other wireless devices. To quiet the noise, avoid wireless electronics that use the 2.8GHz frequency. Instead, look for cordless phones that use the 5.8GHz or 900MHz frequencies.
A: The antennas supplied with your router are designed to be omni-directional, meaning they broadcast in all directions around the router. If your router is near an outside wall, half of the wireless signals will be sent outside your office, and much of your router's power will be wasted.

Since most users operate at peak efficiency in our example, it could be that a few of the users are simply placed too far from the antenna, or the antenna is not placed in the center of the office.
B: Metal, walls, and floors will interfere with your router's wireless signals. The closer your router is to these obstructions, the more severe the interference, and the weaker your connection will be.

QUESTION NO: 29
Refer to the exhibit. Which statement describes DLCI 17?

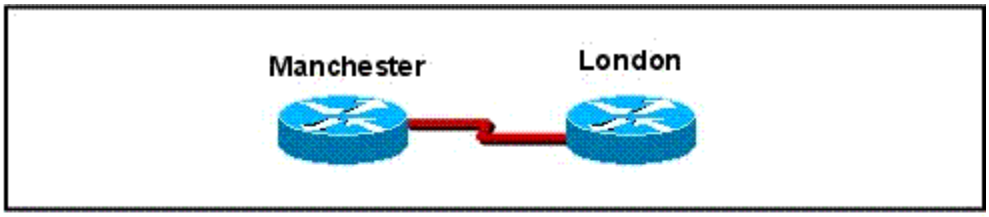


A. DLCI 17 is the Layer 2 address used by R2 to describe a PVC to R3.
B. DLCI 17 describes a PVC on R2. It cannot be used on R3 or R1.
C. DLCI 17 describes the dial-up circuit from R2 and R3 to the service provider.
D. DLCI 17 describes the ISDN circuit between R2 and R3.

Answer: A

Explanation:
DLCI-Data Link Connection Identifier Bits: The DLCI serves to identify the virtual connection so that the receiving end knows which information connection a frame belongs to. Note that this DLCI has only local significance. Frame Relay is strictly a Layer 2 protocol suite

QUESTION NO: 30
Refer to the exhibit. The two exhibited devices are the only Cisco devices on the network. The serial network between the two devices has a mask of 255.255.255.252. Given the output that is shown, what three statements are true of these devices? (Choose three.)




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

<output omitted>
```

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

Answer: B,D,E
Explanation:
1. Use the show cdp entry * command on Device Manchester to find that the IP address of Device London is 10.1.1.2. Therefore, the IP address of the interface of Device Manchester is 10.1.1.1.

2. The results shown by running the show cdp entry command show that the platform of Device London is cisco 2610.
3. Interface: serial0/0 indicates that Device Manchester is connected with Device London through S0/0.